Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 29

A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States

Diana Milanesi

2017

TTLF Working Papers

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Diana Milanesi is an attorney member of the State Bar of California, the New York State Bar, and the International Bar Association. Since 2016, Diana has served as legal adviser to Startup Europe India Network, a high-profile network built in collaboration with the European Commission to connect the pan-European and Indian startup ecosystems and foster growth and investments across the Indian, EU and U.S. technology markets. Prior, from 2013 to 2015 Diana worked as corporate attorney at Squire Patton Boggs LLP (San Francisco (CA) office). Her practice focused on advising domestic and international clients in connection with venture capital transactions, IPOs, Rule 144A/Regulation S offerings, fund formation and capital raising transactions, tech-focused transactions, cross-border reorganizations, and M&As. At Squire Patton Boggs LLP, she also served as attorney contributor on the Squire Patton Boggs Capital Thinking Blog, providing insights and updates on important U.S. financial regulation and securities law developments. Prior to join Squire Patton Boggs LLP, Diana gained experience on seed and early stage venture capital investments in technology companies at an international seed venture capital firm in San Francisco (CA). From 2009 to 2011, she worked as associate in the Banking and Finance Department at Gianni, Origoni, Grippo, Cappelli & Partners (Milan office, Italy), where she gained extensive experience on banking and finance, private equity, and capital markets transactions. Diana has also collaborated as lecturer and researcher at Mind the Bridge Foundation and Startup Europe Partnership, an integrated platform established by the European Commission to support the growth and sustainability of European startups and scaleups.

Diana earned her Bachelor Degree in Judicial Science (LL.B.), *summa cum laude*, in 2007 and her Master Degree in Law (J.D.), *summa cum laude*, in 2009 both from Luigi Bocconi University, Italy. As part of her Master Degree in Law, in 2008 she attended an exchange program at Duke University School of Law, where she focused her studies on business law and financial regulation. In 2010, she received a certificate in debt market from the London School of Economics and Political Science. Diana earned her LL.M. Degree from UC Berkeley School of Law in 2012, with a concentration in securities regulation and corporate finance. During the LL.M. program, she served as member on the Berkeley Business Law Journal. Diana received her J.S.D. Degree from UC Berkeley School of Law in 2017, with a concentration in venture capital, financial derivatives, regulation of capital markets and securities. During the J.S.D. program, she also attended MBA courses in financial derivatives, private equity, and venture capital at UC Berkeley Haas School of Business. Her dissertation thesis examines the operations of central counterparties for over-the-counter financial derivatives (OTC CCPs), analyzes the design of OTC CCPs' default waterfalls, and investigates their systemic risk implications.

Diana has published various articles in the fields of securities law, financial regulation, and venture capital. Her present research focuses on the rapidly evolving legislative and regulatory frameworks for financial technology in the U.S., EU and UK. She has been a TTLF Fellow since 2016.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Diana Milanesi, A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States, Stanford-Vienna TTLF Working Paper No. 29, http://ttlf.stanford.edu.

Copyright

Abstract

Open Banking is an evolution of banking that focuses on how banks share their data, products/services, and functionality, and how they enable consumers to share their financial data, account information, and functionality for access and use by authorized third parties. This evolution is expected to increase transparency, promote competition, and foster innovation in the banking and financial services industry. These positive outcomes, in turn, will help empower consumers and businesses by giving them greater control over their data and finances.

The evolution prompted by Open Banking goes far beyond technology. Open Banking represents a defining moment at which banks are forced to re-think their role and the approach they take to their business. Open Banking focuses on the way banks innovate through partnerships and collaborations with various participants within and outside the financial and banking services industry. It is about the way banks and third parties (co)-create the value and flexibility that speaks to the real-world needs of consumers and businesses by making their financial data and account information more available and widely shared than ever before.

At present, a number of interconnected forces are driving the movement towards Open Banking. These forces include a substantial demographic shift, evolving costumer preferences and expectations, technology advances, and increased competition by new entrants such as fintech companies and large tech giants.

Alongside the described forces, legislative and regulatory reforms in Europe and the United Kingdom are acting both as a catalyst for change and an accelerator of openness in the financial and banking services industry. In parallel to these reforms, governmental authorities and regulators in the United States are starting testing the waters in Open Banking by gathering more information about current practices and potential market developments and improving their engagement with various industry participants and consumer representative groups.

Regulators have certainly an important and constructive role to play in creating and promoting the openness needed for a new paradigm of banking to flourish. In determining whether, and to what extent, to take regulatory actions with respect to Open Banking and consumer-permissioned access to consumer financial data and account information, regulators should be mindful of the global nature of the issues at stake. In fact, overly prescriptive rules regarding access to consumer data will have the negative effects of: depriving consumers of innovative products and services which could help them (re)-gain control over their finances and materially improve their financial health; placing companies subject to any such rules at a significant disadvantage vis-à-vis their competitors in other jurisdictions; creating a fractured regulatory framework to the extent any such rule diverges substantially from international access standards or conventions; and stifling innovation by precluding fintech companies and other new entrants from accessing consumer data and/or scaling internationally. Furthermore, any regulatory action aiming at promoting Open Banking

and facilitating consumer-permissioned access to consumer financial data and account information should coordinate with ongoing industry initiatives and should be subject to public comments to ensure that a measured and effective approach is developed to the benefit of all interested parties.

In addition to enabling consumers to access and share their financial records with trusted third parties without undue restrictions, Open Banking-related regulatory reforms should also provide for the establishment and enforcement of adequate safeguards. This is important because the value of Open Banking can only be realized when openness is nurtured and delivered in a responsible manner, which: maintains the trust critical to the functioning of the banking and the financial system; promotes transparency, privacy, and security in the use and disclosure of consumer financial data and account information by consumers who can control how to start, manage, and terminate access thereof; and ensures the continue safety and soundness of the banking and financial system as a whole.

There are real tensions around many of the issues discussed above. Nevertheless, there is a promising path forward.

In particular, banks that want to gain (and maintain) a leading position in a rapidly evolving Open Banking ecosystem could consider adopting a marketplace strategy or a platform strategy. In the former scenario (banking-as-a-marketplace), the bank's customers can manage their finances and have access to third parties' financial and non-financial products and services, alongside the bank's core product(s) (e.g., a current account). In this context, the bank enters into, and curates, a number of business partnerships with selected and trusted third-party service providers, which agree to offer their services and products throughout the bank's marketplace as either white-labeled or co-branded services and products. By contrast, in the latter scenario (banking-as-a-platform), the bank develops an open set of APIs that any third-party can use to build products and services. Different from the marketplace model, banking-as-a-platform has the potential advantage of providing customers with a greater variety of products and services and a more comprehensive set of capabilities. However, unlike the marketplace model, banking-as-a-platform may come with some lack of centralized control of quality and security on the part of the bank.

At present, fintech companies and other new entrants – particularly challenger banks – appear to be better positioned to deliver on these strategies, relatively to legacy players.

When a bank (be it an incumbent bank or a challenger bank) adopts a marketplace strategy or a platform strategy, the offering by the bank will be defined by the customer's journey (or customer's flow) as the customer searches, buys, and utilizes the products and services offered throughout the bank's marketplace or platform. In this context, differentiation will be based on a number of factors, including: seamless integration, reduced friction throughout the customer's journey, simplicity, personalized user experience, proactive and compelling customer engagement, ongoing support services, insightful predictions of customers' needs and goals, as well as governance, privacy and security checks. A bank that successfully delivers on these critical areas will be able to position itself as a customer's preferred digital point of

entry into integrated non–financial and financial products and services and to acquire a central role at the heart of the customer's daily life.

Importantly, both a banking-as-a-marketplace strategy and a banking-as-a-platform strategy rely heavily on two key elements: first, well-defined APIs to facilitate richness and ease of integration with third parties' services and products; and second, access to customer data and insights, which can be processed and contextualized to drive analytics and provide competitive predictive services. Relevant quantities of customer data (including personal data embedded within customers' transaction information) will likely concentrate around the bank's marketplace / platform. Because of this, monitoring and protecting costumer data throughout each stage of the costumer's journey across the services and products provided on the marketplace / platform will be a key priority.

Finally, when deploying a successful banking-as-a-marketplace strategy or banking-as-a-platform strategy, the bank and the various participants to its ecosystem will be able to leverage network effects generated across the marketplace / platform to scale and grow in value much more efficiently.

Table of Contents

PREFACE

The term "Open Banking" is under development and several definitions have been proposed.[1] For the purposes of this paper, "Open Banking" is defined as an evolution of banking that focuses on how banks share their data, products/services, and functionality, and how they enable consumers to share their data and account functionality for access and use by third parties. This evolution is expected to increase transparency and competition in the banking and financial services industry and to lead to more personalized customer experience, more compelling customer engagement, as well as greater control by customers over their data and finances.

When shared in a secure, transparent, and resilient way, consumer financial data and account information can be used to build useful and innovative applications and services. At present, traditional financial institutions and fintech companies provide a number of financial services and products that rely on consumer-permissioned access to consumer financial data and account information. Among these products and services are the following: personal financial management (PFM), automatic savings, budgeting analysis, product recommendations, account verification, cash flow management, funds transfer and bill payment, loan application verification information, credit decision-making, fraud and identity theft detection, and investment management. In these and countless other cases, data access and sharing constitute the backbone of innovation, creating sustainable value for various stakeholders.

In particular, financial and banking services and products that rely on consumer-permissioned access to consumer financial data and account information create a number of specific, real-life benefits to consumers.[2] For example, some of these products and services enable the provision of real-time information, which helps consumers make better-informed and more efficient decisions about spending, saving, and borrowing; others enable consumers to view and manage their financial account information on a consolidated basis across multiple accounts and financial institutions, thus giving them the convenience of a single window with a panoramic view of their financial activities; some leverage automation and insights to help consumers achieve their savings or budgeting goals; others facilitate more targeted investment, financial planning, and portfolio management solutions; some enable the evaluation of a broader set of data points for credit decision-making beyond a formal credit score, which helps improve underwriting for mortgages and credit cards and expand access to credit for underserved consumers; others

[1] Most of the proposed definitions of "Open Banking" revolve around three elements: (1) the use of open application programming interfaces (APIs) allowing third-party developers to build applications and services around financial institutions; (2) improved competition and increased financial transparency options for account holders; and (3) the use of underlying open source technologies. See, e.g., Competition and Markets Authority (CMA), *What Is Open Banking?*, Competition and Markets Authority Retail Banking Market Investigation: Infographics (2016) (explaining that Open Banking "will mean reliable, personalized financial advice, precisely tailored to [a customer's] particular circumstances delivered securely and confidentially." This will be achieved through the use of APIs "to share information securely, without [the customer] having to reveal [his/her/its] password."); Euro Banking Association (EBA), *Open Banking: Advancing Customer-Centricity. Analysis and Overview*, Euro Banking Association Report, EBA Open Banking Working Group and Innopay Report (March 2017), p. 4, 16-24 (defining "Open Banking" as an "[e]volution of banking, leading to more transparency, customer choice and customer control over personal data" and identifying three key dimensions of Open Banking, "a driver (customer relevance and regulation), an enabler (Open API technology) and a key bank asset (digital identity).").

[2] See, e.g., Open Data Institute (ODI), *Introducing the Open Banking Standard. Helping Customers, Banks and Regulators Take Banking into a Truly 21st-Century, Connected Digital Economy*, Open Data Institute (2016), pp. 2, 5; Financial Solutions Lab, *FinLab Consumer Impact Report*, Financial Solutions Lab (November 16, 2016).

facilitate bookkeeping and make it easier to reconcile payments; and some enable better risk assessment for insurance products and a more streamlined processes for identity verification and fraud detection, which contributes to a more secure and efficient financial services system.

In addition to the foregoing, having access to data that banks have historically held and securely integrating it with customer data help lower barriers to entry for fintech companies and other new entrants in the financial and banking services industry. This, in turn, helps improve efficiency, promote increased competition, and stimulate the creation of groundbreaking products and services.

Moreover, making it easy for customers to grant permission to third parties to securely access and utilize their financial data and account information is also beneficial to incumbent banks and other account providers. In fact, many account providers currently offer their customers financial management tools within their own online or mobile interfaces by leveraging services delivered by data aggregators. Similarly, a large number of account providers now offer their customers a broader set of complementary products and services in partnership with third party services providers. These strategies help incumbent banks and other account providers deepen their customer base, foster customer loyalty, and consolidate their position at the center of their customers' financial lives.

Against the described background, the present paper investigates the question of how the banking and financial services industry and the relevant legislative and regulatory frameworks across three main geographic regions – European Union, the United Kingdom (UK), and the United States – have been evolving to create and promote the openness needed for a new paradigm of banking to flourish. The paper proceeds as follows:

- Chapter 1 analyzes a number of interconnected forces that are driving the movement towards Open Banking. These forces include a substantial demographic shift, evolving costumer preferences and expectations, technology advances, increased competition by new entrants, and legislative and regulatory reforms.

- Chapter 2 examines current practices of consumer financial data and account information access and sharing. It, then, discusses the growing importance of APIs within the financial and banking services industry and analyzes their key features and functionality. Finally, it investigates how banks can leverage the innovative power of APIs and how customers and businesses can benefit from increased API-driven openness.

- Chapters 3, 4 and 5 focus on the role of regulation as a catalyst for change and accelerator of openness in the financial and banking services industry. In particular, the chapters provide an overview of forthcoming Open Banking-related legislative and regulatory frameworks, as well as policy initiatives that are currently being developed and implemented across the European Union (EU) (Chapter 3), the UK (Chapter 4), and the United States (Chapter 5). The chapters offer a critical examination of the

developments that have been made by regulators across these three geographic areas with respect to Open Banking and provide an initial assessment of their potential implications.

- Chapter 6 gauges the progress by incumbent banks in opening up critical infrastructures and operations to facilitate the provision of innovative financial and banking products and services.

- Chapter 7 discusses major drivers behind the raise of challenger banks and examines how challenger banks are redefining the way people and businesses do banking. The chapter, then, concludes identifying a number of opportunities (and challenges) that challenger banks may exploit (and may encounter) as they scale their operations and grow their activities.

CHAPTER 1. DRIVING FORCES OF OPEN BANKING

At present, a number of interconnected forces are driving the movement towards Open Banking, including a paradigm demographic shift, evolving costumer preferences and expectations, technology advances, increased competition by new entrants, and legislative and regulatory reforms. The following sections analyze each of these forces in greater detail.

1.A. Millennials

The past few years have seen a fundamental demographic shift as the millennial generation has come of age.[3] Different from any other demographic group, millennials have demonstrated significantly different consumer expectations and buying appetite.[4] Millennials are digital natives and socially hyper-connected; they have a strong preference for intuitive, on-demand, personalized, and mostly free customer service; and they are considerably more open than any prior generation to exploring options and considering financial and banking services beyond traditional banking.[5]

The emergence of this new consumer base is forcing banks to evolve their services and find creative ways to deliver them. To this end, banks are rapidly embracing a digital-first approach and are deploying new technologies to enable constant and interactive engagement with millennials regardless of their location, the time they choose to bank, and the platform they use (be it through a mobile device - e.g., smartphones, tablets, wearables, embedded sensors, and connected devices, - on the web, in person, via text message, or another channel that works best for them).[6] In addition to flexible engagement, banks are offering increasingly personalized and targeted services to appeal and remain relevant to millennial customers. Moreover, they are gradually implementing a more comprehensive and interactive approach to engage and drive loyalty among millennials. This means, for instance, offering informative and educational tools that are insightful and visually appealing (e.g., blog posts, videos, webinars, and info-graphics, as well as personalized in-app budgeting suggestions) to help millennials better budgeting and more efficiently managing their finances.[7]

[3] Millennials, also referred to as Generation Y, are a demographic cohort with birth years starting on late 1970s / early 1980s and ending in mid-1990s / early 2000s.

[4] See, e.g., Burnmark, *Challenger Banking*, Burnmark Report (October 2016), p. 6; McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives for Banks*, McKinsey Global Banking Report (December 2015), p. 3-4; Massachusetts Institute of Technology (MIT), *Digital Banking Manifesto: The End of Banks?*, Massachusetts Institute of Technology Report (2016), p. 6; KPMG, *Setting Course in a Disrupted Marketplace. The Digitally-Enabled Bank of the Future*, KPMG Report (April 2017), pp. 3-5.

[5] See, e.g., American Bankers Association, *Millenians and Banking. The Fastest Growing Customer Base is Changing the Way Banks Do Business*, American Bankers Association Report (January 2017); Scratch, *Millennial Disruption Index*, Scratch Report (2013).

[6] See, e.g., American Banker, *Eight Illuminating Data Points on Millennials and Banking*, American Banker (May 12, 2016), slide #10 (reporting that "92% of millennials said they would make a banking choice based on digital services."); American Bankers Association, *Millenians and Banking. The Fastest Growing Customer Base is Changing the Way Banks Do Business*, cit. (noting that "67% want digital budgeting tools to help them manage their money.").

[7] See, e.g., Microsoft, *Cracking the Millennial Code: Building Better Banking Relationships with Digital Natives*, Microsoft Financial Services - Banking & Capital Markets Insights (August 25, 2016).

1.B. Heightened Customer Preferences and Expectations

Customers of all generations increasingly demand from their banks an omni-channel, tailored, and personalized experience, which matches the digital experiences they have when they interact with technology companies and providers in their everyday lives. They expect intelligent and contextual services woven into their daily interactions with their banks.[8] As more and more transactions take place on mobile devices, customers also demand real-time, instant, and seamless banking experiences.[9] As a result, customers' choice of bank is increasingly influenced by ease of digital access and ease of integration with higher-level services.

When it comes to banking and financial transactions, consumers demand access to data instantly, they expect their banks to know and understand them, to offer suggestions based on past behavior and individual preferences, and to direct them toward the best product/service and pricing.[10] They also expect their banks to remember their preferences and decisions and not presenting them with the same stale offers over and over again. This means – at the very least - that banks should efficiently synchronize all available channels, so that, when customers make a decision or express their preference for a product or a service, they only have to make such decision or express such preferences once. It also means that banks need to provide their services across all available touch points in a seamless way, so that customers can pick up their transaction where they left off on one channel and continue the transaction or complete an action without having to start it over again.[11]

1.C. Advances in Technology

Evolving technologies are a powerful force driving greater openness in the banking and financial services industry. As observed by Thomas Egner, Secretary General of the Euro Banking Association (EBA), "[m]uch of the thinking about Open Banking is not in itself new, but until recently the technology was not available to further evolve this thinking and put it into practice, so the mindset of the industry just wasn't aligned."[12]

Advances in technology have a significant impact on how consumers access and use their banking and financial services, as well as the ways banks deliver them. For instance, the always-on interconnected web and the ubiquity of mobile devices have enabled a new banking and financial paradigm where favored digital interactions are increasingly mobile; this, in turn, has begun to undercut the advantages of physical

[8] Cfr., e.g., Deloitte, *Open Banking: What Does The Future Hold?*, Deloitte Digital Report (April 2017), p. 6.
[9] See, e.g., Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, Accenture Payment Services Report (2016), p. 3; McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives for Banks*, cit., pp. 9-10.
[10] See, e.g., Juan Pedro Moreno, *Banking at a Digital Crossroads*, The Financial Times (January 28, 2014); Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, White Paper (2017), p. 14.
[11] See, Microsoft, *Banking on Technology: Enabling an Omnichannel Approach in Financial Services*, Microsoft Financial Services - Banking & Capital Markets Insights (August 30, 2016).
[12] See, Finextra, *PSD2 and Open Banking: Defining Your Role in the Digital Ecosystem*, Finextra White Paper (September 2016), p. 7.

distribution that banks enjoyed for a long time.[13] Consumers of all generations increasingly use smart mobile devices to conduct their banking activities and to manage their personal finances, including accessing their bank accounts, viewing their balances, making and receiving payments.[14]

In addition to widespread online and mobile connectivity, recent years have also witnessed a massive increase in data availability and a substantial decrease in the cost of computing power.[15] The rise of cloud-based services and data center investments by large technology players (e.g., Amazon, Google and Microsoft) coupled with improved tools for data analysis is now driving low-cost data availability and analysis and is enabling companies to react to customer behavior in real time and to deliver an instant and a more fulfilling customer experience.[16]

Open-source software and cloud architectures have also created unprecedented opportunities to innovate at a higher pace and at lower costs. In particular, they help banks increase flexibility and reduce the cost of on-premises IT infrastructure and associated personnel. This, in turn, enables banks to optimize the use of their resources, efficiently develop new banking services and products, and be more responsible and adaptable to changing markets.[17] Furthermore, the increased processing power of the cloud provides banks with the speed and scalability to handle much higher transaction volume and variability, and its adaptability makes it easier to update infrastructure or integrate with other solutions in the future.[18] In addition to the foregoing, the power and cost-effectiveness of cloud-based technology can help banks effectively comply with ever-changing national and international security, privacy and compliance standards, as well as legislative and regulatory requirements in the financial and banking services industry.[19]

The list of new potentially game-changing technologies is constantly growing and it continues to drive customer expectations. Some of the most notable groundbreaking technologies include artificial intelligence, cognitive services, deep learning, machine learning, big data, predictive analytics, blockchain, distributed ledger technologies, biometrics authentication, voice controlled devices, and robotics. The advent of these technologies, among others, is both easing and empowering customers' journeys in ways that were impracticable only a few years ago. This, in turn, raises the bar on what consumers expect to be

---

[13] See, e.g., McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives for Banks*, cit., pp. 1-3, 9; Deloitte, *Open Banking: What Does The Future Hold?*, cit., p. 6; The Economist, *Retail Banking - In Tech We Trust*, The Economist Intelligence Unit Report (2016), pp. 7-8; Ernst & Young, *Landscaping UK Fintech*, Ernst & Young Report Commissioned by UK Trade & Investment (2014), p. 3.

[14] See, PWC, *Who Are You Calling a 'Challenger'? How Competition is Improving Customer Choice and Driving Innovation in the UK Banking Market*, PWC Report (2017), p. 21.

[15] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives for Banks*, cit., p. 3.

[16] See, e.g., McKinsey & Company, *The New Rules for Growth through Customer Engagement*, McKinsey on Payments, Vol. 8, No. 22, pp. 32-38 (October 2015), p. 33; McKinsey & Company, *Banking on the Cloud*, McKinsey Digital Report (April 2016); Deloitte, *Open Banking: What Does The Future Hold?*, cit., p. 7.

[17] See, Microsoft, *Banking on the Cloud: Financial Institutions Reach the Stratosphere of Efficiency*, Microsoft Financial Services - Banking & Capital Markets Insights (April 6, 2017); McKinsey & Company, *Banking on the Cloud*, cit.

[18] See, e.g., The Atlantic, *How Connectivity is Moving Banks Forward*, The Atlantic Report (2016); Matthew Finnegan, *How Technology Will Transform Banking in 2017: Blockchain, Cloud Computing and Digital Challenger Banks*, Computerworld UK (December 16, 2016).

[19] Cfr., e.g., The Atlantic, *How Connectivity is Moving Banks Forward*, cit.; Microsoft, *Banking on the Cloud: Financial Institutions Reach the Stratosphere of Efficiency*, cit.; Microsoft, *Enabling Mobile Banking While Keeping Customers' Safe*, Microsoft Financial Services - Banking & Capital Markets Insights (October 18, 2016); PWC, Global Economic Crime Survey 2016 - Adjusting the Lens on Economic Crime: Preparation Brings Opportunity Back Into Focus, PWC Report (2016).

able to do, in terms of quality, speed, usability and control of banking and financial services and products.[20] Technology developments driving customers' expectations are likely to accelerate in the near-term and new cutting-edge technologies will soon emerge promising to revolutionize the art of the possible. In order to remain relevant to their customers, banks will need to reposition themselves and to master the flexibility to rapidly experiment with, and adapt to, emerging technologies.[21]

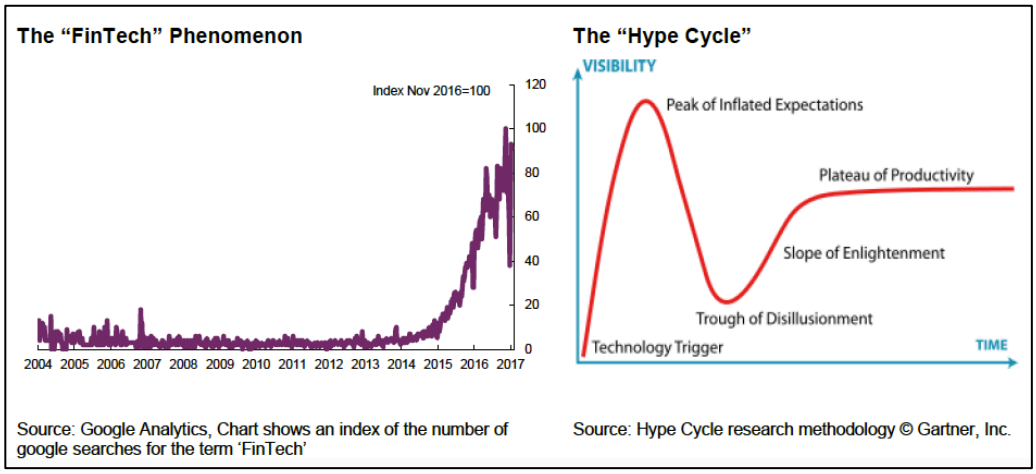
1.D. Increased Competition by Non-Traditional Players

In addition to the driving forces discussed above, increased competition by non traditional players, such as financial technology companies ("fintech companies") and well-established technology companies, is prompting greater openness in the banking and financial services industry.

1.D.i. Fintech Companies

Fintech Companies – Common Features. The pace of innovation and the investments in technology applied to financial and banking services ("fintech") have increased exponentially in recent years. In particular, the past six years have seen the emergence of fintech companies all over the world establishing new business models and providing innovative digitally-enabled banking and financial products and services[22] (see, Figure 1).

Figure 1. The "FinTech" Phenomenon; The "Hype Cycle"



Source: Mark Carney (Governor of the Bank of England), *The Promise of FinTech – Something New Under the Sun?*, Speech at the Deutsche Bundesbank G20 Conference on "Digitising finance, financial inclusion and financial literacy" (Wiesbaden (DE), January 25, 2017), p. 12.

[20] See, e.g., PWC, *Who Are You Calling a 'Challenger'? How Competition is Improving Customer Choice and Driving Innovation In the UK Banking Market*, cit., p. 21; Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., p. 3; Microsoft, *Will Digital Acceleration Simplify Banking?*, Microsoft Financial Services - Banking & Capital Markets Insights (April 17, 2017).

[21] See, Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., p. 16.

[22] See, e.g., Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., p. 3; Deloitte, *Open Banking: What Does The Future Hold?*, cit., p. 5; Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., p. 15.

Successful fintech companies generally have a very narrow focus on specific modules, or components, of banking services or products. They also tend to leverage existing infrastructures and offer services/products tailored to niche customer segments, such as millennials, small businesses, and the underbanked. Within these segments, many customers are open to utilize innovative and personalized services/products not offered by incumbent banks.[23] For example, Earnest, LendUp, Affirm, Kabbage, LendingHome, and Borro are among those fintech companies leading the growth in the lending and underwriting market. They primarily lend directly online and/or facilitate consumers' and small businesses' access to credit scoring, often using machine learning technologies and other nontraditional methods to assess creditworthiness. In the world of marketplace lending, firms like SoFi, Upstart, Commonbond, Funding Circle, and Zopa are providing groundbreaking peer-to-peer (P2P) lending platforms for consumer borrowers to connect with willing lenders. Some of them focus on personal loans and a few target students and young professionals, while others focus on small businesses' needs. Companies like TransferWise, WorldRemit, Stripe, CurrencyCloud, GoCardless, Klarna and Adyen are bringing groundbreaking technologies and new business models to payment and money transfer services. Firms like eToro, Robinhood, and Nutmeg are servicing retail investors with automated, social, or other innovative investment vehicles and advice. Betterment and Wealthfront are among leading investment management startups that focus on providing fully automated, algorithm-driven investments. Digit and Acorn have launched recently to provide automatic saving services. Credit Karma, Credit Sesame, NerdWallet, and Mint offer tools and advice to manage personal accounts, expenses, budgeting, and personal financial planning. These include free credit scores, reports, and insights, as well as comparison tools for a wide range of banking and financial products and services.

In addition to the features discussed above, successful fintech companies are also generally unburdened by legacy IT systems[24] and they typically build groundbreaking technologies from scratch, either in house or in collaboration with other emerging fintech or established vendors.

Moreover, successful fintech companies tend to orient themselves around their customers and they excel at putting customers first. For them technology is the means, but customer experience is the ultimate goal.[25] They leverage digital distribution channels and advanced technologies (e.g., artificial intelligence, machine learning, distributed ledger technology, cloud computing, and big data analytics), which enable them to offer compelling and personalized user experiences and drive customer acquisition, engagement, and retention.

[23] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives for Banks*, cit., pp. 6-7.
[24] See, The Economist, *The Fintech Revolution: A Wave of Startups is Changing Finance — For the Better*, The Economist (May 9, 2015) (noting that "Lending Club's ongoing expenses as a share of its outstanding loan balance is about 2%; the equivalent for conventional lenders is 5-7%. That means it can offer better deals to the borrowers and lenders who congregate on its platform. Half of the loan applications Funding Circle gets from small businesses arrive outside normal business hours. TransferWise takes a machete to the hefty fees that banks levy to send money across borders.").
[25] See, Ernst & Young, *Revolutionary Change is Transforming the Financial Services Landscape*, Financial Services Leadership Summit December 2016, Ernst & Young View Points (2016), p. 5.

While some among the most successful fintech companies focus on simplifying and improving the quality and efficiency of existing banking and financial services, others provide entirely new services ranging from service and product comparison, to fast-switching services, new credit underwriting mechanisms, and cross-border payments solutions.[26]

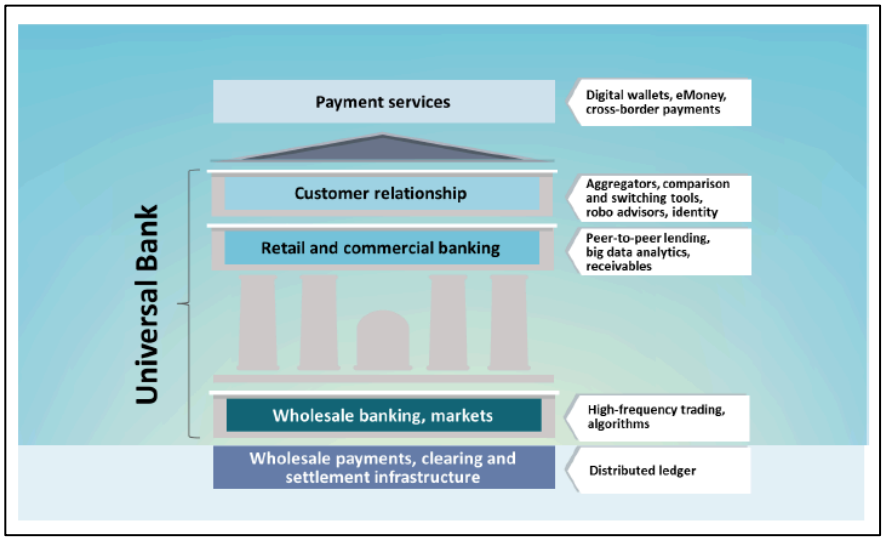
The Impact of Fintech Innovation. The scope of fintech innovation is enormous, as it touches nearly every aspect of the financial value chain and involves the entire banking sector, including front, middle and back-office activities, as well as services for both retail and wholesale markets.[27]

As observed by Mark Carney, Governor of the Bank of England, during a speech at the Deutsche Bundesbank G20 conference in January 2017, the true promise of fintech "springs from its potential to unbundle banking into its core functions of: settling payments, performing maturity transformation, sharing risk and allocating capital."[28] This possibility – Carney explains - is being driven by new entrants (e.g., payment service providers, aggregators and robo advisors, peer-to-peer lenders, and innovative trading platforms) and is being influenced by incumbents, which are increasingly adopting new advanced technologies in an effort to strengthen the economies of scale and scope of their business models.[29]

Figure 2 below illustrates the financial service value chain of a traditional universal bank, combining payment services, customer relationship, retail and commercial deposits and lending, and a wide range of activities in wholesale money and capital markets.

[26] See, e.g., Deloitte, *Open Banking: What Does The Future Hold?*, cit., p. 5; McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., p. 6.
[27] See, Cemal Karakas and Carla Stamegna, *Financial Technology (FinTech): Prospects and Challenges for the EU*, European Parliamentary Research Service (March 2017), p. 2 (noting that "[f]inTech, the abbreviation for financial technology, is a broad term … [t]oday, the interpretation of FinTech has expanded to include any technological innovation in the financial sector, including innovations in financial literacy and education, retail banking, investment or office improvement (e.g. back-office functions). The expression FinTech has also become a synonym for the emerging financial services sector in the 21st century. In this context, FinTech covers a broad range of services and products, such as cashless payments, peer-to-peer (P2P) lending platforms, robotic trading, robo-advice, crowdfunding platforms, and virtual currencies, and is expected to expand further in the coming years."); Patrick T. Harker (President and Chief Executive Officer Federal Reserve Bank of Philadelphia), *Fintech: Revolution or Evolution?*, Remarks at the University of Pennsylvania School of Engineering and Applied Science (Philadelphia (PA), April 3, 2017).
[28] See, e.g., Mark Carney (Governor of the Bank of England), *The Promise of FinTech – Something New Under the Sun?*, Speech at the Deutsche Bundesbank G20 Conference on "Digitising finance, financial inclusion and financial literacy" (Wiesbaden (DE), January 25, 2017), p. 3; Mark Carney (Governor of the Bank of England), *Building the Infrastructure to Realise FinTech's Promise*, Speech at the International FinTech Conference 2017, Old Billingsgate (London (UK), April 12, 2017), pp. 5-6.
[29] See, Mark Carney (Governor of the Bank of England), *The Promise of FinTech – Something New Under the Sun?*, cit., p. 3.

Figure 2. Financial Services Value Chain



Source: Mark Carney (Governor of the Bank of England), *The Promise of FinTech – Something New Under the Sun?*, cit., p. 5.

Fintech companies can now perform each of the functions illustrated above independently:

- Payment Services - Traditional payment services have long relied on cash, debit and credit cards, and wire transfers. By contrast, fintech companies can now provide domestic and cross-border payment services on significant scale through "digital wallets" or pre-funded "eMoney". In so doing, they not only impact banks' payment revenues, but they also (and most importantly) take the totality of customer transaction data.[30]

- Customer Relationship - The customer relationship is being opened up to fintech companies. For example, aggregators are making use of banks' Application Programming Interfaces (APIs) to provide customers with price comparison and switching services. At the same time, "robo advisors" are increasingly utilized to deliver affordable investment advice to retail customers.[31]

- Retail and Commercial Banking – Leading fintech companies are also driving competition in retail and commercial banking by offering innovative lending and borrowing platforms for retail and corporate customers.[32]

- Wholesale Banking and Markets – The relevance of high frequency traders has grown exponentially from early 2000s to account for up to three-quarters of equity trading volumes and around 40% of FX. Their emergence has been largely driven by technological advancements and the growth of multilateral trading venues.[33]

[30] Id., pp. 4-7.
[31] Id., pp. 5-6.
[32] Id., p. 6.
[33] Ibidem.

- Wholesale Payment, Clearing, and Settlement Infrastructure - Emerging technologies, including distributed ledger technology, hold the potential to significantly improve the accuracy, efficiency, and security of processes across payments, clearing, and settlement, as well as to improve and support better regulatory compliance.[34]

The process of unbundling discussed above creates significant benefits for customers, businesses, and the industry as whole:[35]

- Consumers can enjoy access to a broader range of innovative banking and financial products and services, which are better-targeted to customers' needs; and they can leverage new technology to manage money and control spending more efficiently;

- Small and medium sized businesses can tap into new sources of credit and can take advantage of innovative credit opportunities;

- By leveraging the power of fintech innovation, traditional banks themselves may become more productive and efficient, with speedier transaction chains, greater capital efficiency, and stronger operational resilience;

- Fintech innovation can bring new products to unbanked or underserved segments, and can facilitate a better understanding of their financial patterns – their inflows and outflows and how they find ways to manage the gaps; and

- The aforesaid positive outcomes, in turn, can benefit the entire financial system by making it more resilient, with greater diversity, redundancy, and depth.[36]

Notwithstanding the described advantages, the process of unbundling of financial and banking products and services also poses severe risks for banks, in terms of disintermediation, loss of market centrality, and reduced relevance to customers.[37] Moreover, by unbundling traditional financial and banking services, fintech innovation may affect the resilience of the financial system as whole. This is illustrated in Figure 3 below:[38]

---

[34] Id., p. 7.

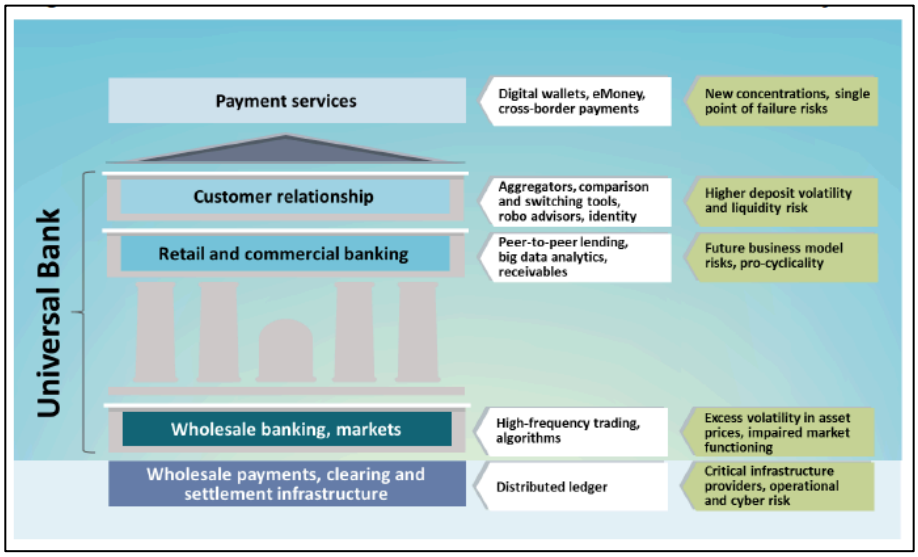
[35] See, e.g., Consumer Compliance Outlook, *Perspectives on Fintech: A Conversation with Governor Lael Brainard*, Consumer Compliance Outlook - Federal Reserve System Publication, Issue No. 3 (2016), pp. 1, 12-14; John C. Williams (President and CEO, Federal Reserve Bank of San Francisco), *Fintech: The Power of the Possible and Potential Pitfalls*, Presentation Delivered at the LendIt USA 2016 Conference (San Francisco (CA), April 12, 2016).

[36] See, Mark Carney (Governor of the Bank of England), *Enabling the FinTech Transformation: Revolution, Restoration, or Reformation?*, Speech at the Lord Mayor's Banquet for Bankers and Merchants of the City of London at the Mansion House (London (UK), June 16, 2016), p. 4 (noting that the described benefits "spring from FinTech's potential to deliver a great unbundling of banking into its core functions of settling payments, performing maturity transformation, sharing risk and allocating capital. This would mean revolution, fundamentally re-shaping the financial system. At the same time, some financial technologies could make incumbent banks more efficient and profitable, reinforcing existing economies of scale and scope in banking. This would mean a restoration, reinforcing incumbents' power. The balance of these forces may yield a third alternative – a reformation – a more diverse, resilient and effective system for consumers. One where large banks exist alongside new entrants who compete across the value chain."); Mark Carney (Governor of the Bank of England), *Building the Infrastructure to Realise FinTech's Promise*, cit., pp. 8-9.

[37] See, e.g., Sarah Todd, *Banks' Real Fight with Fintech: Who Owns the Customer?*, American Banker (June 19, 2015).

[38] See, e.g., Mark Carney (Governor of the Bank of England), *The Promise of FinTech – Something New Under the Sun?*, cit, pp. 3, 8-12 (warning about potential financial stability issues raised by the fintech revolution; and explaining that, as fintech companies progressively unbundle banking into its core functions, "systemic risks will evolve. Changes to customer loyalties could influence the

Figure 3. Financial Services Value Chain with Potential Issues for Financial Stability



Source: Mark Carney (Governor of the Bank of England), *The Promise of FinTech – Something New Under the Sun?*, cit., p. 10.

Against this evolving background, financial authorities are called to play a critical role in supporting fintech innovation, while managing the associated risks to financial stability. In particular, to help realize fintech's promise, financial regulators across a number of countries are now evolving their supervisory approaches and are undertaking a variety of fintech-related initiatives, which include the introduction of regulatory sandboxes, the adoption of simplified authorization processes, and the expansion of access to central bank money to non-bank payments service providers ("PSPs"). These initiatives are discussed in more detail in the following chapters.

Fintech Venture Capital (VC) Investment Trends. Over the past few years, the promise of fintech innovation has drawn an abundance of venture capital investments.[39]

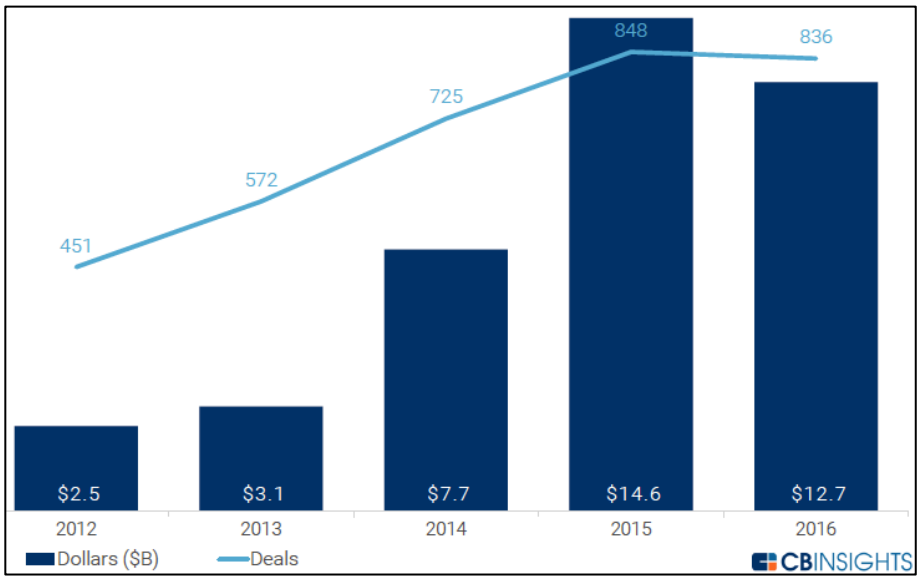
According to a CB Insights report,[40] globally nearly $12.7 billion across 836 VC financings have been deployed to VC-backed fintech startups in 2016 (see, Figure 4). While this represents both a decline in number of deals (down 1%) and a drop in aggregate dollar value (down 13%) from 2015's highs, it is still a significant increase compared to 2012's 451 deals raising $2.5 billion.

stability of bank funding. New underwriting models could impact credit quality and even macroeconomic dynamics. New investing and risk management paradigms could affect market functioning. A host of applications and new infrastructure could reduce costs, probably improve capital efficiency and possibly create new critical economic functions. The challenge for policymakers is to ensure that FinTech develops in a way that maximises the opportunities and minimises the risks for society.").

[39] See, KPMG, *Global Fintech Investment Sees Sharp Decline in 2016 Despite Record VC Funding: KPMG Q4'16 Pulse of Fintech Report*, KPMG Insights (February 20, 2017); KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, KPMG Report (February 21, 2017), pp. 7, 9-13.

[40] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, CB Insights Reports (February 15, 2017), pp. 8-9.

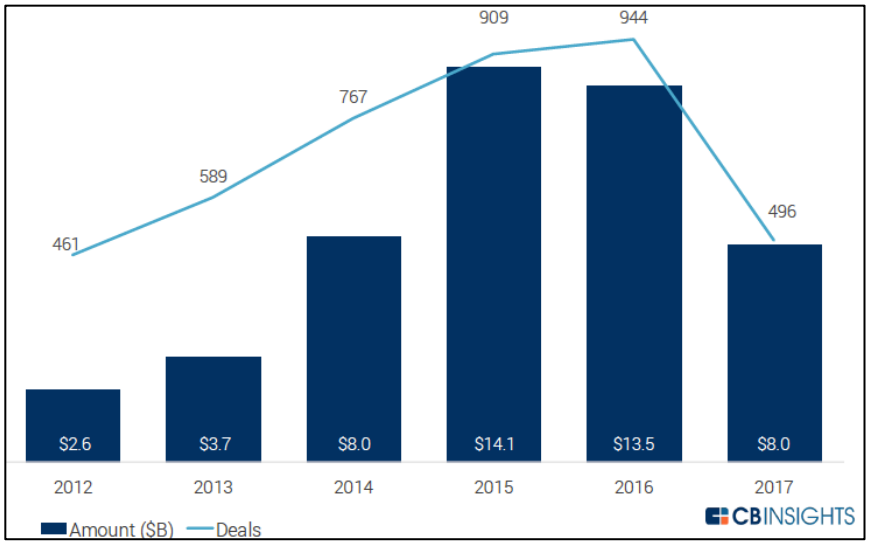
Figure 4. Annual Global Financing Trend to VC-Backed Fintech Companies (2012 – 2016)



Source: CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, CB Insights Reports (February 15, 2017), p. 9.

A more recent CB Insights report[41] indicates that in Q2 2017, global VC-backed fintech startups raised $5.2 billion across 251 deals (see, Figure 5 and Figure 6). At the current run-rate, investment dollars to VC-backed fintech companies in 2017 are on pace to rise 19% from 2016. If the H2'17 sustains H1'17's deal pace, then global fintech deal activity could surpass 2016's all-time high.

Figure 5. Annual Global Financing Trend to VC-Backed Fintech Companies (2012 – 2017 YTD (Q2'17))



Source: CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, CB Insights Reports (July 2017), p. 9.

[41] See, CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, CB Insights Reports (July 2017).

Figure 6. Quarterly Global Financing Trends to VC-Backed Fintech Companies (Q2'12 – Q2'17)

Source: Id., p. 10.

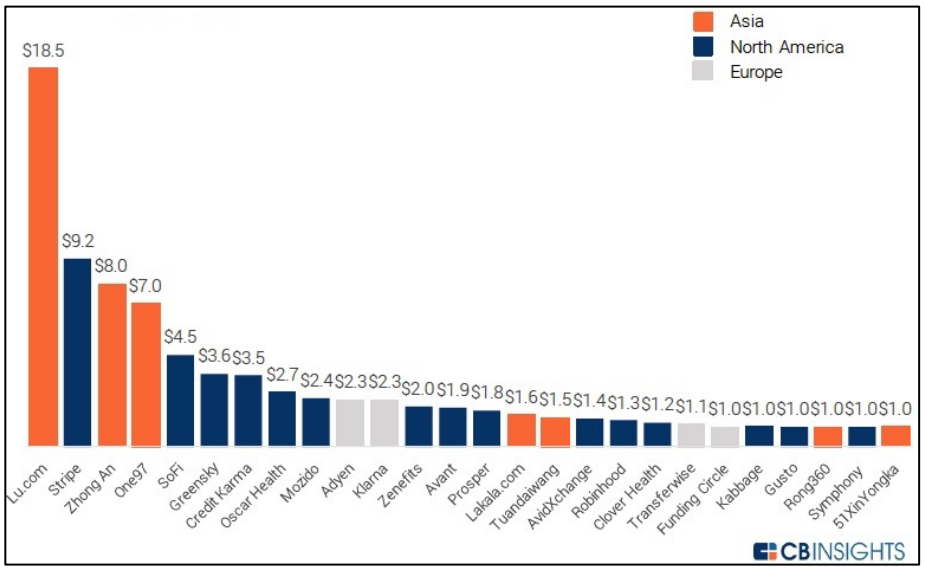
In 2016 early stage (seed and series A) fintech companies raised $2 billion across 484 deals. This represents a 3% drop in global early-stage deals and a 18% increase in global early-stage fintech funding on a year-over-year basis.[42] On a quarterly basis, seed deal share fell below 30% in Q4'16 to hit a five-quarter low and the median global early-stage (seed and series A) deal size among VC-backed fintech companies in Q4'16 rose to a five-quarter high in Q4'16 to hit $2.8M, which represents a 27% increase compared to Q4'15 median global early-stage fintech deal size.[43] Contrary, series D deal share increased up to 7% in Q4'16, marking a five-quarter high. [44]

More recently, seed stage fintech deal share slipped to a 5-quarter low in Q2'17, while global Series A fintech deal share grew from 21% in Q1'17 to 27% in Q2'17.[45] Early-stage fintech funding jumped 43% on a quarterly basis in Q2'17, mainly driven by several large Series A deals including R3, Upgrade, and Next Insurance. Early-stage fintech deals also hit a 5-quarter high at 144 deals. [46] Median early-stage deal size among VC-backed fintech companies in Q2'17 rose slightly after falling to $2.5M in Q1'17. [47] Moreover, in Q2'17 the median late-stage fintech deal size hit a 5-quarter high of $34M and grew 66% on a quarterly basis, recovering from a 4-quarter low of $20.5M in Q1'17. [48]

[42] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 13.
[43] Id., p. 14.
[44] Id., p. 12.
[45] See, CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 11.
[46] Id., p. 12.
[47] Id., p. 13.
[48] Id., p. 14.

As reported by CB Insights report, at present there are 27 fintech unicorns (private companies that have a valuation of over $1 billion) globally valued at $83.8 billion, of which 15 are based in the United States and 4 in Europe (see, Figure 7).

Figure 7. Global VC-Backed Fintech Unicorns By Valuation (Q2'16 – Q2'17)



Source: Source: CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 20.

With respect to verticals, over the past five years fintech VC investments have been largely focused around payments. However, in 2016 the payment segment began to show signs of maturity and investment opportunities in new fintech segments – including, insurance tech (insurtech), risk technology (risktech), and regulation technology (regrech) – significantly increased.[49] Investment dollars to VC-backed companies in the payments tech field (online and mobile payments, point of sales systems) increased 19% on a quarterly basis in Q4'16, as deals fell slightly after remaining flat for two consecutives quarters.[50] Moreover, funding for blockchain and bitcoin companies fell to $69M across 17 deals in Q4'16 compared to a high $153M across 22 deals in Q1'16.[51] By contrast, investment in insurtech increased significantly, with insurtech companies raising $1.6 billion across 109 deals in 2016.[52]

[49] See, Accenture, *Fintech and the Evolving Landscape: Landing Points for the Industry*, Accenture Report (2016), pp. 4-5 (Exhibit 3).
[50] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 24.
[51] Id., p. 23. See, also, KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, cit., p. 23 (reporting that "[t]otal venture investments in bitcoin & blockchain-related companies increased from $441.0 in 2015 to $543.6 in 2016. However, the aggregate number of deals declined from 191 in 2015 to 132 in 2016. The decrease in financings by count indicates that "initial hype is fading and more proof of robust applications will be required by venture investors.").
[52] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 22. See, also, KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, cit., p. 25 (noting that "[t]otal venture investments in global insurance tech companies increased from $592.0M in 2015 to $1,192.7M in 2016. The aggregate number of deals also increased from 74 in 2015 to 91 in 2016.").

The above trends continued in H1'17. In particular, in Q2'17 deals to VC-backed insurance tech companies rose 81% on a quarterly basis, while funding increased 205% on a quarterly basis.[53] Moreover, in Q2'17 funding to VC-backed wealth tech companies surged 208%, while deals to VC-backed wealth tech companies slipped for the second consecutive quarter and were flat the same quarter a year prior.[54] Funding to VC-backed blockchain and bitcoin startups climbed for the second consecutive quarter growing 100% on quarterly basis. [55]

Across different geographic areas:

United States – The overall trend in US fintech VC investments was much the same as in the broader market. In 2016, U.S. based VC-backed fintech companies saw a drop-off in both deals and funding with $5.5 billion raised across 422 deals. In particular, investment dollars fell 29% from 2015 highs, while deal count dropt to match 2014's levels.[56] On a quarterly basis, the United States saw funding to VC-backed fintech companies raise 44% in Q4'16, after falling for two consecutive quarters,[57] and fintech deals increased 7% in Q4'16, after falling for two consecutive quarters.[58]

Seed-stage deal share to VC-backed US fintech companies fell to a 5-quarter low, accounting for 23% of deals in Q4'16. Contrary, Series A deal-share reached a 5-quarter high taking 28% of deals in Q4'16. [59] Moreover, although US early-stage fintech deal activity declined 11% year-over-year in 2016, US early-stage funding hit a 5-year high with $1.2 billion across 231 deals. [60] Notwithstanding the described decline in both deals and funding, VC investments remained robust and the slow down appeared more a sign of caution rather than concern.[61]

More recently, in Q2 2017, US VC-backed fintech startups raised $1.9 billion across 96 deals.[62] At the current run rate, US fintech funding activity is on pace to grow 11% on a year-over-year basis in 2017. [63]

In particular, in Q2'17 seed/angel fintech deal share in the U.S. fell to a 5-quarter low, while Series A deal share rebounded to hit 29% compared to 21% in Q1'17. [64] Seed and series A deals to VC-backed fintech companies in the U.S. dropped for the third consecutive quarter to a 5-quarter low in Q2'17. By contrast,

[53] See, CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 21.
[54] Id., p. 22.
[55] Id., p. 23.
[56] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 29.
[57] Id., p. 30.
[58] Ibidem.
[59] Id., p. 31.
[60] Id., p. 32.
[61] See, also KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, cit., pp. 48-50.
[62] See, CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 27.
[63] Id., p. 26.
[64] Id., p. 28.

funding hit a 5-quarter high up to 86% on quarterly basis, mainly driven by several larger deals.[65] Median late-stage fintech deal size rose to $38.5M in Q2'17 from $25.5M in Q1'17.[66]

Across the United States, the availability of VC funding remained concentrated in traditional hubs, such as California and New York. California fintech deal activity dropped as funding was slightly up in Q4'16.[67] Among the financings making up the largest deals in Q4'16 were Stripe's $150M Series D and BlueVine's $49M Series D.[68] New York VC-backed fintech companies raised $420M across 20 deals in Q4'16, a slight increase over Q3'16 levels.[69] Funding activity trended downward after Q3'16, but rose 175% on a quarterly basis in Q4'16.[70] More recently, in Q2'17 California fintech deals declined 18% on an annual basis. Although the funding decreased 3% on a quarterly basis, it did reach total $700M for the second straight quarter, including 4 of Q2'17's top 10 fintech deals in the United States.[71] By contrast, fintech funding to VC-backed New York companies grew 19% on a quarterly basis in Q2'17.[72]

Various U.S. investors actively participated in the fintech space in 2016 and again in 2017. Among VC investors, New Enterprise Associates, Khosla Ventures, and Andreessen Horowitz were the three most active VC investors in U.S.-based fintech companies over the period from Q2'16 to Q2'17.[73] Major banks continued to invest in fintech startups, as well. Moreover, corporate participation in U.S. deals to VC-backed fintech companies remained low in 2016, but returned to grow in 2017, counting for 35% of all VC-backed fintech deals in Q2'17.[74]

Europe - European VC-backed fintech companies raised $1.2 billion across 179 deals in 2016. While funding fell 25% on a year-over-year basis, European fintech deals rose 11% in 2016 and 124% compared to 2012's total.[75] On a quarterly basis, European VC-backed fintech companies raised $272M across 44 deals in Q4'16.[76] Still, fintech deals in H2'16 were down 17% from H1'16, while funding decreased 28%. More recently, in H1'17 deals to European VC-backed fintech companies surpassed 2014's year end total. At the current run-rate, Europe fintech deal activity is expected to top 2016's deal total by 40%, while funding could break the $2 billion mark.[77]

---

[65] Id., p. 29.
[66] Id., p. 31.
[67] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 38.
[68] Ibidem.
[69] Id., p. 39.
[70] Ibidem.
[71] Id., p. 35.
[72] Id., p. 36.
[73] See, CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 34.
[74] Id., p. 33.
[75] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 42. See, also KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, cit., p. 65 (recording 242 closed venture capital rounds (representing a 7 year high) for a total value of $1.4 billion).
[76] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 43.
[77] See, CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends*, *Top Deals, Active Investors, and Corporate Activity*, cit., p. 38.

In 2016, early-stage (seed and series A) fintech activity in Europe increased 15%, while funding increased 4%.[78] In particular, European VC-backed early-stage fintech companies raised $366M across 114 deals, a 5-year high in deal and funding activity.[79] On a quarterly basis, early-stage deal share accounted for 60%+ of all deals in Q4'16 for the third straight quarter.[80] More recently, seed and series A deal share to European fintech companies reached 53% in Q2'17.[81]

Although Europe saw zero $50M+ VC-backed fintech rounds in 2016,[82] the top 10 VC-backed European fintech deals accounted for nearly $350M in total funding.[83] In particular, German and UK dominated Europe top 10 fintech deals in 2016: German VC-backed fintech companies raised $34M across 7 deals in Q4'16[84] and UK VC-backed fintech companies raised $173M across 16 deals in Q4'16.[85] The trend continued in 2017, with the top 10 deals in Q2'17 to European VC-backed fintech startups raising more than $370M in total funding and a first 100M+ VC-backed fintech deal closed in Germany.[86] UK VC-backed fintech deals decreased 40% from 25 in Q1'17 to 15 in Q2'17, while funding dropped 52% from $339M in Q1'17 to $164M in Q2'17.[87] German VC-backed fintech funding reached $150M in Q1'17 and $177M in Q2'17, across 17 deals in Q1'17 and 12 deals in Q2'17 respectively. [88]

During the period from Q2'16 to Q2'17, SpeedInvest was the most active by fintech investments to European companies, followed by Seedcamp and Index Ventures.[89] Corporate investments in European fintech companies also increased from 7% in Q4'15 to 39% in Q4'16.[90] However, corporate participation in Europe VC-backed fintech deals fell for 2 consecutive quarters to 33% in Q1'17 and then to 29% in Q2'17.[91]

---

[78] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors*, *and Corporate Activity*, cit., p. 45.
[79] Ibidem.
[80] Id., p. 44.
[81] See, CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 40.
[82] See, *CB Insights, The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 20.
[83] Id., p. 48. See, also, KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, cit., p. 67 (noting that "[m]edian financing sizes across all stages increased in 2016. This signifies the perceived growth opportunities for startups Europe.").
[84] See, *CB Insights, The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 52. See, also, KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, cit., p. 74 (estimating total $376M venture capital investment in fintech companies across 31).
[85] See, *CB Insights, The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 52. See, also, KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, cit., p. 72 (reporting total $609M venture capital investment in fintech companies across 96 deals and noting that "London is seen as one of the truly global financial centers which, along with a vibrant tech startup sector, has helped created a strong environment for fintech firms to start up and scale. Venture capitalists continue to show a strong interest in the sector and plenty of fintech businesses have been able to raise significant sums.").
[86] See, CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 43.
[87] Id., p. 46.
[88] Id., p. 47.
[89] Id., p. 45.
[90] See, CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 49. See, also, KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, cit., p. 69 (indicating that "VC arms of large technology companies and financial institutions continue to invest in the fintech sector: aggregate investments reached a high $363.7M in 2016.").
[91] See, CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, cit., p. 44.

1.D.ii. Large Technology Companies

Over the past few years, the playing field in the banking and financial services industry has expanded beyond traditional banking institutions to allow competition by recognized tech giants.[92] Leading technology companies like Amazon, Google, Apple, Uber and Alibaba, are now driving real changes in the banking and financial services landscape in four major ways:

- Technology giants increasingly play around the periphery of banking and financial services and progressively integrate payment services within their customers' journeys.[93] For instance, Paypal, Alibaba's Alipay and Tencent's WeChat have all used P2P payments to gain and consolidate a large user base for adjacent services, particularly e-commerce. Similarly, large technology players like Apple, Google, and Facebook have developed their own P2P solutions that allow them to further empower their engagement with existing customers and consolidate their control over the mobile commerce experience.

- A number of technology giants now offer financial services targeted to specific customer needs. For example, Amazon lends online sellers capital to purchase inventory and grow their business on the Amazon marketplace through a service called Amazon Lending; while Uber runs a car-leasing program designed for Uber drivers through Xchange Leasing.

- Leading technology companies provide fully integrated and contextual customer experiences, whereby products and services can be easily and securely accessed across multiple devices with a single log-in, with no fuss and (mostly) at no cost. In so doing, leading technology companies are resetting the benchmark for customers' expectations and are raising customers' appetite for a more personalized, intuitive, and seamless experience. This, in turn, creates a "liquid expectation" challenge for banks: customers of technology companies tend to assess the quality of the services/products that they receive from banks against the quality of technology companies' products and services;[94] when interacting with banks, customers expect to have an experience very similar to the one they have with technology companies and may, therefore, perceive any relative deficiency or shortcoming from banks as a service failure.[95]

---

[92] See, Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., p. 8; Accenture, *Fintech and the Evolving Landscape: Landing Points for the Industry*, cit., pp. 8-9.

[93] See, e.g., McKinsey & Company, *Gauging the Disruptive Potential of Digital Wallets*, McKinsey on Payments, Vol. 8, No. 21, pp. 3-10 (May 2015); McKinsey & Company, *Faster Payments: Building a Business, Not Just an Infrastructure*, McKinsey on Payments, Vol. 8, No. 21, pp. 23-29 (May 2015), pp. 27-28; McKinsey & Company, *The New Rules for Growth through Customer Engagement*, McKinsey on Payments, Vol. 8, No. 22, pp. 32-38 (October 2015), p. 32; Accenture, *Fintech and the Evolving Landscape: Landing Points for the Industry*, cit., pp. 2, 8; McKinsey & Company, *Building a Digital-Banking Business*, McKinsey Financial Services Report (April 2016), p. 8.

[94] See, Fjord and Accenture, *The Era of Living Services*, Fjord and Accenture Report (2015).

[95] See, e.g., McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., pp. 9-10; McKinsey & Company, *The Digital Battle that Banks Must Win*, McKinsey Financial Services Report (August 2014); McKinsey & Company, *Digital Banking: Winning the Beachhead*, McKinsey on Payments, pp. 3-10 (May 2014), pp. 3-5.

- Large technology companies are gradually position themselves between banks and banks' customers, thus capturing the vital customer relationship and creating the risk for banks of being relegated to a limited role as back-office utilities.[96]

1.E. Fintech Related Regulatory Reforms and Policy Initiatives

Regulation plays a key role as swing factor in how fintech innovation plays out, as it affects both the speed of fintech innovation and the extension of its impact.[97]

Regulation also presents a double-edged sword to incumbent banks: on one hand, it helps protect incumbent banks within their traditional businesses; on the other hand, it restricts incumbent banks in their response to fintech companies.[98] In particular, following the financial crisis of 2008-2009, financial regulators across a number of countries have adopted a sway of new regulations and have tightened the requirements on banks, covering aspects such as reporting standards, risk-management practices, capital requirements, anti-money laundering (AML) and know-your-customer (KYC) requirements. The combination of these new requirements, in turn, has made it more expensive to run a bank and much more difficult to establish and expand new business models within the banking system.[99] At the same time, following the financial crisis of 2008-2009, financial regulators around the world have also pushed ahead with the goal of bringing greater competition to the financial and banking services industry by lowering the barriers to entry. To that end, a variety of initiatives (e.g., regulatory sandboxes, innovation hubs, special fintech licenses, etc.) have been implemented, which have sought to create an appropriate environment for, and leverage the opportunities presented by, new entrants.

In addition, many of the novel products ad services developed by fintech companies cut across existing regulatory frameworks and do not squarely fit within current legislative and regulatory regimes. This, in turn, raises challenging issues for banking and financial regulators, which are called upon to oversee and control fintech innovation to ensure continue protection of customers, investors, and markets. The remaining part of this section discusses this point in greater detail, specifically investigating fintech related regulatory reforms and policy initiatives recently undertaken by regulators in the UK and the United States.[100]

---

[96] See, McKinsey & Company, *A Brave New World for Global Banking*, McKinsey Financial Services Report (January 2017); Wayne Busch and Juan Pedro Moreno, *Banks' New Competitors: Starbucks, Google, and Alibaba*, Harvard Business Review (February 20, 2014); Juan Pedro Moreno, *Banking at a Digital Crossroads*, cit.; PWC, *Who Are You Calling a 'Challenger'? How Competition is Improving Customer Choice and Driving Innovation In the UK Banking Market*, cit., p. 22]

[97] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., p. 7 (noting that "[a]lthough unlikely to change the general direction, regulation could affect the speed and extent of disruption, if there were material shocks that warranted stronger regulatory involvement, e.g., cyber-security issues with leading FinTechs.").

[98] See, The Economist, *The Disruption of Banking*, The Economist Intelligence Unit Report (2015), p. 5.

[99] See, McKinsey & Company, *A Brave New World for Global Banking*, cit., pp. 1-2 (noting that "[b]anks face enormous challenges to digest the wave of regulation that followed the financial crisis … [c]ontrol costs in risk, finance, legal, and compliance have shot up in recent years. And additional proposals, termed "Basel IV," are likely to include stricter capital requirements, more stress testing, and new guidelines for conduct and compliance risk.").

[100] See, e.g., Microsoft, *Banking as a Digital Platform*, Microsoft Financial Services - Banking & Capital Markets Insights (January 26, 2017); Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., p. 16 (observing that "[t]he old regulatory barriers that had kept competitors at bay no longer seem to work. … Rather than coming to the banks' aid with new types of protection, regulators have thus far encouraged competitors, with measures such as

1.E.i. The UK Fintech Regulatory Framework

The UK is widely regarded as being one of the most welcoming countries for fintech companies. UK financial authorities and regulators have taken an early lead in the fintech space by helping create a best-in-class financial innovation ecosystem and being increasingly progressive in their use of principle-based regulation and policies to support new banks and banking models.[101] While supporting fintech innovation, UK regulators have also taken relevant steps to ensure that relevant financial regulations and standards be upheld and that the financial stability and integrity of the financial system be protected.[102]

For example, the Bank of England has been actively supporting fintech innovation through a number of key initiatives, including by: (1) widening access to central bank money to non-bank payments service providers (PSPs), including firms granted the status of either an e-money or payment institution in the UK;[103] (2) being open to providing access to central bank money for new forms of wholesale securities settlement;[104] (3) exploring the use of distributed ledger technology in its core activities, including the operation of real-time gross settlement (RTGS);[105] (4) partnering with fintech companies on projects of direct relevance to the Bank of England's mission, including the creation of a Fintech Accelerator to help harness fintech innovations for central banking;[106] and (5) calibrating its regulatory approach to fintech developments.[107]

In addition to the Bank of England, the Financial Conduct Authority (FCA) has been playing a key role in promoting fintech innovation. Pursuant to its statutory mandate to promote competition in financial services, in October 2014 the FCA established Project Innovate to encourage innovation in the interests of consumers and to promote competition and growth in the financial and banking services industry by supporting small and large businesses that are developing products that could genuinely improve services for consumers.[108] Three of the most important initiatives launched under Project Innovate are the Innovation Hub, the Regulatory Sandbox, and the Advice Unit:[109]

PSD2, Open Banking, and the U.S. Office of the Comptroller of the Currency's proposed fintech charter. Unbundling of banking services has become yet another tool for the prudential regulator to employ in combating moral hazard.").

[101] See, Ernst & Young, *Landscaping UK Fintech*, cit., pp. 10-12; Ernst & Young, *UK FinTech on the Cutting Edge. An Evaluation of the International FinTech Sector*, Ernst & Young Report Commissioned by UK HM Treasury (2014), pp. 10-11, 50-59.

[102] Cfr., e.g., Mark Carney (Governor of the Bank of England), *Enabling the FinTech Transformation: Revolution, Restoration, or Reformation?*, cit.; Mark Carney (Governor of the Bank of England), *The Promise of FinTech – Something New Under the Sun?*, cit.; Mark Carney (Governor of the Bank of England), *Building the Infrastructure to Realise FinTech's Promise*, cit.

[103] See, Mark Carney (Governor of the Bank of England), *Enabling the FinTech Transformation: Revolution, Restoration, or Reformation?*, cit., pp. 5-6.

[104] Id., pp. 7-8.

[105] Ibidem.

[106] Id., pp. 9-10. For further information on the Bank of England's FinTech Accelerator, visit: http://www.bankofengland.co.uk/Pages/fintech/default.aspx.

[107] Id., p. 10.

[108] See, Financial Conduct Authority (FCA), *Project Innovate: Call for Input*, Financial Conduct Authority (July 2014); Financial Conduct Authority (FCA), *Project Innovate: Call for Input - Feedback Statement*, Financial Conduct Authority (October 2014).

[109] For additional information on the initiatives launched under Project Innovate, visit the FCA's website at https://www.fca.org.uk/firms/fca-innovate.

- The FCA opened the Innovation Hub in October 2014.[110] The Innovation Hub is focused on encouraging innovation in financial services in the interests of consumers by supporting innovator businesses, both regulated and non-regulated, that are looking to introduce groundbreaking or significantly different financial products or services to the market.[111]

- The FCA introduced the Regulatory Sandbox in May 2016.[112] The Regulatory Sandbox is a supervised "safe space" open to both authorized and unauthorized firms, which provides firms with reduced time-to-market at potentially lower cost, appropriate consumer protection safeguards built in to new products and services, and better access to capital. The Regulatory Sandbox allows businesses to test innovative products, services, business models, and delivery mechanisms in the real market, with real consumers, without immediately incurring all the normal regulatory consequences of engaging in the activity in question. In addition, the Regulatory Sandbox offers tools such as restricted authorization, individual guidance, waivers, and no enforcement action letters. The FCA closely oversees trials using a customized regulatory environment for each pilot (including safeguards for financial consumers). Sandbox tests must have a clear objective and must be conducted small scale, so that firms can test their innovation for limited duration with a limited number of customers.[113]

- The FCA established the Advice Unit in 2016 following a recommendation from the Financial Advice Market Review (FAMR). The Advice Unit provides regulatory feedback to firms developing automated models to deliver lower cost advice and guidance to consumers. Until 29 June 2017, the Advice Unit focused on models addressing gaps in the current financial advice market identified by the FAMR, including investments, pensions, and protection. Thereafter, the scope of the Advice Unit has been expanded to cover also firms developing automated models within the mortgage, general insurance, and debt sectors.[114]

---

[110] See, Financial Conduct Authority (FCA), *Innovation Hub Now Open for Business*, Financial Conduct Authority Press Release (October 28, 2014).

[111] Through the Direct Support function of the Innovation Hub, the FCA offers the following services to firms that meet the eligibility criteria: (a) a dedicated team and contact for innovator businesses; (b) assistance for these businesses to understand the regulatory framework and how it applies to them; (c) assistance in preparing and making an application for authorization; and (d) a dedicated contact for up to a year after an innovator business is authorized. Through international engagement the Innovation Hub supports the FCA's competition objective by promoting the UK as a centre for innovation in financial services. It does this by: (a) facilitating the entry of innovative overseas firms to the UK; (b) facilitating the expansion of UK-based innovative firms into overseas markets; and (c) signing co-operation agreements and frameworks with overseas regulators (e.g., Australia, Singapore, Hong Kong, Canada, and Japan) in order to support (a) and (b). Information on the Innovation Hub eligibility criteria and objectives is available on the FCA's website at https://www.fca.org.uk/firms/innovate-innovation-hub.

[112] See, Financial Conduct Authority (FCA), *Financial Conduct Authority's Regulatory Sandbox Opens to Applications*, Financial Conduct Authority Press Release (May 9, 2016) (in commenting the opening of the FCA's Regulatory Sandbox, Tracey McDermott (Acting Chief Executive at the FCA) said "[s]upporting innovation is an essential part of our role in promoting competition in the interests of consumers. Our aspiration is that the sandbox not only enables innovative ideas to be tested and brought to market but also helps to reduce the time and the cost of getting them there.").

[113] Further information on the eligibility criteria and the sandbox options is available on the FCA's website at https://www.fca.org.uk/firms/regulatory-sandbox.

[114] Further Information on the activities and services provided by the Advice Unit is available on the FCA's website at https://www.fca.org.uk/firms/advice-unit.

1.E.ii. The U.S. Fintech Regulatory Framework

The rapid pace of change and the large number of actors in the fintech sector have raised questions among U.S. regulators about how to effectively conduct regulatory and supervisory activities. The key challenges for regulators are: establishing the right balance between the opportunities and risks created by fintech innovation; determining appropriate practices, supervisory expectations, and regulations to facilitate fintech innovations that produce benefits for consumers, businesses, and the financial system as a whole; and coordinating their efforts to achieve consistency in their approaches.

Any proposed reform will need to address the described challenges, manage related risks, and ensure consumers' and investors' protection, while safeguarding markets' and financial institutions' safety and soundness. To date, notable steps taken by U.S. regulators include the following:

- U.S. Consumer Financial Protection Bureau (CFPB) - As further discussed in Chapter 5 below, in 2012 the U.S. Consumer Financial Protection Bureau (CFPB) launched Project Catalyst to facilitate responsible financial innovation. As part of Project Catalyst, the CFPB has developed programs and policies that support consumer-friendly innovation, such as the policy to encourage trial disclosure programs and the policy on no-action letter.[115] Most recently, in November 2016, the CFPB issued a Request for Information with the objective to learn more on: (1) the extent to which consumers that authorize access to their financial records can choose how their records are being shared; (2) how the market is currently functioning, how financial records are currently being shared, and how safe and secure such process is; and (3) how much transparency and control consumers have over their own financial records. The CFPB Request for Information and the comment letters submitted in response to it are discussed in greater detail in Section 5.A.iii. below.

- U.S. Federal Reserve System (Federal Reserve) - In addition to the initiatives discussed in Section 5.B. below, the U.S. Federal Reserve System (Federal Reserve) has sought to gain a robust understanding of the technologies and activities in which banks and other financial firms are engaging to inform the development of its fintech policy and supervisory approaches. To this end, the Federal Reserve has established a multidisciplinary working group that is engaged in a 360-degree analysis of fintech innovation. The group brings together members with diverse expertise across the Federal Reserve, covering key areas of responsibility from supervision to community development, from financial stability to payments, with the goal to assess the impact of technological development on the Federal Reserve's responsibilities. As part of this effort, Federal Reserve senior officials and staff have been closely watching developments in fintech, evaluating the effects of fintech on financial services and its regulation.[116]

---

[115] See, Consumer Financial Protection Bureau (CFPB), *CFPB Finalizes Policy to Facilitate Consumer-Friendly Innovation*, Consumer Financial Protection Bureau Press Release (Washington (DC), February 18, 2016); Consumer Financial Protection Bureau (CFPB), *Policy on No-Action Letters; Information Collection*, 81 Fed. Reg. 8,686 (February 2, 2016).

[116] See, e.g., Lael Brainard (Federal Reserve Board Governor), *The Opportunities and Challenges of Fintech*, Remarks at the Conference on Financial Innovation at the Board of Governors of the Federal Reserve System (Washington (D.C.), December 2, 2016); Teresa Curran (Then Executive Vice President and Division Director, Financial Institution Supervision and Credit, Federal Reserve Bank of San Francisco), *Tailoring, Fintech, and Risk Culture: The Talk of the (Community Banking) Town*, Speech Delivered

- U.S. Federal Deposit Insurance Corporation (FDIC) – In October 2016, the U.S. Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board, and the Office of the Comptroller of the Currency (OCC) jointly issued an advanced notice of proposed rulemaking seeking comments on a new set of enhanced cyber risk management standards for large and interconnected entities under their supervision and those entities' service providers.[117] A number of leading financial firms and technology companies submitted comment letters in response to this joint advance notice of proposed rulemaking and the various questions set forth therein.[118]

---

at the Western Independent Bankers Annual Conference for Bank Presidents, Senior Officers & Directors (Waikoloa (HI), April 4, 2016); Teresa Cunnan (Executive Vice President and Division Director, Financial Institution Supervision and Credit, Federal Reserve Bank of San Francisco), *Fintech: Balancing the Promise and Risks of Innovation*, Consumer Compliance Outlook - Federal Reserve System Publication, Issue No. 3 (2016), pp. 2-4; Consumer Compliance Outlook, *Perspectives on Fintech: A Conversation with Governor Lael Brainard*, cit., pp. 1, 12-14; Tim Marder (Fintech Senior Supervisory Analyst, Financial Institution Supervision and Credit Division, Federal Reserve Bank of San Francisco), *Fintech for the Consumer Market: An Overview*, Consumer Compliance Outlook - Federal Reserve System Publication, Issue No. 3 (2016), pp. 4-5; Tracy Basinger (Group VP of Financial Institution Supervision and Credit (FISC) Federal Reserve Bank of San Francisco), *Is Fintech Changing Banking Supervision?*, San Francisco Fed Blog (July 29, 2016).

[117] The advance notice of proposed rulemaking on enhanced cyber risk management standards was published in the Federal Register on 26 October 2016. See, Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), *Joint Advance Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards*, Federal Reserve System Docket No. R-1550 and RIN 7100-AE-61, OCC Docket ID OCC-2016-0016 and RIN 1557-AE06, FDIC RIN 3064-AE45 (October 19, 2016).

[118] Comments were due by February 17, 2017. See, e.g., Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), *Proposed Rulemaking on Enhanced Cyber Risk Management Standards – Extension of Comment Period*, Joint Press Release (January 13, 2017). Comments submitted in response to the Proposed Rulemaking on Enhanced Cyber Risk Management Standards are available on the Federal Reserve's website at https://www.federalreserve.gov/apps/foia/ViewComments.aspx?doc_id=R%2D1550&doc_ver=1. See, e.g., Amazon Web Services, Commentary to the Advance Notice of Proposed Rulemaking (ANPR) on Enhanced Cyber Risk Management Standards (February 17, 2017) (offering the following recommendations: (A) in evaluating the scope of applicability for future rulemaking, the Federal Financial Institutions Examination Council (FFIEC) should consider that cloud service providers (CSPs) already comply with stringent cyber security requirements and that Amazon Web Services (AWS) customers, including entities regulated by the FFIEC already, have the freedom necessary under the AWS services to control and maintain their own cybersecurity posture in the cloud; (B) the FFIEC should leverage a risk-based, outcome-focused approach to classifying systems as critical depend on (i) purpose for which it is used, (ii) impact to the FS institution or sector from a prolonged disruption, failure and/or compromise, and (iii) risk posture of the system or function. When considering these three factors, according to AWS, cloud services do not rise to the threshold established for sector-critical systems; (C) any final rule should leverage existing industry and where appropriate governmental standards that establish best practices for cyber security governance; and (D) a requirement should allow for a risk assessment of the chances of a disruption to the service and a time frame commensurate with the risk.); American Bankers Association, Response to Enhanced Cyber Risk Management Standards, (Fed) Docket No. R- 1550 and RIN 7100-AE61, (OCC) Docket ID OCC-2016-0016, (FDIC) RIN 3064-AE45 (February 17, 2017) (recommending that any rule resulting from the joint advance notice of proposed rulemaking should (a) determine the application of requirements based on risk in addition to entity size; (b) use a risk-based approach and avoid imposing prescriptive and one-size-fits-all requirements; and (c) be harmonized and reconciled with existing cybersecurity frameworks and regulations.); BSA I The Software Alliance (BSA), Comments on the Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (February 17, 2017) (providing four high level recommendations: (1) ensure the enhanced standards are risk-based, outcome-oriented and technology neutral; (2) align the enhanced standards around the NIST cyber security framework; (3) identify the scope of third-party services subject to the enhanced standards; and (4) clarify how the enhanced standards will apply to third-party services.); Business Roundtable, Comments on the Enhanced Cyber Risk Management Standards Joint Advance Notice of Proposed Rule Making, Dkt. R 1550, RIN 7100- AE- 61 (Federal Reserve System), Dkt. ID OCC-2016-0016, RIN 1557- AE06 (OCC), RIN 3064-AE45 (FDIC) (February 13, 2017) (encouraging a more flexible and risk-based approach to cybersecurity that complements existing cybersecurity requirements and results in better cybersecurity outcomes for everyone); CME Group, Depository Trust & Clearing Corporation and Options Clearing Corporation, Joint Comment on the Enhanced Cyber Risk Management Standards Advance Notice of Proposed Rulemaking, Docket No. R-1550 RIN 7100-AE-61 (January 17, 2017) (offering six main recommendations: the regulatory approach should ensure harmonization, and avoid duplication, of regulation; a risk based approach should be adopted, with focus on critical, or core, systems; systemically important financial market utilities' should not be subject to third-party service provider due diligence conducted by covered entities; firms should be afforded flexibility in implementing the three lines of defense risk management framework; risk-based testing is appropriate; further discussion and analysis should be conducted on how several factors might inform an appropriate recovery time objective (RTO) to a cyber event based on the facts and circumstances of a given event.); Consumer Financial Data Rights Group (CFDR Group), CFDR Group Comment Letter to "Enhanced Cyber Risk Management Standards" Docket ID OCC-2016-0016 (February 17, 2017) (see Chapter 5 for a more in depth analysis of the CFDR Group response); Envestnet Yodlee, Comment Letter to "Enhanced Cyber Risk Management Standards" Docket ID OCC-2016-0016 (February 17, 2017) (arguing that: (1) the enhanced standards should take into account the different levels of risk that various activities financial institutions and their third parties engage in may raise in the wake of a cyber attack and any such standard should only apply to entities that engage in activities that pose risks that could have a significant impact on the safety and soundness of the

- U.S. Securities and Exchange Commission (SEC) As the fintech sector continues to grow and mature, the U.S. Securities and Exchange Commission (SEC) has begun to focus its attention and to devote significant resources to monitoring and addressing issues that arise in connection with fintech innovation.[119] Toward that end, the SEC has undertaken a number of initiatives, including the establishment of a Distributed Ledger Technology (DLT) Working Group and a Fintech Working Group.[120]

Moreover, as part of its ongoing efforts to foster collaboration and understanding between regulators and fintech industry participants, on 14 November 2016, the SEC held a public forum at its Washington (DC)

---

entity other financial entities, and the U.S. financial sector as a whole; (2) the enhanced standards should operate as a flexible standard that can be met by a variety of cybersecurity measures that are suitable to the unique operations and structure of all potentially covered institutions that is based on the types of risk data presents; (3) the definition of "external dependencies" should be clarified to focus on whether the "external dependency" poses cyber risk (and, if it does, the level of cyber risk it presents) and to differentiate between those that are and are not currently examined and supervised by prudential bank regulators which have already implemented the governance and risk management standards required by those regulators.); Financial Services Roundtable/BITS (FSR/BITS), Comments on Joint Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (February 16, 2017) (arguing that the agencies should adopt a risk-based approach to cyber regulation of the financial services sector and discussing the need for harmonization of existing frameworks.); Information Technology Industry Council (ITI), Comments in Response to Banking Agencies' Advanced Notice of Proposed Rulemaking regarding Enhanced Cyber Risk Management Standards (February 17, 2017) (offering five recommendations: orient financial sector cybersecurity approaches around the cybersecurity framework; eliminate or clearly narrow the applicability of the enhanced standards to third-parties; streamline existing financial sector cybersecurity regulatory efforts to avoid duplicative requirements; assess and leverage existing policies and build upon existing public-private partnerships to address financial sector cybersecurity challenges; and prioritize investment in cybersecurity workforce development and training.); Institute of International Bankers (IIB), Comments on Joint Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (February 17, 2017); MasterCard, Response to Request of Comments on the Joint Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards - Federal Reserve System Docket No. R-1550 and RIN 7100-AE-61, OCC Docket ID OCC-2016-0016 and RIN 1557-AE06, FDIC RIN 3064-AE45 (January 17, 2017) (arguing that there exist significant differences between the banking institutions that would be subject to the Standards under the Joint Advance Notice of Proposed Rulemaking and their third-party service providers in terms of size, interconnectedness, and the types of services each provides. Based on these differences, MasterCard urge the regulators to exclude third-party service providers from the scope of the Joint Advance Notice of Proposed Rulemaking.); Microsoft, Comments on Joint Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk Management Standards (February 17, 2017) (recommending that: (1) the proposed standards expressly recognize that covered entities may use third-party service providers to support sector-critical systems, and the standards be appropriately tailored in their application to such third-party service providers; (2) identification of covered services and sector-critical systems be based on whether those services and systems perform functions that are truly critical within the financial services industry, and sector-critical standards be applied in a manner that recognizes the inherent capabilities of the underlying technologies; (3) the standards be implemented as a combination of a regulatory requirement for covered entities to maintain a risk management framework for cyber risks, along with a policy statement or guidance that describes minimum expectations for such a framework; (4) the FFIEC Cybersecurity Assessment Tool could be an appropriate measurement instrument for quantifying cyber risk, subject to some improvements; (5) in the context of cloud and other online services, the proposed standards recognize that service provider commitments regarding service availability and downtime can provide covered entities with assurance concerning service resilience; and (6) with respect to mitigation strategies to address black swan scenarios, the agencies consider the significant security and resilience advantages that cloud services can offer in relation to managing and responding to constantly evolving cyber risks.); North American Chief Risk Officers Council, Comments on Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (January 17, 2017) (discussing the need to: avoid legislating obsolescence, ensure that the risk addressed by the new regulation be clearly defined, and that the proposed solutions be feasible); The Clearing House Association and The Clearing House Payments Company, Comments on the Joint Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (Federal Reserve Docket No. R- 1550 and RIN 7100-AE 61; OCC Docket ID OCC-2016-0016; FDIC RIN 3064-AE45) (February 17, 2017); The Risk Management Association, Response to Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (the "ANPR"): Office of the Comptroller of the Currency 12 CFR Part 30, Docket No. OCC-2016-0016, RIN 1557-AE06; Federal Reserve System, 12 CFR Chapter II, Docket No. R-1550, RIN 7100 AE-61; Federal Deposit Insurance Corporation, 12 CFR Part 364, RIN 3064-AE45 (January 13, 2017) (supporting the regulators' work to determine whether to establish enhanced standards for the largest and most interconnected entities under their supervision and promoting the use of a principles-based approach); VivoSecurity, Comments on Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards; Federal Reserve Docket No. R-1550, RIN 7100-AE-61; OCC Docket ID OCC- 2016-0016; FDIC RIN 3064- AE45 (February 17, 2017) (recommending that the financial regulatory agencies adopt a mandate for statistical cyber risk quantification based on empirical data, as part of the adoption of the Enhanced Cyber Risk Management Standards for medium- and large-scale financial institutions).

[119] See, Mary Jo White (Then SEC Chairperson), *Keynote* Address at the SEC-Rock Center on Corporate Governance Silicon Valley Initiative (Stanford (CA), March 31, 2016); Michael Piwowar (SEC Acting Chairman), *Remarks* before the 27th International Institute for Securities Market Growth and Development (Washington (DC), March 27, 2017).

[120] More information on fintech related activities and initiatives undertaken by the SEC is available on the SEC's website at https://www.sec.gov/spotlight/fintech.

headquarters to discuss fintech innovation in the financial services industry.[121] The event was open to the public and was attended by a number of prominent current and former state and federal regulators, policy experts, advisors, and industry stakeholders. The fintech forum was divided into four panels. The initial three panels addressed developments, opportunities, and challenges relating to three primary areas of innovation: automated investment advice / robo-advisors; distributed ledger technology and blockchain; and online marketplace lending and crowdfunding. The fourth panel covered issues relating to investor protection in the fintech era.[122]

The event highlighted the key role and increasing steps undertaken by the SEC in monitoring and regulating fintech innovation. SEC Chair Mary Jo White opened the forum with introductory remarks.[123] After explaining that "[f]intech innovations have the potential to transform key parts of the securities industry, and to do so in ways that could significantly benefit investors and … capital markets,"[124] SEC Chair White highlighted several developments of interest to the SEC, including: (i) automated investing advice; (ii) distributed ledger technology; and (iii) online marketplace lenders and crowdfunding portals. In describing the SEC's role with respect to such innovations, SEC Chair White stressed the need to ensure that "new developments are not rushed to market or implemented in a way that facilitates a risk of fraud or harm to investors."[125] She noted the important responsibility of regulators to evaluate the adequacy of existing regulations in light of the challenges and opportunities presented by fintech innovation. SEC Chair White, further, explained that she had directed the creation of a Fintech Working Group at the SEC to evaluate the emerging technologies, and had tasked the group to provide "specific, tailored recommendations . . . about what the SEC should do to provide clarity on existing regulatory requirements and help foster responsible innovation."[126] Lastly, she clarified that the SEC is at an early phase in its outreach to investors, innovators, and other stakeholders in the fintech sector, with the fintech forum being an important part of this process.

In its remarks at the fintech forum, SEC Commissioner Michael Piwowar, who championed the idea of the SEC hosting a public fintech forum, emphasized the potential benefits and risks associated with fintech innovation and encouraged the panelists to tackle the challenging regulatory questions that fintech innovation raises.[127] In particular, he suggested exploring initiatives proposed both domestically and internationally, including regulatory sandboxes, which – he argued – could help "encourage fintech innovations, without creating undue risks to the marketplace or imposing artificial limits on activities."[128]

---

[121] See, Securities and Exchange Commission (SEC), *SEC to Hold Forum to Discuss Fintech Innovation in the Financial Services Industry. Forum to be Held on November 14 at SEC Headquarters,* Securities and Exchange Commission Press Release (Washington (DC), September 27, 2016); Securities and Exchange Commission (SEC), *SEC Announces Agenda, Panelists for Nov. 14 Fintech Forum*, Securities and Exchange Commission Press Release (Washington (D.C.), November 3, 2016).
[122] See, Securities and Exchange Commission (SEC), *Fintech Forum - The Evolving Financial Marketplace*, Fintech Forum Transcript (Washington (DC), November 14, 2016).
[123] See, Mary Jo White (Then SEC Chairperson), *Opening Remarks* at the Fintech Forum (Washington (DC), November 14, 2016).
[124] Ibidem.
[125] Ibidem.
[126] Ibidem.
[127] See, Michael Piwowar (Then SEC Commissioner), *Statement* at the Financial Technology Forum (Washington (DC), November 14, 2016).
[128] Ibidem.

SEC Commissioner Piwowar, further, stressed the need for clarity in the sector, noting that the most common regulatory challenge that fintech companies in the United States currently face is navigating the myriad of regulatory portals. To address this problem, he argued the SEC "should take the lead regulatory role in the [f]intech space."[129] In support of this statement, he noted that: (i) "[m]any of the firms pursuing [f]intech are already SEC registrants, and others are providing services that are squarely within the [SEC]'s oversight, such as investment advice and trading and settlement functionalities"; the SEC "is the only agency with a mission that explicitly includes facilitating capital formation"; and the SEC "has 11 regional offices, several in areas that are centers of [f]intech innovation, that could serve as intake centers for [f]intech startups seeking regulatory information and guidance."[130]

Most recently, in January 2017, while announcing its Office of Compliance Inspections and Examinations' (OCIE) 2017 priorities, the SEC re-stated its focus on fintech innovation, with particular attention to fintech developments in electronic investment advice.[131]

- U.S. Commodity Futures Trading Commission (CFTC) – In May 2017, the U.S. Commodity Futures Trading Commission (CFTC) announced the launch of LabCFTC, an initiative aimed at promoting responsible fintech innovation to improve the quality, resiliency, and competitiveness of the markets overseen by the CFTC. Located in New York, the LabCFTC also operates to facilitate the CFTC's engagement with fintech and regulatory technology (regtech) solutions, which may enable the CFTC to carry out its mission responsibilities more effectively and efficiently.[132]

- U.S. Department of the Treasury – In May 2016, the U.S. Department of the Treasury published a white paper in which it examined a number of benefits and risks associated with online marketplace lending, and discussed certain best practices applicable both to established and emerging market participants.[133]

- U.S. Federal Trade Commission (FTC) – The U.S. Federal Trade Commission (FTC) has committed to protecting consumers in the fast-moving fintech sector. In particular, it focuses on how consumers are putting fintech tools to use, covering areas from mobile payments to virtual currencies to crowdfunding, and many more. Toward this end, the FTC conducts workshops, hosts forums, and writes reports covering issues related to fintech and examining relative benefits and risks to consumers

[129] Ibidem.
[130] Ibidem.
[131] See, Securities and Exchange Commission (SEC), *SEC Announces 2017 Examination Priorities. New Areas of Focus Include Electronic Investment Advice, Money Market Funds, and Senior Investors*, Securities and Exchange Commission Press Release (Washington (DC), January 12, 2017); Securities and Exchange Commission (SEC), *Examination Priorities for 2017*, Office of Compliance Inspections and Examinations (OCIE) of the Securities and Exchange Commission (SEC) (January 12, 2017).
[132] See, Commodity Futures Trading Commission (CFTC), *CFTC Launches LabCFTC as Major FinTech Initiative*, Commodity Futures Trading Commission Press Release (Washington (DC), May 17, 2017); Sharon Y. Bowen (CFTC Commissioner), *Statement* on the Launch of LabCFTC (May 17, 2017); Christopher Giancarlo (CFTC Acting Chairman), *Announcing Launch of LabCFTC*, Acting Chairman's Keynote Remarks at the New York FinTech Innovation Lab Annual Reception (New York (NY), May 17, 2017).
[133] See, Department of the Treasury, *Opportunities and Challenges in Online Marketplace Lending*, Department of the Treasury White Paper (May 10, 2016).

created by fintech innovations.[134] In addition, the FTC uses its authority under the FTC Act and other laws to bring law enforcement actions against companies whose deceptive or unfair actions harm consumers.[135]

- U.S. Office of the Comptroller of the Currency (OCC) – Since the launch of its innovation effort in the summer of 2015, the U.S. Office of the Comptroller of the Currency (OCC) has undertaken a number of key initiatives specifically directed at the fintech sector. These initiatives include holding public forum and meetings, publishing practical guiding principles, establishing a framework to support responsible innovation in the federal banking system, creating an Office of Innovation, and evaluating charter applications from fintech companies. These initiatives are discussed in greater detail in Section 7.B.iii. below.

[134] See, e.g., Federal Trade Commission, *Paper, Plastic ... or Mobile? An FTC Workshop on Mobile Payments*, Federal Trade Commission Report (March 2013); Federal Trade Commission, *Mobile Cramming*, Federal Trade Commission Report (July 2014); Federal Trade Commission, *What's The Deal? An FTC Study on Mobile Shopping Apps*, Federal Trade Commission Report (August 2014); Federal Trade Commission, *Internet of Things. Privacy & Security in a Connected World*, Federal Trade Commission (January 2015); Federal Trade Commission, *Big Data. A Tool for Inclusion or Exclusion? Understanding the Issues*, Federal Trade Commission Report (January 2016).

[135] Additional information on fintech related activities undertaken by the FTC is available on the FTC's website at https://www.ftc.gov/news-events/media-resources/consumer-finance/financial-technology.

CHAPTER 2. CONSUMER FINANCIAL DATA AND ACCOUNT INFORMATION ACCESS AND SHARING PRACTICES

Prior sections have analyzed a number of interconnected forces driving the movement towards Open Banking. As this movement gains traction, the use and relevance of application programming interfaces (APIs) within the banking and financial services industry grows significantly. Banks around the world are increasingly compelled to embrace APIs to improve customer experience and engagement, as well as to drive innovation through broader, more open, and dynamic collaborations with developers and partners.

As further discussed in the following chapters, regulators themselves are aligning behind openness — whether to drive competition, encourage innovation, enhance transparency, and/or increase security in the financial and banking services industry. In particular, in Europe, the Second Payment Services Directive (PSD2)[136] together with the European Banking Authority (EBA)'s Regulatory Technical Standards (RTS) for PSD2 are forcing banks to provide secure access, subject to customer consent, to specific account information, data, and functionality to regulated third parties and to enable third-party payment initiation. At the same time, in the UK, the UK Government Open Banking Working Group (OBWG)'s Open Banking Standards and the UK Competition and Markets Authority (CMA)'s Retail Banking Markets Investigation Report and Final Order are creating an API framework that extends beyond the requirements of PSD2 to support new openness. While Europe and the UK are paving the way, other countries will likely follow with similar Open Banking regulations and standards in the upcoming years.

Thus, as openness becomes mainstream, APIs are rapidly emerging as key building blocks of the new Open Banking ecosystem. This chapter digs a little deeper into this point, by examining current practices of consumer financial data and account information access and sharing. It, then, discusses the growing importance of APIs in the financial and banking services industry and analyzes their key features and functionality. Finally, it concludes investigating how banks can leverage the innovative power of APIs and how customers and businesses can benefit from increased API-driven openness.

2.A. Current Mechanisms for Consumer Financial Data and Account Information Access and Sharing

While banks and other account providers can easily access the consumer financial data and account information that they hold, at present third-party services providers (e.g., fintech companies and other consumer-facing applications providers) face significant hurdles in accessing and sharing such data and information. To tackle this problem, some third-party services providers interact directly with banks and other account providers; while others enter into individual contracts with aggregators. The aggregators, in turn, may have direct contracts with different banks, financial institutions, and other account providers

[136] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

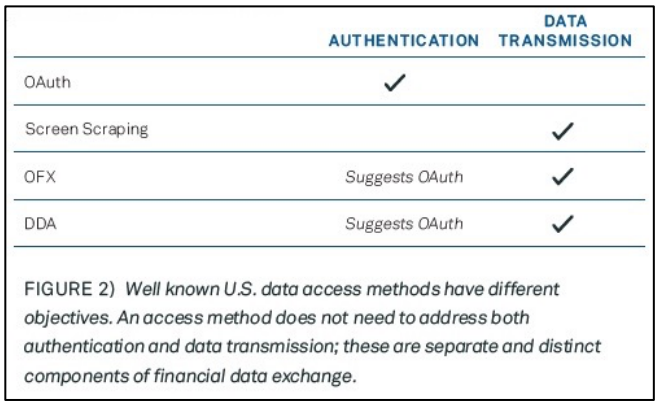
governing the aggregators' access to consumer financial data and account information or they may primarily operate through data access techniques such as screen scraping.[137]

The exchange of consumer financial data and account information consists of two major components, authentication and data transmission:

- Authentication is the process through which access to data is permissioned. Current practices of authentication encompass tokenization solutions, OAuth, and OAuth derivatives such as Screenless Exchange.[138]
- Data transmission includes three main elements: availability (what data is made available), format (how the data is structured), and transfer (how the data is moved). Traditional practices of data transmission include screen scraping and Open Financial Exchange (OFX); while new practices are being explored and implemented with a primary focus on API-based data access specifications such as Durable Data API (DDA).

As illustrated in Figure 8 below, authentication and data transmission components are generally interoperable. For instance, it is possible to combine OAuth with screen scraping and OAuth with APIs.

Figure 8. Common Data Access Methods



	AUTHENTICATION	DATA TRANSMISSION
OAuth	✓	
Screen Scraping		✓
OFX	*Suggests OAuth*	✓
DDA	*Suggests OAuth*	✓

FIGURE 2) *Well known U.S. data access methods have different objectives. An access method does not need to address both authentication and data transmission; these are separate and distinct components of financial data exchange.*

Source: Plaid Technologies, *Financial Data Access Methods: Creating a Balanced Approach*, Plaid Technologies White Paper (October 2016), p. 3.

The remaining part of Section 2.A. examines the use of screen scraping, OFX, and DDA. The following Section 2.B. discusses APIs in greater detail.

2.A.i. Screen Scraping

Screen scraping refers to the practice of collecting - or scraping - data from the consumer's account information environment. There are two basic types of screen scraping, served-based scraping and client-

[137] See below for further discussion on this point.
[138] See Section 2.B.i. below.

based scraping.[139] In both scenarios, a consumer shares his/her bank authentication credentials with a fintech company, which passes them to a data aggregator and, then, deletes them from its own records. The data aggregator stores the consumer's bank authentication credentials, creates an associated UID, and returns the UID to the fintech company. At that point, in the server-based scraping scenario, the data aggregator enters the bank authentication credentials into the bank's website and "scrapes" the required consumer's data. By contrast, in the client-based scraping scenario, the data aggregator passes the bank authentication credentials to a small application on the consumer's local computer, which, then, redirects the bank authentication credentials to the bank's website.[140]

The practice of accessing data through screen scraping creates a number of challenges and costs across the data-sharing ecosystem. In particular, screen scraping may raise challenges and risks for consumer, which include the following:[141]

- Through screen scraping a consumer's bank authentication credentials are passed over the internet to the bank's website. In addition, in a client-based scraping scenario, the authentication credentials are exposed on the consumer's computer each time data is being aggregated, which increases exposure to attack from local malware.
- As further discussed below, the lack of coordination among the various parties involved through the screen scraping process may lead to disrupted connections, as well as unreliable, poor-quality and outdated data and information. This, in turn, may adversely affect consumers, by creating confusion and, even more dangerously, causing them to take actions that negatively impact their financial health (e.g., paying a bill or making a purchase without sufficient funds in their account, thereby triggering an overdraft fee).
- Permissioned third parties (e.g., data aggregators, fintech companies and other consumer-facing applications providers) may abuse the access. For example, when the data aggregator gains access to a consumer's account through screen scraping, it can potentially scrape out any data that is available to the consumer through that account environment, regardless of whether the portal is limited to the specific financial account for which the consumer has permissioned access, or contains multiple accounts for that consumer. In addition, when consumers provide his/her bank authentication credentials to a data aggregator, they may end up giving access to their data for an unlimited period of time. Finally, data aggregators may use the data for purposes beyond the specific service that the customer sought, without the consumer's knowledge and request for any additional services or marketing.

[139] See, Personal Capital, Response to the Consumer Financial Protection Bureau's Request for Information Regarding Consumer Access to Financial Records, Personal Capital (February 21, 2017), pp. 9-10 (discussing similarities and differences between server-side scraping and client-side scraping).
[140] Ibidem (noting that this technique is used primarily when a bank attempts to prevent a data aggregator from accessing its website directly.)
[141] See, e.g., National Consumers Law Center, Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048 (February 21, 2017), pp. 2-3.

- There may be little effort by the permissioned third parties to inform consumers about what data is being taken, the way(s) the data is being used or shared, the frequency and the length of time the data is being accessed.
- Screen scraping practices heighten the possibility that consumers may experience an account compromise and that their data may become the target of a data breach or even be stolen by identity thieves.
- There exist serious concerns that consumers may not be made well aware of the mechanics of screen scraping or how screen scraping may affect their legal rights and obligations.

In addition to the foregoing, screen scraping also presents numerous concerns for banks and other account providers, including the following:[142]

- As the practice of screen scraping grows in usage, the screen-scraped banks (and other account providers) may experience spikes in volume, as well as heavy and sometimes unpredictable traffic patterns on their website. The irregular and high traffic load that gets placed onto their website, in turn, can cause a strain on their systems, can increase the costs and complexities for managing their infrastructures, and can cause inconvenience for individual customers who are trying to directly access their account information at the same time. In such a scenario, the banks (and other account providers) will seek to protect individual customers' access by making permissioned parties wait and access the banks' (or other account provider's) systems only during non-peak hours.
- Screen scraping gives banks' and other account providers' very limited visibility into the security capabilities and practices of third parties that are accessing data through screen scraping mechanisms; banks and other account providers usually are not notified about the steps permissioned parties have taken to mitigate security breach and fraud risks; and permissioned parties may be reluctant to fully disclose how they will protect, use, share, or otherwise process data. These obstacles, in turn, restrict the banks' and other account providers' ability to monitor the security of their customers' accounts and potentially create heightened risk for data protection.
- Under certain circumstances, screen scraping practices may resemble dangerous automated account validation scripts, which have the potential to seriously compromise customer accounts. In an effort to protect from such attacks, banks and other account providers may end up unnecessarily cutting off access to permissioned third parties.[143]

---

[142] See, e.g., Consumer Bankers Association (CBA), Response to Request for Information Regarding Consumer Access to Financial Records, Docket No.: CFPB-2016-0048 / Document No.: 2016-28086 (February 21, 2017), pp. 4-6; American Bankers Association, Response to Request for Information Regarding Consumer Access to Financial Records, Docket No.: CFPB-2016-0048 (February 21, 2017).

[143] See, Lalita Clozel, *Cordray Reignites Bank-Fintech Fight After Comments on Data Sharing*, American Banker (October 25, 2016) (quoting Rob Morgan, Vice President of emerging technologies at the American Bankers Association arguing that "some of the screen scrapers coming in you can tell... that a login is coming from a computer … What is really hard to tell is, is that a benign computer or is it a malicious one? … At the end of the day it really is, how do you facilitate this sharing of data in a way that protects the customer? … It's not so easy to do … [but] there are a lot of banks working on this and looking at the ways to make that data available whether it's through APIs or partnerships with some of these data aggregators.").

For permissioned parties (e.g., data aggregators, fintech companies and other consumer-facing applications providers), relevant obstacles include the following:[144]

- When the bank's (or other account provider's) website is redesigned, changed, or otherwise updated, the programs that collect data from the bank's (or other account provider's) website may stop working. As a result, data aggregators, fintech companies and other consumer-facing applications providers may be forced to frequently adapt to changing electronic interfaces.

- The lack of coordination among the various entities involved in the screen scraping process may cause disruptions in the flow of data, may generate high latency in the receipt of data from the account provider, and may lead to data that is (significantly) unreliable and outdated. This, in turn, limits a third-party's ability to provide personalized and high-quality services and products and may render its services and products less useful to consumers.

The described risks and challenges have created the need to improve existing screen scraping practices.[145] This need, in turn, has spurred a debate around the opportunity to transition from screen scraping to more secure, transparent, and efficient data access and sharing techniques. The following sections will discuss this point in more detail.

2.A.ii. Open Financial Exchange (OFX)

OFX is the earliest data transmission specification for financial data collection and exchange.[146] A coalition of leading technology companies - Intuit, Microsoft, and Checkfree - developed OFX in 1997.[147] The initial specification combined elements of Intuit's OpenExchange, Microsoft's Open Financial Connectivity, and Checkfree's electronic banking and payment protocols. Since its initial release, OFX has been adopted by thousands of financial institutions.[148]

---

[144] Center for Financial Services Innovation (CFSI), Response to CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records (February 21, 2017), pp. 4-6; Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 (February 21, 2017), pp. 7-10; Envestnet Yodlee, Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, Docket No.: CFPB-2016-0048 (February 21, 2017), pp. 7-11; Financial Innovation Now (FIN), Response to Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 (February 21, 2017), pp. 4-5; Plaid Technologies, Response to CFPB regarding Consumer Access to Financial Records Docket No. CFPB-2016-0048 (February 21, 2017), pp. 15-21.

[145] See, e.g., Plaid Technologies, *Financial Data Access Methods: Creating a Balanced Approach*, Plaid Technologies White Paper (October 2016), pp. 6-7 (discussing advances in screen scraping practices, with focus on Screenless Data Collection (SDC)).

[146] See, Open Financial Exchange (OFX), *About OFX – Background Summary*, Open Financial Exchange (to date) (explaining "Open Financial Exchange (OFX) is an open standard for client-server systems and cloud based APIs for exchanging financial data, and performing financial transactions between financial institutions, and financial applications. Further, the API allows the exchange to be facilitated either directly or via an intermediary such as data aggregation service providers."). The OFX specification is publicly available for implementation by any financial institution or vendor, and is available for review on the OFX's website. More information can be found at http://ofx.org.

[147] See, Open Financial Exchange (OFX), *FAQ*, Open Financial Exchange (to date) (noting that the original goal was to develop a technical specification that "would enable financial institutions to exchange financial data over the Internet with Web users and users of popular software such as Quicken and Microsoft Money. The objective was to eliminate confusion and uncertainty with a single, unified, open specification.").

[148] See, Open Financial Exchange (OFX), *About OFX – Background Summary*, cit. (noting that OFX has been "actively deployed at over 7,000 financial institutions, and the remaining institutions have easy access to certified OFX servers via all major technology providers and systems integrators."); See, Open Financial Exchange (OFX), *FAQ*, cit. (explaining that "[w]ith more 7,000 banks and brokerages as well as major payroll processing companies using OFX, the specification is the most widely adopted open standard for the exchange of financial information between consumers and financial services providers.").

The OFX specification evolved gradually during its first 10 years.[149] The rate of adoption accelerated significantly in 2006, when the financial and banking services industry introduced multi-factor authentication (MFA) and OFX moved to support it.[150] Thereafter, developments slowed down until 2015, when a consortium re-launched the initiative with the support of a wide range of industry representatives.[151] At present, OFX is developed and maintained by an active consortium of leading financial application, aggregation services, and financial services providers. Prominent members include Intuit, Xero, Enterprise Engineering, Finicity, and Silicon Valley Bank with active participation of 14 other industry leaders.[152]

OFX has been enhanced through the years from OFX 1.0, which used a SGML syntax, to the current OFX 2.2, which uses XML. The current OFX 2.2 was released in 2016: it maintains all of the features of previous versions (including backward compatibility and MFA), while also including a new OAuth token-based authentication model and expanded data access.[153]

The OFX specification is open[154] and has been broadly implemented across top financial institutions and financial applications in the United States, Europe, South America, and Australia.[155] Although the OFX specification is open for development, there is no current public list of financial institution OFX server URLs and OFX request/response connectivity details are normally proprietary.[156]

Although the OFX specification is a very mature and widely adopted mechanism for the exchange of financial information between consumers and financial services providers, it does present a number of technical limitations. For instance, the OFX specification remains highly prescriptive and generally requires technical experts to enable implementation. In addition, OFX standards have not been updated to support all modern technologies and needs.[157] Over time OFX has also become increasingly specific about authentication, conflating this with data transmission.[158] Finally, the OFX specification can be implemented

[149] See, Open Financial Exchange (OFX), *About OFX – Background Summary*, cit. See, also, Steve Bills, *OFX Proposal to Make Aggregation Easier*, American Banker (December 6, 2004).
[150] Ibidem.
[151] See, Open Financial Exchange (OFX), *FAQ*, cit. (explaining that the Consortium updated the OFX specification after 10 years of inactivity to "continually improve the security and reliability of financial data connectivity across the industry. Reactivating the OFX Consortium helps to ensure that the OFX specification and OFX solutions meet institutional and consumer needs in today's technology landscape.").
[152] See, Open Financial Exchange (OFX), *About OFX – Background Summary*, cit.
[153] See, Open Financial Exchange (OFX), *Open Financial Exchange 2.2 [OFX2.2]*, OFX (2016).
[154] See, Open Financial Exchange (OFX), *FAQ*, cit. (explaining that "[o]pen specifications are more compelling than closed proprietary solutions for financial institutions because they can easily use open standards to create custom implementations for their unique needs. OFX combines industry-standard authoring, networking, and security into a highly effective and durable standard. Open Financial Exchange has helped accelerate the adoption of online financial services by financial institutions and their customers.").
[155] Ibidem.
[156] Ibidem.
[157] See, Plaid Technologies, *Financial Data Access Methods: Creating a Balanced Approach*, cit., p. 8 (observing that "[d]espite [its] specificity, OFX does not support the exchange of several new types of financial data, which developers need to innovate. For example, OFX is not equipped to accommodate extensive identity information (for fraud prevention) or certain complex account types. OFX also relies on an older architecture and data format, making it cumbersome to evolve the specification (such as to widen data availability). Nimbleness is necessary for any modern financial data specification, as innovation often demands quick changes to meet new consumer and developer needs.").
[158] Ibidem (noting that "[f]or instance, OFX accommodates OAuth, recommending a redirect flow to authenticate users. This specificity may not work for all institutions, some of which may choose to prioritize a native user experience.").

in multiple ways and many customized implementations have been deployed. As a result, in practice the OFX specification is not a truly consistent, interoperable data transmission standard.[159]

2.A.iii. Durable Data API (DDA)

DDA is a data specification released in 2015 by an industry working-group from the Financial Services Sharing and Information Sharing and Analysis Center (FS-ISAC).[160] Since its initial release, DDA has garnered substantial interest from a number of stakeholders in the data-sharing ecosystem.

DDA calls for authentication through OAuth and is largely designed for personal financial management (PFM). It can be improved, in particular by broadening potential uses beyond PFM and softening its focus on authentication.[161]

With regard to its objectives, DDA was intended to improve data exchange relative to OFX. In general, it is a modern, concise, lightweight, and more flexible specification that places greater emphasis on developers' needs.[162] DDA also has marginal advantages over Screenless Data Collection. Significantly, it delivers greater control to banks regarding who accesses what data on their systems and helps ensure accuracy of the data being delivered.[163]

2.B. Open Banking Building Blocks: APIs

2.B.i. Key Features and Types of APIs

APIs are interfaces that enable communication between software applications (both within and between organizations), where one application calls upon the functionality of another application.[164] APIs essentially bring a new level of connectivity and data sharing to multiple applications. Though APIs, developers can communicate with a services provider (for example a bank), which releases a precise API specification that must be adhered to when developers want to access the services. The API indicates what functionality is available, the format used to communicate, and the requirements and conditions for using the services.

---

[159] Id., pp. 8-9.

[160] The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a non-profit member-driven corporation that was established in 1999. The FS-ISAC works with members that have operations around the globe to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy. The FS-ISAC disseminate physical and cyber threat alerts and other critical information; conducts coordinated, and manages rapid response communications for both cyber and physical events; conducts education programs, training programs, and contingency planning exercises; and fosters collaborations with and among other key sectors and government agencies. More information on FS-ISAC is available on FS-ISAC's website at http://www.fsisac.com.

[161] See, Plaid Technologies, *Financial Data Access Methods: Creating a Balanced Approach*, cit., (October 2016), pp. 9-10.

[162] Id., p. 9 (noting that "for example, DDA allows for standard, modern data formats; by contrast, OFX uses a custom, legacy format.").

[163] Ibidem.

[164] See, Euro Banking Association (EBA), *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, EBA Working Group on Electronic Alternative Payments and Innopay Information Paper (May 2016), p. 7 (defining API as "a specific software architectural approach that revolves around the view that interfaces should be scalable, reusable and secure while offering ease of use for developers through self-service. APIs therefore hold the promise to reduce cost and lead time of interfacing between systems, allowing for faster, cheaper and better innovation on a larger scale.").

Most APIs - whether they are closed or open[165] - are built around the following open globally accepted technical standards relating to data transmission, data exchange, data access, and API design:[166]

- Data Transmission - In practice, most APIs use HTTP/HTTPS as a transport layer, because it is straightforward, widely accepted and compatible. However, there are APIs that can be used over a variety of other transport protocols that provide compelling alternatives to HTTP/HTTPS.

- Data Exchange - Two of the most common formats for exchanging data are XML (Extensible Markup Language) and JSON (JavaScript Object Notation). XML has long been used and has slightly more functionality than JSON. Yet, JSON has become increasingly more popular, because it is more flexible, intuitive, and lightweight, and it is relatively faster and better machine-readable. Some API providers offer the ability to choose which format to consume, whilst others only have one format available.[167]

- Data Access - Popular standards include SAML (Security Assertion Markup Language) and OAuth 2.0. SAML is an XML-based framework and is most commonly utilized in business-to-business interfacing. OAuth 2.0 is a protocol that originated in the consumer web services world.[168]

- API Design - Common API standardized architectural principles are REST (Representational State Transfer) and SOAP (Simple Object Access Protocol). Between the two, REST is currently more popular and widely adopted due to its focus on enabling and improving desirable properties such as performance, scalability, simplicity, flexibility, visibility, portability, and reliability.[169]

---

[165] See below for further discussion on this point.

[166] See, Euro Banking Association (EBA), *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, cit., p. 7.

[167] See, Open Banking Working Group (OBWG), *The Open Banking Standard. Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation*, Open Banking Working Group (February 2016), p. 29 (discussing the industry favor for JSON over XML and explaining that JSON " is a popular, lightweight format that is easy for computers to parse and generate, and easy for humans to read and write. It is also programming language-independent and widely adopted for modern APIs. However, unlike JSON, XML is currently in use in several existing financial formats. Consequently, there is a tension between the reuse of a financial standard (in XML) against developer preferences and their forward-facing expectations (supported by JSON's position as the default for modern APIs)."

[168] See, e.g., Plaid Technologies, Financial Data Access Methods: Creating a Balanced Approach, cit., pp. 4-6; Personal Capital, Response to the Consumer Financial Protection Bureau's Request for Information Regarding Consumer Access to Financial Records (February 21, 2017), pp. 1, 3-5, 11-13 (discussing the use of OAuth by financial institutions and arguing that OAuth would restrict consumer access and weaken the cybersecurity protecting the money in consumer bank accounts); Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 (February 21, 2017), pp. 13-14.

[169] See, e.g., Open Banking Working Group (OBWG), *The Open Banking Standard. Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation*, cit., p. 29 (explaining "Microsoft originally developed SOAP as a replacement for older technologies that were not optimized for the internet. SOAP is based on XML, which works better over the internet than older RPC protocols using binary messaging. It is also extensible, with a wide range of existing standard extensions for security, addressing, messaging, etc. However, while SOAP is a mature technology, many developers find it heavyweight and difficult to use. The XML messages can be large and cumbersome, and the extensions can be complex to use … REST is a lighter-weight alternative to SOAP; it describes the architectural style of the Web. The Web's simplicity represents a key strength and RESTful APIs (i.e. APIs that follow the REST style) follow this simplicity by using URIs to address resources, HTTP methods and headers for actions, and representations for transferring state. RESTful APIs are therefore easier for developers to use; the majority of modern Web APIs now use REST rather than SOAP."); Accenture, *Driving Innovation in Payments — Powered by APIs & Open Banking*, Accenture Payments Report (2016), p. 6.

In addition to the described technical requirements, the growing use of APIs in the financial and banking service industry has created the need to apply further control and standardization dimensions to cover legal, operational, and functional aspects.[170]

As mentioned above, APIs are extremely powerful tools that can underpin both external and internal ecosystem. The level of openness of an API is critical as it determines the potential reach of the functionality offered through the API. In this context, APIs can be broadly distinguished between "closed APIs" or "private APIs" (when APIs can only be accessed within the boundaries of an organization) and "open APIs" (when APIs can also be accessed by third parties outside of the boundaries of the organization).[171]

Within these two broad groups, APIs can be further classified into various categories. For example, Forrester lists four categories of APIs:[172]

- Internal ("Private") APIs – Internal ("Private") APIs enable internal systems of an organization to communicate to each other more easily. They help improve organizational agility, effectiveness, and efficiency.[173]

- B2B ("Partner") APIs – B2B ("Partner") APIs enable highly customized integrations between an organization and select business partners, customers, and other stakeholders, usually for a specific business process and pruposes. They are used to optimize processes and relationships outside single organizations.[174]

- Open Web ("Public") APIs – These APIs allows an organization to open data, product catalogs, business processes, or other business assets to a larger community of developers. They help organizations expand their market reach, increase sales, generate new revenue streams, and accelerate innovation through openness.[175]

[170] See, Euro Banking Association (EBA), *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, cit., p. 10.
[171] Id., p. 7.
[172] See, Forrester Research, *Four Ways APIs Are Changing Banking. How Financial Services Firms Are Exploiting the API Economy*, Forrester Research Report (May 2016), pp. 5-6 (explaining that "[e]ach of the four [categories] has different primary design goals and governance requirements, but they also have overlapping design considerations — a given API may fit into more than one category.").
[173] Id., p. 5 (noting that with respect to internal APIs "[t]he challenge is ensuring that APIs package up true business capabilities, not just wrap old-style application functionality. Digital business executives must implement strong API governance to ensure that the project-level design follows guidelines and contributes to the evolution of a coherent business portfolio of APIs ready for reuse across any touch-point."). See, also, Forrester Research, *Drive Business Agility and Value by Increasing Your API and SOA Maturity - Forrester's Eight Central Elements of Service-Based Maturity Provide a Foundation for Achieving Business Agility Via APIs and SOA*, Forrester Research Report (September 2013); Forrester Research, *Best Practices for Agile-Plus-Architecture - Enterprises Need Sustainable Business Agility, Not Just Agile Development*, Forrester Research Report (February 2015).
[174] See, Forrester Research, Four Ways APIs Are Changing Banking. How Financial Services Firms Are Exploiting the API Economy, cit., p. 5 (noting that "[w]hen designing B2B APIs, digital business professionals must clearly understand the processes and business outcomes that the APIs improve in order to provide rock-solid, efficient business operations through cross-enterprise, real-time flows of transactions, data, and insight.").
[175] Id., p. 6 (explaining that "[t]he main design challenge that digital business executives face with open web scenarios is understanding the synergies between their business and a broad community — and then creating APIs that make it easy for others to participate in creative ecosystem innovation.").

- Product APIs – These APIs add value to products by connecting and integrating them into wider ecosystems.[176]

In a similar fashion, Euro Banking Association has proposed a classification of APIs, which distinguishes among five API categories:[177]

- Private APIs – Closed APIs exclusively accessible by parties within the boundaries of an organization.

- Partner APIs – APIs exclusively accessible, at the discretion of the provider of the APIs, to selected partners based on bilateral agreements.

- Member APIs – APIs open to everyone who is a formal member of a community/group and complies with the community/group's membership rules and regulations.

- Acquaintance APIs – APIs open to everyone complying with a predefined set of requirements.

- Public APIs – APIs accessible by anyone, usually with some form of registration for identification and authentication purposes.

2.B.ii. Wide Spread Cross-Industry Adoption of APIs

APIs are far from being new developments, as the idea behind APIs has existed since the beginning of computing and structured programming.[178] However, it is only during the last 10 years, that APIs have grown significantly both in usage and sophistication and have become increasingly scalable, monetized, and ubiquitous. In particular, over the past decade, the innovative power of APIs has led many companies to the realization that APIs could be a very critical component of their enterprise solutions and could materially contribute to efficiencies, growth, and innovation. This, in turn, has facilitated an expansion of the conversation around APIs from a mere technical need to a business priority. As a result, the relevance of APIs has increased exponentially and has moved past traditional borders of the IT department into the broader business organization.[179]

The API revolution has been extremely pervasive: a wide spectrum of industries have embraced APIs, including telecommunications and media, travel, tourism, and real estate. Companies operating across these industries are now using APIs to deliver superior customer value, to empower customer experience and engagement, and to extend their business and innovative capabilities through partner channels and

[176] Ibidem (explaining that "because they enable direct control of and integration with a product or service, product APIs are primarily of interest to those who buy and use the product and to the ecosystem players that add value to the product. The key design challenge of a product API is understanding the context in which a product is used and building support for useful flows of data and control between the product and its ecosystem.").
[177] See, Euro Banking Association (EBA), *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, cit., p. 8.
[178] For a brief history of APIs, see, e.g., Kin Lane, *History of APIs*, API Evangelist Blog (December 20, 2012); Deloitte, *Tech Trends 2015 - The Fusion of Business and IT*, Deloitte University Press (2015), pp. 22-23 (discussing the evolution of API since 1960-1980 to present).
[179] See, Deloitte, *Tech Trends 2015 - The Fusion of Business and IT*, cit., p. 23 (quoting Jyoti Bansal, Founder and CEO of AppDynamics, explaining that "APIs started as enablers for things companies wanted to do, but their thinking is now evolving to the next level. APIs themselves are becoming the product or the service companies deliver.").

ecosystem engagement initiatives.[180] In addition, more and more companies across these industries are adding business logic at the API tier to accelerate digital initiatives without disrupting their back-ends; and they are also using the API tier for data transformations to tie disparate backend systems and formats seamlessly. Moreover, many companies are progressively leveraging the API tier to improve app performance and availability; and they are increasingly storing persistent data in the API tier to improve app performance and accelerate app development.[181] Finally, enterprises operating across the described industries are increasingly looking to APIs for key security advantages, including built-in privacy, threat protection, visibility and governance.[182]

Most notable examples of companies leveraging the power of APIs include Salesforce, Google, Amazon, eBay, Facebook, Uber, Netflix, Expedia, and Twitter. Without the business accelerating capabilities of APIs, these and many other companies could have not grown so fast and could have not scaled their operations to become global leaders. This is because APIs have enabled a flourishing ecosystem and have helped them promote partnerships, spur innovation, and build new disruptive business models. By deploying deeply valuable open API-driven strategies, these companies have placed themselves squarely at the center of their users' daily lives and now successfully serve millions of consumers and businesses all around the world.[183]

APIs are not new to the financial and banking services industry either, although this industry has been relatively slow and risk averse in the adoption of these capabilities. Established payment technology solutions and payment services providers (e.g., PayPal),[184] established financial institutions (e.g., Visa[185] and MasterCard[186]), fast growing fintech companies (e.g., Stripe,[187] Transferwise,[188] Vemno,[189] and Paymency[190]), and digital-only challenger banks[191] have adopted and deployed successful API strategies.

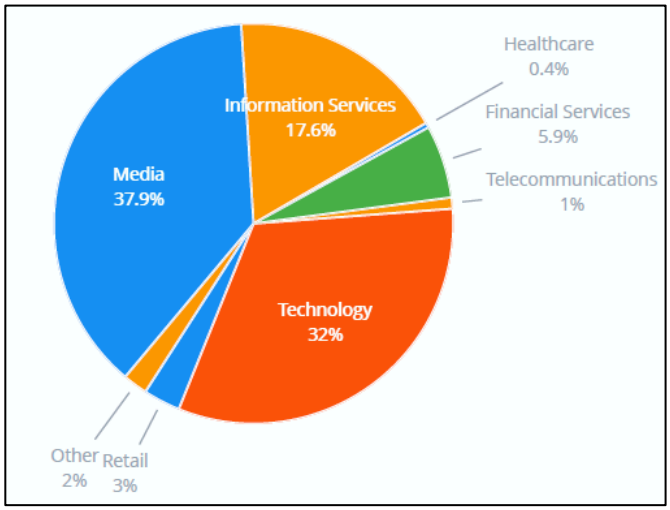
Moreover, many incumbent banks already have APIs. However, until relatively recently, most banks have built and operated APIs mainly to facilitate easier technology system integration; whilst very few banks

[180] See, Apigee, *The State of APIs - 2016 Report on Impact of APIs on Digital Business*, Apigee Report (2016), slides 6-7.
[181] Id., slides 13-14, 16.
[182] Id., slide 15.
[183] For an in-depth analysis of the current state of digital transformation and APIs across industries, see, e.g., Apigee, *The State of APIs - 2016 Report on Impact of APIs on Digital Business*, cit.; and Apigee, *The State of APIs - 2017 Report: How APIs Power Digital Ecosystems*, Apigee Report (2017) (providing an interesting analysis of the impact of APIs across various industries; discussing common use cases driving digital transformation in different industries; and examining best practices of API-driven enterprises); MuleSoft, *Connectivity Benchmark Report - The State of Digital Transformation and APIs*, MuleSoft Report (May 2016) (surveying 802 IT decision makers globally across Australia, the Netherlands, Hong Kong, Singapore, Sweden, the United Kingdom and the United States; and assessing how organizations of all sizes are executing on digital transformation, including building and managing APIs); Deloitte, *Tech Trends 2015 - The Fusion of Business and IT*, cit., pp. 22, 25-26; Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., p. 6 (analyzing traditional business models across a variety of industries that have already experienced dramatic change driven by APIs).
[184] PayPal was one of the pioneers of open APIs, launching the PayPal API in 2004. See, PayPal, *API Reference* at https://developer.paypal.com/reference/. See, also, Deepak Nadig (Head of API Platform Engineering at Paypal), *Evolution of the Paypal API: Platform & Culture*, Presentation at Craft Conference (April 23, 2015).
[185] See, Visa, *Visa Developer Center* at https://developer.visa.com.
[186] See, MasterCard, MasterCard Developers – APIs at https://developer.mastercard.com/apis.
[187] See, Stripe, Stripe API – API Reference at https://stripe.com/docs/api.
[188] See, TransferWise – API Documentation at https://api-docs.transferwise.com/v1/use-cases
[189] See, Vemno, Vemno Developer at https://developer.venmo.com.
[190] See, Paymency, Paymency API at www.paymency.com.
[191] See Chapter 7 for further discussion on challenger banks.

have deployed accessible customer-centric APIs to create and deliver new services and improve customer engagement.[192] Among the latter are Credit Agricole,[193] BBVA,[194] Barclays,[195] Lloyds Bank,[196] RBS,[197] and Capital One.[198]

Significantly, when compared with other industries, the rate of adoption of APIs in the financial and banking service industry is quite low. For instance, Programmable Web has a current listing of little more than 100 banking related APIs, out of 16,000 APIs listed on its website.[199] The relative limited rate of adoption of APIs in the banking and financial services industry compared to other industries is further illustrated in Figure 9 below. As shown below, technology, media, and information services industries still lead the pack in building digital business platforms with APIs.

Figure 9. Distribution of Top-Quartile Companies by Industry (- To Date)



Source: Apigee, *The State of APIs - 2017 Report: How APIs Power Digital Ecosystems*, Apigee Report (2017), slide 9.

2.B.iii. Leveraging the Power of APIs

Banks can utilize APIs to achieve a number of goals:

- First, banks can use APIs to decouple their mobile, web, wearable, apps and other customer experiences from complex legacy banking systems. APIs give banks the opportunity to expose information within their organizations more timely and effectively and enable changes to rapidly evolving customer-facing systems independently of the pace of change of back-end systems. This, in turn, can help banks increase customer-centric agility.

[192] See, e.g., Penny Crosman, *Fintech Glasnost: Why U.S. Banks Are Opening Up APIs to Outsiders*, American Banker (July 8, 2015).
[193] See, Credit-Agricole, API CA Store at https://www.creditagricolestore.fr/castore-data-provider/docs/V1/rest.html.
[194] See, BBVA, BBVA API Market at https://www.bbvaapimarket.com.
[195] See, Barclays, Barclays Developer Network at https://developer.barclays.com/bdn/#/home/landing.
[196] See, Lloyds Bank, Lloyds Bank APIs at https://developer.lloydsbank.com.
[197] See, RBS, RBS APIs at http://www.bankofapis.com.
[198] See, Capital One, Capital One Capital One DevExchange at https://developer.capitalone.com.
[199] See, ProgrammableWeb, API Directory – Banking APIs, available at https://www.programmableweb.com/category/banking/api.

- Second, banks can use APIs to connect to customers, partners, and suppliers. In particular, by using APIs banks can securely expose data and insights to select partners or, even more openly, to a wider community of developers. In so doing, banks gain the opportunity to collaborate with third parties to provide innovative solutions for their clients. At the same time, through APIs banks can dynamically source and consume data and functionality to enrich their current offerings. As a result, banks can innovate faster, cheaper, and more aligned to the needs of their customers. This, in turn, helps banks enhance customer engagement, drive customer loyalty, and increase their appeal to prospective customers.

- Third, banks can leverage the power of APIs to integrate and grow their influence into the rapidly evolving Open Banking ecosystem. To regain a position of market centrality and avoid being disintermediated completely by new entrants, banks must rapidly re-imagine their business and revenue models. Toward this end, banks can deploy API-driven marketplace and platform strategies. As discussed in more detail below, banks that adopt these strategies have the opportunity to position themselves as customer's preferred digital point of entry into financial and banking services and to provide a single experience for customers through one integrated interface combining the best of in-house and third party products and services. This, in turn, can help banks unlock new revenue streams, extend their value proposition, and remain relevant to their customers.

- Fourth, banks can use APIs to foster innovation and accelerate product development. In particular, APIs ensure consistency across touch-points and speed up development via reusable blocks of capability. This facilitates the innovation process and helps reduce time to market. By getting to market quickly, banks benefit from early feedback that can be incorporated into subsequent versions of their products and services.[200]

- Fifth, banks can utilize APIs to deploy innovative product and distribution strategies. By using APIs to connect to third parties in a secure and easy-to-consume manner, banks can develop new combinations of services, functionality, and data, as well as explore innovative, dynamic, and more flexible distribution channels. At the same time, by using APIs for interfacing between product and distribution, banks can decouple these functions. The resulting combination of opening up and decoupling gives banks the opportunity to play new and different roles along the financial value chain with regards to the offering of financial and banking products and services and their distribution.[201]

---

[200] See, Microsoft, *Empowering the Digital Bank: The API Economy: Helping Financial Services Companies to Build Better Products*, Microsoft Financial Services - Banking & Capital Markets Insights (May 27, 2015) (noting that "[t]raditionally on boarding developers, creative agencies or even working with existing partners to do experiments was a long costly affair leaving businesses frustrated with the lack of agility. By making small changes to the way you partner, design, execute and orchestrate has big impacts on cost savings and agility."); Accenture, *Payments APIs: Too Compelling To Ignore, Accenture Perspectives - Interview at Accenture's Jeremy Light*, Accenture Report (2016); Penny Crosman, *Fintech Glasnost: Why U.S. Banks Are Opening Up APIs to Outsiders*, American Banker (July 8, 2015).

[201] See, Euro Banking Association (EBA), *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, cit., p. 16, 24; Forrester Research, *Four Ways APIs Are Changing Banking. How Financial Services Firms Are Exploiting The API Economy*, cit., p. 1; Apigee, *The State of APIs - 2017 Report: How APIs Power Digital Ecosystems*, cit., slides 13-14; Accenture, *Payments APIs: Too Compelling To Ignore, Accenture Perspectives - Interview at Accenture's Jeremy Light*, cit.

- Sixth, banks can use APIs in the context of open events, such as hackathons, to remark their commitment to Open Banking, to recruit talents, and to engage an active community of developers, which is crucial to foster API-driven innovation.[202]

- Seventh and as further discussed in the following chapters, banks can utilize APIs to improve control and security in connection with consumer-permissioned access to consumer financial data and account information. In general, there are a number of advantages in using APIs over traditional screen scraping technologies. APIs allows consumers to grant third parties limited access to financial data and account information without having to provide their online banking credentials to such third parties. In addition, APIs allow banks (and other account providers) to obtain from the consumer an unequivocal consent to provide data to a third party and help reduce issues regarding the scope and extent of the authority being granted to the permissioned third party. Furthermore, banks (and other account providers) can maintain greater control and can work closely with permissioned third parties to ensure that appropriate consumer financial data and account information is available for access through APIs. APIs also help mitigate the risks of errors occurring due to updates to banks' (or other account providers') websites and reduce the risks of sharing out of date, incorrect, or incomplete data. In addition, using APIs can help rationalize the number of data calls made by permissioned third parties. This, in turn, helps reduce spikes in volume, as well as heavy and unpredictable traffic patterns on the banks' (or other account providers') websites and enables greater protection of their broader customer base. Lastly, using APIs can facilitate greater standardization of formats for data accessed by permissioned third parties.

- Finally, banks can utilize APIs to meet new Open Banking regulatory requirements. This point is discussed in more detail in the following chapters.

2.C. Evolving Data Sharing Ecosystem

Although various methods to access and share consumer financial data and account information are available (including those discussed in the prior sections), presently there is no industry-wide standard for enabling consumer-permissioned access to such data and information, which can be applied and updated on an ongoing basis.

The diversity of business models, application functionality and technical methods, combined with the lack of coordination among entities within the data-sharing ecosystem, creates a number of challenges and risks. These include the following: lack of consistency in timing, volume, and contents of data transfers; delays in

[202] For instance, in 2014 Citi launched Citi Mobile Challenge, a global initiative through which developers are invited to build new fintech solutions using Citi's APIs, and to present their working prototypes at Demo Day events held throughout Latin America, the United States, Europe, and Asia. For more information about Citi Mobile Challenge, visit www.citimobilechallenge.com. See, also, David Berlind, *How 200-Year-Old Citibank Totally Nailed Its Hackathon*, ProgrammableWeb (December 15, 2014). In a similar fashion, Barclays has run hackathon events in an effort to stimulate the growth of fintech startups and to identify new and innovative products and services for the banking industry. More information on Barclays Rise Hackathon is available at http://www.risehackathon.com/uk.html. Similarly, in 2014 BBVA launched the Innova ChallengeMX, a global development contest designed to develop creative uses of BBVA's data and ways to combine such data with other sources of information. The contest also includes an agenda of events, workshops and seminars, both in person and online, in Spain, Mexico and the United States. More information about InnovaChallenge MX can be found at bbvaopen4u.com.

accessing real-time information for consumer-decision making; broad and recurring data pulls, which may increase potential data breach losses; lack of clarity about optimal data storage timelines and transfers of excess, outdated, and/or incomplete data and information; uncertainty about the way(s) in which consumers can provide, modify and revoke their consent to third-parties to access on their behalf data from banks, financial institutions or other account providers; lack of clarity and uniformity about the corresponding terms of service disclosures; reduced interoperability and restricted data availability and formats, which create complexities for developers in scaling connected solution and building innovative services and inclusive products; heavy and unanticipated loads on banks' and other account providers' systems; significant technical, operating, security and legal costs incurred by banks and other account providers; and limited visibility and control over data access and resulting security concerns for banks and other account providers.

These challenges and risks, in turn, can lead to suboptimal results for both providers and consumers. In particular, without reliable access to consumer financial data and account information, many third parties and account aggregators are unable to deliver high-quality and tailored services and products. At the same time, gaps and obstacles in accessing consumer financial data and account information may deprive consumers of new and valuable financial products and services that can empower them and help improve their financial lives.

On an industry level, obstacles and impediments to consumer-permissioned access and sharing of consumer financial data and account information can significantly hamper innovation, by discouraging the development of new products and services that rely on access to such data and information.

In addition, the described challenges and risks may at times ignite conflicts among various participants in the data-sharing ecosystem. Significantly, although banks and other account providers do not "own" consumer financial data and account information, they do have almost exclusive authority to facilitate or restrict consumer-permissioned access to such data and information. Therefore, in spite of strong consumer interest and the potential for significant consumer benefits, banks and other account providers may decide to restrict permissioned access to consumer financial data and account information.[203] To that end, banks and other account providers may: give consumers alarming and deceptive warnings about liability risks; refuse to cooperate with aggregators and third-party services providers and cut off data flows to them; revise their user agreements to prohibit consumers from sharing (or limit the ability of consumers to share) financial data and account information; modify account security to preclude aggregators and third-party services providers from accessing consumer financial data and account information; negotiate onerous contractual terms, including unlimited liability via insurance policies for breach exposure; implement data usage limitations or use case restrictions, or require deletion of consumer information at their request; force consumers to navigate cumbersome and confusing user interfaces; require consumers to complete additional forms or give certifications in order to request their information and data; once requested by the

[203] See, e.g., Penny Crosman, "*Banks Don't Want to Give Access to Everything: Yodlee Exec*," American Banker (June 7, 2016).

consumer, produce an incomplete record of data and/or a record that is not in a standardized format usable by the customer, account aggregators, or permissioned parties.

For instance, tensions flared in 2015 when several banks (allegedly) blocked access to permissioned third party service providers and account aggregators:[204] JP Morgan Chase reportedly blocked Quicken's access to Chase-held bank accounts;[205] Wells Fargo reportedly temporarily prevented aggregators from automatically retrieving customer data;[206] and Bank of America Merrill Lynch allegedly cut off the flow of account information and data to some sites and mobile applications that aggregate consumer financial data.[207]

Against this background, a growing number of market participants have recently begun to address the challenges and risks discussed above. While the usage of services and products that rely on consumer-permissioned access to consumer financial data and account information continues to expand and benefits a broader consumer audience, a variety of initiatives have been undertaken, which include the following:

- Some banks and other account providers are engaging in informal conversations with third parties to collect more information about their services, operations, and security practices, and are "whitelisting" those who meet selected criteria. Others are creating an API-driven ecosystem with selected partners.[208]

- Some banks and other account providers are taking initial steps to build the technical systems, authentication procedures, and risk management protocols to allow consumers to grant more tailored access to certain financial data and account information through APIs available on the bank's (or other account provider's) platforms.[209]

- Certain leading banks and financial institutions are now working with technology companies through constructive bilateral arrangements to facilitate greater permissioned access to consumer financial account data. For example, both JP Morgan Chase and Wells Fargo have announced deals with Intuit to enable mutual customers to permission access to their financial data and account information through APIs with Intuit's financial management applications, including Mint, TurboTax Online, and QuickBooks Online.[210] Wells Fargo has also entered into bilateral arrangements with: Xero, creating an API that allows small businesses to have their bank account data poured directly into the accounting software provided by

[204] See, Penny Crosman, *The Truth Behind the Hubbub Over Screen Scraping*, American Banker (November 12, 2015); Ethan Wolff-Mann, *Big Banks Are Attacking Personal Finance Apps Like Mint*, Time (November 9, 2015).
[205] See, e.g., Bogleheads Community Forum, *Chase No Longer Works with Quicken?*, Bogleheads Community Forum (October 21, 2015); Peter Rudegeair, *J.P. Morgan Warns It Could Unplug Quicken and Quickbooks Users*, Wall Street Journal (November 24, 2015).
[206] See, e.g., Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, The Wall Street Journal (November 4, 2015).
[207] See, e.g., Daniel Huang and Peter Rudegeair, *Bank of America Cut Off Finance Sites From Its Data*, The Wall Street Journal (November 9, 2015).
[208] See Chapters 6 and 7 for further discussion on this point.
[209] See Section 2.B. for further discussion on this point.
[210] See, e.g., Mary Wisniewski, *JPMorgan Chase and Intuit Partner to Share Data via API*, American Banker (January 25, 2017); Robert Barba, *Why the JPM-Intuit Partnership Is a Big Step for Data Sharing*, American Banker (January 25, 2017); Intuit, *Chase, Intuit to Give Customers Greater Control of their Information*, Intuit Press Release (January 25, 2017); Wells Fargo & Co., *Intuit Signs New Data-Exchange Agreement with Wells Fargo*, Press Release (February 3, 2017).

Xero;[211] and most recently Finicity, to provide an API-based method for sharing Wells Fargo customer information with the financial apps and services that Finicity supports.[212] In a similar fashion, Silicon Valley Bank and CapitalOne have announced deals with Xero.[213]

- Other banks and large financial institutions are investing in aggregators and third-party services providers to support the creation of more secure channels for customers to share their financial data and account information. For instance, both Citi and American Express have made investments in data aggregator Plaid (joining Goldman Sachs), citing the goal of "better access to clean, high-quality financial data, enabling innovation and a secure infrastructure for the financial services ecosystem."[214]

- Finally, a large number of financial institutions and technology companies are strengthening their collaborative efforts through participation in industry wide representative groups, to facilitate more secure consumer-permissioned access to consumer financial data and account information; and are establishing and supporting lobby groups, to promote the adoption of open API framework(s) for data access.[215]

A trend towards bilateral agreements and industry-wide collaborative initiatives such as the ones discussed above presents an opportunity for market participants to demonstrate that (at present) regulatory interventions are not necessary and that the industry can self-regulate. To that end, an effective self-regulatory system would require, among others, a degree of uniformity in bilateral agreement terms. In addition, consumers would need to be provided with a clear explanation of how their financial data and account information are collected, used, stored, and shared by permissioned parties, and would need to be offered reliable and secure method to control those activities, as well as to promptly amend and revoke their consents.

Moreover, notwithstanding the bilateral agreements and industry-wide collaborative initiatives discussed above, there continues to be a potential gap for a number of stakeholders, including: those consumers that are not customers of large banks and financial institutions which have entered into bilateral agreements; and those third party services providers that have built their applications with the consumer's broader financial picture in mind. Because of this, in addition to the bilateral agreement and collaborative initiatives discussed above, market participants should consider developing and applying common industry standards and best practices for consumer-permissioned access to financial data and account information. These industry standards and practice could be based, for example, on those envisioned by the Center for Financial Services Innovation ("CFSI") and/or those contemplated by the Financial Services Information

[211] See, e.g., Wells Fargo & Co., *Wells Fargo, Xero Agree on New Data-Exchange Method*, Wells Fargo Press Release (June 7, 2016); Penny Crosman, *Wells Fargo's Bid to Vanquish Screen Scraping*, American Banker (June 7, 2016); Bryan Yurcan, *Will 2017 Be a Breakthrough Year for Data Portability?*, American Banker (December 12, 2016).
[212] See, e.g., Finicity, *Finicity and Wells Fargo Ink Data Exchange Deal*, Finicity Press Release (April 4, 2017); Penny Crosman, *Wells-Finicity Deal Furthers Data Détente*, American Banker (April 4, 2017).
[213] See, e.g., Silicon Valley Bank, *Xero and Silicon Valley Bank Partner to Offer Innovative Companies Next-Generation Financial Management*, Silicon Valley Bank Press Release (July 16, 2014); Xero and Capital One, *Xero and Capital One Partner to Automate Small Business Accounting and Transform Banking*, Xero and Capital One Joint Press Release (May 10, 2017).
[214] See, Plaid Technologies, *Plaid Announces $44 Million Series B Led by Goldman Sachs Investment Partners*, Plaid Technologies Press Release (June 20, 2016); Plaid Technologies, *Plaid Unveils Investments by Citi Ventures and American Express Ventures*, Plaid Technologies Press Release (February 6, 2017).
[215] See below for further discussion on this point.

Sharing and Analysis Center ("FS-ISAC").[216] The development and implementation of these industry standards and practices would facilitate the establishment of a data-sharing ecosystem that is not only secure and innovative, but also inclusive of all financial institutions and their customers.[217]

Finally, going forward, market participants should also consider how regulation - particularly principles-based regulation - might help clarify the rights and obligations of the many parties involved in the data-sharing ecosystem, while also promoting competition and facilitating further technology innovations. This point is analyzed in great detail in the following chapters.

[216] See, Section 5.C. below. See, also, Jennifer Tescher and Beth Brockland, *One-Off Data-Sharing Deals Aren't Enough*, American Banker (January 27, 2017); Mary Wisniewski, *The Data Access Debate Is About to Get a Lot More Interesting*, American Banker (January 27, 2017).

[217] Industry-wide collaborations are needed to develop solutions and frameworks that are inclusive of smaller institutions and their customers. Indeed, customers are increasingly pressuring smaller institutions, including many community banks and credit unions, to develop ways to allow them to share their data securely with third-party services providers. At present, smaller institutions face significant obstacles in addressing these costumer needs. In particular, they generally lack the user base and/or the technical, legal, financial and other resources necessary to justify substantial investments in the development, implementation, and ongoing maintenance of API infrastructures, as well as the negotiation of data-sharing partnerships with third parties. See, e.g., Independent Community Bankers of America, Response to Docket No. CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records (February 21, 2017), pp. 2-3; Let's Talk Payment (LTP), *Community Banks Call Regulators to Toughen up on FinTech for the Common Good*, LTP (June 7, 2016); Penny Crosman, *"Data Wants to Be Free": Why Banks Should Open APIs to Others*, American Banker (June 23, 2016).

CHAPTER 3. OPEN BANKING LEGISLATIVE AND REGULATORY FRAMEWORK – EUROPEAN UNION (EU)

Prior chapters have analyzed a number of forces that are driving the movement towards Open Banking and have discussed technology advancements that can be leveraged to enable greater openness. The present chapter and the following two chapters focus on the role of regulation as a catalyst for change and accelerator of openness in the financial and banking services industry.

In particular, the chapters provide an overview of forthcoming Open Banking-related legislative and regulatory frameworks, as well as policy initiatives that are currently being developed and implemented across the European Union (EU) (Chapter 3), the UK (Chapter 4), and the United States (Chapter 5). The chapters offer a critical examination of the developments that have been made by regulators across these three geographic areas with respect to Open Banking and provide an initial assessment of their potential implications.

3.A. The Second Payment Services Directive (PSD2)

Technological innovation has been at the heart of recent EU legislation with the adoption of the revised Payment Services Directive (PSD2),[218] a fundamental piece of payments-related legislation that is now accelerating the movement towards Open Banking across Europe.

PSD2 amends and replaces the original Payment Services Directive (PSD), introduced in 2007, as the central framework of rules on payment services and payment service providers in Europe.[219] PSD2 came into force on 12 January 2016, giving all Member States two years (until 13 January 2018) to transpose it into national law (with the exception of certain provisions on security and the technical requirements, which will go live towards the end of 2018 at the earliest). Its main goals are: enhancing consumer protection; encouraging innovation; promoting competition; increasing transparency and security of payment services; and contributing more integration and efficiency across the European payments market. To achieve these goals, PSD2 builds upon a number of areas within the original PSD, extends and clarifies some of the original provisions, and drives higher focus on payments innovation to address significant changes in the payments landscape occurring after the original PSD was enacted.

The changes introduced by PSD2 are far-reaching and will have significant implications for a range of parties including banks, payment service providers (PSPs),[220] fintech companies, and customers. Some of the most relevant changes are highlighted below.

---

[218] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[219] PSD2 is relevant for the European Economic Area (EEA), which comprises 28 EU Member States plus three of the four Member States of the European Free Trade Association (EFTA) – that is Iceland, Liechtenstein, and Norway. Switzerland, the fourth EFTA member, has not joined the EEA and, therefore, does not need to be compliant with PSD2.

[220] Article 4(11) of PSD2 defines "payment service provider" as "a body referred to in Article 1(1) or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33." Article 1(1) of PSD2 identifies six categories of PSPs: credit institutions;

3.B. All Currencies and One-Leg Payment Transactions

Under the original PSD, EU payment services rules apply to all European Economic Area (EEA) currency payments where the PSPs of both the payer and payee are located within the EEA. By contrast, PSD2 extends the scope of its requirements to cover non-EEA currency payments between EEA-domiciled PSPs and "one-leg" transactions (that is, transactions where one of the PSPs is located outside of the EEA) in any currency.

3.C. Narrowing the Scope of Selected Exclusions

PSD2 continues to exclude from the scope of its requirements certain payment transactions undertaken by non-bank organizations. However, different from PSD, PSD2 narrows the scope of permitted exclusions to increase legal certainty and ensure consistent application of the legislative framework across Member States.

For example, the current exclusion of payment transactions through a "commercial agent" is being narrowed to apply when agents act only on behalf of the payer or only on behalf of the payee, regardless of whether or not they are in possession of client funds. Where agents act on behalf of both the payer and the payee (e.g., certain e-commerce platforms), they are excluded only if they do not at any time enter into possession or control of client funds.[221] Similarly, the "limited network" exclusion is being narrowed to prohibit the use of the same instrument to make payment transactions to acquire goods and services within more than one limited network or to acquire an unlimited range of goods and services.[222] Moreover, the exclusion relating to certain payment transactions by a provider of electronic communications networks or services, offered in addition to electronic communications services for a subscriber to the network or service, is being narrowed to cover only payments made for the purchase of digital content and voice-based services (regardless of the device used for the purchase or consumption of the digital content and charged to the related bill) or performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets. In both scenarios, the exclusion applies provided that the value of any single payment transaction does not exceed Euro 50 and the cumulative value of payment transactions does not exceed Euro 300 per month for an individual subscriber or for a pre-funded account.[223]

3.D. Authorization Rules, Passporting, and Supervision of Payment Institutions

Under the current regime, payment institutions must satisfy a number of requirements to obtain full authorization to offer payment services. PSD2 enhances the authorization process and introduces some

---

electronic money institutions; post office giro institutions; payment institutions; the European Central Bank and national banks when not acting in their capacity as monetary authority or other public authorities; and Member States or their regional or local authorities when not acting in their capacity as public authorities.

[221] See, Article 3(b) of PSD2.

[222] See, Article 3(k) of PSD2 (payment instruments covered by the "limited network" exclusion include public transport cards, store cards, membership cards, fuel cards, parking ticketing, and meal vouchers or vouchers for specific services. The "limited network" exclusion no longer applies where the specific-purpose instrument develops into a general-purpose instrument.).

[223] See, Article 3(l) of PSD2.

additional operational and security requirements. In addition, under PSD2 PSPs have to meet certain prudential requirements and hold either professional indemnity insurance or a comparable guarantee.[224]

Similarly to PSD, PSD2 provides that payment institutions are supervised by the Member State where they are authorized to provide defined payment services (i.e. the 'home' Member State). Supervision largely remains with the home Member State even where services are provided in other ('host') Member State(s).

PSD2 strengthens the investigative and supervisory powers of the host Member State and introduces a more detailed passporting procedure to facilitate cooperation and to ensure better communication between the competent authorities of the Member States responsible for the supervision of PSPs.[225] In particular, the competent authority of the host Member State can take precautionary measures in emergency situations, where immediate action is necessary to address a serious threat to the collective interests of the payment service users in the host Member State.[226]

3.E. Consumer Protection

PSD2 seeks to increase consumer protection in a number of ways, which include the following:

- The amount a payer could be obliged to pay in an unauthorized payment transaction scenario shall not exceed Euro 50, unless the payer has acted fraudulently or with gross negligence.[227] This provision aims at providing an incentive for the payer to notify, without undue delay, the PSP of any theft or loss of a payment instrument and, thus, reducing the risk of unauthorized payment transactions.

- Where the payer has neither acted fraudulently nor with gross negligence, Member States may reduce the described liability, taking into account, in particular, the nature of the personalized security credentials and the specific circumstances under which the payment instrument was lost, stolen, or misappropriated.[228]

- There will be no liability where the payer is not in a position to become aware of the loss, theft or misappropriation of the payment instrument. In particular, the payer will not be liable for an unauthorized payment transaction if: (a) the loss, theft or misappropriation of the payment instrument was not detectable by the payer prior to a payment, except where the payer has acted fraudulently; or (b) the loss was caused by acts or lack of action of an employee, agent or branch of a PSP or of an entity to which its activities were outsourced.[229]

[224] See, Article 5 of PSD2. The European Banking Authority (EBA) has been given mandate to develop guidelines in accordance with Article 16 of Regulation (EU) No. 1093/2010 on the criteria to be used by Member States to establish the minimum monetary amount of professional indemnity insurance or comparable guarantee.
[225] See, Articles 26-31 of PSD2.
[226] See, Article 30 of PSD2. The described precautionary measures shall be undertaken in parallel to the cross-border cooperation between competent authorities and pending measures by the competent authorities of the home Member State as set forth in Article 29.
[227] See, Article 74(1) of PSD2.
[228] Ibidem.
[229] Ibidem.

- In the scenario where the payer's PSP does not require strong customer authentication (SCA), the payer shall not bear any financial losses unless he/she/it has acted fraudulently. Where the payee or the payee's PSP fails to accept SCA, then he/she/it will be liable for any unauthorized payment and will have to refund the financial damage caused to the payer's PSP.[230]

- The payer will not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument if it notifies the PSP (or the entity specified by the PSP) without undue delay on becoming aware of the loss, theft, misappropriation or unauthorized use of the payment instrument, except where the payer has acted fraudulently.[231]

- In case of an unauthorized payment transaction, the payer's PSP shall immediately refund the payer the amount of the unauthorized payment transaction, and in any event by no later than the end of the next business day after noting or being notified of the transaction.[232] However, where the payer's PSP has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing, the PSP should be able to conduct, within a reasonable time, an investigation before refunding the payer.

- PSD2 provides a legislative basis to the unconditional refund right for a period of 8 weeks from the date when the funds were debited.[233]

- In the context of the pre-authorization of card payments, where the final amount of the transaction is not known in advance, the payer's PSP may block funds (and, thus, the payee will be able to "ring fence" funds) on the payer's payment account only if the payer has given consent to the exact amount of the funds to be blocked.[234] The payer's PSP is required to release those funds without undue delay once information about the exact final amount of the payment transaction is received and, at the latest, immediately after receipt of the payment order.[235]

- In the event of an unauthorized, non-executed, defective or late executed payment initiated via a payment initiation service provider (PISP),[236] the account servicing payment service provider (ASPSP) is required to immediately refund to the payer the amount of the non-executed, defective or late payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.[237] If the PISP is liable for the non-execution, defective or late execution of the payment transaction, it is required to immediately compensate the ASPSP

[230] See, Article 74(2) of PSD2.
[231] See, Article 69(1) and Article 74(3) of PSD2. If the PSP does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as required under point (c) of Article 70(1) of PSD2, the payer shall not be liable for the financial consequences resulting from use of that payment instrument, except where the payer has acted fraudulently.
[232] See, Article 73 of PSD2.
[233] See, Article 77 of PSD2.
[234] See, Article 75(1) of PSD2.
[235] See, Article 75(2) of PSD2.
[236] See below for further discussion on this point.
[237] See, Article 90(1) of PSD2.

at its request for the losses incurred or sums paid as a result of the refund to the payer.[238] The burden of proof lies with the PISP to prove that "the payment order was received by the payer's account servicing payment service provider [ASPSP] in accordance with Article 78 and that within its sphere of competence the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the non-execution, defective or late execution of the transaction."[239]

- PSPs must put in place adequate and effective dispute resolution procedures and will be required to respond to payment complaints from payment service users (PSUs) within 15 business days of receipt. In exceptional circumstances beyond the PSP's control, a holding reply can be provided, clearly indicating the reasons for a delay in answering the complaint and specifying the deadline by which the payment service user will receive the final reply. In any event, the deadline for receiving the final reply shall not exceed 35 business days.[240]

- In the event of a major operational or security incident, PSPs will have to notify the competent authority in the PSPs' home Member State "without undue delay".[241] Upon receipt of the notification, the competent authority of the home Member State will have to provide, without undue delay, the relevant details of the incident to the EBA and the European Central Bank (ECB).[242] In the event the incident has or may have an impact on the financial interests of the PSUs, the PSP will also be required to inform its PSUs without undue delay and advise them of all measures that they can take to mitigate any adverse consequences.[243]

To assist this process, PSD2 requires the EBA, working in close cooperation with the ECB and after consultation with all relevant stakeholders, to issue guidelines addressed to: (a) PSPs on the classification of major incidents and on the content, format, templates and procedures for notification; and (b) competent authorities on the criteria of how to assess the relevance of the incident and the details of the reports to be shared with other domestic authorities.[244]

[238] See, Article 90(2) of PSD2.
[239] See, Article 90(1) of PSD2.
[240] See, Articles 101-103 of PSD2. Member States may introduce or maintain rules on dispute resolution procedures that are more advantageous to the PSU. In such scenario, those rules shall apply. In addition, Member States are required to designate competent authorities to ensure and monitor compliance with PSD2 and to establish that adequate, independent, impartial, transparent and effective ADR procedures for the settlement of disputes between PSUs and PSPs.
[241] See, Article 96(1) of PSD2.
[242] See, Article 96(2) of PSD2. EBA and the ECB, in cooperation with the competent authority of the home Member State, will have to assess the relevance of the incident to other relevant Union and national authorities and to notify them accordingly. The ECB will also be required to notify the members of the European System of Central Banks on issues relevant to the payment system. On the basis of that notification, the competent authorities will take, where appropriate, all of the necessary measures to protect the immediate safety of the financial system.
[243] See, Article 96(1) of PSD2.
[244] See, Article 96(3) to Article 96(5) of PSD2. EBA, in close cooperation with the ECB, will have to review these guidelines on a regular basis and in any event at least every 2 years. In addition, while issuing and reviewing these guidelines, EBA will have to take into account standards and/or specifications developed and published by the European Union Agency for Network and Information Security for sectors pursuing activities other than payment service provision.

- At least on an annual basis, PSPs will be required to report to their national competent authority: updated operational and security risk assessments;[245] a report on the adequacy of the control and mitigation measures deployed;[246] and statistical data on fraud relating to different means of payment.[247]

3.F. XS2A (Access to Account) Rule and New Payment Services

PSD2 defines "payment service" as "any business activity set out in Annex I."[248] The list of business activities set forth therein has ben expanded to include two new payment services, which will now be regulated under PSD2:

- "Payment initiation service" (PIS), defined as "a service to initiate a payment order at the request of the payment service user [PSU] with respect to a payment account held at another payment service provider [PSP]."[249] PSPs of PISs are termed "payment initiation service providers" (PISPs).[250] Notable examples of PISPs are Sofort Banking and Trustly.

- "Account information service" (AIS), defined as "an online service to provide consolidated information on one or more payment accounts held by the payment service user [PSU] with either another payment service provider [PSP] or with more than one payment service provider [PSP]".[251] PSPs that provide AISs are termed "account information service providers" (AISPs).[252] A notable example of AISP is ING.

PSD2 acknowledges the development and increasing usage of PISs and AISs. Significantly, following the adoption of the original PSD: PISs have contributed to open the retail payments market by making less costly and much easier processing online payments for consumers and companies; and AISs have facilitated the raise of personal finance management services and have opened up new financial opportunities for consumers. These changes reflect the rise of new technological developments, the wide spread use of internet and mobile payments, the remarkable growth in e-commerce activities, as well as a trend viewing customers having relationships with multiple account providers.[253]

---

[245] See, Article 95(2) of PSD2.
[246] Ibidem.
[247] See, Article 96(6) of PSD2.
[248] See, Article 4(3) of PSD2. See, also, Preamble 21 of PSD2 (providing that "[t]he definition of payment services should be technologically neutral and should allow for the development of new types of payment services, while ensuring equivalent operating conditions for both existing and new payment service providers.").
[249] See, Article 4(15) of PSD2. See, also, Preamble 27 of PSD2 (observing that "[s]ince the adoption of Directive 2007/64/EC [original PSD] new types of payment services have emerged, especially in the area of internet payments. In particular, payment initiation services in the field of e-commerce have evolved. Those payment services play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's account servicing payment service provider in order to initiate internet payments on the basis of a credit transfer.").
[250] See, Article 4(18) of PSD2.
[251] See, Article 4(16) of PSD2. See, also, Preamble 28 of PSD2 (noting that "technological developments have given rise to the emergence of a range of complementary services in recent years, such as account information services. Those services provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider. The payment service user is thus able to have an overall view of its financial situation immediately at any given moment.").
[252] See, Article 4(19) of PSD2. PISPs and AISPs are collectively referred to as third-party service providers (TPPs).
[253] See, Article 66(1) and Article 67(1) of PSD2.

Against this background, PSD2 makes it clear that customers have a right to use PISs and AISs, where the payment account is accessible online and where they have given their explicit consent. At the same time, PSD2 acknowledges that, because PISs and AISs are currently not subject to PSD, they are not necessarily supervised by a competent authority and are not required to comply with PSD provisions. This regulatory gap, in turn, has raised a number of legal issues, including consumer protection, security and liability, as well as competition and data protection related issues. Thus, to increase legal certainty and to provide consumers with adequate protection for their payment and account data, PSD2 extends the scope of PSD to expressly regulate PISs and AISs and the providers of these services.

More in detail, PSD2 mandates PSPs that provide and maintain a "payment account" for a payer[254] - referred to as account servicing payment service provides (ASPSPs)[255] - to grant "access" to the account, subject to the account holder's consent, to AISPs and PISPs, for free and in a regulated and secure way (so called, "Access to Account" (XS2A) rule). Under the Access to Account (XS2A) rule, the ASPSPs are required to facilitate access to payment accounts, when the account holder has given explicit consent, to enable the following services free of charge for regulated third-party providers: (i) confirmation on the availability of funds; (ii) PISs; and (iii) AISs.[256] As further discussed below, in order to provide this access to accounts, ASPSPs must meet stringent requirements for strong authentication and secure communication, which are to be determined by the EBA's Regulatory Technical Standards (RTS) on strong customer authentication and secure communication.[257] In addition, PSD2 provides that the provision of PISs and AISs shall not be dependent upon the existence of any contractual relationship between the PISP/AISP and the ASPSP.

The XS2A rule represents a significant shift in terms of accessibility of customer data to third parties and creates new opportunities to bank for consumers, by removing the need for them to interact with an ASPSP directly. Forcing ASPSPs to open up has major operational and systems impacts and is expected to upend the banking system across Europe to the benefit of consumers. Details of this rule with respect to PISs and AISs are further discussed below:

- Payment Initiation Services (PISs). PISPs offer online services by virtue of which a payer can initiate a payment from his/her/its payment account(s) to an e-merchant or other beneficiary via a

[254] Article 4(12) of PSD2 defines "payment account" as "an account held in the name of one or more payment service users [PSUs] which is used for the execution of payment transactions." At present, the issue of what types of account qualify as "payment account" under PD2 is being debated. In the UK, more clarity on this topic has gradually emerged during the process of implementation. See, HM Treasury (HMT), *Implementation of the Revised EU Payment Services Directive (PSDII)*, HM Treasury Press Release (February 2, 2017); HM Treasury (HMT), *Draft Impact Assessment on the Implementation of the EU Payment Services Directive II*, HM Treasury (February 2017); HM Treasury (HMT), *Implementation of the Revised EU Payment Services Directive II (and Draft Regulations (Annex B))*, HM Treasury (February 2017), p. 36 (clarifying that the following types of accounts will likely fall within the definition of "payment account" under PSD2: personal current accounts, business current accounts, credit card accounts, flexible savings accounts, and e-money accounts); Financial Conduct Authority (FCA), *Implementation of the Revised Payment Services Directive (PSD2)*, Financial Conduct Authority Press Release (April 13, 2017); Financial Conduct Authority (FCA), *Consultation Paper - Implementation of the Revised Payment Services Directive (PSD2): Draft Approach Document and Draft Handbook Changes*, Financial Conduct Authority CP 17/11 (April 2017) (explaining that the definition of "payment accounts" under PSD2 include, for example, current accounts, e-money accounts, flexible savings accounts, credit card accounts and current account mortgages.).

[255] See, Article 4(17) of PSD2.

[256] For any additional services, PSD2 does not forbid ASPSP to charge fees.

[257] See below for further discussion on this point.

PISP, rather than by direct interaction with the ASPSP(s) where the payer's payment account(s) is(are) held. Under PSD2, once the payer has given a payment order via the PISP, the ASPSP will have to treat the payment order without any discrimination other than for objective reasons, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer.[258] The ASPSP must communicate with the PISP in a secure way.[259] Immediately after receipt of the payment order from the PISP, the ASPSP will need to provide or make available all information on the initiation of the payment transaction and all information accessible to it regarding the execution of the payment transaction to the PISP and won't be able to charge for this activity.[260] In addition, PSD2 clearly indicates that the provision of PISs shall not be dependent on the existence of any contractual relationship between the PISPs and the ASPSPs for that purpose.[261]

At the same time, to guarantee the payer's protection, PSD2 prohibits PISPs: to actually possess the funds being transferred at any given time;[262] and to use, access, or store any data for purposes other than for the provision of the PIS as explicitly requested by the payer.[263] PISPs are also prohibited: to store any of the sensitive payment data of the PSU;[264] and to request from the payer any data other than those necessary to provide the PIS.[265] The PSU's personalized security credentials will be protected in that they can only ever be shared with the PSU and the ASPSP that issued them in the first place and they must be transmitted by the PISP through safe and efficient channels.[266] Moreover, any information about the PSU (other than his/her/its personalized security credentials), obtained by a PISP when providing PISs, can be provided only to the payee and only with the PSU's explicit consent.[267] Finally, PISPs will be required to identify themselves towards the ASPSP of the payer every time a payment is initiated, and they must communicate with the ASPSP, the payer and the payee in a secure way.[268]

Typically, a merchant may integrate a PIS provided by a PISP into its online checkout process, thus enabling the PISP to offer the merchant's customers the option of online credit transfers as an alternative to card payments.[269]

In regulating PISs and PISPs, PSD2 contemplates a simplified payments value chain where the card network can be fully disintermediated. As illustrated in Figure 10 below, in the PISP value

[258] See, Article 66(4)(c) of PSD2. This means that ASPSPs cannot allocate payments from bank accounts initiated by PISPs at the end of the queue, nor they can charge differently for payments initiated through the PISPs than they would for payments initiated by the PSU through their own system.
[259] See, Article 66(4)(a), and Article 98(1)(d) of PSD2.
[260] See, Article 66(4)(b) of PSD2.
[261] See, Article 66(5) of PSD2.
[262] See, Article 66(3)(a) of PSD2.
[263] See, Article 66(3)(g) of PSD2.
[264] See, Article 66(3)(e) of PSD2.
[265] See, Article 66(3)(f) of PSD2.
[266] See, Article 66(3)(b) of PSD2.
[267] See, Article 66(3)(c) of PSD2.
[268] See, Article 63(3)(d) and Article 98(1)(d) of PSD2.
[269] See, Preamble (29) of PSD2 (noting that PISPs "offer a low-cost solution for both merchants and consumers and provide consumers with a possibility to shop online even if they do not possess payment cards.").

chain the payment is initiated by the PISP directly from the PSU's payment account via an API call to the APSP in question. In this scenario, the PISP is the only intermediary to which the merchant service charge is to be distributed. Because of this, it is highly likely that PISs will be offered at a discount to existing rates of merchant service charge, while industry competition will drive these rates downwards. A PISP-based model could, therefore, improve buying experience for customers, increase the speed of execution, and reduce buying friction, as well as overall cost of processing the payment. In addition, it could reduce the liquidity risk within the payment transaction and accelerate the clearing of funds.[270] On the other hand, a PISP-based model may pose a threat for issuing and acquiring banks, as well as processor and card networks, which are at risk of loosing all fees that they receive through existing card-based payments models. A PISP-based model could also severely impact current revenue streams from dynamic currency conversion and foreign exchange on card transactions, and could create new opportunities for a redistribution of ownership and delivery of these activities throughout the value chain.[271]

- Account Information Services (AISs). AISPs act as aggregators of PSU payment account information. At present, a PSU with more than one account needs to access each payment account individually through separate interfaces. By contrast, as illustrated in Figure 10 below, when using the services of an AISP, the PSU can view consolidate information from multiple payment accounts via a single interface.[272]

  Under PSD2, subject to the PSU's explicit consent,[273] the AISP will be allow to access information from designated PSU's payment accounts and associated payment transactions and can, then, present the PSU with an aggregate viewpoint of transactions and balances.[274]

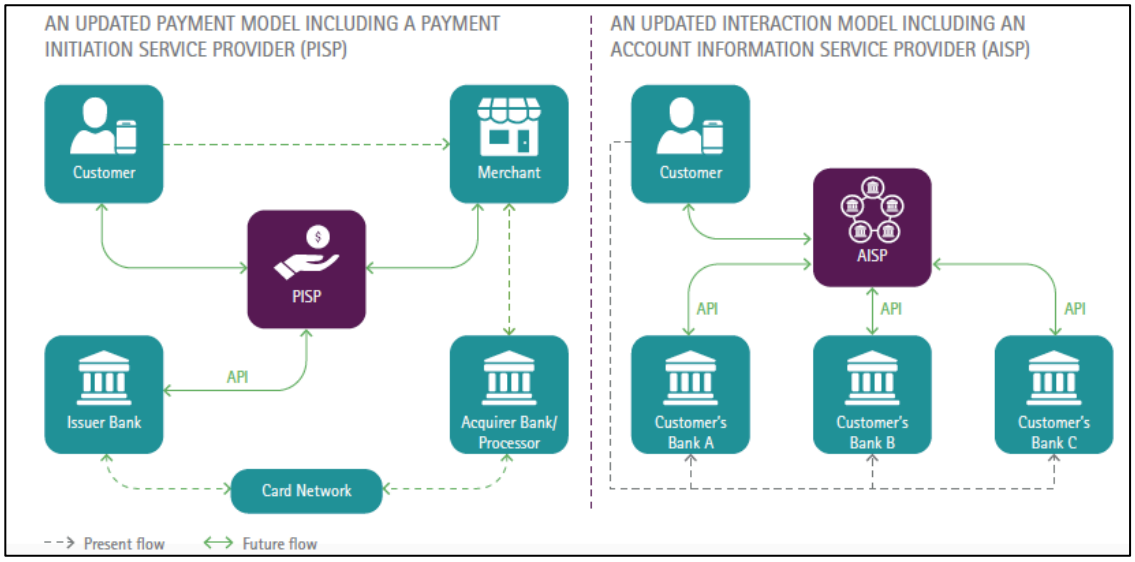
  The PSU's personalized security credentials will be protected in that they may only ever be shared with the PSU and the ASPSP that issued them at first, and they must be transmitted by the AISP through safe and efficient channels.[275] In addition, for each communication session, the AISP will need to identify itself towards the PSU's ASPSP(s) in question and securely communicate with the PSU and the PSU's ASPSP(s).[276] Moreover, the AISP will not be permitted to request sensitive payment data linked to the payment accounts, and will not be allowed to use, access, or store any

[270] See, Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., p. 9. (arguing that "PISP services could account for up to 16 percent of online retail payments by 2020, led by the displacement of up to 33 percent of online debit card transactions and up to 10 percent of online credit card transactions. Taking the UK market as an example, this would result in the loss of over £1.45bn of card transaction revenues between 2017 and 2020—money that was previously captured by the banks and card networks.").
[271] Id., p. 8.
[272] AISs could also be offered alongside PISs as a means to transfer funds from one payment account to another based on the information gathered.
[273] The consent could be given on "an on going basis" or for "one-off access" (for example, an affordability check to be performed when applying for a loan or a mortgage).
[274] See, Articles 67(2)(a) and 67(2)(d) of PSD2.
[275] See, Article 67(2)(b) of PSD2.
[276] See, Article 67(2)(c) and Article 98(1)(d) of PSD2.

data for purposes other than for performing the AIS explicitly requested by the PSU, in accordance with data protection rules.[277]

In turn, the ASPSP(s) where the PSU's payment accounts are held must communicate securely with the AISP.[278] Once the PSU has given consent to AISP's access, the ASPSP(s) where the PSU's payment accounts are held must treat the request of access without any discrimination other than for objective reasons, free of charge, and without the need for any contractual relationship to subsist between the ASPSP and the AISP at issue.[279]

Figure 10. Payment Initiation Services (PISs) and Account Information Services (AISs)



Source: Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, Accenture Payment Services Report (2016), p. 5.

Any PSP (including an ASPSP) could potentially offer PISs or AISs, subject to having the appropriate authorization and in compliance with all applicable legislative and regulatory provisions. At present, fintech companies are well positioned to provide PISs and AISs.[280] Incumbent banks may themselves capitalize on the opportunities introduced by PSD2 and offer PISs and/or AISs. This could help them mitigate the loss of fee revenues likely to result from the provision of PISs and AISs by third parties. Similarly, large merchants that have sufficient scale and are willing to vertically integrate their business model could provide PISs.

Under PSD2, PISPs and AISPs will have to apply for authorization with the competent financial supervision authority before their activities are permitted and the entitlement to payment account access is

[277] See, Articles 67(2)(e) and 67(2)(f) of PSD2.
[278] See, Article 67(3)(a) and Article 98(1)(d) of PSD2.
[279] See, Article 67(3)(b) and Article 67(4) of PSD2.
[280] See, Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., p. 9. (noting that "[t]he PISP model is also applicable to physical point-of-sale (POS) transactions where the PISP is integrated to a contactless mobile wallet app. It is entirely possible that mobile wallet providers including the likes of Apple Pay may consider a transition to a PISP model in the future. These developments will further reduce the volume of card-based transactions within Europe and the related Interchange and [a]cquirer revenue streams for banks.").

granted.[281] In particular, in the case of both PISPs and AISPs, the application will need to comprise, among others: a programme of operations; a business and budget plan for the next three financial years; a description of the applicant's governance and internal control mechanism; a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaint; a security policy document; the applicant's internal structure, details of the directors and other members of management; the applicant's legal status and articles of association; and the address of the applicant's head office.[282] Finally, as a condition of their authorization, PISPs and AISPs must hold a professional indemnity insurance (or an equivalent guarantee), the minimum monetary amount of which is to be determined by the EBA.[283]

PSD2 defines a lighter prudential regime for AISPs, which are treated as payment institutions but are only subject to some of the provisions regarding transparency, information, rights and obligations.[284] By contrast, the PISPs will have to fulfill some additional requirements. In particular, PISPs must contribute and maintain a minimum capital of Euro 50,000 (when the provision of no other payment services is contemplated),[285] and must provide the identity of persons with (direct or indirect) qualifying holdings in the applicant (including description of the size of such holdings and evidence of their suitability).[286]

In addition to the foregoing, the EBA is also required to develop, operate, and maintain a publicly available electronic central register containing information drawn from the public registers in each Member State as notified by the competent authorities, identifying the payment services for which each payment institution is authorized or for which an AISP is registered.[287] Once the competent authority of the home Member State has granted the authorization, PISPs and AISPs can, then, expand their services throughout the EU/EEA through a streamlined passporting process.[288]

3.G. Confirmation of Availability of Funds

Under PSD2, ASPSPs will have the obligation, upon the request of a PSP issuing card-based payment instruments, to immediately confirm whether funds necessary for the execution of a card-based payment transaction are available on the payment account of the payer, which must be accessible online at the time of the request.[289]

This obligation is subject to the payer's explicit consent being given to the ASPSP to respond to requests from a specific payment PSP to confirm that the amount corresponding to a certain card-based payment transaction is available on the payer's payment account.[290] In addition, the PSP may request the

[281] See, Article 5 and Article 33 of PSD2.
[282] See, Articles 5(1), (5) and (6) and Article 33(1) of PSD2.
[283] See, Articles 5(2) to (4) of PSD2.
[284] See, Article 33 of PSD2.
[285] See, Article 7(b) of PSD2.
[286] See, Article 5(1)(m) of PSD2.
[287] See, Article 15 of PSD2.
[288] See, Article 28 and Article 29 of PSD2.
[289] See, Article 65(1)(a) of PSD2.
[290] See, Article 65(1)(b) and Article 65(1)(c) of PSD2.

confirmation of available funds where all of the following conditions are met: (a) the payer has given explicit consent to the PSP to request the confirmation; (b) the payer has initiated the card-based payment transaction for the amount in question using a card based payment instrument issued by the PSP; and (c) the PSP authenticates itself towards the ASPSP before each confirmation request, and securely communicates with the ASPSP in accordance with PSD2 provisions.[291] As with the PISs and AISs, communications between the card-based payment instrument issuer and the ASPSP are addressed by the EBA RTS on strong customer authentication (SCA) and common and secure communication (CSC).[292]

The confirmation of available funds can consist in a simple "yes/no" response, and cannot be stored or used for purposes other than for the execution of the card-based payment transaction at issue.[293] In addition, the confirmation will not allow the ASPSP to block funds on the payer's payment account[294] and the payer may request the ASPSP to communicate to the payer the identification of the PSP and the answer provided.[295]

3.H. Authentication and Secure Communication

Except in defined circumstances, PSD2 requires PSPs to apply strong customer authentication (SCA) and have in place adequate security measures to protect the confidentiality and the integrity of PSUs' personalized security credentials (PSCs) when the payer (directly or indirectly through PISPs and AISPs):[296]

(a) Accesses its payment account online;[297]

(b) Initiates an electronic payment transaction;[298]

(c) Carries out any action through a remote channel, which may imply a risk of payment fraud or other abuses.[299]

In addition, in case of initiation of electronic remote payments (whether the payment is initiated by the PSU directly or indirectly through a PISPs), PSPs will have to apply SCA that includes elements that dynamically link the transaction to a specific amount and a specific payee.[300]

---

[291] See, Articles 65(2)(a) to 65(2)(c) and Article 98(1)(d) of PSD2.
[292] See below for further discussion on this point.
[293] See, Article 65(3) of PSD2.
[294] See, Article 65(4) of PSD2.
[295] See, Article 65(5) of PSD2.
[296] See, Article 97(1) and Article 97(3) of PSD2.
[297] See, European Banking Authority (EBA), *Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication under the Revised Payment Services Directive (PSD2)*, EBA/DP/2015/03 (December 8, 2015), p. 12, Section 4.1. - Issues for discussion No. 27.i (explaining that online access to payment accounts covers all services where a PSU is using a device (e.g. PC, mobile device, chip card, ATM) to log into the payment account for to retrieve information on the payment account).
[298] Ibidem, Section 4.1. - Issues for discussion No. 27.ii (explaining that the initiation of electronic payment transactions covers all payment transactions within the scope of PSD2 (such as card payments, credit transfers, e-money transactions, direct debits), except where the payment instruction is not electronic (such as physical mail-order, paper based credit transfer or paper based direct debits or telephone orders).
[299] Ibidem, Section 4.1. - Issues for discussion No. 27.iii (clarifying that this category covers all actions intrinsically linked to payment services not already included in the categories (a) and (b) above. Examples include actions related to the activation and deactivations of payment functionalities, the amendment of trusted beneficiaries ("white lists") - or blocked beneficiaries ("black-lists"), the setting of limits or the generation of virtual cards or changing PSU data that may imply a risk of payment fraud or other abuses. It only includes actions that are conducted via the internet or through a device that can be used for distance communication (e.g. mobile devices).

PSD2 requires ASPSPs to allow PISPs and AISPs to rely on the authentication procedures that the ASPSPs have provided to the PSUs in accordance with Article 97(1) and (3) and, where the PISPs are involved, in accordance with Article 97(1), (2) and (3), as discussed above.[301] Notwithstanding this provision, PSD2 clearly indicates that all PSPs (including PISPs and AISPs) must establish and maintain adequate security measures to protect the confidentiality and integrity of PSU's PSCs.[302]

PSD2 defines "authentication" as "a procedure which allows the payment service providers [PSPs] to verify the identity of a payment service user [PSU] or the validity of the use of a specific payment instrument, including the use of the user's personalized security credentials [PSC]."[303] PSD2, further, defines "strong customer authentication" (SCA) as "authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data."[304] As further clarified by EBA,[305] the "knowledge" element covers, among others, static passwords, codes or a personal identification number known only by the PSU; the "possession" element includes, among others, the possession of a physical object or potentially data controlled only by the PSU; and the "inherence" element covers, among others, biometric characteristics of the PSU such as a fingerprint or an iris scan.

Finally, PSD2 defines "personalized security credentials" (PSCs) as "personalized features provided by the payment service provider [PSP] to a payment service user [PSU] for the purposes of authentication."[306] As clarified by EBA, for SCA the PSCs can be either a valid combination of the three elements themselves or something which is only generated when all the elements have been provided (e.g. an algorithm in a chip produces a one-time password or cryptogram, based on challenge responses where the PSU is asked for a PIN).[307]

---

[300] See, Article 97(2) of PSD2. See, also, European Banking Authority (EBA), *Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication under the Revised Payment Services Directive (PSD2)*, cit., p. 12, Section 4.1. - Issues for discussion No. 33-34 (indicating that "[i]n the understanding of EBA, the purpose of "dynamic linking" and the "dynamic code" mentioned in the recitals is to ensure that the authentication value used for a remote transaction can neither be used for any other purpose than originally intended by the payer nor be re-used if it is disclosed. Thus dynamic linking aims at providing a high assurance that the PSU has been identified and is authorising a specific payment transaction.").

[301] See, Article 97(5) of PSD2.

[302] See, Article 97(3) of PSD2.

[303] See, Article 4(29) of PSD2.

[304] See, Article 4(30) of PSD2.

[305] See, European Banking Authority (EBA), *Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication under the Revised Payment Services Directive (PSD2)*, cit., p. 12, Section 4.1. - Issue for discussion No. 29.

[306] See, Article 4(31) of PSD2.

[307] See, European Banking Authority (EBA), *Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication under the Revised Payment Services Directive (PSD2)*, cit., p. 13, Section 4.1. - Issue for discussion No. 31.

3.I. EBA Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common and Secure Communication (CSC)

PSD2 has conferred 11 mandates to the EBA, requiring the EBA to issue 5 sets of guidelines and to develop 6 draft Regulatory Technical Standards (RTS). Among these mandates, there are the following:

- A mandate to issue guidelines on the establishment, implementation and monitoring of the security measures, including certification processes where relevant, for the management of operational and security risks.[308]

- A mandate to issue guidelines with regard to: (a) PSPs, on the classification of major incidents, and on the content, the format (including standard notification templates), and the procedures for notifying such incidents; and (b) competent authorities, on the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities;[309] and

- A mandate to draft RTS addressed to PSPs specifying:[310]

  (a) The requirements of SCA when the payer accesses his payment account online; initiates an electronic payment transaction; or carries out any action, through a remote channel, which may imply a risk of payment fraud or other abuses;[311]

  (b) The exemptions from the application of SCA, based on (1) the level of risk involved in the service provided; (2) the amount, the recurrence of the transaction, or both; or (3) the payment channel used for the execution of the transaction;[312]

  (c) The requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the PSU's PSCs;[313] and

  (d) The requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between ASPSP, PISPs, AISPs, payers, payees and other PSPs.[314]

The third mandate discussed above (set forth in Article 98(1) of PSD2) is critical for the achievement of the goals of PSD2 of enhancing consumer protection, promoting innovation and improving the security of

[308] See, Article 95(3) of PSD2. The EBA is required to issue the described guidelines by 13 July 2017, working in close cooperation with the ECB and after consulting all relevant stakeholders. In addition, the EBA, in close cooperation with the ECB, will have to review these guidelines on a regular basis and in any event at least every 2 years.
[309] See, Article (96)(3) and Article (96)(4). The EBA is required to issue these guidelines by 13 January 2018, working in close cooperation with the ECB and after consulting all relevant stakeholders. In addition, the EBA, in close cooperation with the ECB, will have to review these guidelines on a regular basis and in any event at least every 2 years.
[310] See, Article 98(1) and Article 98(5). Under PSD2, the EBA is granted the mandate to draft the RTS in close cooperation with the ECB and after consulting all relevant stakeholders; while the European Commission is delegated the power to adopt the RTS. The RTS will be applicable 18 months after its entry into force, which would suggest an application date of the RTS at the end of 2018 at the earliest. In addition to drafting the RTS, the EBA is also required to review and, if appropriate, update the RTS on a regular basis in order to take account of innovation and technological developments. See below for further discussion on this point.
[311] See, Article 98(1)(a) of PSD2.
[312] See, Article 98(1)(b) and Article 98(3) of PSD2.
[313] See, Article 98(1)(c) of PSD2.
[314] See, Article 98(1)(d) of PSD2.

payment services across the EU/EEA. In this regard, PSD2 requires the EBA to develop draft RTS under Article 98(1) in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved.[315] It also expressly requires the EBA to develop such RTS in accordance with the following objectives: (a) ensure an appropriate level of security for PSUs and PSPs, through the adoption of effective and risk-based requirements; (b) ensure the safety of PSUs' funds and personal data; (c) secure and maintaining fair competition among all PSPs; (d) ensure technology and business-model neutrality; and (e) allow for the development of user-friendly, accessible and innovative means of payment.[316]

As acknowledged by the EBA,[317] when developing the draft RTS under Article 98(1), the EBA had to take into account a number of difficult trade-offs between competing demands. For example:

- High security requirements (which may suggest a high degree of prescription in the requirements as to avoid circumvention of rules) versus facilitation of the development of innovative security solutions in years to come (which may suggest high level requirements that provide certain flexibility);

- High security and safety requirements (which may suggest that the payment user will be subject to multiple security and authentication steps) versus customer convenience requirements (which may suggest user-friendly approaches, such as "one-click" payments); and

- Very detailed requirements for common and open standards of communication to be implemented by all ASPSPs for communication between ASPSPs, PISPs, AISPs, payers, payees and other PSPs (which may lead to the adoption of a single standard to facilitate interoperability, reduce barriers for AIS and PIS to provide their services, and minimize the risk of fragmentation that will undermine the objective of the PSD2 of integrating retail payments in the EU/EEA and facilitating competition across the EU/EEA) versus less detailed requirements (which may result in many different market-driven solutions to emerge across the EU/EEA that could allow future innovations in communication standards).

3.I.i. EBA Discussion Paper and Consultation Paper on Draft RTS on SCA and CSC

On 8 December 2015, the EBA published a Discussion Paper on the future draft RTS on SCA and CSC (DP on SCA and CSC), inviting market participants to share their views and inputs on: certain identified issues related to SCA; the exemptions to the application of SCA; the protection of the personalized security credentials of the PSUs; the requirements for common and secure open standards of communication; and possible synergies with e-IDAs Regulation on electronic identities.[318] The consultation period closed on 8

[315] See, Article 98(1) of PSD2.
[316] See, Article 98(2) of PSD2.
[317] See, European Banking Authority (EBA), *Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication under the Revised Payment Services Directive (PSD2)*, cit., pp. 9-10; European Banking Authority (EBA), *Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2*, EBA/CP/2016/11 (August 12, 2016), p. 6.
[318] See, European Banking Authority (EBA), *Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication under the Revised Payment Services Directive (PSD2)*, cit.

February 2016: 118 responses were submitted to the EBA, among which 82 gave permission for publication on the EBA's website.[319]

The EBA assessed the responses to the DP on SCA and CSC and started drafting the RTS shortly after closure of consultation. The initial draft RTS was published on 12 August 2016, included into a Consultation Paper on draft RTS on SCA and CSC (CP on SCA and CSC).[320] The consultation period for the CP on SCA and CSC closed on 12 October 2016: 224 responses were submitted to the EBA, in which more than 300 distinct concerns or requests for clarifications were raised.[321] All the major types of participants in the payment services market were represented among the respondents, including current (and prospective) AISPs, PISPs and unregulated service or IT providers, as well as payment and e-money institutions, merchants, acquirers and card schemes.[322]

In parallel, the EBA held a public hearing on 23 September 2016 at its office in London (UK)[323] and participated to the European Commission PSD2 transposition workshop, where further clarifications were provided to Member States to ensure a harmonized implementation of the PSD2 at EU level.

3.I.ii. EBA Final Draft RTS on SCA and CSC

Following 18 months of intensive policy development work and review of an unprecedentedly wide number of market players' views and input, the EBA published the final draft RTS on SCA and CSC on 23 February 2017.[324] Alongside the final draft RTS on SCA and CSC, the EBA also published a feedback table, which provides an exhaustive and comprehensive list of all the responses received by the EBA during the consultation period, the EBA's assessment of such responses, as well as any changes that the EBA decided to make to the initial draft RTS on SCA and CSC in consideration of such responses, where applicable.[325]

In order to explain how the EBA arrived at the provisions in the final draft RTS on SCA and CSC, the rationale section summarizes the EBA's understanding of some of the PSD2 provisions where relevant, and elaborates on three key issues raised in the responses to the CP on SCA and CSC, namely:

---

[319] This represents the second highest number of responses to a discussion or consultation paper ever received by the EBA. Responses to the DP on SCA and SC are available on the EBA's website at: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/discussion-paper#responses_1303933.

[320] See, European Banking Authority (EBA), *Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2*, cit.

[321] This represents the highest number of responses to a consultation paper ever received by the EBA.

[322] Responses to the CP on SCA and SC are available on the EBA's website: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper#responses_1548180.

[323] See, European Banking Authority (EBA), *Public Hearing on Strong Customer Authentication & Secure Communication (SCA & CSC) under Article 97 PSD2*, Presentation by Dirk Haubrich, Geoffroy Goffinet, Consumer Protection, Financial Innovation and Payments (London (UK), 23 September 2016).

[324] See, European Banking Authority (EBA), *EBA Paves the Way for Open and Secure Electronic Payments for Consumers Under the PSD2*, European Banking Authority Press Release (February 23, 2017); European Banking Authority (EBA), *Final Report - Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2)*, EBA/RTS/2017/02 (February 23, 2017).

[325] See, European Banking Authority (EBA), *Final Report - Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2)*, cit., Chapter 4.3.3, Feedback Table, pp. 48-153.

(a) The scope and technology-neutrality of the draft RTS on SCA and CSC;[326]

(b) The exemptions, including scope, thresholds and the request of many respondents to add an exemption for transactions identified as low risk as a result of what some respondents referred to as transaction risk-based analysis (TRA);[327] and

(c) The access to payment accounts by third party providers and the requirements around the information communicated.[328]

These 3 key issues are discussed below in greater details.

a) Scope and Technology-Neutrality of the RTS on SCA and CSC

With respect to the issue of scope and technology-neutrality of the RTS on SCA and CSC, the EBA has clarified, among others, that:

- PSD2 Article 97(1)(b) applies to electronic payments initiated by the payer, or by the payer through the payee (e.g., credit transfers or card payments), but it does not apply to electronic payments initiated by the payee only. Given Article 97(1)(c), an exception is a transaction where the payer's consent for a direct debit transaction is given in the form of an electronic mandate with the involvement of its PSP. The different types of payment instruments include e-money payment transactions. For instance, credit transfers include e-money transfers.

- In relation to how Article 97(1)(b) should be applied by PSPs for the provision of PISs, PISPs have the right to rely on the authentication procedures provided by the ASPSP to the user. In such cases, the authentication procedure will remain fully in the sphere of competence of the ASPSP.

- Based on the clarification received from the European Commission on the most plausible interpretation of PSD2, the payee's PSP has the option not to accept SCA in two cases: (a) before and during the transitional period between the application date of PSD2 (13 January 2018) and the application date of the RTS under consultation; and (2) after this transitional period only within the limits of the authorized exemptions and where applicable. The liability rules as described in article 74(2) PSD2 apply before, during, and after the transitional period.

- In case of cross-border transactions where payment instruments issued under a national legal framework that does not require the use of SCA (e.g., magnetic stripe cards) are used within the EU or when the PSP of the acquirer is established in a jurisdiction where it is not legally required to support the SCA procedure designed by the European issuing PSP, then the European PSPs will have to make every reasonable effort to determine the legitimate use of the payment instrument. Those types of cross-border transactions are not included in the transactions for the purpose of the calculation of fraud rates under Article 16 of the final draft RTS on SCA and CSC.

[326] Id., pp. 7-8.
[327] Id., pp. 9-10.
[328] Id., pp. 10-12.

- The RTS should be positioned at a higher level in respect to the characteristics of the three elements that form part of SCA. This is necessary to ensure technology and business-model neutrality and to allow PSPs to be able to continuously adapt to evolving fraud scenarios.[329]

- References to ISO 27001 and HTTPs in the initial draft RTS on SCA and CSC should be removed, in order to ensure technology and business-model neutrality and to allow for future innovations. By contrast, reference to ISO20022 should remain.[330] As clarified in a new Article 28(2), this standard shall apply only to the financial messaging (rather than to the communication technology, e.g. using XML) and solely where ASPSPs are offering a dedicated interface. This, according to EBA, should ensure commonality in terms of the content and format of the messaging, without being too prescriptive on the communication technology used.

B. Exemption for Low Risk Transactions following Transaction-Risk Based Analysis (TRA)

A key concern specifically addressed in the final draft RTS on SCA and CSC relates to the exemptions from the application of SCA on the basis of: the level of risk involved in the service provided ("transaction-risk based analysis" exception (TRA exception)); the amount and recurrence of the transaction; or the payment channel used for the execution of the transaction. The EBA considered the view of the many respondents that had expressed this concern and decided to introduce two new exemptions:

- An exception based on TRA tied to objective and tightly defined fraud levels;[331] and

[329] See, Andrea Enria (Chairperson of the European Banking Authority (EBA)), *Introductory Statement* of the Chairperson of the European Banking Authority at the Committee on Economic and Monetary Affairs (ECON) of the European Parliament (Brussels (BE), March 27, 2017), p. 2 (explaining that "[t]he Consultation Paper contained several references to particular technological approaches and international ISO standards. However, in light of the concerns raised by you and some respondents to the consultation, the EBA concluded that a different balance between these competing objectives should be found. We have, therefore, removed references to specific technological characteristics for the three elements of inherence, possession and knowledge at the basis of SCA, and also either removed references to international ISO standards such as ISO 27001 or narrowed their scope of application to the messaging template and for specific cases only.").

[330] In this sense, see, e.g., Payments UK, Financial Fraud Action UK and The UK Cards Association, Joint Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 8. *But*, see, e.g., Paypal, Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 8; Intuit, Inc., Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 8; IBM, Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 8; Financial API Working Group - Open ID Foundation, Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 8; European Payments Council (EPC), Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 8; Banking Stakeholder Group, Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 8; European Banking Federation, Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 8.

[331] See, Article 16 of the final draft RTS on SCA and CSC. The TRA based exception aims at providing incentives to PSPs to strengthen the protection of customers. Under this exception, where a PSP identifies a transaction through real-time TRA as being of low risk based on a range of parameters defined in the RTS, the PSP will have the option not to use SCA, provided the PSP's fraud rate is below the applicable reference fraud rate. To that end, the EBA has clarified that both payee's and payer's PSPs could trigger the TRA exemption under their own and exclusive responsibility, but with the payer's PSP having the final say. The EBA has set the reference fraud rates to be demanding and achievable. However, the EBA has also acknowledged that the reference rates are based on fraud data that is insufficiently representative of the different payments market in the 28 EU Member States. Therefore, the TRA exemption has been made subject to an 18-month review clause after the application date of the RTS, in order for the reference rates to

- An exception for payments at so called "unattended terminals" for fares related to transport and parking services.[332]

In addition to the above, having assessed the concerns of several respondents, the EBA has decided to increase the threshold for the low-value exemption for remote payment transactions from Euro 10 to Euro 30.[333] On the other hand, the EBA has recognized potential complexities in calculating cumulative monetary thresholds and has, therefore, introduced a choice for PSPs to apply SCA either every time the cumulative threshold Euro 100 is reached or after 5 consecutive individual remote electronic payment transactions.[334]

Finally, to ensure technology neutrality, the exemption focusing on a series of credit transfers with the same payee and the same value has been extended to a series of payments in general, as the risk does not vary between different payment instruments.[335]

c. Access to Payment Account

The majority of the responses received by the EBA on the issue of access to payment account focused on the frequency of requests, the communication exchanges, and the type(s) of information communicated between AISPs, PISPs, PSPs issuing card-based payment instruments (collectively, TPPs) and ASPSPs.

First, with respect to the frequency of requests, the initial draft RTS on SCA and CSC included in the CP on SCA and CSC allowed AISPs to request information from designated payment accounts and associated payment transactions each time the PSU is requesting such information or, where the PSU is not actively requesting such information by connecting to the AIS, no more than 2-times a day. Commenting on this requirement, some respondents have proposed to increase the frequency of requests; a few respondents have suggested an hourly interval; and other respondents have request to specify different expectations for different types of calls. In their views, these approaches would better address the real-time nature of payments and better serve the customers.[336] Furthermore, other respondents have expressed the view that setting any artificial limit on the frequency of data collection would be detrimental to the consumer and the AISP, would negate the value of providers' solution, and would, ultimately, stifle innovation. The concern shared among these respondents was that ASPSPs could be given too much control over the channel by

be updated in light of the fraud data that PSPs will have to submit to national authorities, the ECB and the EBA under Article 96 of PSD2. To further strengthen these provisions, the final draft RTS on SCA and CSC has also reiterated the importance of risk and fraud monitoring in general as a necessary complement to the principle of SCA laid out in PSD2. See, Article 2 and Article 3 of the final draft RTS on SCA and CSC.

[332] See, Article 12 of the final draft RTS on SCA and CSC.

[333] See, Article 15(a) of the final draft RTS on SCA and CSC. The EBA has clarified that PSPs may always revert back to SCA if a risk of fraud or other abuse is identified for a specific transaction. See, Article 18(5) of the final draft RTS on SCA and CSC.

[334] See, Article 15(b) of the final draft RTS on SCA and CSC.

[335] See, Article 13(1)(b) and Article 13(2)(b) of the final draft RTS on SCA and CSC.

[336] See, e.g., IBM, Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 10; Banking Stakeholder Group, Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 10.

which competitors would be allowed to access the data.[337] By contrast, some ASPSPs have requested to limit the frequency of requests to once a day, or specific office hours, or at other specific times. The ASPSPs have argued that these changes would be necessary to allow them to manage the load of information being communicated, as many different TTPs would potentially want to request access to the same information at the same time.

The EBA has considered these concerns and the different views expressed by the various respondents. As a result, the EBA has decided to amend the RTS on SCA and CSC to enable AISPs to access information from designated payment accounts and associated payment transactions held by ASPSPs for the purposes of performing the AISs in either of the following circumstances: (a) whenever the PSU is actively requesting such information; and (b) where the PSU is not actively requesting such information, no more than four times in a 24 hour period, unless a higher frequency is agreed between the AISP and the ASPSP with the PSU's consent.[338]

Second, a number of responses to the CP on SCA and CSC submitted by TPPs, especially PISPs, have requested the EBA to clarify whether or not practices such as "screen scraping" would be allowed under PSD2.[339] In this respect, some respondents have expressed the need to remain free to have access to payment accounts in ways other than through a dedicated interface, including through direct access and existing practices such as screen scraping. In their views, forcing the use of a dedicated interface would not be consistent with the legislators' intentions in PSD2 regarding the principles of neutrality, level playing field and non-discrimination and would, ultimately, stifle innovation and competition.[340] Other respondents have expressed their concerns that, should direct access and existing practices such as screen scraping be prohibited, they would no longer be able to serve their customers as they currently do. This is because – they argue - the ASPSPs would have no incentive whatsoever to provide a reliable service. A number of

[337] See, e.g., Yodlee, Inc., Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 10; Intuit, Inc., Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 10.

[338] See, Article 31(5) of the final draft RTS on SCA and CSC. The EBA notes that the new four-times-a-day frequency limit is consistent with the maximum settlement cycle in a number of countries in Europe. Moreover, the EBA observes, the opportunity for AISPs and ASPSPs to contractually agree to do it more often or differently (e.g., by using push notifications) will help ensure the necessary flexibility for AISPs to continue to service their customers while the burden remains proportionate on the ASPSPs, which are likely to have many different TPPs requiring access at any one time.

[339] See, e.g., Payments UK, Financial Fraud Action UK and The UK Cards Association, Joint Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 7.

[340] See, e.g., Klarna AB, Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 7; Intuit, Inc., Response to the EBA Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2, Answer to Question No. 7. In this sense, see, also, European Parliament's Negotiation Team, *Letter from Markus Ferber and Antonio Tajani (on Behalf of the European Parliament's Negotiation Team) to the European Banking Authority on the Draft Regulatory Technical Standard under PSD2* (Brussels (BE), October 24, 2016) (arguing that the requirement of a dedicated interface "bears the risk of giving the ASPSPs the possibility to exclude or limit direct access to the payer's account via existing online-banking facilities" and "would be against the principle set out in Art. 98(2) of PSD2, which mandates EBA to develop RTS in order to secure and maintain fair competition among all payment service providers and to ensure technology and business-model neutrality." For these reasons, the European Parliament's PSD2 Negotiating Team has suggested amending the RTS to ensure that "PISPs and AISPs can use at all times direct access via all the customer-facing interfaces of the ASPSPs, the ASPSPs fulfills its obligations as outlined in Article 66(4) and 67(3) of PSD2 also when PISP and AISP uses direct access via the interface of the ASPSP, and the ASPSP makes it technically possible for PISPs and AISPs to rely on the authentication procedures offered by the ASPSP to the account holder.").

respondents have, further, suggested that direct online access (not via customer interface) should be allowed as a backup in case other mechanisms are not available. This approach – they have explained – would help ensure neutrality and a level playing field. Other respondents have proposed inserting a transitional period, as time is needed to decode a specification of an IT interface and to develop the component needed. In contrast to these views, a number of respondents have argued that the PSD2 requirement for secure communication can be ensured only via a dedicated interface (i.e. not via the customer-facing online banking interface), because some information included in the online banking facility cannot legally be shared with a third party.

The EBA has examined these concerns and the different views expressed by the various respondents. After consulting with the European Commission on the most plausible interpretation of the PSD2, in the final draft RTS on SCA and CSC the EBA has expressed the view that accessing accounts through screen scraping will no longer be allowed, once the transitional period terminates. As explained by the EBA, this view is based on a number of provisions under PSD2, including Articles 66, 67, and 115.[341]

In addition to the foregoing, the EBA has clarified that ASPSPs that offer to a payer a payment account that is accessible online will have to put in place at least one interface which meets all the following requirements: (a) AISPs, PISPs and PSPs issuing card-based payment instruments can identify themselves towards the ASPSP; (b) AISPs can communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions; (c) PISPs can communicate securely to initiate a payment order from the payer's payment account and receive information on the initiation and the execution of payment transactions.[342] To this end, ASPSPs have the choice of either establishing a dedicated interface (in practice, an API)[343] or adapting the interface used for authentication and communication with their PSUs for AISPs and PISPs to access the customer information they need.[344]

On the other hand, the EBA has acknowledged the legitimate concerns raised by a number of respondents in respect to the smooth and continued access to the dedicated interface. As a result, in the final draft RTS on SCA and CSC the EBA has added additional requirements for ASPSPs that choose to develop and offer these interfaces.[345] In particular, ASPSPs that use a dedicated interface: (a) will have to ensure that such a dedicated interface provides the same level of availability and performance (including support), as well as the same level of contingency measures (in case of unplanned unavailability) as the interface offered to, and used by, their PSUs for directly accessing their payment account online; and (b) will be required to open the interfaces ahead of release so as to enable PISPs and AISPs to test the interfaces.[346] In addition,

[341] See, Andrea Enria (Chairperson of the European Banking Authority (EBA)), *Introductory Statement* of the Chairperson of the European Banking Authority at the Committee on Economic and Monetary Affairs (ECON) of the European Parliament, cit., pp. 4-5.
[342] See, Article 27(1) of the final draft RTS on SCA and CSC.
[343] See, European Banking Authority (EBA), Final Report - Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2), cit., Chapter 4.3.3, Feedback Table, p. 118 (noting that "[t]he EBA requires the ASPSPs to offer at least one interface for TPPs to access the information needed. The RTS do not mandate APIs although the EBA appreciates that the industry may agree that they are suitable.").
[344] See, Article 27(2) of the final draft RTS on SCA and CSC.
[345] See, Article 28 of the final draft RTS on SCA and CSC.
[346] See, Articles 28(1) to 28(4) of the final draft RTS on SCA and CSC.

the EBA has clarified that the ASPSPs have the obligation to provide, upon request, an immediate confirmation to PISPs whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer, to ensure the PISP is able to process the payment. This confirmation can consist of a simple "yes" or "no" answer.[347]

Third and last, the initial draft RTS on SCA and CSC included in the CP on SCA and CSC required the ASPSPs to ensure that the technical specification of their communication interface be documented and that the documentation be made available for free and publicly on their website. Commenting on these requirements, a number of respondents have expressed the concern that the information should not be made publicly available, because of the security risks that such publication would create. In particular, some respondents have argued that the information should be disclosed only based on a contractual agreement between the PSP and the interested parties (PISP, AISP, etc.), while other respondents have suggested a "need-to-know" basis approach.

The EBA has considered these views and has concluded that the documentation should not be disclosed only on the basis of contractual arrangements or on a "need-to-know" basis. On the other hand, the EBA has acknowledged the existence of security risks and, therefore, in the final draft RTS on SCA has provided that ASPSPs must ensure that the technical specification of their interfaces be documented and, as a minimum, available, at no charge, upon request by authorized PISPs, AISPs and PSPs issuing card-based payment instruments, or PSPs that have applied with their competent authorities for the relevant authorization. This documentation will have to specify a set of routines, protocols, and tools needed by PISPs, AISPs and PSPs issuing card-based payment instruments for allowing their software and applications to interoperate with the systems of the ASPSPs. In addition, the EBA has required ASPSPs to publish the summary of the relevant documentation on their websites.[348]

3.I.iii. Letter from the European Commission Regarding the Intention of the European Commission to Amend the Final Draft RTS on SCA and CSC and the EBA's Responding Opinion

The final draft RTS on SCA and CSC discussed above was released by the EBA on 23 February 2017 and, then, submitted to the European Commission for adoption. The European Commission responded with a letter dated 24 May 2017, stating its intention to amend Chapters 1, 3 and 5 of the EBA's final draft RTS on SCA and CSC.[349] The text of the draft RTS incorporating the amendments suggested by the European Commission is attached to the European Commission's letter.

The substantive changes envisaged by the European Commission include the following:

[347] See, Article (31)(1)(c) of the final draft RTS on SCA and CSC.
[348] See, Article 27(4) of the final draft RTS on SCA and CSC.
[349] See, European Commission, *European Commission Letter Addressed to the EBA regarding the European Commission Intention to Amend the Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Open Standards of Communication Submitted by the EBA in Accordance with Article 98(4) PSD2*, European Commission Letter (May 24, 2017).

(1) A proposal that the audit relating to the TRA exemption be performed by statutory auditors to ensure objectivity in the application of this exemption between different providers, independent verification of the conditions imposed by the RTS, and a good quality of the reported data;[350]

(2) A proposal of introducing an additional, standalone exemption to SCA for certain corporate payments when dedicated payment processes or protocols are utilized;[351]

(3) A proposal that PSPs be required to report the outcome of the monitoring and calculation of the fraud rate under the TRA exemption to the EBA, in addition to reporting this information to the national competent authorities;[352] and

(4) A proposal that ASPSPs, which have set up a dedicated interface under the RTS on SCA and RTS, be required to allow AISPs and PISPs to access the ASPSP's user-facing interface as a contingency measure in case of unavailability or inadequate performance of the dedicated communication interface. The use of the contingency measures should be fully documented and reported to the authorities by the relevant providers, upon request, including justification for the use of these measures. Once the dedicated interface is restored to full service, AISPs and PISPs should be obliged to use it.[353]

On 29 June 2017, the EBA published an Opinion responding to the European Commission's Letter concerning the European Commission intention to amend the EBA's draft RTS on SCA and CSC.[354] In its Opinion, the EBA has concurred with the aims sought in the European Commission's amendments, but has voiced its disagreement with some of the means by which the European Commission has proposed to achieve such aims. In particular, the EBA has expressed its disagreement with three of the four amendments proposed by the European Commission, on the basis that the suggested changes would negatively impact the balance created by the EBA in pursuing the various competing objectives of the PSD2.

First, with respect to the proposal by the European Commission to utilize "statutory auditors", the EBA has expressed the view that the use of external "statutory auditors" for the review of the TRA exemption is unlikely to guarantee the quality and independence of assessment that the European Commission seeks to achieve and, rather may result into disproportionate new requirements on a number of PSPs. Yet, the EBA has also recognized the need for the audit to be conducted by auditors that are independent and have the

[350] Id., p. 1.
[351] Id., p. 2.
[352] Ibidem.
[353] Ibidem.
[354] See, European Banking Authority (EBA), *EBA Publishes its Opinion In Response to the European Commission Intention to Amend the EBA Technical Standards for Open and Secure Electronic Payments under the PSD2*, European Banking Authority Press Release (June 29, 2017); European Banking Authority (EBA), *Opinion of the European Banking Authority on the European Commission's Intention to Partially Endorse and Amend the EBA's Final Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication Under PSD*, European Banking Authority (EBA) Opinion (June 29, 2017). The EBA has exercised its competence under Article 10 of the EBA Founding Regulation (Regulation (EU) No 1093/2010), which mandates the EBA to deliver an Opinion on the European Commission's proposed amendments to the RTS as well as revised RTS within 6 weeks of receiving the European Commission's letter.

appropriate expertise. Because of this, the EBA has suggested a number of changes and clarifications to the European Commission's proposal by:[355]

- Replacing in Article 3(2) reference to "statutory audit" with "an audit performed by an auditor with expertise in IT security and payments and operationally independent within or from the payment service provider;"

- Replacing the reference to "statutory auditors'" in Article 3(1) with "auditors with expertise in IT security and payments and operationally independent within or from the payment service provider;" and

- Introducing a requirement for an external audit to be carried out during the first year of the PSP's use of the exemption and at least every 3 years thereafter, and whenever requested by the competent authority.

Second, in responding to the proposal by the European Commission to add an exemption to SCA for certain corporate payments, the EBA has suggested adding a new category under the existing TRA exemption (as opposite to an additional, standalone exception) for specific payment transactions for payers that are not consumers (rather than a reference to "corporate payments"), without a monetary threshold, providing that the fraud rate is equivalent to or below a specific reference fraud rate. The EBA has further indicated that all the requirements and conditions set out in relation to the TRA exemption should apply to this new category.[356]

Third, the EBA has voiced its strong disagreement on the proposal advanced by the European Commission to allow AISPs and PISPs to use a user-facing interface (in practice, a form of screen scraping) as a "fallback" option in case of unavailability or inadequate performance of a dedicated interface.[357] More in detail, the EBA has agreed with the European Commission's objectives to ensure that ASPSPs comply with their obligation under PSD2 to share customer information with TPPS without any discrimination and in compliance with the security requirements under PSD2. In fact, the EBA has recognized that this is critical to ensure that AISPs and PISPs can access the data they need to provide services and effectively compete against banks and other PSPs. Furthermore, based on a review of a number of responds to the CP on SCA and CSC published in August 2016, as well as discussions with the European Parliament, the EBA has acknowledged that there exist genuine concerns among some TPPs that ASPSPs may not have sufficient incentive to provide the best possible interface to competitors. In addition, the EBA has acknowledged that

[355] See, European Banking Authority (EBA), *Opinion of the European Banking Authority on the European Commission's Intention to Partially Endorse and Amend the EBA's Final Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication Under PSD*, cit., pp. 3-4.
[356] Id., pp. 5-6.
[357] Id., pp. 7-11. See, also, European Banking Federation, *EBF Asks Commission to Support Ban on Screen Scraping*, European Banking Federation Statement (Brussels, 16 May 2017) (asking the European Commission to support the ban on screen scraping and expressing the view that the EBA standards are "a common solution that ensures security and as a significant catalyst for innovation into the future in the European payments market, fully compliant with the EU's General Data Protection Regulation (GDPR).").

there have been significant lobbying activities from various market participants following the release of the initial and the final draft RTS on SCA and CSC.[358]

Yet, against this background, the EBA has stated its view that imposing a "fallback" requirement such as the one proposed by the European Commission would go beyond the legal mandate given to the EBA under Article 97 PSD2 and would have a number of negative consequences. These negative effects would include: cost increases;[359] fragmentation compromising the development of APIs;[360] competitive disadvantage for new entrants; a lack of improved technical reliability; incompatibility with PSD2's security requirements; supervisory constraints;[361] and unclear consumer understanding and consent. For these reasons, the EBA has voiced its disagreement with the proposal by the European Commission and has suggested including four new requirements in the RTS on SCA and CSC:

- A requirement for ASPSPs to define transparent key performance indicators and abide by at least the same service level targets as for the customer interface, regarding both the availability and the performance of the interface, as well as qualitative measures to assess whether or not they are doing so;

---

[358] See, e.g., Future of the European Fintech, *PSD2-Compliant Access not Subject to an Alleged "Screen Scraping Ban,"* Future of the European Fintech Alliance (2017); Future of the European Fintech, *Manifesto for the Impact of PSD2 on the Future of European Fintech*, Future of the European Fintech Alliance (2017). Sixty organizations (including, fintech companies and associations, AISPs and PISPs, banks and financial Institutions and other companies using TPP technologies) have joined forces to protest against the EBA RTS on SCA and CSC that would ban screen scraping of customer data from online banking interfaces under PSD2. These organizations have expressed the view that "the EBA's RTS … are distorting [the principles laid down in PSD2] by banning a secure proven technology such as Direct Access via the bank's existing – and well maintained – customer-facing online banking interface (sometimes derogatively referred to as screen scraping)… [i]f the RTS articles on the communication interface were to be adopted in their current form … [b]anks would be given technological control over Fintech businesses and would be able to ring-fence consumers' data. This will inevitably result in the very opposite of the political intentions behind PSD2: instead of enhancing competition, fostering innovation and giving consumers more choice, innovation will be banned, competition will decrease and consumer choice will be significantly diminished … [moreover] if the RTS were adopted as they currently stand, then the mandatory use of newly developed, proprietary dedicated interfaces would inevitably give Banks (ASPSPs) full control regarding any future innovation on the financial services space." Further, these organizations have argued that "[d]irect [a]ccess is a secure technology that has been used for the last 15 years by both European Fintechs and Banks to provide AIS and PIS services to millions of consumers … there hasn't been, until this day, one single documented incident of data fraud or compromise of personal credentials. Hence, there is no factual basis or empirical data to support EBA's decision to ban Direct Access technology. In fact, Direct Access (using screen scraping) is a well-established technology that has been used and leveraged by other industries … [b]y using the exact same identification mechanism, as the one requested for the dedicated interface in the RTS, [d]irect [a]ccess becomes Secure Authenticated Direct Access (screen scraping combined with TPP identification) and therefore, fully compliant with PSD2 … Secure Authenticated Direct Access would not only uphold the principles of data ownership, but also provide an easy and secure way for Banks (ASPSP) to be compliant both with … PSD2 and … GDPR." Therefore, these organizations have concluded that "[t]he only way to ensure that Banks (ASPSPs) have the right incentives to provide and maintain a well-functioning dedicated interface and that competition and innovation continue to grow, is to make them optional … [and RTS should] be amended so that TPPs can identify themselves at the customer-facing online banking interface and use Secure Authenticated Direct Access even if the Bank (ASPSP) provides a dedicated interface."

[359] See, European Banking Authority (EBA), *Opinion of the European Banking Authority on the European Commission's Intention to Partially Endorse and Amend the EBA's Final Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication Under PSD*, cit., p. 8. According to EBA the fallback option proposed by the European Commission would increase PSD2 compliance costs for both ASPSPs, on one hand, and AISPs and PISPs, on the other hand. In particular, the compliance costs for ASPSPs would increase because, in addition to developing a dedicated interface and maintaining their customer interface, ASPSPs would have to develop, and continuously maintain, a PSD2-compliant customer interface to ensure that the fallback option also complied with the rules under PSD2. Likewise, the compliance costs for AISPs and PISPs would increase, because they would have to pay to be able to access the dedicated interface and the customer-facing interface of any given ASPSP.

[360] Id., p. 9. The EBA has expressed the view that requiring ASPSPs to have a fallback option in place may discourage ASPSPs from developing and maintaining dedicated interfaces, and instead may create strong incentive for them to opt for customer-facing interfaces that are PSD2-compliant. This, in turn, would make it extremely challenging to achieve an EU-wide communication standard, and would undermine the PSD2's goals of creating a standardize access across the EU Member States and a more integrated single EU payments market. As a result, according to EBA, the proposal of this "fallback option" would, ultimately, compromise the development of standardized APIs across the EU, and would increase their fragmentation, along geographical or other boundaries.]

[361] Id., p. 10. The EBA has voiced its concern that the proposed fallback requirement could also be extremely difficult to supervise. This is because, according to the EBA, competent authorities would most likely not be able to conduct any checks or intervene in the ante, given the limited 30-second duration. On the other hand, intervention ex post might be equally challenging.

- A requirement for PSPs to monitor and publish their availability and performance data on a quarterly basis;

- A requirement for ASPSPs to make the interfaces available for testing at least 3 months before the application date of the RTS; and

- A review of the functioning of the interfaces as part of the review planned for 18 months after the application of the RTS under Article 36, to ensure that information access and sharing are working as intended.

Finally, in addition to the substantive changes examined above, the EBA has considered a number of drafting changes proposed by the European Commission. In particular, the EBA has agreed with the European Commission that it may be preferable to delete the reference to, and requirement to, define communication messages that are compliant with ISO 20022. As acknowledged by the EBA, this would help ensure technological neutrality, although it might also pose the risk of undermining greater harmonization at the EU level.[362]

With the publication of the aforesaid Opinion and its submission to the European Commission, the EBA has formally concluded its work on the RTS on SCA and CSC mandate. At the time of writing, it is up to the European Commission to make the final decision on the text of the RTS on SCA and CSC and to adopt the standards as a delegated Act in the Official Journal of the EU. During the adoption process, the European Council and the European Parliament have a scrutiny right. The RTS on SCA and CSC will enter into force the day following their publication in the Official Journal and will be applicable 18 months after their entry into force. This would suggest an application date of the RTS on SCA and CSC in late 2018 at the earliest. The intervening period aims at providing the industry with sufficient time to develop industry standards and/or technological solutions that are compliant with the EBA's RTS on SCA and CSC.[363]

3.J. Implementation of PSD2 and RTS on SCA and CSC and Risk of Fragmentation

In fulfilling its mandates under PSD2, the EBA has sought to make the draft RTS on SCA and CSC as clear as possible, without forcing market participants into using technologies that might become obsolete (and even insecure) shortly after the RTS comes into force. Getting this right has turned out to be a very challenging task, because the EBA had to balance a number of conflicting concerns: on one hand, if the RTS on SCA and CSC are too specific, the compliance obligations will be clearly set out but at the cost of hampering future innovation; on the other hand, if the RTS on SCA and CSC are too broad, market participants subject to RTS requirements will enjoy more flexibility, but they will also face increased

[362] Id., p. 12.
[363] The delay in the process of drafting and subsequent approval means that the RTS on SCA and CSC will not yet be in force in January 2018, the set deadline for compliance with PSD2. This misalignment of timelines adds an additional hurdle to the process of implementation of PSD2 and contributes significant uncertainly around how communication between banks and TPPs will be handled during the transition period between January 2018 and the date at which the RTS will come into force. Against this background, it is likely that market participants will look at the Open Banking regulatory framework and standards for the sharing and use of banking data via APIs, which are currently being developed in the UK. This point is further detailed in the following sections.

uncertainty as to what exactly is expected in terms of compliance. Because of this, the EBA has deliberately taken a principle-based approach to the draft RTS on SCA and CSC, so not to inadvertently stifle payments and security innovation. At the same time, the EBA has also sought to be proportionate and technology neutral, so that market participants could still innovate without having to give up flexibility, and PSUs could still benefit from new payment methods and technologies without having to give up privacy and security.

The described objectives pursued by the EBA are certainly laudable. However, the final draft of the RTS on SCA and CSC shows just how difficult it can be to meet them, and still make the legal obligations clear. In fact, a number of provisions in the RTS on SCA and CSC remain controversial; while other provisions seem to leave excessive discretion to market participants on how to concretely implement the legal requirements. The resulting debate and the increasing uncertainty surrounding the RTS on SCA and CSC, in turn, have fuelled concerns of renewed fragmentation across Member States.[364]

For example, a large number of market players believe that APIs will be the technological means used to ensure compliance with PSD2 and its RTS. Moreover, in the feedback table accompanying the RTS on SCA and CSC, the EBA itself has expressed its support to the view of those market participants that see APIs as a suitable means to achieve PSD2 compliance.[365] Nevertheless, neither the PSD2 nor the RTS on SCA and CSC explicitly mention APIs. This means that, while an increased utilization of open APIs under PSD2 framework does not appear to be disputed, doubts do remain as to who will define the APIs that will underpin PSD2.

Furthermore, perhaps a challenge greater than creating APIs will be doing it in a standardized way. In this regard, growing concerns are arising among market participants about whether or not, and how to, reach standard APIs. Some market participants have voiced their disagreement on establishing standardized APIs, which in their view would preclude future innovation and would limit opportunities for competition by new players.[366] On the other hand, a number of market participants have argued that, if European ASPSPs were to define their own APIs under PSD2 in subtly different ways, it would become extremely difficult (and more expensive) for third-parties developers to connect to them all. The resulting complexity and lack of interoperability, in turn, would negatively affect customers and frustrate PSD2 objectives of commonality

[364] See, Helmut Wacket (Head of Market Integration Division, European Central Bank), *Provision of Integrated Payment Initiation Services – The Role of the ERPB*, slides 9-12, in Open Forum on Open Banking, Meeting Presentation, Open Forum on Open Banking (Brussels (BE), March 20, 2017).

[365] See, *European Banking Authority (EBA), Final Report - Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2)*, cit., Chapter 4.3.3, Feedback Table, p. 118.

[366] See, Finextra, *PSD2 and Open Banking: Defining Your Role in the Digital Ecosystem*, cit., pp. 25-26 (quoting: Colm Lyon, CEO and Founder at Fire Financial Services, arguing that "[w]e need to have competition in data services as we do in payments. APIs are brilliant but if everyone makes the same APIs, they will be useless. We need to nurture the creation of good, smart APIs and then rely on aggregators – gateway providers – for API authentication;" and Fabrice Denèle, Head of Cards & Payments at Groupe BPCE, arguing that "[A]PIs have not been done. They are still to be done. It's something relatively new, and starting on a standard now for something that is not yet in place would harm innovation and probably limit the initiatives that happen and will ultimately harm the ability of some players to operate in the way they want. A better journey is to leave the initiative to the market so everyone can do what they want provided it is compliant with the RTSs. If something is needed in terms of a standard it will emerge: there's a time for everything, and it's not the time for a standard. It would be quite incredible to see the regulators limiting innovation just at the time they are introducing regulation to foster innovation.").

and harmonization. Because of these reasons, these market participants have argued that the variability of API standards across Europe should be minimized. In their opinion, a minimum level of standardization would enable developers to write innovative applications that work efficiently across European ASPSPs and across borders in a harmonized way, and would provide some "cornerstones" of a framework within which the full potential of Open Banking could be unlocked.[367]

EU regulators have expressed similar concerns. In particular, on 17 May 2017, the European Parliament voted in plenary to adopt a resolution on fintech and the influence of technology on the future of the financial sector.[368] This vote follows the publication by the European Parliament's Committee on Economic and Monetary Affairs (ECON) of a report on fintech, which included the resolution, on 28 April 2017.[369]

The resolution by the European Parliament and the report backed by the vote of the ECON have clearly acknowledged the importance of APIs, as a complement to other tools that can be used by the consumer, in providing new actors with access to financial infrastructure. Because of this, the European Parliament and ECON have recommended the creation of a set of standardized APIs that vendors can use in parallel with the possibility for such vendors to design their own software. In addition, the resolution by the European Parliament and the report backed by the vote of the ECON have recognized the importance of interoperability of fintech services (both within Europe and through engagement with third-country jurisdictions and with other economic sectors) as a key condition for the future development of the European fintech sector and the full realization of the opportunities that it can create. In order to facilitate interoperability, they have encouraged standardizing data formats in PSD2. Finally, the European Parliament and ECON have called on the European Commission to coordinate the work of the Member States and market participants in order to ensure interoperability among the different national e-identification schemes, and have stressed the importance of interoperability of traditional and new payments solutions in order to achieve an integrated and innovative European payment market.

Given the described background, the EBA will most likely let the industry develop relevant API standards in compliance with PSD2 and RTS. To this end, a number of actions could be undertaken, ranging from the development of a pan-European standard API to the adoption of more local solutions. Initiatives such as the

[367] Id., pp. 5, 24-27.
[368] See, European Parliament, *The Influence of Technology on the Future of the Financial Sector*, European Parliament Resolution on FinTech, TA-PROV(2017) 0211 (May 17, 2017). The Parliament has instructed its president to forward this resolution to the Council of the EU and the European Commission.
[369] See, European Parliament's Committee on Economic and Monetary Affairs (ECON), *EU Needs to Accelerate FinTech Development*, European Parliament's Committee on Economic and Monetary Affairs Press Release (April 25, 2017); European Parliament's Committee on Economic and Monetary Affairs (ECON), *Report on FinTech: The Influence of Technology on the Future of the Financial Sector*, Report prepared by Cora van Nieuwenhuizen, European Parliament's Committee on Economic and Monetary Affairs (April 28, 2017). The report was prepared by Cora Van Nieuwenhuizen and was designed to encourage the EU to further support fintech development. The ECON adopted the report with 45 votes in its favor (6 against and 1 abstention) a few days prior to its publication. The report is addressed to the European Commission and is to be read alongside the European Commission's Consultation Document on fintech, which was published on 23 March 2017.

UK's Open Banking Working Group[370] are looked up as drivers for standardization, while increasing calls are arising for a similar initiative to be taken at the European level, as well.[371]

[370] See Chapter 4 for further discussion on this point.

[371] Recent years have witnessed a significant growth in the number of industry initiatives aiming at creating standards for APIs grow. Most of these initiatives cover the full scope (functional, operational and legal aspects) of API standards as. The initiators and governing bodies are diverse in their representation. See, Sections 2.B and Section 2.C above. See, also, Euro Banking Association (EBA), *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, cit., pp. 11-14 (providing an overview of some of the most relevant API standardization initiatives, including the UK Open Banking Working Group (OBWG), CAPS, Open Bank Project, Open API iniative, Open Financial Exchange (OFX), and the Berlin Group).

CHAPTER 4. OPEN BANKING REGULATORY AND POLICY FRAMEWORK – THE UNITED KINGDOM (UK)

The United Kingdom (UK) has taken bold steps to position itself as a global leader in fintech, attracting and nurturing steady waves of fintech companies. Three main initiatives have been undertaken that promise to extend the UK's leadership into the Open Banking ecosystem, while also helping drive further fintech innovation and foster competition in the financial and banking services industry: (1) the UK Government Open Banking Working Group (OBWG)'s Open Banking Standard; (2) the UK Competition and Markets Authority (CMA)'s Retail Banking Markets Investigation Report and Final Order; and (3) the UK process of implementation of PSD2 and the EBA RTS.

4.A. UK HM Treasury (HMT)

4.A.i. The Fingleton Report

The UK HM Treasury (HMT) initiated the drive towards Open Banking in the UK in 2014 with the publication of a report titled "*Data Sharing and Open Data for Banks,"* written by the Open Data Institute and the consultancy firm Fingleton Associates and published in autumn 2014 (the "Fingleton Report").[372] The Fingleton Report concluded that "greater access to data has the potential to help improve competition in UK banking"[373] and recommended that banks create standardized APIs that would be accessible to third parties (e.g. fintech companies, developers, and other corporates).

Shortly after the publication of the Fingleton Report, in January 2015 the HMT published a consultation, sourcing views from across the financial services industry, consumer representative groups, business groups, and the fintech community.[374] Building upon the recommendations presented in the Fingleton Report and the responses to its consultation,[375] in the 2015 March Budget, the HMT published a statement on the consultation and the next steps, announcing its intention to deliver an open standard for APIs and data sharing in UK retail banking. The HMT expressed the view that this standard would help customers have more control over their data and would make it easier for fintech companies or other businesses to make use of bank data on behalf of customers in a variety of helpful and innovative ways. This, in turn, would help drive more competition in banking to improve outcomes for customers, and further support the UK's world-leading fintech industry.

---

[372] See, HM Treasury (HMT), *Data Sharing and Open Data for Banks*, HM Treasury Press Release (December 3, 2014); Open Data Institute (ODI) and Fingleton Associates, *Data Sharing and Open Data for Banks - A Report for HM Treasury and Cabinet Office*, Open Data Institute (ODI) and Fingleton Associates (September 2014).

[373] See, Open Data Institute (ODI) and Fingleton Associates, *Data Sharing and Open Data for Banks - A Report for HM Treasury and Cabinet Office*, cit., pp. 4, 10.

[374] See, HM Treasury (HTM), *Data Sharing and Open Data in Banking: Call for Evidence*, HM Treasury Press Release (January 28, 2015); HM Treasury (HTM), *Call for Evidence on Data Sharing and Open Data in Banking*, HM Treasury (January 28, 2015 – updated March 18, 2015); HM Treasury (HTM), *Data Sharing and Open Data in Banking: Response to the Call for Evidence*, HM Treasury (March 18, 2015).

[375] Many of the respondents to the consultation expressed their support to the development of open industry standards for data-sharing in banking in order to increase competition and innovation in banking. The consultation also highlighted potential risks around data privacy, consumer education, and interoperability.

4.A.ii. The UK Open Banking Working Group (OBWG)'s Open Banking Standard

The work discussed above led to the formation of the Open Banking Working Group (OBWG) in the summer of 2015, which was tasked with taking the work on Open Banking forward. Three were the OBWG's main objectives: (a) deliver a framework for the design of an open API standard in UK banking focusing on personal and business current accounts; (b) evaluate how increased levels of open data in banking can benefit consumers, businesses and society; and (c) publish recommendations in a paper by the end of 2015 outlining how an open API standard can be designed, delivered, and administered, alongside a timetable and implementation roadmap.[376]

The OBWG brought together a wide range of relevant stakeholders, including representatives and industry experts from banks and other financial institutions, fintech companies, consumer bodies, and government. It finalized its report at the end of 2015. In February 2016, the OBWG report was published, containing an ambitious set of proposals for the creation of an Open Banking Standard ("OBWG Open Banking Standard Report").[377]

The aim of the OBWG in drafting the OBWG Open Banking Standard Report was to construct an Open Banking Standard framework that would facilitate the creation of an Open Banking Standard in the UK.[378] In particular, the OBWG Open Banking Standard Report sets out the framework for:

- An open API[379] for data that is shared (including, but not limited to, customer data). This would allow, for instance, an individual or business to consent to a third party provider accessing account level data stored with their bank or financial institution, including the ability to initiate payments; and

- An open data API for market information and relevant open data.[380]

At its core, the framework outlined in the OBWG Open Banking Standard Report constitutes a set of foundational recommendations covering various aspects of data-sharing in an API environment.[381] Three standards are considered, which in combination form the proposed Open Banking Standard:[382]

---

[376] See, Open Banking Working Group (OBWG), *Open Banking Working Group (OBWG) Terms of Reference*, Open Banking Working Group (September 2015), Article 1.
[377] See, Open Banking Working Group (OBWG), *The Open Banking Standard. Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation*, cit. See, also, Open Data Institute (ODI), *Introducing the Open Banking Standard. Helping Customers, Banks and Regulators Take Banking into a Truly 21st-Century, Connected Digital Economy*, cit.
[378] See, Open Banking Working Group (OBWG), *The Open Banking Standard. Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation*, cit., pp. 3-4.
[379] Id., pp. 4-5 ("Open API" is defined as "is a means of accessing data based on an open standard: it is a public interface." The data accessed via an open API may be closed, shared or open data. Any individual's personal bank details or a company's transaction data are considered closed or shared data. This data will be made available via an open API as a result of the implementation of the UK OBWG's Open Banking Standard, but access to it would be subject to consent of the individual or business to whom the data belongs and specific governance related to that. Such data will not be licensed or made public as open data as a result of the implementation of the OBWG's Open Banking Standard.).
[380] Id., pp. 5, 17-19 ("Open data" is defined as "data that anyone can access, use and share. An open data API, therefore, is a public interface that provides access to open data." Examples of open data could be financial product information and ATM locations.).
[381] Id., pp. 11-12 (In the context of the OBWG's final report, data-sharing is considered from two perspectives: 1. Where an individual or business consents to a third party accessing account-level data stored with a data attribute provider (like their bank or financial services provider), typically on a restricted basis; 2. Greater publication of standardized open data (e.g. bank product data released on money supermarket/price comparison websites).
[382] Id., p. 24.

1. Data Standards: rules by which data are described and recorded, potentially including, among other characteristics, agreements on representation, format, definition and structure.[383]

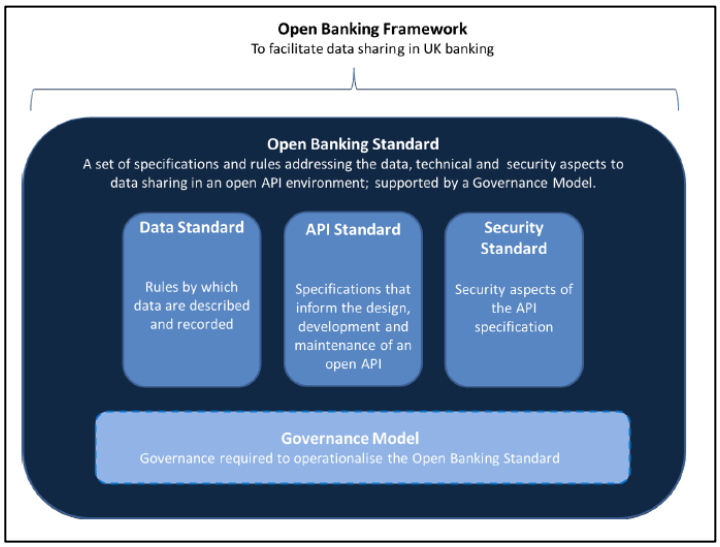
2. API Standards: specifications informing the design, development and maintenance of an API. This can include guidelines pertaining to architectural design, resource formats, documentation, and versioning.[384]

3. Security Standards: security aspects of the API specification; standards and policies, through which consumers' data will be protected from fraudulent access and utilization, and access rights will be securely delegated.[385]

In addition to these three standards, the OBWG Open Banking Standard Report describes: a governance model, to provide issue resolution mechanisms and govern the standards;[386] and developer resources, to enable developers and third parties to innovate, educate, and experiment.[387] (see, Figures 11(a) to 11(c)).

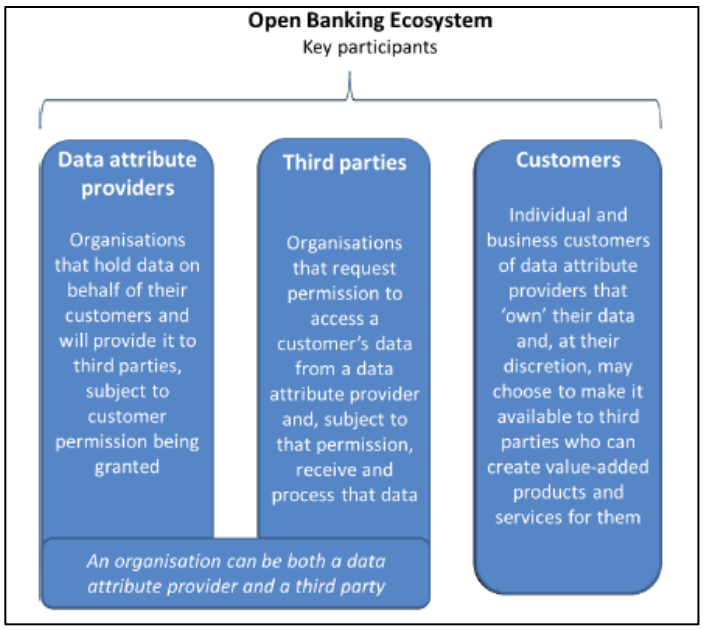
[383] Id., pp. 33-35.
[384] Id., pp. 25-26, 28-33. The OBWG Open Banking Standard Report provides that the API Standard should comprise the following specifications and/or meet the following criteria: use of REST as an architectural style and HTTP as the transport; use of JSON as the resource format; achievement of Level 2 from the Richardson Maturity Model; adoption of a vendor and technology independent definition. In addition, the API Standard should comply with the following versioning requirements: support for major and minor releases; backwards compatibility for all minor – and as far as possible – major releases; prescription of minimum support time periods for major releases; and embedded flexibility/response speed for security or functional errors. Finally, the API Standard should be designed with the following features: a controlled core – hosting shared resources should be established and this should represent the slowest-changing part of the standard; local extensions "at the edges" should be permitted, allowing for API provider innovations with subsequent potential incorporation back into the core; specific characteristics allowing API providers (data attribute providers) to address scalability challenges.
[385] Id., pp. 41-54. The OBWG's final report covers a variety of customer protection measures, including enhanced security, authentication, fraud detection/monitoring, accreditation for firms, and the ability for customers to easily withdraw their permissions whenever they choose. These measures, among others, are intended to ensure that customers understand and have confidence in giving informed consent to third parties and that customers know how they are protected if something goes wrong and how they can withdraw consent should they want to. See, Open Data Institute (ODI), *Introducing the Open Banking Standard. Helping Customers, Banks and Regulators Take Banking into a Truly 21st-Century, Connected Digital Economy*, cit., p. 10 (noting that "[i]t is crucial that we protect data that needs to be kept private, just as it is crucial that we openly publish data that should be open for everyone to use. Because both privacy and openness help create trust.").
[386] See, Open Banking Working Group (OBWG), *The Open Banking Standard. Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation*, cit., pp. 55-63.
[387] Id., pp. 37-40.

Figure 11(a). Open Banking Framework



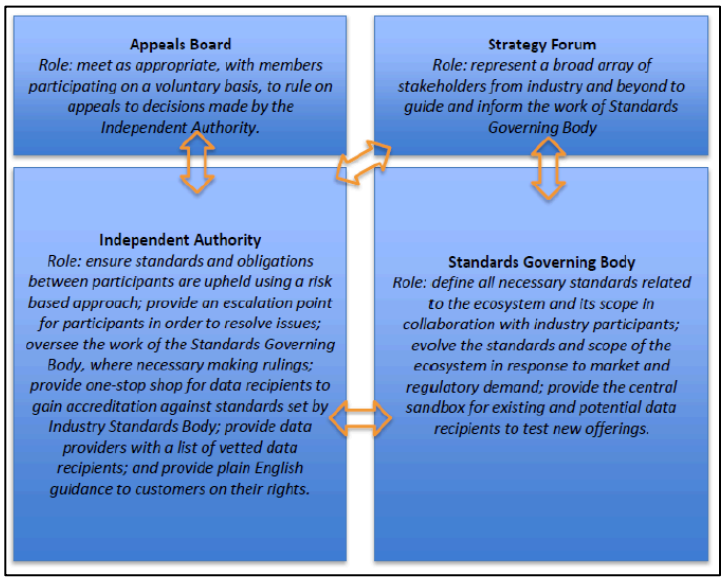
Source: Open Banking Working Group (OBWG), *The Open Banking Standard. Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation*, Open Banking Working Group (February 2016), p. 9.

Figure 11(b). Open Banking Ecosystem – Key Participants



Source: Id., p. 10.

Figure 11(c). Open Banking Governance



Source: Id., p. 11.

The OBWG envisaged an Open Banking Standard that would be developed and maintained collaboratively and transparently and be accessed and used by anyone.[388]

Alongside the technical considerations involved in defining and implementing an Open Banking Standard, the OBWG Open Banking Standard Report addresses critical issues to take forward around governance, security, liability, standards, communications, regulation and legal, and it outlines the OBWG's recommendations in respect to each of these areas. Among them, the following key recommendations are worth highlighting:[389]

- An independent authority should be created, in collaboration with the industry, to oversee the development and deployment of the Open Banking Standard.

- The Open Banking API should be built as an open, federated and networked solution, as opposed to a centralized/hub-like approach. This approach echoes the design of the Web itself and enables far greater scope for innovation.[390]

- Customer transaction data (data that is presented to customers in their financial statements, including underlying transaction history, and data that relates to a customer's account through which

[388] Id., p. 5.
[389] Id., pp. 5-6.
[390] Id., p. 5. See, also, Open Data Institute (ODI), *Introducing the Open Banking Standard. Helping Customers, Banks and Regulators Take Banking into a Truly 21st-Century, Connected Digital Economy*, cit., p. 9 (explaining that "[b]arriers to participation will be kept deliberately low to cultivate an engaged developer community.").

payments can be initiated) should be made available, with consent, via the Open Banking API as both customer-related data and aggregated data.[391]

- Protocols should be developed and shared with all participants in the Open Banking Standard to ensure that redactions in data that is shared via the open APIs are truly exceptional, based on specific risk considerations. Further work should be undertaken to explore the extent of redaction and what alternatives may be available.

- As a principle, existing standards, datasets and structures should be reused where possible and appropriate.

- The Open Banking Standard should be managed within a transparent and open governance framework that will support accessibility, usability and innovation.

- An Independent Authority should be established, whose scope would include consideration of how complaints are handled, how data is secured once shared, as well as the security, reliability and scalability of the APIs provided.

- The Independent Authority would vet third parties, accredit solutions and publish its outcome through a whitelist of approved third parties.

- Customers (individuals and businesses) of services built through the Open Banking Standard would need to understand their responsibility for ensuring their data is protected. When issues arise between participants, third parties and data attribute providers would be expected to resolve these quickly. Where customers are affected they should be able to contact either their third party or data attribute provider to initiate this process. Where issues are not resolved within a specific time period, participants should be able to escalate them to the Independent Authority, which would make a ruling as to whether standards have been breached.

- The Open Banking Standard should have a clear and explicit versioning policy and procedure and use an open repository to maintain and manage changes.

- The Open Banking Standard should be made available under a license that permits it to be freely used, reused, and distributed.[392]

- Permission to access data should only be granted on the basis of informed customer consent and be subject to constraints (e.g. duration or transaction size); and the customer (or, if required for objective reasons, the data attribute provider) should be able to revoke such permission as easily as it granted it.

---

[391] See, Open Banking Working Group (OBWG), *The Open Banking Standard. Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation*, cit., p. 17 ("Aggregated data" in this context is defined as "[s]ets of averaged or aggregated data across transactions, balances, other customer data or open data sources." Examples of aggregated data include average number of cash withdrawals per month across a postcode area, successful lending applications by businesses within a SIC code, etc. Any personal data that is released as open data would need to be annonymized and made unable to be de-annonymised.).
[392] Id., p. 26.

- Permission to both "read" and "write" certain data should be granted to third parties via an open API.[393]

- A control framework should be implemented to address the risk profile to set reasonable Open Banking Security Standards in such a way that allows flexibility for future threats and technical flexibility to allow innovation in implementation of the controls.

The recommendations set forth in the OBWG Open Banking Standard Report include a broad implementation plan, covering three distinct phases over the period between 2016 and 2019.[394] The implementation is expected to follow the release schedule below:

- Release 1 (To be completed within 12 months of the OBWG Open Banking Standard Report publication) – Delivery of a "minimum viable product" (MVP) including: 1) the establishment of required governance entities (and their initial scope and processes); and 2) the launch of a tightly scoped Open Banking API, enabling select, read-access, open data use cases (e.g., branch location and hours, ATM locations, etc.).

- Release 2 (To be completed by end of Q1 2017) – Extension through implementation of select, read-access capability for customer transaction data. By this release's conclusion, third parties would be able to access the midata personal customer data sets via the Open Banking API on a read-only basis.

- Release 3 (To be completed by end of Q1 2018) – Significant build-out of governance entities and further development of the Open Banking API to cover the majority of use cases supported by open data and anonymized and aggregated data. Similar functionality outlined in Release 2 to be provided for midata business customer data sets, as well.

- Release 4 (To be completed by end of Q1 2019) – All recommendations to be implemented by this stage. This release would deliver full read and write functionality under the Open Banking Standard as per its target scope.

4.A.iii. Implementation of the Open Banking Standard

The OBWG Open Banking Standard Report discussed in the prior section has placed the UK in a very strong position. Indeed, other countries in Europe and beyond have only recently begun to implement aspects of an Open Banking standard, but none of them has produced a definitive outline of such a standard nor it has defined a clear roadmap for its implementation as the one outlined by the OBWG. As a result, there is now a significant opportunity for the UK to take the lead in Open Banking and to drive the development of similar international Open Banking standards.

---

[393] Id., pp. 18-19 ("read access" is defined as the "permission that is granted to a third party enabling them to read but not modify a file, set of files, or set of data"; while, "write access" refers to the "permission that is granted to a third party to modify or execute a file, set of files, and set of data. In the context of this report, write access includes payment initiation.").

[394] Id., pp. 6-7, 76-80 (explaining that "[t]he recommendations made in this report should be implemented without undue delay. However, there will not be a single API – there will be many, and the standard envisioned by this report will emerge continuously, through an iterative process, rather than a single event.").

In addition, by building on the Open Banking Standard framework discussed above, the OBWG is expected to set precedents for other sectors and to pave the way for similar open frameworks to be developed across various industries. This, in turn, would give the UK the opportunity to take the lead in open innovation across a number of different industries, thus strengthening its economy and giving it a continued advantage over other countries.[395]

A few months after the publication of the OBWG Open Banking Standard Report, in August 2016, the Open Data Institute (ODI)[396] announced the launch of an Open Banking Development Group (OBDG) to drive innovation around an Open Banking standard, on a UK and international basis.[397] The OBDG builds on the work carried out by the OBWG and extends it by creating a global community open to everyone - including large banks, smaller challenger banks, fintech companies, data aggregators, privacy groups, consumer advocacy groups and individuals - to work together to build an open future for banking.[398] The launch of the OBDG has been welcomed by the nine UK banks mentioned in the CMA Final Report on its retail banking investigation discussed below[399] and the ScaleUp Institute.[400]

Going forward, the OBDG is expected to play an important role in shaping any Open Banking initiatives in the UK, including any regulatory developments, such as the implementation of the EBA RTS on SCA and CSC (discussed in the prior chapter) and the UK CMA's final retail banking remedies (discussed in the following sections).

4.B. The UK Competition and Markets Authority (CMA)

4.B.i. The CMA's Retail Banking Markets Investigation and Final Report

On 6 November 2014, the UK Competition and Markets Authority (CMA) board launched a market investigation into the supply of retail banking services to personal current account (PCA) customers and to

[395] See, Open Data Institute (ODI), *Introducing the Open Banking Standard. Helping Customers, Banks and Regulators Take Banking into a Truly 21st-Century, Connected Digital Economy*, cit., p. 7.
[396] The Open Data Institute (ODI) is a non-partisan, not-for-profit organization that connects, equips, and provide guidance to people around the world to innovate with data. In 2015, the ODI co-chaired the OBWG initiated by the HMT.
[397] See, Open Data Institute (ODI), *Announcing the Open Banking Development Group*, Open Data Institute Press Release (August 2, 2016).
[398] As an open standards project, participation (e.g. mailing lists, contributions to GitHub, etc) in the OBDG is open to anyone for free. Patrons, sponsors, and members of the OBDG receive additional benefits in return for a financial contribution. See, Open Banking Development Group (OBDG), *Open Banking Development Group Membership Details*, Open Banking Development Group (2016); Open Banking Development Group (OBDG), *Vision and Values*, Open Banking Development Group (2016).
[399] See, Open Data Institute (ODI), *Announcing the Open Banking Development Group*, cit. (quoting Paul Horlock (Chair, Implementation Entity Steering Group) commenting "[t]he ODI's expertise and knowledge of this growing sector will provide vital input as the work develops … AIB Group, Bank of Ireland, Barclays, Danske, HSBC Group, Lloyds Banking Group, Nationwide, RBS Group and Santander are currently working together to create the Implementation Entity that will deliver an open API standard, open data and data sharing. The institutions believe strong stakeholder engagement is critical to ensuring the successful delivery of this work in an open and transparent process, part of which will be working with the Implementation Trustee once appointed, to ensure the appropriate governance is in place for this to happen effectively.").
[400] Ibidem (quoting Irene Graham (CEO, Scale-Up Institute) stating "[t]he Scale-Up Institute welcomes this collaborative initiative to drive forward financial services innovation to the benefit of consumers and place the UK at the leading edge of open data standards in banking, which should enable further growth opportunities across sectors … Working together, the banking, fintech and consumer communities can achieve real step change. We look forward to the developments this initiative will bring.").

small and medium-sized enterprises (SMEs) in the UK. An inquiry group of five independent members was formed to conduct the investigation and, then, collect the findings of the investigation in a final report.[401]

The CMA released the final report on its retail banking investigation ("CMA Final Report") on 9 August 2016.[402] The CMA Final Report identifies a number of positive developments, including the following: entry by new banks; adoption by some new entrants of new business models; offering specialist products and exploiting opportunities offered by new technologies (e.g., digital-only banks); rapid wide spread adoption of mobile banking; and introduction of new types of payment services. Despite these positive developments, the CMA Final Report also highlights a number of problems. In particular, the CMA Final Report notes that older and larger banks, which still account for the large majority of the retail banking market, do not have to compete hard enough to win and retain customers and that it is difficult for new and smaller providers to attract customers. These shortcomings have a significant negative effect on customers, particularly overdraft users and smaller business. They mean that many people are paying more than they should and are not benefiting from new services. They, also, mean that the market is still not as innovative or competitive as it needs to be.[403]

To tackle the described problems, the CMA concluded that a far-reaching package of reforms should be imposed. Central to the proposed reforms are measures to ensure that personal and small business customers benefit from technological advances and that new entrants and smaller providers are able to compete more fairly.[404]

More specifically, in the CMA Final Report, the CMA announced the adoption of the following three foundation remedies:

- Open Banking Standard – In an effort to accelerate technological change in the UK retail banking sector,[405] the CMA announced that the nine banks in Great Britain and Northern Ireland with the largest

[401] The members of the Retail Banking Market Investigation Group are Professor Alasdair Smith, Professor Tom Hoehn, Professor Philip Marsden, Jill May, and Ed Smith. Members' biographies are published on the CMA's website.

[402] See, Competition and Markets Authority (CMA), *CMA Paves the Way for Open Banking Revolution*, Competition and Markets Authority Press Release (August 9, 2016); Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Final Report*, Competition and Markets Authority (August 9, 2016); Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Final Report Corrigendum*, Competition and Markets Authority (August 11, 2016); Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Summary of Final Report*, Competition and Markets Authority (August 9, 2016); Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Overview*, Competition and Markets Authority Press Release (August 9, 2016); Competition and Markets Authority (CMA), *Making Banks Work Harder for You*, Competition and Markets Authority (August 9, 2016).

[403] See, Competition and Markets Authority (CMA), *Making Banks Work Harder for You*, cit., p. 6 (arguing that "the fundamental problem is that even when new entrants and smaller banks introduce competitive products it takes a long time to build customer numbers. The remedies we are introducing will enable customers to be more responsive and reduce the advantages of the existing banks. They will also provide stronger incentives on all banks to compete and make the market more attractive to new banks and other providers, as well as facilitating innovation.").

[404] See, Competition and Markets Authority (CMA), *CMA Paves the Way for Open Banking Revolution*, cit. (quoting Alasdair Smith, Chair of the Retail Banking Investigation, commenting "[t]he reforms we have announced today will shake up retail banking for years to come, and ensure that both personal customers and small businesses get a better deal from their banks. We are breaking down the barriers, which have made it too easy for established banks to hold on to their customers. Our reforms will increase innovation and competition in a sector whose performance is crucial for the UK economy. Our central reform is the Open Banking programme to harness the technological changes, which we have seen transform other markets.").

[405] See, Competition and Markets Authority (CMA), *Making Banks Work Harder for You*, cit., p. 6 (observing that "Open APIs can transform the financial services sector. There is already a very active and growing FinTech community, which has been developing and introducing new products using existing digital technology. Requiring the banks to adopt and maintain a common open standard

market share[406] would be required to develop and implement and open API standard, which will permit authorized intermediaries to access, subject to the required consents, data about bank services, prices, service quality, and customer usage. As the nine largest banks in Great Britain and Northern Ireland have a dominant aggregated market share, this foundation measure will create a *de facto* mandatory standard for the UK marketplace. The development and implementation of this measure is, thus, expected to enable new services tailored to the specific needs of customers delivered securely and confidentially. Customers, in turn, will benefit from a broader range of innovative services and will be able to (re)gain control over their finances.[407]

In announcing this foundation measure, the CMA has drawn directly on the work of the OBWG discussed in the prior section.[408] To ensure that enough time is available to work through the details of this foundation measure, the CMA has required that the release of information and data thereunder be phased-in: the least sensitive information (e.g., banks' prices, terms and conditions (T&Cs), and branch location) to be made available by the end of March 2017; while all other aspects of the Open Banking standard to be finalized and implemented by early 2018.[409]

- Service Quality Information – The CMA announced a second foundation measure, aiming at providing customers with much better information on service quality. To that end, all providers of personal current accounts (PCAs) or business current accounts (BCAs) (or both) in Great Britain and Northern Ireland would be required to publish core indicators of service quality based on customers' willingness to recommend their bank to friends, family or colleagues. Moreover, the providers would have to collect and publish a wider range of additional quality measures.

- Customer Prompts – As a third foundation measure, the CMA announced that all providers of PCAs or BCAs (or both) in Great Britain and Northern Ireland would be required to send out suitable periodic "prompts" (e.g., a reminder included in an annual statement) and event-based "prompts" (e.g., in the event of closure of a local branch or increase in charges) to remind their customers to review their arrangements, see whether they are getting the best value, and switch banks if they do not.

---

will accelerate the pace of this change. Without our intervention, the process of developing open APIs cannot be guaranteed and could take a long time, with the effect of denying customers the early benefits of these new services. We are therefore also imposing a challenging, but realistic, timeframe on banks for this process.").

[406] These banks are Lloyds Banking Group plc (LBG), Royal Bank of Scotland Group plc (RBSG), HSBC Group (HSBCG), Barclays Bank plc (Barclays), Nationwide Building Society (Nationwide), and Santander UK plc (Santander) in Great Britain, and Allied Irish Bank (AIB), Bank of Ireland (UK) plc (BoI), and Northern Bank Limited trading as Danske Bank (Danske) in Northen Ireland.

[407] See, Competition and Markets Authority (CMA), *Making Banks Work Harder for You*, cit., pp. 6-8 (noting that "[t]he types of new and improved services that will result from this remedy include applications which: a. Allow banking customers, through a single application, to manage accounts held with several providers; b. Allow customers to authorize the movement of funds between current and deposit accounts to help avoid overdraft charges or to benefit from higher interest payments; Let customers make simple, safe and reliable price and service quality comparisons tailored to their own usage patterns; d. Monitor a current account and forecast a customer's cash flow, helping to avoid overdraft charges; e. Use a small business's transaction history to allow a potential lender other than their bank to reliably assess the business's creditworthiness and offer better lending deals than they would without this information.").

[408] See, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Final Report*, cit., pp. 446-447. The recommended API will use the Open Banking Standard framework, developed by the OBWG.

[409] The second stage of the implementation process of Open Banking Standard is aligned to the upcoming EU PSD2. See below for further discussion on this point.

In addition to the three foundation remedies discussed above, the CMA announced that a series of measures targeting more specific aspects of the banking market would also be imposed. These measures include the following:

- Current Account Switching - The CMA announced a set of measures to make current account switching work better, including building on and improving the existing current account switch service.[410] For example, the CMA required that customers of all current account providers in Great Britain and Northern Ireland be able to get a copy of their transaction history after account closure; and that BCA providers in Great Britain and Northern Ireland adopt a core set of standard information and evidence requirements for opening a BCA.

- PCA Overdrafts – Further measures were announced targeting unarranged overdraft PCA users, a group of customer that makes up approximately 25% of all PCA customers and has suffered particularly from the competition failures in the PCA market.[411] The goal of these measures is to enable personal customers to take more control over their use of overdraft services, as well as to improve the switching process for these customers. To this end, the CMA announced that all providers of PCAs in Great Britain and Northern Ireland would be required to: send alerts (e.g., by txt message) to customers going into unarranged overdraft; inform them though the alert of a grace period during which customers have an opportunity to avoid charges; and set a monthly cap on unarranged overdraft charges, and notify their customers about it.

- Needs of Small Business – Through its investigation, the CMA found that small businesses lack tools providing comprehensive information about what different banks can offer them in terms of charges, service quality, credit availability etc. To address these challenges, the CMA decided to support the Open Up Challenge run by innovation charity Nesta, which seeks to enable the development and delivery of comparison and advice services. In addition, the CMA announced a set of measures aimed at enhancing SME access to information through new comparison tools and requiring banks to offer an indicative price quote and eligibility indicator tool and to agree and adopt a core set of standards for SMEs opening a BCA and additional published information.

[410] See, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Final Report*, cit., p. xi, xiii, xxiii, xxxix-xl, 158-159, 166 (noting that only 3% of personal and 4% of business customers switch to a different bank in any year. This is despite many personal customers, in particular overdraft users, could make significant savings by switching to a different current account. For example, personal customers in Great Britain being able to save £92 on average per year by switching provider, with savings of around £80 a year on average available for small businesses. Larger savings are available for overdraft users – for example, personal customers who are overdrawn for one or two weeks every month could save £180 per year on average). See, also, Competition and Markets Authority (CMA), *Making Banks Work Harder for You*, cit., p. 9 (observing that "[m]any personal and small business customers would benefit from switching banks but they need to have confidence in the switching process. The risk of something going wrong is of particular concern to those small businesses which make or receive many payments directly to their bank account.").

[411] See, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Final Report*, cit., p. 431 (noting that banks make £1.2 billion a year from unarranged overdraft charges.).

4.B.ii. The CMA's Retail Banking Markets Investigation Order

On 23 November 2016, the CMA published a notice of its intention to make an order as part of a package of measures to remedy, mitigate and prevent the adverse effects on competition and any resulting customer detriment, as identified in the CMA Final Report discussed above. [412]

The CMA, then, opened a consultation on a draft order and a draft explanatory note for the implementation of the remedies set out in the CMA Final Report.[413] The consultation closed on 23 December 2016 and the final order ("CMA Final Order") and final explanatory note ("CMA Final Explanatory Note") were issued on 2 February 2017.[414] During the consultation phase, the CMA received 26 submissions relating to the draft order and the draft explanatory note.[415]

The CMA Final Order formally implements the reforms outlined in the CMA Final Report and sets out a strict timetable for the introduction of key measures, including: Open Banking-related measures; a monthly maximum unarranged overdraft charge; standardized business current account opening procedures; and the publication of service quality statistics.[416] Among them, the Open Banking-related measures are of particular interest.

In more details, the provisions relating to Open API standards and data sharing are set forth in Part 2 of the CMA Final Order. Article 10.1 of the CMA Final Order provides for the creation of an implementation entity ("Implementation Entity") [417] to be headed by an independent implementation trustee ("Implementation Trustee"), who will be accountable to the CMA.[418] The Implementation Entity will develop read-only open and common technical and product data standards (specified in Articles 12 and 13

---

[412] See, Competition and Markets Authority (CMA), *Retail Banking Market Investigation – Retail Banking Market Investigation Order 2017. Notice of Intention to Make an Order under Sections 161 And 165 of, and Schedule 10 to, the Enterprise Act 2002 and Public Consultation on the Draft Order*, Competition and Markets Authority (November 23, 2016).

[413] See, Competition and Markets Authority (CMA), *Open Banking Transformation Moves a Step Closer*, Competition and Markets Authority Press Release (November 23, 2016); Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Draft Order – Consultation. The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (November 23, 2016); Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Draft Explanatory Note. The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (November 23, 2016).

[414] See, Competition and Markets Authority (CMA), *Open Banking Revolution Moves Closer*, Competition and Markets Authority Press Release (February 2, 2017); Competition and Markets Authority (CMA), *Retail Banking Market Investigation - Retail Banking Market Investigation Order 2017. Notice of Making an Order Under Sections 138 and 161 of the Enterprise Act 2002 Issued under Section 165 of, and Schedule 10 to, the Enterprise Act 2002*, Competition and Markets Authority (February 2, 2017); Competition and Markets Authority (CMA), *Retail Banking Market Investigation: The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (February 2, 2017); Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (February 2, 2017); Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Final Order Corrigendum*, Competition and Markets Authority (February 28, 2017).

[415] Non-confidential versions of the responses received are published on the CMA's website at: www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk. See, also, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Summary of Responses to the Consultation on the Draft Retail Banking Market Investigation Order and Explanatory Note*, Competition and Markets Authority (February 2, 2017) (discussing some of the main points raised in response to the consultation.).

[416] More precisely, the package of remedies outlined in the CMA Final Report are implemented by: (a) the Final Order; (b) undertakings entered into by Bacs Payment Schemes Limited; and (c) recommendations to HM Treasury, the Department for Business, Energy and Industrial Strategy, and the Financial Conduct Authority.

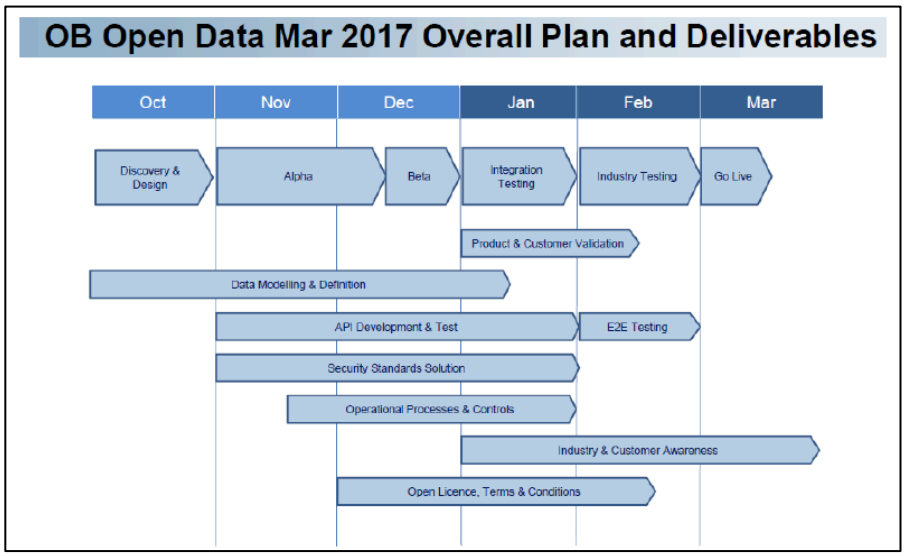
[417] See, Article 10.1 of the CMA Final Order. See, also, Article 10.3 of the CMA Final Order (the composition, governance arrangements, budget and funding for the Implementation Entity (the "Agreed Arrangements") shall be those proposed by the nine banks in Great Britain and Northern Ireland with the largest market share that are subject to the Final Order; and shall be mandated by the CMA, as set out in Part A of Schedule 1 to the Explanatory Notes.).

[418] See, Articles 10.5, 11.1 to 11.6 of the CMA Final Order (setting out the process for the appointment and possible replacement of the Implementation Trustee).

of the CMA Final Order) and read and write, open and common banking standards for the secure sharing of transaction data (as specified in Article 14 of the CMA Final Order). The read-only data standard and read/write data standard will include provisions relating to an Open API standard, data format standards, security standards, governance arrangements, and customer redress mechanisms for the read/write data standard.[419] As expressly required in the CMA Final Order, neither the read-only data standard nor the read/write data standard shall include provisions that are incompatible with PSD2 requirements.[420]

Schedule 1 – Part B attached to the CMA Final Explanatory Note sets forth the agreed timetable and project plan for the implementation of Open API standards and data sharing, as illustrated in the Figure 12(a) and Figure 12(b) below:

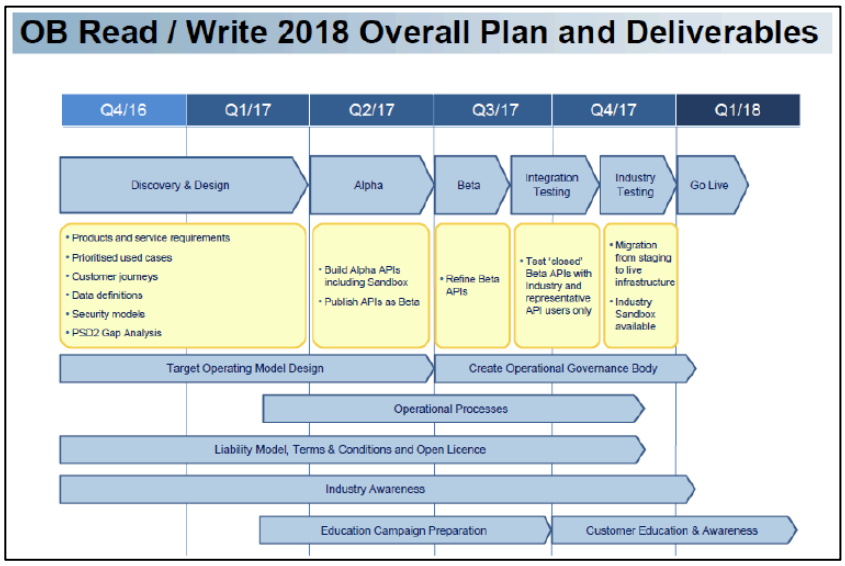
Figure 12(a). Open Banking Open Data March 2017 Overall Plan and Deliverables



Source: Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (February 2, 2017), p. 42.

[419] See, Article 10.2 of the CMA Final Order.
[420] Ibidem. See, also, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, cit., Schedule 1 – Part A, paragraphs 15-16.

Figure 12(b). Open Banking Read / Write 2018 Overall Plan and Deliverables



Source: Id., p. 43.

Article 12.1 of the CMA Final Order[421] further requires the nine banks in Great Britain and Northern Ireland with the largest market share (LBG, RBSG, HSBCG, Barclays, Nationwide, Santander, AIB, BoI, and Danske) to release and make continuously available[422] without charge and without any restriction as to its use, in accordance with the read-only data standard:

(1) Reference information (including, all branch and business center locations; all branch opening times; all ATM locations; and any other reference information reasonably stipulated by the Implementation Trustee and agreed by the CMA); and

(2) Product information, before the application of any negotiated changes, for each of their on-sale PCA products,[423] BCA products[424] and SME lending products,[425] which shall include, where relevant: (a)

[421] See, Article 12.1 of the CMA Final Order. See, also, Article 12.2 of the CMA Final Order (providing that the list set forth in Article 12.1 is subject to any further information the Implementation Trustee considers necessary for the effectiveness of the remedy, in which case the Implementation Trustee will seek approval from the CMA to expand the scope of the product and reference data.).
[422] See, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, cit., p. 11, paragraph 36 (explaining that the reference to "continuously available" in Articles 12 to 14 of the Final Order means that "providers are required to publish information on an ongoing basis from the date the relevant Article comes into force.").
[423] See, Article 12.4.1 of the CMA Final Order (providing that for the purposes of Article 12, "PCA products" include: (a) any PCA whether or not it includes an overdraft facility; (b) Basic Bank Accounts (that is, a payment account with basic features as defined by Regulation 19(1) of PAR); (c) packaged accounts; (d) reward accounts; (e) student or graduate accounts; (f) youth accounts; and (g) any other product reasonably specified by the Implementation Trustee provided it falls within the Terms of Reference of the CMA's retail banking market investigation and the adverse effects on competition identified and has been agreed by the CMA.).
[424] See, Article 12.4.2 of the CMA Final Order (providing that for the purposes of Article 12, "BCA products" include: (a) BCAs; (b) standard tariff unsecured business overdrafts; and (c) any other product reasonably specified by the Implementation Trustee provided it falls within the Terms of Reference of the CMA's retail banking market investigation and the adverse effects on competition identified and has been agreed by the CMA.).
[425] See, Article 12.4.3 of the CMA Final Report (providing that for the purposes of Article 12, "SME lending products" include: (a) commercial credit cards (meaning credit cards intended for use by SMEs for business purposes); (b) unsecured loans up to a value of £25,000; and (c) any other product reasonably specified by the Implementation Trustee provided it falls within the Terms of Reference of the CMA's retail banking market investigation and the adverse effects on competition identified and has been agreed by the CMA. Article 12.4.3 further provides that for the purposes of Article 12, "SME lending products" do not include: (d) charge cards (meaning

product prices, which may include credit interest; (b) all charges, including the interest rates (credit and debit) which apply to the product, the fees and charges which may apply to activity on the account, and the circumstances in which these charges apply; (c) features and benefits, including credit interest and constituent parts of packaged accounts; (d) MMC once MMCs have been introduced in accordance with Part 7 of the CMA Final Order; (e) terms and conditions; (f) customer eligibility criteria; and (g) any other product information reasonably required by the Implementation Trustee and agreed by the CMA.

Article 13 of the CMA Final Order[426] provides that the nine banks in Great Britain and Northern Ireland with the largest market share (LBG, RBSG, HSBCG, Barclays, Nationwide, Santander, AIB, BoI, and Danske) must release and make continuously available,[427] without charge, in accordance with the read-only data standard:

(1) Service quality indicators to be published and released under Article 15; and

(2) All underlying data anonymized generated from responses to survey questions (approved by the CMA in accordance with Article 16.1) to be made available in accordance with the read-only data standard unless the information has already been released in a manner consistent with the read-only data standard through other means (e.g. by the British Bankers Association (BBA) or the research company or companies undertaking the surveys). Such information may include survey results relating to providers who are not subject to Part 2 of the CMA Final Order.[428]

Article 14 of the CMA Final Order deals with the use of APIs for transaction data.[429] It requires the nine banks in Great Britain and Northern Ireland with the largest market share (LBG, RBSG, HSBCG, Barclays, Nationwide, Santander, AIB, BoI, and Danske) to make up to date PCA and BCA transaction data sets continuously available,[430] without charge, for: (1) read access in accordance with the relevant provisions of the read/write data standard; and (2) write access in accordance with the relevant provisions of the read/write data standard. Compared to Articles 12 and 13 discussed above, the provisions set forth in Article 14 of the CMA Final Order are less articulated, thus reflecting the need for the Implementation Entity and Implementation Trustee to provide the details of how such provisions are to be achieved and to identify the specific products within the scope of the remedy.[431] As clarified in the CMA Final Explanatory Note accompanying the CMA Final Order, the Implementation Entity and Implementation Trustee in

---

credit cards for use with an account which must be paid in full when a statement is issued and for which no interest is charged); (e) enterprise finance guarantee loans; (f) managed loans; (g) partnership capital loans; (h) property development loan; (i) commercial mortgages (meaning any SME lending product secured by a charge over land); and (j) investment property loans.).

[426] See, Article 13 of the CMA Final Order.

[427] See, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, cit., p. 11, paragraph 36.

[428] See, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, cit., p. 11, paragraph 34 (explaining that the underlying data "will likely be in database format to an agreed specification, which preserves respondent anonymity. It is envisaged that data will be made available for each brand subject to Part 3. Therefore while the obligation to release this data only applied to providers subject to Part 2, the various databases released will include granular data for all brands included in the surveys.").

[429] See, Article 14 of the CMA Final Order.

[430] See, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, cit., p. 11, paragraph 36.

[431] Id., p. 11, paragraph 35.

taking forward this measure will need to consider the wider context of PSD2 implementation and to give particular attention to the views of PSPs subject to PSD2.[432]

Additional provisions set forth in Part 3 of the CMA Final Order are also relevant for Open Banking Standard and data sharing. In particular, Article 15 of the CMA Final Order requires all providers of PCAs or BCAs (or both) in Great Britain and Northern Ireland to publish, in relation to each of their brands to which Part 3 applies,[433] service quality indicators to show the willingness of their PCA customers, who have used the account or a relevant service in a defined period prior to the survey taking place, to recommend to friends and family: (1) the brand; (2) the brand's online and mobile banking services; (3) the brand's branch services; and (4) the brand's overdraft services.[434] All providers of PCAs or BCAs (or both) in Great Britain and Northern Ireland must also publish, in relation to each of their brands to which this Part 3 applies, service quality indicators showing the willingness of their BCA customers, who have used the account or relevant service in a defined period prior to the survey taking place, to recommend to other SMEs: (1) the brand; (2) the brand's relationship/account management; (3) the brand's online and mobile banking services; (4) the brand's branch and business centre services; and (5) the brand's credit (overdraft and loan) services.[435]

All the service quality indicators set out in Article 15 of the CMA Final Order must be generated from data collected in accordance with Article 16 the CMA Final Order and must be published in accordance with Article 17 of the CMA Final Order (to be read alongside Schedule 2 to the CMA Final Explanatory Note).[436] Article 13 in Part 2 of the CMA Final Order discussed above is also relevant to this remedy as it sets forth the mechanism for the release of underlying granular details (unless this information is made available by other means).

With respect to the timeline for implementation of this measure, Article 15.4 of the CMA Final Order provides that all providers of PCAs or BCAs (or both) in Great Britain and Northern Ireland must publish the first set of service quality indicators as set forth under Article 15 on 15 August 2018 falling six weeks after all the data, incorporating results from October 2017 (at the latest) to June 2018, has been collected.[437] Thereafter, the service quality indicators must be updated on the first working day after 14 February and 14 August each year, based on data collected on a rolling basis over the 12 months from, respectively: (1) the beginning of January to the end of December of the previous calendar year; and (2) the beginning of July to

[432] Id., p. 11, paragraph 38; and p. 41, Schedule 1 Part A - Agreed Arrangements, paragraphs 15 to 16.
[433] See, Article 9.1 of the CMA Final Order (defining "brand" as "the name or image that links PCAs, BCAs, or SME Lending products (and possibly other products and services) provided by a single Provider under that name or image together for the purposes of providing a common identity for marketing and other purposes").
[434] See, Article 15.1 of the CMA Final Order.
[435] See, Article 15.2 of the CMA Final Order.
[436] See, Article 15.3 of the CMA Final Order.
[437] See, Article 15.4 of the CMA Final Order. See, also, Competition and Markets Authority (CMA), Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017, Competition and Markets Authority (February 2, 2017), paragraph 43 at p. 13 (clarifying that "[t]he flexibility of collecting data for the first publication over a shorter period does not mean that it would be acceptable for those indicators to be based on a sample size smaller than that used for future indicators.").

the end of June incorporating six months of results from the previous calendar year and six months from the prevailing calendar year.[438]

4.B.iii. Implementation of the CMA's Retail Banking Markets Investigation Order

The process of implementation of the Open Banking related remedies set out in the CMA Final Report discussed above started in 2016. As a precursor to creating the Implementation Entity, the nine banks in Great Britain and Northern Ireland with the largest market share (LBG, RBSG, HSBCG, Barclays, Nationwide, Santander, AIB, BoI, and Danske) formed an initial Open Banking Implementation Entity Steering Group in July 2016. Payments UK[439] provided support by acting as Secretariat to the initial Open Banking Implementation Entity Steering Group and by facilitating the necessary engagement with all appropriate stakeholders.[440] As part of its role of providing support and acting as Secretariat, Payments UK also made available the minutes of the initial Open Banking Implementation Entity Steering Group on its website.[441]

The initial Open Banking Implementation Entity Steering Group started seeking expertise and insights from a broad range of stakeholders, including consumer and SME representative groups, representatives from financial institutions and payment service providers, representatives from the fintech sector, as well as various advisory groups. Regular updates on the progress of the activities conducted by the initial Open Banking Implementation Entity Steering Group were published on Payments UK's website.[442]

As one of its activities, the initial Open Banking Implementation Entity Steering Group hosted an opening Stakeholder Event in London on 7 September 2016.[443] The views, opinions, and insights shared at the event helped form a rounded view of what's needed to deliver the Open Banking API standard to best serve individual and businesses customers, industry, and all other organizations involved in its delivery and use.

In September 2016, Open Banking Ltd – the Implementation Entity mandated by the CMA Final Order – was set up to develop the Open Banking API standards and frameworks. On 31 October 2016, Andrew

---

[438] Ibidem.

[439] Payments UK is the trade association launched in June 2015 to support the rapidly-evolving payments industry. It brings its members and wider stakeholders together to make the UK's payment services better for customers and to ensure UK payment services remain world class. All nine banks in the Great Britain and Northern Ireland with the largest market share, which are subject to the CMA Final Order, are members of Payments UK. Since 1 July 2017, a new trade association - UK Finance - represents the finance and banking industry operating in the UK. UK Finance represents around 300 firms in the UK providing credit, banking, markets and payment-related services. The new organization takes on most of the activities previously carried out by the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association. Content and updates from UK Finance are available on its website at www.ukfinance.org.uk.

[440] Payments UK has played an important role in helping a number of Open Banking initiatives get off the ground in the UK and in supporting their ongoing development. To date this has included supporting the industry's development of the Open Banking Standard report for HM Treasury discussed above; acting as Secretariat to the IESG; and working as official representative of PSD2 stakeholders on the Open Banking IESG.

[441] The minutes of the Steering Group Meetings are published on Payments UK'w website at: https://www.paymentsuk.org.uk/policy/payments-CMA-remedy-phase1/temporary/minutes-steering-group-meetings.

[442] During the initial phase, an interim website for the Implementation Entity was hosted by Payments UK on its website at: http://www.paymentsuk.org.uk/policy/payments-CMA-remedy-phase1/temporary. A new website for the Implementation Entity was launched in February 2017 and it is now available at https://www.openbanking.org.uk.

[443] See, Implementation Entity Steering Group (IESG), *Stakeholder Event: Developing An Open API Standard*, *Open Data and Data Sharing Out of the CMA Market Investigation – An Early Opportunity to Share Views, Thinking and Progress to Date. Event Summary*, Implementation Entity Steering Group (September 7, 2016) (providing a brief summary of the event, highlighting the key points and comments made by the panelists, and discussing some of the key questions asked by the delegates).

Pinder CBE (a former government consultant with extensive experience working in senior tech roles in the financial services sector) was appointed as Implementation Trustee, leading the work with responsibility to deliver the open API standard for banking set out in the CMA Final Report and Final Order.[444] On 13 April 2017, Imran Gulamhuseinwala (London-based partner in EY's financial services practice and its Global Head of Fintechs) succeeded Andrew Pinder CBE as Implementation Trustee.[445]

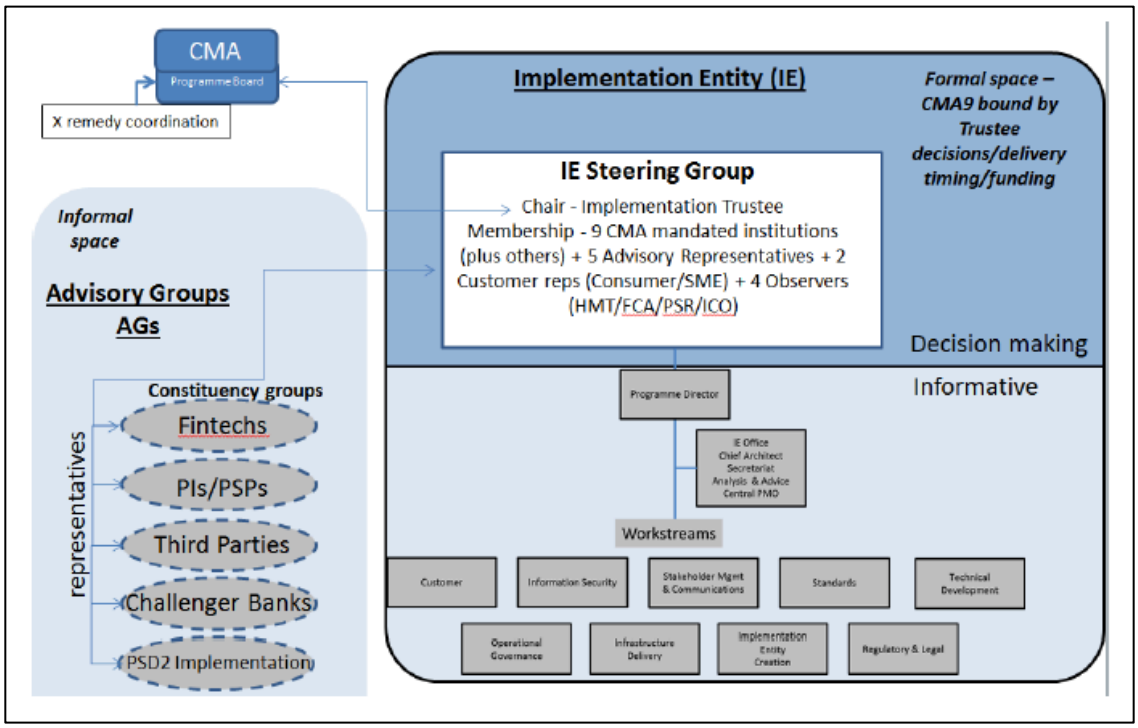
As illustrated in Figure 13 below, the Implementation Trustee is supported to take fast and agile decisions through an Implementation Entity Steering Group (IESG), which he chairs. The Implementation Entity Steering Group (IESG) comprises of one representative from each of the nine largest banks in Great Britain and Northern Ireland subject to the CMA mandate (LBG, RBSG, HSBCG, Barclays, Nationwide, Santander, AIB, BoI, and Danske), five representatives responsible for convening the Advisory Groups,[446] two customer representatives (one consumer, one small business), and four observers - one each from HM Treasury, the Payment Systems Regulator (PSR), the Financial Conduct Authority (FCA), and the Information Commissioners' Office.

[444] See, Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Implementation Trustee Appointed to Lead Open Banking Revolution*, Open Banking Limited Press Release (October 31, 2016).

[445] See, Open Banking Limited (Open Banking Implementation Entity (OBIE)), *CMA Appoints New Trustee for Open Banking Implementation Entity*, Open Banking Limited Press Release (April 13, 2017); Competition and Markets Authority (CMA), *Imran Gulamhuseinwala appointed Open Banking Implementation Trustee*, Competition and Markets Authority Press Release (April 13, 2017).

[446] Four advisory groups ("Advisory Group") have been established, which are open to all interested parties to help shape the development of the standards: Fintechs; PIs/PSPs; Third Party Providers; Challenger Banks; PSD2 Implementation. On 15 December 2016, the following Advisory Groups Convenors were named: Gavin Littlejohn (Chairman of a fintech trade association and CEO at Money Dashboard), to convene the fintech Advisory Group; Ian Major (Director at Runpath), to convene the third party providers Advisory Group; Thaer Sabri (CEO at Electronic Money Association), to convene the PIs/PSPs Advisory Group; and James Whittle (Director at Payments UK), to convene the PSD2 Implementation Advisory Group. See, Open Banking Limited (Open Banking Implementation Entity (OBIE)), Open Banking Advisory Group Heads Named, Open Banking Limited Press Release (December 15, 2016). Mark Mullen (CEO at Atom Bank) was named Challenger Banks Advisory Group Convenor on 30 June 2017. See, e.g., Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Atom Bank CEO Joins Open Banking Initiative as Challenger Bank Representative*, Open Banking Limited Press Release (June 30, 2017). The Advisory Group heads are called to represent the views of their constituency and assist the Implementation Entity to bring qualified experts into the work streams, ensuring the representation of stakeholders' views in the programme of work.

Figure 13. Implementation Entity (IE) – Governance and Composition



Source: Implementation Entity Steering Group (IESG), *Update to CMA – Executive Summary*, Implementation Entity Steering Group (October 2016), p. 4.

As previously discussed, the Open Banking delivery is split between two key deadlines:

- March 2017, being focused on Open Data, making available information on ATMs, branches, PCAs, BCAs (for SMEs) and SME unsecured lending and commercial credit cards.
- January 2018, which is aligned to the upcoming EU PSD2, when authorized third parties can be given consent by the account holder to access their bank accounts to extract statement information and to initiate payments.

The Implementation Entity Steering Group (IESG) has openly recognized the complexities involved in the process of implementation of these measures. In the updated submitted to the CMA in October 2016, it noted that "[i]n considering the approach to reference and product information, our initial analysis has identified a lack of suitable open standards. We will therefore need to establish the standards from the ground up."[447]

Furthermore, the Implementation Entity Steering Group (IESG) warned that "[t]he delivery of the initial API standard by Q1 2017 will be challenging. For example, considerable detailed legal and technical work

[447] See, Implementation Entity Steering Group (IESG), *Update to CMA – Executive Summary*, Implementation Entity Steering Group (October 2016), p. 2. See, also, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (February 2, 2017), Schedule 1 – Part A, paragraphs 17-18 (discussing the need to see the implementation process for the CMA's remedies in a wider context and to coordinate such process with a number of Open Banking related initiatives, including the OBWG's Open Banking report).

will be required to agree precisely the personal current account (PCA) and business current account (BCA) products and data that are in scope."[448] It, then, warned that "[t]he sharing of customer transaction data is much more complex. It requires, for example, robust security arrangements and identity management to protect this far more sensitive information. These protections will need to consider both the General Data Protection Regulations (GDPR)[449] and the 4th Anti-Money Laundering Directive [450]."[451]

Finally, the Implementation Entity Steering Group (IESG) acknowledged a need to coordinate the work performed in implementing the CMA's remedies discussed above with Open Banking initiatives at EU-level, significantly PSD2 and the EBA RTS on SCA and CSC. It stated "[t]o ensure an efficient outcome for customers, the APIs we develop will allow adopters to comply with the Payment Services Directive 2 (PSD2) requirements. We must seek to minimize the potential for any customer confusion that could arise in the absence of this constancy. We aim to establish a clear technical framework to facilitate the safe introduction of PSD2, without removing the ability for innovation at the edges. We will align write-functionality with the payment initiation services that apply under PSD2. The work programme will need to iterate with the clarification of standards for PSD2 and a specific Advisory Group will be set up to help achieve a successful outcome."[452] It further warned of potential difficulties ahead in aligning the two projects explaining that "[r]esolving the competing tensions across this complex regulatory landscape will be challenging, as there are obvious conflicts and contradictions that need to be balanced. To safeguard customers, it may be important to establish some kind of widely recognized "trust mark" that institutions participating in the Open Banking Service can display. This should be reinforced through a "white list" of certified participants available via the central registry. The central registry will also form the centre of the inter-institution trust model, required to ensure that technical measures can be implemented to minimize the risk of rogue parties attempting to impersonate institutions to defraud customers."[453]

Notwithstanding the described challenges, over the past five months Open Banking Ltd (the Implementation Entity) made significant progresses in the process of implementation of the CMA's remedies. In particular, on 13 March 2017, the nine banks in Great Britain and Northern Ireland with the largest market share (LBG, RBSG, HSBCG, Barclays, Nationwide, Santander, AIB, BoI, and Danske), through the work of the Open Banking Ltd (the Implementation Entity), delivered on the first of the CMA

[448] See, Implementation Entity Steering Group (IESG), *Update to CMA – Executive Summary*, cit., p. 3.
[449] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)).
[450] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (The 4th Anti-Money Laundering Directive). Although the 4th Anti-Money Laundering Directive has yet to be implemented, the EU has developed a proposal for a 5th Anti-Money Laundering Directive that will amend the 4th Anti Money Laundering Directive to target terrorist financing more effectively and prevent tax avoidance and money laundering through stricter transparency rules. At present, negotiations among the EU Commission, Parliament, and Council are ongoing.
[451] See, Implementation Entity Steering Group (IESG), *Update to CMA – Executive Summary*, Implementation Entity Steering Group (October 2016), p. 3.
[452] Ibidem.
[453] Ibidem, See, also, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, cit., Schedule 1 Part A - Agreed Arrangements, paragraphs 17-18.

remedies set out in the CMA Final Report and Final Order, with the release of a common accessible platform to provide standardized data on banking products, branches, and ATM location.[454]

Two months later, on 17 May 2017, Open Banking Ltd (the Implementation Entity) announced its collaboration with the OpenID Foundation's Financial API Working Group.[455] This partnership is expected to provide ongoing valuable support to ensure that the Open Banking ecosystem, both in the UK and internationally, sets a secure and solid benchmark for the future.[456]

Then, on 5 July 2017, Open Banking Ltd (the Implementation Entity) announced the release of its Accounts and Transaction Information and Payments Initiation API Specifications.[457] These standardized API specifications determine how banks and building societies, subject to the customer's express consent, should enable other regulated companies to access accounts and send payments. Using these standardized API specifications, banks and authorized third parties have the opportunity to develop innovative products and services tailored to the specific needs of consumers and businesses. In particular, the payments initiation API will enable third parties to set up secure payments on behalf of customers and, once authorized by the customer, submit the payment for processing.[458] In commenting the release of the Accounts and Transaction Information and Payments Initiation API Specifications, Imran Gulamhuseinwala, Trustee of Open Banking Ltd (the Implementation Entity), stated: "[t]he specifications … , which will be live from January [2018], provide the platform for developers from banks, fintechs and other organizations to build new web and mobile applications that will deliver a safer, more personalized and easier banking experience for consumers wishing to search, select and switch financial products in a secure environment … We are on track with our plans to develop a world leading Open Banking service where consumers will be able to significantly benefit from moving, managing and making more of their money"[459] The standardized API specifications are now available on Open Banking Ltd's website.[460]

Most recently, on 10 August 2017, Open Banking Ltd (the Implementation Entity) announced the release of Open Data API Specifications Version 2 for banking products, branches and ATMs.[461] This release follows the successful release of Version 1 in March 2017 discussed above. Version 2 introduces a number of

---

[454] See, Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Platform for Distributing Bank Product, Branch & ATM Data Available*, Open Banking Limited Press Release (March 13, 2017).

[455] See, Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Open Banking Forms Collaboration With OpenID Foundation*, Open Banking Limited Press Release (May 17, 2017) (explaining that "[t]his collaboration demonstrates the growing global adoption of OpenID Connect as a security standard in the most dynamic and challenging online environment today; the highly regulated world of online Banking and the rapidly expanding Fintech sector."). The OpenID Foundation is a non-profit international standardization organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies. Formed in June 2007, OpenID Foundation serves as a public trust organization representing the open community of developers, vendors, and users. More information is available on OpenID Foundation's website at http://openid.net/foundation/ and http://openid.net/wg/fapi/.

[456] Ibidem.

[457] See, Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Open Banking Launches Account Information and Payment Initiation API Specifications*, Open Banking Limited Press Release (July 5, 2017).

[458] Ibidem (explaining that "[t] he specification currently caters for the submission of a single, immediate, domestic payment from UK personal and business current accounts and is payment scheme agnostic, meaning that processing can take place via any payment system operator.").

[459] Ibidem.

[460] For more information, visit Open Banking Ltd's website at www.openbanking.org.uk.

[461] See, Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Open Banking Announces New Open Data and R/W Releases*, Open Banking Limited Press Release (August 10, 2017).

interesting improvements, including a more comprehensive and easier to implement data model, an updated and more detailed data directory, and an implementation guide with real world examples.[462] Furthermore, on the same date, Open Banking Ltd (the Implementation Entity) also announced the release of the Open Banking Security Profile (Implementer's Draft), which defines how the Open Banking Read/Write APIs are secured using Mutual TLS, OAuth 2.0 and Open ID Connect. [463]

4.C. PSD2 Implementation in the UK

4.C.i The UK HM Treasury (HM Treasury)

The HM Treasury transposed the Payment Services Directive (PSD) into UK law in 2009 through the Payment Services Regulations (PSRs 2009) and by a small number of related FCA rules set out in the FCA Handbook of Rules and Guidance (the "FCA Handbook"). These regulations and rules form the basis of the current payment services regime in the UK. Under this regime, the FCA is responsible for the authorization/registration and prudential requirements for payment institutions and for the conduct of business rules for the provision of payment services by all PSPs; while the Payment Systems Regulator (PSR) is the competent authority for provisions relating to access to payment systems.

HM Treasury is now responsible for transposing the revised Payment Services Directive (PSD2) into UK national law by 13 January 2018.[464] To this end, on 2 February 2017, the HM Treasury published a consultation paper on the implementation of PSD2.[465] In the consultation paper, the HM Treasury explained the scope of PSD2 and highlighted its key changes compared to PSD. The HM Treasury, then, proposed that PSD2 (similar to PSD) be implemented largely through regulations. In this regard, Annex B to the consultation paper contains a draft version of the Payment Services Regulations 2017 (PSRs 2017), which will revoke and replace the PSRs 2009.

The HM Treasury's intention in implementing PSD2 is to build on the existing framework. This approach will help ensure consistency with the EU framework, while also minimize the cost for businesses and consumers, and keep the payment services regime as tailored to the UK payment market as possible. For this reason, large parts of the new draft PSRs 2017 reproduce the equivalent parts of the PSRs 2009.

---

[462] API providers can access these standards with immediate effect and update to this new version. To access the Open Data API standards, visit http://www.openbanking.org.uk/open-data-apis/.

[463] The Open Banking Security Profile is available at http://www.openbanking.org.uk/read-write-apis/security-profile/. The Open Banking Profile is based on the OpenID Foundation's Financial API Read and Write API Security Profile (see http://openid.net/specs/openid-financial-api-part-2.html), which in turn is based on the Read Only specification (see http://openid.net/specs/openid-financial-api-part-1.html).

[464] On 23 June 2016, the EU referendum took place and the people of the UK voted to leave the EU. Until exit negotiations are concluded, the UK remains a full member of the EU and all the rights and obligations of EU membership remain in force. During this period, the UK Government will continue to negotiate, implement and apply EU legislation. The outcome of these negotiations will determine what arrangements apply in relation to EU legislation in future once the UK has left the EU.

[465] See, HM Treasury (HMT), *Implementation of the Revised EU Payment Services Directive (PSDII)*, cit.; HM Treasury (HMT), *Implementation of the Revised EU Payment Services Directive (PSDII) (and Draft Regulations (Annex B))*, cit.; HM Treasury (HMT), *Draft Impact Assessment on the Implementation of the EU Payment Services Directive II*, cit.

In consequence of the proposed amendments to the provisions in the PSRs 2009, other existing legislations will need to be amended, including provisions set forth in the Electronic Money Regulations 2011 (EMRs 2011).[466]

In the consultation paper, the HM Treasury further indicated that: the FCA would remain the relevant competent authority responsible for supervising PSPs under PSD2, and would produce supervisory procedures for, among others, registration, passporting, settlement of disputes, and precautionary measures; while the PSR would be responsible for certain aspects relating to payment systems.

Appendix A to the consultation paper provides a list of questions for which the HMT has sought input from various stakeholders. The consultation period closed on 16 March 2017.

4.C.ii. The UK Financial Conduct Authority (FCA)

On 10 February 2016, the FCA published a call for input on its approach to the current payment services regime, as a result of the requirement to transpose PSD2 into UK law by January 2018.[467] In its call for input, the FCA explained that PSD2 brings about changes to the way payment services are regulated, and these changes would need to be reflected in the guidance that the FCA published in 2009 to assist firms in complying with their legal requirements under the payment services regime. This guidance includes the FCA Payment Services Approach Document[468] and Chapter 15 of the FCA Perimeter Guidance Manual (PERG).[469] With the call for input, the FCA has sought views from firms, trade bodies, and other interested parties on whether the guidance has kept pace with market developments and the growth in payment services, so that it could take that into account when updating the guidance. The call for input included 6 questions and remained open until 23 March 2016.

On 15 November 2016, the FCA published a summary of the feedbacks received following the call for input in February 2016.[470] The FCA received 18 responses from various stakeholders, including payment service providers, trade bodies, and other interested parties. Although respondents seemed broadly satisfied with the existing guidance, they also suggested the FCA revise such guidance to take into account most recent changes in the market, as well as new technologies and business models. In addition, they requested the FCA to provide appropriate guidance on the relevant legislation or regulatory initiatives that have taken

[466] The draft of the PSRs 2017 contains selected consequential amendments to other legislation, including in particular some of the amendments to the Electronic Money Regulations 2011 (EMRs 2011). The final draft of the PSRs 2017 will include all necessary consequential amendments.
[467] See, Financial Conduct Authority (FCA), *Call For Input: The FCA's Approach to the Current Payment Services Regime*, Financial Conduct Authority Press Release (February 10, 2016); Financial Conduct Authority (FCA), *Call For Input: The FCA's Approach to the Current Payment Services Regime*, Financial Conduct Authority (February 2016).
[468] See, Financial Conduct Authority (FCA), *The FCA's Role under the Payment Services Regulations 2009 - Our Approach*, Financial Conduct Authority (June 2013).
[469] See, Financial Conduct Authority (FCA), *FCA Handbook - The Perimeter Guidance Manual (PERG)*, Chapter 15.
[470] See, Financial Conduct Authority (FCA), *Call For Input: The FCA's Approach to the Current Payment Services Regime – Feedback Statement*, Financial Conduct Authority Press Release (November 15, 2016); Financial Conduct Authority (FCA), *Call For Input: The FCA's Approach to the Current Payment Services Regime – Feedback Statement*, Financial Conduct Authority (November 2016).

place since the FCA published the original guidance.[471] The FCA has considered these feedbacks and input carefully in updating and developing the existing guidance for PSD2.

Alongside the February 2016 Call for Input, the FCA has been proactively engaging with relevant stakeholders. Among the various initiatives undertaken, the FCA has reconvened the Payment Services Stakeholder Liaison Group, whose first meeting took place on 12 July 2016. Following the initial meeting, the Payment Services Stakeholder Liaison Group further convened on 13 September 2016, 14 October 2016, and 1 December 2016.[472]

Most recently, on 13 April 2017, the FCA published a consultation paper proposing a revised approach document (the "Revised Approach Document"), which sets out the FCA's proposed approach to interpreting and applying the PSRs 2017 and the amended EMRs 2011.[473] The Revised Approach Document consists of a single document combining two existing documents: the Payment Services and E-Money Approach Documents.[474] In addition to the changes necessary as a result of PSD2, the revised Approach Document includes some proposed clarifications of existing guidance and some new guidance, mostly introduced in response to the February 2016 Call for Input previously discussed.

With the April 2017 consultation, the FCA also proposed changes to the FCA Handbook (including changes to the rules, guidance, and directions that apply to PSPs and e-money issuers and to other providers of retail banking services), as well as amendments to the FCA PERG and new directions that will apply to providers of excluded services.[475]

The consultation period closed on 8 June 2017. The FCA will consider the feedbacks received and will finalize its rules, directions, Perimeter Guidance, and Revised Approach Document, after the HM Treasury

---

[471] Respondents pointed to a number of aspects where the guidance could be updated. Most significantly, respondents suggested that the guidance should be reviewed to clarify whether new payment types and related technologies developments (e.g., contactless and mobile payments, online and mobile banking, digital currencies, and cheque imaging) that were not foreseen in the existing guidance fall within the regulatory perimeter. In addition, some respondents warned of the need to ensure that the guidance remains technology neutral and flexible enough to accommodate future developments. Further, other respondents suggested that the guidance could be updated to take into account developments or new business models in providing payment services that were not foreseen in the existing guidance. A number of respondents also pointed to the issue of prospective PSPs' ability to secure payment account services and the issue of "de-risking." In addition, respondents suggested that the guidance should be revised to take into account a number of regulatory initiatives, including the FCA's Cash Savings Market Study and the UK implementation of the Payment Accounts Directive that have created new rules and guidance for PSPs. Finally, some respondents suggested that the FCA should incorporate or reference guidance developed by industry bodies since 2009.

[472] The agenda and the minutes of the Payment Services Stakeholder Liaison Group's meetings are published on the FAC's website at https://www.fca.org.uk/firms/payment-services-e-money-stakeholder-liaison-groups.

[473] See, Financial Conduct Authority (FCA), *Implementation of the Revised Payment Services Directive (PSD2)*, Financial Conduct Authority Press Release (April 13, 2017); Financial Conduct Authority (FCA), *Consultation Paper - Implementation of the Revised Payment Services Directive (PSD2): Draft Approach Document and Draft Handbook Changes*, cit.; Financial Conduct Authority (FCA), *Draft For Consultation: Payment Services and Electronic Money – Our Approach. The FCA's Role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011*, Financial Conduct Authority (April 2017); Financial Conduct Authority (FCA), *The Payment Systems Regulator (PSR)'s Proposed Approach to Monitoring and Enforcing the Revised Payment Services Directive (PSD2)*, Financial Conduct Authority (April 2017).

[474] See, Financial Conduct Authority (FCA), *Consultation Paper - Implementation of the Revised Payment Services Directive (PSD2): Draft Approach Document and Draft Handbook Changes*, cit., p. 10 paragraph 1.12 (explaining that the FCA is combining the Payment Services Approach Document with the E-Money Approach Document into a single guidance document because "many of the authorization requirements are similar for PIs and EMIs. Consolidating the two Approach documents will avoid duplication, an issue which stakeholders acknowledged in response to our Call for Input. It will also give e-money issuers one point of reference to understand their capital and conduct obligations where they also provide payment services.").

[475] See, Financial Conduct Authority (FCA), *Consultation Paper - Implementation of the Revised Payment Services Directive (PSD2): Draft Approach Document and Draft Handbook Changes*, cit., Appendix 1 and Appendix 2.

has finalized the PSRs 2017.[476] At the date of writing, the FCA is expected to publish its policy statement setting out its finalized guidance and revised Approach Document in Q3 2017.

4.C.iii. The UK Payment Systems Regulator (PSR)

At the same time the FCA is working on finalizing its approach to PSD2, the PSR is consulting on its approach to monitoring and enforcing the four Regulations in the PSRs 2017 that it is the competent authority for.[477] The PSR will consider feedbacks and will finalize its Approach Document and powers and procedures guidance after the HM Treasury has finalizes the PSRs 2017. At the date of writing, the PSR is expected to publish these final documents in Q3 2017.

4.C.iv. Coordinating PSD2 Implementation with UK Open Banking Policy and Regulatory Initiatives

CMA Final Report and CMA Final Order. PSD2 is being implemented at the same time as the nine banks in Great Britain and Northern Ireland with the largest market share (LBG, RBSG, HSBCG, Barclays, Nationwide, Santander, AIB, BoI, and Danske) have been required by the CMA to develop and maintain common API standards discussed above. The CMA Final Order effectively accelerates the adoption of PISP and AISP access mandated under PSD2.

In particular, the CMA sees the same role for open APIs in the financial and banking services industry that PSD2 is advancing across the EU/EEA. It also recognizes that compatibility between PSD2 and CMA Final Order is critical. Without coherence between the two initiatives, the aim of open APIs delivering innovative solutions for the benefit of consumers and businesses, as well the objective of promoting greater competition in the financial and banking service industry could not be fully realized. Because of this:

- The CMA Final Order expressly states that neither the read-only data standard nor the read/write data standard mandated by the CMA shall include provisions that are incompatible with PSD2 requirements;[478]

- The CMA Final Explanatory Note expressly indicates that, in taking forward the CMA's mandate remedies, the Implementation Entity and the Implementation Trustee will have to take into account the wider context of PSD2 implementation and to give particular attention to the views of PSPs subject to PSD2;[479]

[476] The PSRs 2017 are still under consultation, and, therefore, the FCA's proposals remain subject to any future change to the PSRs.
[477] See, Payment Systems Regulator (PSR), *The PSR's Proposed Approach to Monitoring and Enforcing the Revised Payment Services Directive (PSD2)*, Payment Systems Regulator (April 2017). The PSR is responsible for monitoring compliance with Regulation 61 (Information on ATM withdrawal charges) and Part 8 (Access to payment systems and bank accounts) of the PSRs 2017 in the UK, and for taking enforcement action where appropriate. Part 8 of the PSRs 2017 comprises Regulations 102 to 105. Both the PSR and the FCA have been appointed as competent authorities for monitoring and enforcing compliance with Regulation 105 (Access to bank accounts).
[478] See, Section 4.B.ii above.
[479] See, Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, cit., p. 11, paragraph 38.

- Schedule 1 – Part A to the CMA Final Explanatory Note further clarifies that, to ensure an efficient outcome, the APIs developed in furtherance of the CMA's mandates shall allow adopters to comply with the PSD2 requirements and that the work programme would need to iterate with the clarification of standards for PSD2.[480] To that end, the Implementation Entity is called to (a) minimize the potential for any customer confusion that could have arisen in the absence of this consistency; (b) establish a clear technical framework to facilitate the safe introduction of PSD2, without removing the ability for innovation at the edges; and (c) align write functionality with the PISs that apply under PSD2;[481] and

- A specific Advisory Group (PSD2 Advisory Group), chaired and supported by Payments UK, has been established to help achieve a successful outcome.[482]

The Fingleton Report. The Fingleton Report expressly refers to PSD2, recognizing its potential for leading to significant market changes. It, further, suggests that taking forward proposals to implement an open API in the UK banking would give the UK an opportunity to get ahead of PSD2 and to build some of the infrastructures needed to implement the requirements of PSD2 in a way that delivers the good outcomes for both (individual and business) customers and industry.[483]

OBWG's Open Banking Standard. The process of implementation of PSD2 also needs to coordinate with the development and implementation of the OBWG's Open Banking Standard discussed above. The main differences between PSD2 and the OBWG's Open Banking Standard are around regulatory construction, scope, governance, and timelines.[484] In particular, the OBWG's Open Banking Standard envisages open APIs being used in a much broader context than the payments market to which PSD2 requirements will apply.

Notwithstanding these differences, there exists excellent coordination between the two initiatives. In terms of key objectives, the rationality behind the OBWG's Open Banking Standard can be compared to the legislative intention underlying PSD2: improving the competition and stimulating innovation for the benefit of consumers and businesses. Moreover, as discussed in detail above, many in the payments industry believe that the requirements of PSD2 can be met at best through the use of APIs.

---

[480] Id., Schedule 1 Part A - Agreed Arrangements, paragraph 15.
[481] Ibidem.
[482] Id., Schedule 1 Part A - Agreed Arrangements, paragraph 16.
[483] See, Open Data Institute (ODI) and Fingleton Associates, *Data Sharing and Open Data for Banks - A Report for HM Treasury and Cabinet Office*, cit., pp. 43-44 (noting that "PSD2 may impose similar requirements on banks as some of the recommendations on APIs considered here … As it currently reads, banks would have to allow third parties, via an interface (an API), to initiate payments from bank accounts. That access must be given on the same basis as if to account owner, i.e., if the owner can initiate a payment at zero cost, then so must a third party, obviously with appropriate consents. Telecom companies, among others, are keen to develop this ability. This has potentially profound consequences for banks, as it may reduce their ability to use current account relationships as gateway products for the sale of other products and services. This could encourage UK banks to consider strategies for addressing these changes at an early stage. It may challenge the behaviour whereby bank account customers often, by default, buy and use other financial services such as loans, mortgages, savings, foreign exchange and even online access from their core account providers. It could facilitate easier access for customers to competitors who might have keener price points and more innovative or user-friendly functionality. It may also incentivise existing banks to develop and match these innovative features.").
[484] See, Open Banking Working Group (OBWG), *The Open Banking Standard. Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation*, cit., p. 84, Appendix 1, paragraph 4.

In addition, as noted earlier, the OBWG has worked to ensure that, to the extent possible, coordination with PSD2 requirements be factored into the recommendations on the framework for an Open Banking Standard and open data API in UK banking. For example, Chapter 5 (Scope of Data) of the OBWG Open Banking Standard Report indicates that "[i]n defining this scope, and as a driving principle, this report has sought alignment to products and channels defined by PSD2 … This alignment delivers two key clear advantages should recommendations from this report be acted upon: (1) it simplifies compliance requirements on participating institutions, and (2) it simplifies communications to customers. It should be noted, however, that as of the time this report was written, relevant regulations (such as PSD2 and the EU's GDPR) had not been finalized. As such, subsequent work following this report may further refine or expand the scope as appropriate."[485] Furthermore, Paragraph 7.a.12.1 (Regulatory incentive – alignment with PSD2) of the OBWG Open Banking Standard Report states that "[t]here is clearly an opportunity to leverage the regulatory drivers of PSD2 to ensure that at least the core elements of standardization proposed in [the OBWG's Open Banking Standard] report are adopted … As this work progresses, it will be important to take a collaborative approach which engages with the transposition of PSD2 so that respective policy processes are aligned."[486] Finally, Appendix 1, Paragraph 5, of the OBWG Open Banking Standard Report envisages that "the output from the Open Banking Working Group will help [HM Treasury] and the FCA in shaping the transposition and implementing legislation of PSD2."[487]

[485] Id., p. 17, Chapter 5.
[486] Id., p. 36, paragraph 7.a. 12.1.
[487] Id., pp. 84-85, Appendix 1, paragraph 5.

CHAPTER 5. OPEN BANKING REGULATORY AND INDUSTRY-DRIVEN INITIATIVES – THE UNITED STATES (U.S.)

As the EU and the UK finalize the process of implementation of PSD2 and develop specific guidelines and technical standards for Open Banking, regulators and market participants in the United States will keep closely monitoring the progress made in these regions. While it remains to be seen whether in the coming years the United States will follow suit with similar regulation, at present the push for Open Banking in the United States continues to be primarily driven by the market.

Chapter 5 examines Open Banking initiatives in the United States. Specifically, it starts by analyzing the views expressed by the U.S. Consumer Financial Protection Bureau (CFPB) and the U.S. Federal Reserve System (Federal Reserve) on consumer-permissioned access to consumer financial data and account information. It, then, focuses on market-led proposals and discusses approaches to Open Banking suggested by various market participants.

5.A. U.S. Consumer Financial Protection Bureau (CFPB)

The CFPB has been among the most active federal agencies in engaging the fintech industry and testing the waters in Open Banking.

Under the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act"),[488] the CFPB has a number of statutory purposes. Among them, one key purpose is to implement and consistently enforce federal consumer financial laws in order to ensure that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive.[489] In addition, the CFPB is authorized to exercise its authorities under federal consumer financial law for the purposes of ensuring that, among others, markets for consumer financial products and services operate efficiently and transparently to facilitate access and innovation.[490] As previously discussed, permissioned access to financial account data can generate significant benefits for consumers and the broader financial services industry. Because of this, permissioned access to consumer financial account data is a core component of promoting the CFPB's statutory purposes.

Furthermore, unlike other regulators, the CFPB has authority over both banks and nonbank financial companies, which means it can oversee the entire marketplace to protect consumers, regardless of the institutional type at issue. This is particularly relevant when it comes to access and sharing of consumers' financial records and information, as much of the related innovation does not fit squarely within the bailiwick of "banking" (or "business of banking"), but is often a consumer financial product or service.

[488] Pub. L. No. 111-203, 124 Stat. 1376 (2010).
[489] See, Dodd-Frank Act Section 1021(a) (codified at 12 U.S.C. Section 5511)]
[490] See, Dodd-Frank Act Section 1021(b)(5) (codified at 12 U.S.C. Section 5511(b)(5)).

5.A.i. CFPB Director Richard Cordray's Speeches

On 23 October 2016, CFPB Director Richard Cordray delivered a speech at the Money 20/20 conference in Las Vegas (NV), in which he emphasized: (1) the CFPB's mission of protecting consumers in the financial marketplace while facilitating access and innovation; and (2) the CFPB's efforts in ensuring that all consumers have access to consumer financial products and services in markets that are fair, transparent, and competitive.[491] In particular, CFPB Director Cordray discussed the CFPB's Project Catalyst and its objective of encouraging marketplace innovation. He indicated that the CFPB has participated in several discussions regarding innovation with regulators in Europe and elsewhere, with which the CFPB shares "a growing enthusiasm for finding ways to leapfrog forward to products that are more accessible, more affordable, more convenient, and more empowering of consumers." [492]

Among the issues addressed in his speech, CFPB Director Richard Cordray expressed the CFPB's concern over the ability of consumers to access their own data. He mentioned that reports have indicated "that some financial institutions are looking for ways to limit, or even shut off, access to financial data rather than exploring ways to make sure that such access, once granted, is safe and secure."[493] With this statement, he seemed to suggest that the CFPB believes banks are hurting their consumers by not readily opening their systems to data aggregators or other third-parties providing similar services.

Furthermore, in his speech, CFPB Director Cordray remarked the CFPB's belief that consumers should be able to access their financial information and give their permission for third-party companies to access this information as well. He noted that consumers gain the opportunity to access a growing number of innovative financial and banking services from a wide range of providers. For example, some of these innovative products and services can assist consumers monitor relationships with multiple financial institutions through a single interface, making spending decisions, and managing their finances. This, in turn, generates tremendous benefits to consumers in terms of simplicity, efficiency, speed, and transparency; it also spurs further innovation in the financial and banking service industry and helps make markets more competitive.[494] CFPB Director Cordray acknowledged that the existence of these products and services heavily depends on whether consumers can authorize access to their digital financial

[491] See, Richard Cordray (CFPB Director), *Prepared Remarks* of CFPB Director Richard Cordray at Money 20/20 (Las Vegas (NV), October 23, 2016).
[492] Ibidem.
[493] Ibidem. In 2015, several large banks cut off aggregators' access to consumers' financial account information. The banks pointed to a number of concerns, including internal data security, privacy, and operational limitations. This issue is discussed in more detail below.
[494] Ibidem. On this issue, see, also, Richard Cordray (CFPB Director), *Prepared Remarks* to Be Delivered at the Field Hearing on Consumer Access to Financial Records Salt Lake City (Salt Lake City (UT), November 17, 2016) (noting that "[a]ccess to digital financial records can be especially important to consumers who want to borrow money but lack enough credit history to generate a credit score or whose score may not accurately reflect their current creditworthiness. By allowing a prospective creditor to access the consumer's transaction account, the creditor may be able to extend the credit needed at a fair price.").

records.[495] For this reason, he concluded that consumer-permissioned access to consumer digital financial data and records is critical.[496]

CFPB Director Richard Cordray, then, explained that the U.S. Congress itself had already recognized the need for consumers to be able to access and use their digital financial records and information. In particular, he observed that the U.S. Congress had provided the right to do so in Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act"), which states that "subject to regulations issued by the CFPB, a covered person [including a financial provider] shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person."[497] This includes "information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[498] Section 1033 requires that this information "be made available in an electronic form usable by consumers."[499] With this statement CFPB Director Cordray appeared to rebuke banks that would deny third parties access to customer digital financial records and information. In so doing, he effectively reignited the ongoing dispute between banks and fintech firms over screen scraping discussed in prior chapters.[500]

Finally, CFPB Director Richard Cordray concluded his speech announcing the intent of the CFPB to discuss the issue of consumer-permissioned access to consumer financial data and records with fintech companies, consumer advocacy organizations, and other regulatory agencies.[501] This point is analyzed in greater detail in the following sections.

5.A.ii. CFPB's Project Catalyst Report

The day after Cordray's speech at the Money 20/20 conference in Las Vegas (NV), the CFPB published its first ever report on Project Catalyst (Project Catalyst Report),[502] the initiative launched by the CFPB in 2012 to support responsible financial innovation.[503]

The Project Catalyst Report provides an overview of Project Catalyst's work to promote consumer friendly innovation and highlights its focus on facilitating marketplace innovation, so that new and emerging

---

[495] See, Richard Cordray (CFPB Director), *Prepared Remarks* of CFPB Director Richard Cordray at Money 20/20, cit.
[496] Ibidem. See, also, Richard Cordray (CFPB Director), *Prepared Remarks* to Be Delivered at the Field Hearing on Consumer Access to Financial Records Salt Lake City, cit. (arguing that access to digital financial records "is all about taking control and becoming a more active participant in your own financial life.").
[497] See, Dodd-Frank Act Section1033(a) (codified at 12 U.S.C. Section 5533(a)).
[498] Ibidem.
[499] Ibidem.
[500] See, Lalita Clozel, *Cordray Reignites Bank-Fintech Fight After Comments on Data Sharing,* cit. (quoting Anil Arora (CEO at Yodlee) commenting on the speech delivered by Cordray saying that "[w]hat the director said is that what's paramount for all of us is first and foremost making sure that consumers have access to all their data.").
[501] See, Richard Cordray (CFPB Director), *Prepared Remarks* of CFPB Director Richard Cordray at Money 20/20, cit.
[502] See, Consumer Financial Protection Bureau (CFPB), *Project Catalyst Report: Promoting Consumer-Friendly Innovation*, Consumer Financial Protection Bureau Press Release (October 24, 2016); Consumer Financial Protection Bureau (CFPB), *Project Catalyst Report: Promoting Consumer-Friendly Innovation*, Consumer Financial Protection Bureau Innovation Insights (October 2016).
[503] See, Consumer Financial Protection Bureau (CFPB), *CFPB Launches Project Catalyst to Spur Consumer-Friendly Innovation*, Consumer Financial Protection Bureau Press Release (November 14, 2012).

products that are safe and beneficial for consumers can be developed.[504] It, then, discusses a number of market developments that hold the potential to generate significant tangible benefits for consumers. These developments are: (1) cash flow management; (2) Improved credit assessment ("big data" underwriting); (3) consumer financial data access; (4) Student lending and refinancing; (5) mortgage service platforms; (6) credit reporting accuracy and transparency; (7) peer-to-peer payments; and (8) savings. In the Project Catalyst Report, the CFPB stated its intent to learn more about each one of these areas and to leverage its policies and programs as appropriate to help facilitate innovation.

The list of marketplace developments above is interesting in that it provides a window into the CFPB's thinking about innovation. In particular, with regard to the issue of consumer financial data access,[505] in the Project Catalyst Report the CFPB observed that, over the last few years, consumer-permissioned data access has begun to power a wave of innovative financial products and services, including personal financial management tools and mechanisms to reduce the time to verify consumers' accounts. It, further, noted that improving the reliability, privacy, and security of consumer financial data access is important for the development of such financial products and services. On the other hand, it warned "the loss of appropriate access to consumers' account data could cripple or even entirely curtail the further development of such products and services."[506] Against this background, the CFPB stated its interest in learning more about consumer and third-party account access and in "supporting the ability of consumers to access and share personal information about their own financial lives with others where they believe it is in their interest to do so."[507]

5.A.iii. CFPB's Request for Information

On the heels of the CFPB Director Richard Cordray's speech at the Money 20/20 conference and the publication of the Project Catalyst Report discussed above, on 14 November 2016 the CFPB announced an inquiry to learn more about consumers' ability to access, use, and share their digital financial records (the "Request for Information").[508]

During prepared remarks delivered at a field hearing held by the CFPB in Salt Lake City (UT) on 17 November 2016, CFPB Director Richard Cordray explained that, in issuing the Request of Information, the CFPB's goals were: (1) learning the extent to which consumers that authorize access to their financial records can choose how their records are being shared; (2) learning how the market is currently functioning, gaining more insight into the process for sharing financial records, and how safe and secure

[504] See, Consumer Financial Protection Bureau (CFPB), *Project Catalyst Report: Promoting Consumer-Friendly Innovation*, cit., pp. 11-20. To further its mission, Project Catalyst acts in the following ways: (1) establishing communication channels with a diverse group of stakeholders through a number of initiatives, including by coordinating with government agencies and holding "office hours" where the CFPB meets with interested parties; (2) developing programs and policies that support consumer-friendly innovation, such as the policy to encourage trial disclosure programs and the policy on no-action letter; and (3) engaging in pilot projects and research collaborations.
[505] Id., pp. 22-23.
[506] Ibidem.
[507] Ibidem.
[508] See, Consumer Financial Protection Bureau (CFPB), *Request for Information Regarding Consumer Access to Financial Records*, Docket No. CFPB 2016-0048 (November 14, 2016).

such process is; and (3) learning about transparency and how much control consumers have over their own financial records.[509]

In the Request of Information, the CFPB indicated that it relies on the following two distinct provisions of the Consumer Financial Protection Act of 2010 ("CFPA") for the potential regulation of consumer financial data aggregation activities and aggregators themselves:[510]

- Section 1033(a) of the CFPA. As previously discussed, Section 1033(a) of the CFPA requires that "[s]ubject to rules prescribed by the [CFPB], a covered person shall make available to a consumer, upon request, information in the control or possession of such person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, or series of transactions, to the account including costs, charges, and usage data."[511] Section 1033(a) further provides that the information must be made available "in an electronic form usable by the consumer."[512] Rulemaking authority in respect to this provision lies with the CFPB.[513]

- Sections 1031 and 1036 of the CFPA. The CFPB's authority over data security issues is also based on the prohibition of unfair, deceptive, or abusive acts or practices (UDAAPs) under Sections 1031 and 1036 of the CFPA.[514] In this respect, the Request for Information cited a recent CFPT's data security case against Dwolla[515] and certain FTC's past data security activities as relevant precedents to assert that "[a]n entity's consumer data privacy or security practices can violate UDAAP standards."[516]

After clarifying the foundation of its statutory authority, in the Request for Information the CFPB observed that in recent year increasing availability of consumer financial account data in electronic form (in real-time or near-real-time) has generated tremendous benefits to consumers. In fact, when made readily available, such data "foster consumer convenience, … can help consumers understand and control their financial

[509] See, Richard Cordray (CFPB Director), *Prepared Remarks* to Be Delivered at the Field Hearing on Consumer Access to Financial Records Salt Lake City, cit.
[510] The CFPA was enacted as Title X (Sections 1001-1100H) of the Dodd-Frank Act (codified at 12 U.S.C. Sections 5301 et seq.).
[511] See, Dodd-Frank Act Section 1033(a) (codified at 12 U.S.C. Section 5533(a)). The statute exempts certain records from being provided, including: confidential commercial information; information collected to prevent fraud or money laundering; information required to be kept confidential by law; and information that a consumer "cannot retrieve in the ordinary course of its business." See, Dodd-Frank Act Section 1033(b)(1)-(4) (codified at 12 U.S.C. Section 5533(b)(1)-(4)).
[512] Ibidem.
[513] See, Dodd-Frank Act Section 1033(e) (codified at 12 U.S.C. Section 5533(e)) requires that the CFPB consult with the federal banking agencies and the Federal Trade Commission (FTC), when prescribing any rule under Section 1033.
[514] See, Dodd-Frank Act Section 1031 and Section 1036 (codified at 12 U.S.C. Section 5531 and Section 5536)]
[515] In the Matter of Dwolla, Inc., File No. 2016-CFPB-0007, Consent Order (March 2, 2016). See, RFI, p. 6 and accompanying note 9 (explaining that "[i]n March 2016 the FCPB entered into a consent order with a provider of a consumer-facing, online payment network [Dwolla]. Among other things, the FCPB found that [Dwolla] falsely represented to consumers that it employed reasonable and appropriate measures to protect data obtained from consumers from unauthorized access.").
[516] See, Consumer Financial Protection Bureau (CFPB), *Request for Information Regarding Consumer Access to Financial Records*, cit., p. 6 note 9 (explaining that "[r]elying on Section 5 of the Federal Trade Commission Act, which makes unlawful all "unfair or deceptive acts or practices in or affecting commerce," see 15 U.S.C. 45(a)(1), the FTC has also taken action against companies that fail to take reasonable measures to protect the security of consumer data. See, e.g., FTC Matter/File Numbers 1023142-X120032 (Wyndham Worldwide Corporation); 052-3148 (CardSystems Solutions, Inc.); 052-3136 (Superior Mortgage Corp.); 052-3096 (DSW Inc.); 052-3117 (Nations Title Agency, Inc.); 062-3057 (Guidance Software, Inc.); 072-3046 (Life is good, Inc.); 072-3055 (TJX Companies); and 052-3094 (Reed Elsevier, Inc.).).

lives, make useful decisions, monitor spending and debt, set and achieve savings goals, communicate effectively with their financial service providers, and solve financial problems in timely ways."[517]

The CFPB further noted that banks and traditional account providers have long been the predominant users of consumer account data, which they have utilized to supplement their use of existing in-house data for online advisory and account management services.[518] However, the CFPB acknowledged, over time new players have entered the markets and have begun to offer innovative consumer products and services, which critically rely on consumer-permissioned, electronically-sourced account data.[519] The CFPB provided a detailed list of these products and services, including: personal financial management; automatic or motivational savings; budgeting analysis and advice; product recommendations; account verification; loan application information verification; credit decision making; cash flow management; and funds transfer and bill payment; fraud and identity theft detection.[520] Some consumer-permissioned services providers have used their own proprietary technology solutions to access data from consumer financial account providers; while others have relied on third-party "account aggregators" to provide the necessary technology given the large number of potential data sources and the transaction costs associated with obtaining consumer account data.[521]

Advancements in technology have contributed to the development of aggregation services and have facilitated the associated delivery of products and services that rely on consumer account data access. In this respect, in the Request for Information the CFPB recognized that current "methods to access consumer account data—and to obtain consumer permission to do so—are technically complex and actively evolving."[522] The CFPB observed that, in order to enable access by third parties, consumers are often requested to share their online account credentials (e.g., user name and password) and other forms of authentication (e.g., knowledge-based security questions). Depending on the product or service, consumers may be requested to authorize access only to a single account or to multiple accounts held by a number of financial institutions and other companies. Consumers' credentials are, then, typically utilize to obtain consumer's account data through either: (1) a structured data feed or API hosted by the company or financial institution holding the account; or (2) the consumer-facing website of the company or financial institution holding the account (screen-scraping).[523] The access can be on a single or a recurring basis. At

[517] Id., p. 7.
[518] Id., p. 8 note 14. See, also, Office of the Comptroller of Currency (OCC), *OCC Bulletin 2001-12, Bank-Provided Account Aggregation Services*, Office of the Comptroller of Currency (February 28, 2001).
[519] Id., p. 8 note 15 (referring to Mint as a notable example of aggregators). The Request for Information uses the term "consumer-permissioned access" to refer to consumer access to consumer financial account and account-related information, whether directly or through a third-party acting with the consumer's permission. See, Id, p. 15.
[520] Id., pp. 10-11.
[521] Id, p. 8 (noting that "[i]n either case, the process of accessing consumer account data is often referred to as account or data aggregation.").
[522] Id., p. 9.
[523] Ibidem, note 17 (explaining that "[f]or example, Yodlee, an account aggregator, reports that 75 percent of the data it aggregates from over 14,500 sources is collected through structured feeds from its financial institution customers and other financial institutions. See Envestnet, 2015 Annual Report, at 14 (Feb. 29, 2016), available at http://ir.envestnet.com/phoenix.zhtml?c=235783&p=irol-IRHome.").

that point, if an account aggregator is an intermediary in this process, it generally transmits the consumer's data aggregated to permissioned parties through an API.

Yet, despite the benefits discussed above, the CFPB also recognized that financial data sharing does create a number of legitimate risks, which need to be carefully addressed. These risks include the following:[524]

- Privacy and security-related concerns raised by some consumer financial account providers about: (1) whether account aggregators or permissioned parties utilize adequate security and privacy procedures with respect to consumers' online account credentials and consumer account data obtained through aggregation;[525] (2) whether account aggregators or permissioned parties obtain or retain more consumer information than is necessary for the specific product or service being provided; and (3) the extent to which, and the terms under which, account aggregators or permissioned parties may use the data for purposes other than providing the requested product and service and may share such data with other entities.[526]
- Concerns raised by a number of parties about the application of the Fair Credit Reporting Act in the area of consumer-permissioned access to consumer financial data and records.[527]
- Concerns raised by some consumer financial account providers about their liability for unauthorized transactions arising in the event of a breach of consumer credentials or consumer financial account data held by an account aggregator or a permissioned party.[528]

In the Request for Information, the CFPB acknowledged that increasing discussions on these and other security and privacy-related issues are ongoing among market participants; it also recognized that most market participants continue to address their working arrangements, often bilaterally, with respect to consumer account data, covering aspects such as the sharing of technical burdens, the frequency and volume of data provision, counterparty vetting, consumer protection obligations (especially in the event of a data breach), compensation, and indemnity.[529] However, the CFPB also warned that "such market participants do not necessarily share common views about consumer protection and other consumer interests" and that consumer views might have not been adequately represented in this area. For this reason, it expressed its concern that some financial institutions may "decide to restrict consumer-permissioned access to data in ways that undermine consumer interests identified in Section 1033 [of the Act] — and that are broader than necessary to address legitimate privacy and security concerns."[530]

---

[524] Id., pp. 12-13.
[525] See, Chapter 2 above.
[526] See, e.g., Bradley Hope, *Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors*, The Wall Street Journal (August 6, 2015) (reporting that Yodlee sells some of the data it collects to investment firms but that Yodlee has not publicly disclosed that it does so, and that Yodlee has stated that individuals' identities cannot be discerned from its data set).
[527] See, e.g., Federal Reserve Bank of Philadelphia, Compliance Corner (Q4 2001), On-line Aggregation: Benefits and Risks, at CC4]
[528] See, e.g., JP Morgan Chase & Co., Jamie Dimon (Chairman and Chief Executive Officer), *Letter to Shareholders*, JPMorgan Chase & Co. (April 6, 2016) (expressing "extreme concern" over, among other things, data security and privacy, because customers have let aggregators access their bank accounts and account information); See, also, Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, cit.
[529] See, Consumer Financial Protection Bureau (CFPB), *Request for Information Regarding Consumer Access to Financial Records*, cit., pp. 12-13.
[530] Id., p. 14.

Given this background, in the Request for Information the CFPB asked 20 questions on practices (and potential practices) concerning consumer-permissioned access to consumer financial account data.[531]

As explained by CFPB Director Richard Cordray in his remarks at the Field Hearing on 17 November 2016,[532] first of all the CFPB wanted to understand how the market is currently functioning. To this end, the CFPB asked the following 4 questions:

- What types of products and services are currently made available to consumers that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data? What benefits do consumers realize as a result? (Question #1)
- How many consumers are using or seeking to use such products or services? What demographic or other aggregate information is available about these consumers? (Question #2)
- To provide or assess eligibility for these products and services, what kinds of consumer financial account data and nonfinancial consumer account data are being accessed, by what means, under what terms, and how often? How long is accessed data stored by permissioned parties or account aggregators? (Questions #3 and #4)

In addition to the above, with the Request for Information the CFPB sought to learn about the incentives that would facilitate or discourage people from accessing and using their own digital financial records. For this reason, the CFPB asked the following 4 questions:

- What types of companies offer products and services that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data, either to deliver the product or service or to assess eligibility for the product or service? To what extent are such products and services offered by entities that offer transaction accounts? To what extent are they offered by other market participants? (Question #5)
- In what ways, if any, do consumer products and services that rely, at least in part, on consumer-permissioned electronic access to consumer financial account data differ according to whether the offering company provides or does not provide transaction accounts to consumers? Do any such differences impact consumers? If so, how? (Question #6).
- To what extent do market participants compete to offer consumer products and services that rely, at least in part, on consumer-permissioned access to consumer financial account data? How does such competition impact consumers? (Question #7)
- What incentives or disincentives exist for consumer financial account providers to facilitate or discourage consumer-permissioned access to the account data that they hold by permissioned parties or account aggregators? In what ways do consumer financial account providers directly or indirectly facilitate or restrict consumer-permissioned access to account data? What are the associated impacts to consumers and other market participants? (Question #8)

As explained by CFPB Director Cordray in its remarks at the Field Hearing on Consumer Access to Financial Records Salt Lake City,[533] before issuing the Request for Information the CFPB had considered certain operational concerns raised by banks, credit unions, and others that hold consumer financial records and information about when and how they are supposed to share the information with third-party providers. The CFPB wanted to learn more about this and, therefore, asked the following question:

- What impediments, obstacles or risks do consumer financial account providers currently face in providing data to or allowing access to data by permissioned parties or account aggregators? (Question #9)

The Request for Information highlighted the CFPB's belief that both consumers and their authorized third parties should be able to access their digital financial records and to share their records with third-party

[531] Id., pp. 14-19.
[532] See, Richard Cordray (CFPB Director), *Prepared Remarks* to Be Delivered at the Field Hearing on Consumer Access to Financial Records Salt Lake City, cit.
[533] Ibidem.

providers of products or services of their preference. In its remarks at the Field Hearing on Consumer Access to Financial Records Salt Lake City, CFPB Director Cordray reaffirmed this belief and pointed to a range of concerns about consumers' ability to access and share their account information electronically.[534] As he explained, impeding access to digital financial records (or making it unreasonable difficult to do so) "not only blocks innovation from new entrants, it also reduces the incentives for financial institutions to innovate."[535] To gain deeper insights on this point, in the Request for Information, the CFPB asked the following 2 questions:

- What impediments, obstacles or risks do permissioned parties or account aggregators currently face in obtaining such data? Describe specific operational costs, risks, and actual or potential losses, and identify their specific causes. (Question #10)
- What impediments, obstacles or risks do consumers currently face in obtaining— including permitting access to—such data? (Question #11)

A key area of concern for the CFPB relates to the need that access and use of consumer financial records and information be done safely and securely. As explained by CFPB Director Cordray, "[i]t would be problematic for everyone involved if granting access to third parties were to compromise consumer privacy or put consumers' funds and account relationships at risk."[536] Because of this, in the Request for Information, the CFPB sought to gain more information about how financial records are obtained, stored, and used by third parties. In particular, the CFPB asked the following 2 questions:

- What security and other risks do consumers incur if they permit access to their financial account data in order to obtain a particular product or service? What steps have consumer financial account providers, account aggregators, permissioned parties and other users of consumer-permissioned account data taken to mitigate such risks? What information do these parties communicate to consumers about associated risks? (Question #12)
- In what ways, do account aggregators or permissioned parties use consumer-permissioned account data for purposes other than offering or facilitating the delivery of a specific product or service to the permissioning consumer? Do such companies continue to access or store data after the consumer ceases to use the product for which the permissioned data use was intended by the consumer? Do such companies share the data with other parties and, if so, under what terms and conditions? What are the associated impacts to consumers? (Question #13)

Another key are of concern is control. The CFPB stressed the importance that access and use of consumer financial records be transparent and that consumers be able to control and direct the sharing and use of their personal financial data. In the Request for Information, the CFPB sought to gain more information on how consumers can currently control how authorized companies use data. In particular, the CFPB asked the following 4 questions:

---

[534] Ibidem (noting the CFPB's concerns "that some financial institutions have threatened to cut off the flow of information to some websites and mobile applications" and that some financial institutions "make consumers jump through so many hoops to access or authorize access to their own financial records that they are discouraged from even trying.").

[535] Ibidem (arguing that "[i]f financial institutions that house digital financial records make it difficult or impossible for consumers to authorize access or share their information, that blocks opportunities for consumers to benefit from this information. The result could be to thwart new entrants from entering the market with consumer-friendly products and services, even those not currently being offered by the financial institutions themselves … Without new companies introducing consumer-friendly products or services into the market, established companies are likely to feel less pressure to compete in this manner. And authorizing access to their financial records can make it easier for consumers to shop for an alternative provider with more favorable pricing, given the consumer's usage patterns. To be clear, it is unacceptable for financial institutions to block access to consumer information as a means of gaining a competitive advantage in the marketplace.").

[536] Ibidem.

- When consumers permit access to their financial account data, what do they understand about: what data are accessed; how often and for what purposes the data are used; whether the permissioned party or account aggregator continues to access, store or use such data after the consumer ceases to use the product or service for which the permissioned data use was intended by the consumer; and with which entities a permissioned party or account aggregator shares the data and on what terms and conditions? What drives or impacts their level of understanding? What impact does their level of understanding have on consumers and on other parties? (Question #14)

- To what extent are consumers able to control how data is used by permissioned parties or account aggregators that obtain that data via consumer-permissioned access? Are they able to request that permissioned parties, account aggregators, or other users delete such data? Is such data otherwise deleted and, if so, when and by what means? To what extent are consumers consenting to permissioned party and account aggregator practices with respect to access, use and sharing of consumer financial account data? (Question #15)

- Do consumer financial account providers vet account aggregators or permissioned parties before providing data to them? Do consumer financial account providers perform any ongoing vetting of account aggregators or permissioned parties? If so, for what purposes and using what procedures? What are the associated impacts to consumers and to other parties? (Question #16)

- What industry standards currently exist, in development or otherwise, to enable consumer-permissioned access to financial account data? (Question #17)

Finally, in the Request for Information, the CFPB invited commenters to describe how they believe market practices may or should change over time. Specifically, the CFPB asked the following 3 questions:

- What changes are or may be expected to happen to any market practice described in response to questions 1 through 17, why, and with what impacts to consumers, consumer financial account providers, permissioned parties, and account aggregators? (Question #18)

- What changes should happen to any market practice described in response to questions 1 through 18, why, and with what impacts to consumers, consumer financial account providers, permissioned parties, and account aggregators? (Question #19)

- Are "industry standard" practices that provide consumers with data access comparable to that envisioned by section 1033 of the Dodd-Frank Act likely to be broadly adopted by consumer financial account providers, permissioned parties and account aggregators in the absence of regulatory action? If not, how will "industry standard" practices be insufficient? What marketplace considerations are likely to bear on such developments? Generally, how will the advent of standard practices for consumer-permissioned access to consumer financial account data affect competition and innovation in various consumer financial service markets? (Question #20)

The CFPB encouraged a wide range of stakeholders to respond to the questions above.[537] A host of banks, credit unions, non-bank consumer financial service providers, industry and consumer groups, technology firms, aggregators, and fintech companies responded to the CFPB's Request for Information, highlighting the diversity of perspectives that exist regarding the adequacy and application of existing regulations to data aggregation activities.

Responses to the CFPB's Request for Information predominantly came from three groups: (a) financial institutions and associations representing them; (b) data aggregators, fintech companies, and their industry representative groups; and (c) consumer group representatives. Selected responses are summarized below:

(a) Summary of Selected Responses from Financial Institution and Associations Representing Them.

[537] See, Consumer Financial Protection Bureau (CFPB), *Request for Information Regarding Consumer Access to Financial Records*, cit., pp. 3-4. Comments in response to the Request for Information were due 90 days after the Request for Information was published in the Federal Register. Comments are available at https://www.regulations.gov/docketBrowser?rpp=50&so=DESC&sb=commentDueDate&po=0&D=CFPB-2016-0048.

1) Financial Institutions and association representing them denied the claims of improper restrictions to customer-permissioned financial records access and explained that any measure had been taken to protect consumers and to adequately manage operational, security, and privacy risks.

- "[The statement delivered by CFPB Director Richard Cordray at a November 17, 2016, field hearing in Salt Lake City] suggests the CFPB believes banks are doing consumers a disservice by not readily opening their systems to data aggregators. However, in reality, if a customer freely hands over their login credentials to third party aggregators, banks have no control over how third party aggregators are keeping customer's account information safe." - Consumer Bankers Association (CBA), Response to Request for Information Regarding Consumer Access to Financial Records, Docket No.: CFPB-2016-0048 / Document No.: 2016-28086 (February 21, 2017), p. 3.

- "Today, consumers trust that their financial data are being protected and handled appropriately ... Current practices in the data aggregation market, however, may leave consumers exposed and create risk that undermine this trust … When consumers share their login credentials with an aggregator, they are giving the aggregator *carte blanche* access to their financial data … Yet consumers are not given adequate information or control over what information is being taken, how long it is accessible, and how it will be used in the future. Moreover, consumers are unaware of the differences in the legal and supervisory standards applicable to bank and nonbank participants in the financial services marketplace. Once the information is shared, it leaves a secure bank environment, where it is accorded longstanding legal protections, and it is released into the data services market where it is accorded no more special status than data created through a consumer's use of a social media platform. - American Bankers Association, Response to Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 (February 21, 2017), p. 2.

- "BBVA Compass has taken steps to manage [concerns about third-part's data security and data sharing practices] by working directly with aggregators ... Some financial institutions have voiced worries over the stress that unrestricted aggregation volume could place on the institution's technology infrastructure. To help mitigate that operational risk, [BBVA Compass] has invested substantial time and resources to create a dedicated channel for aggregators that directly connect to BBVA Compass to retrieve consumer financial account data. [BBVA Compass] must maintain a separate server in order to route aggregator traffic through that channel. Utilizing this separate channel to manage the bulk of aggregator activity, [BBVA Compass] has not had cause to restrict consumer-permissioned access to account data due to site performance issues … To help mitigate security and privacy risks…, [BBVA Compass has] worked closely with [its] trusted service providers to incorporate their aggregation services into [its] online offerings. Through established vendor management processes, [BBVA Compass] is in a position to evaluate these aggregators more fully than consumers are generally. As discussed above, [BBVA Compass] has also taken steps to develop APIs that can provide a secure channel to deliver financial account data to the aggregator without requiring consumers to divulge their banking credentials to a third party." - BBVA Compass, Response to Request for Information Regarding Consumer Access to Financial Records ("RFI") Docket No. CFPB-2016-0048 (February 17, 2017), pp. 3-4.

2) Financial Institutions and association representing them also argued that technology advancements could help address privacy and security challenges related to consumer-permissioned access to consumer financial records and data.

- "The financial services industry is employing technology solutions for the secure exchange and access of financial information. These technologies involve the implementation and use of application programming interfaces ("APIs") … [and] authentication process, called "open authorization" ("OAuth") … There are many advantages in using the API and OAuth processes over traditional screen scraping technologies. First, the model eliminates instances of sharing account access credentials by consumers with third parties. … Second, this model allows financial institutions to obtain from the consumer an unequivocal consent to provide data to a third party … and it eliminates issues regarding the authority that was granted by the consumer to the aggregation service to obtain financial account data. … Third, financial institutions can work with aggregators to ensure that appropriate financial account and account-related data is available for access through the API. … Fourth, … Under this model, scraping errors cannot occur … In addition, the model can help to rationalize the number of data calls. … Finally, this data access model promotes standardization of formats for data accessed by aggregation services as contemplated by section 1033 of the Dodd-Frank Act."- Fidelity Investments, Response to Request for Information Regarding Consumer Access to Financial Records; Docket No. CFPB-2016-0048 (February 21, 2017), pp. 6-7.

- "[BBVA Compass] believes the API model could alleviate many security and privacy concerns associated with consumer-permissioned access because the consumer's banking credentials remain confidential, the account provider receives assurances of the consumer's permission and knows which data are being accessed and why. This model also helps third parties by eliminating the risk exposure and cost involved in maintaining a repository of

sensitive banking credentials. Further, API technology is often a more efficient, reliable, and manageable method of delivering account data than screen-scraping. Widespread adoption of this model likely requires some greater degree of industry standardization, both to help smaller account providers offer user-permissioned access in a cost-effective manner and to promote standardized integration for third parties needing to connect with many account providers." - BBVA Compass, Response to Request for Information Regarding Consumer Access to Financial Records, cit., p. 6.

3) Financial institutions and association representing them generally suggested that the CFPB should define data aggregators as "larger participants" and should subject such larger participants to consistent regulatory supervision.

- [The Dodd-Frank Act] … provided that the [CFPB] has authority over "any covered person who … is a larger participant of a market for other consumer financial products or services, as defined by rule." [See 12 U.S.C. §5514(a)(1)(B) and §5514(b)-(d).] … Considering the potential risks to consumers and the financial system arising from data aggregators and the unique structure of the data aggregator market … the CFPB should define "larger participants" in this market, thereby expressly subjecting these entities to direct the CFPB supervision and examination." - The Clearing House Association, Request for Information Regarding Consumer Access to Financial Records, Docket No. Bureau–2016–0048 (February 21, 2017), p. 14.

- "[The American Bankers Association] recommend[s] that the [CFPB]: … [should exercise its authority under Dodd-Frank Act §1024 to] identify "larger participants" in the market for consumer financial data that are subject to supervision by the [CFPB] and begin to supervise those entities." - American Bankers Association, Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp. 3, 11-12.

4) Furthermore, financial institutions and associations representing them highlighted the overall lack of consumer regulations, as promulgated by the banking agencies, applicable to data aggregators and other fintech companies that access and process consumer data. They, then, outlined a number of regulatory reforms that in their view would bring data aggregators and fintech companies more in line with banking industry standards, including more uniform compliance with existing rules under the Gramm-Leach-Bliley Act (GLBA).

- "[The American Bankers Association] believe [that] … [c]onsumers deserve bank-level security and protection regardless of where they choose to share their data. This means that consumer data are treated the same – and subject to GLBA protections – whether at a bank or a third party … [The American Bankers Association] recommend[s] that the [CFPB]: [c]larify that data aggregators are "financial institutions" subject to the requirements of the Gramm-Leach-Bliley Act (GLBA) that apply to financial institutions under the FTC's Safeguards Rule and Bureau's Regulation P; [t]ake steps to ensure data aggregators are subject to the same standards as depository institutions for safeguarding financial data and notifying customers about security breaches; [c]larify that data aggregators are "service providers" under the Electronic Funds Transfer Act (EFTA) and are liable for unauthorized electronic fund transfers that exceed the consumer's liability under EFTA." - American Bankers Association, Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp. 2-3, 4-7.

- "The release and storage of sensitive customer information by data aggregators creates an increased risk of data breaches and, accordingly, PFMs must ensure compliance with applicable laws with regard to data privacy and security. Under the Gramm-Leach-Bliley Act (GLBA), financial institutions, including [Personal financial management companies], are responsible for the implementation of well-established data security requirements and responsibilities to keep consumer data secure." - Consumer Bankers Association (CBA), Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp. 4-6.

- "Data Aggregators Are Financial Institutions Subject to GLBA … Congress included an intentionally robust and expansive definition of "financial institution" in the GLBA. The definition of a "financial institution" incorporates by reference any business that engages in financial activities identified by the Board of Govemors of the Federal Reserve System … pursuant to section 4(k) of the Bank Holding Company Act of 1956 (12 USC 1843(k)). Section 4(k) incorporates the § 225.28 of the Federal Reserve Board's Regulation Y, which is a list of non banking activities that are so closely related to banking "as to be a proper incident thereto" … Also, the FTC determined that data aggregators qualify as "financial institutions" under the GLBA. In the preamble to the FTC's regulation implementing privacy provisions of the GLBA, the FTC explained that the broad language used to describe "data processing" in section 225.28 "brings into the definition of financial institutions an internet company that compiles, or aggregates, an individual's online accounts … at that company's web site as a service to the individual, who may then access all of its

account information through that internet site." The FTC's regulation implementing the GLBA has been incorporated in Regulation P, issued by the CFPB post-Dodd-Frank. The CFPB has stated that it generally will follow the guidance issued by other agencies whose regulations CFPB has restated. Thus, given their fundamental data processing activities, data aggregators fall within the expansive definition of financial institution in the GLBA." — Capital One, Response to CFPB Request for Information Regarding Consumer Access to Financial Records, Docket No. Bureau-2016-0048 (February 21, 2017), pp. 2, 5-8.

- "While the GLBA's security safeguards responsibilities would apply to data aggregators (through enforcement by the Federal Trade Commission), their compliance is unclear as, unlike financial firms, they are not subject to routine regulatory examination. In addition, no federal notification requirement exists to require data aggregators that experience a breach to notify consumers or impacted financial institutions." - Financial Services Roundtable ("FSR") and the FSR's Technology Policy Division – BITS, Response to CFPB Request for Information Regarding Consumer Access to Financial Records, Docket No. CFPB-2016-0048 (February 21, 2017), p. 12.

- "Data aggregators are "financial institutions" in their own right, for the purposes of multiple federal consumer protection requirements (e.g., Gramm-Leach-Bliley Act ("GLB Act")), and should be directly supervised and examined as such." - The Clearing House Association, Request for Information Regarding Consumer Access to Financial Records, cit., p. 3.

5) Several financial institutions and associations representing them also argued that the limitations on consumer liability for "unauthorized transactions" set forth in Regulation E should not apply with respect to an account provider if the improper transactions are initiated as a result of a data aggregator breach or other misconduct.[538] In addition, they argued that account providers should not be liable for unauthorized transactions initiated by or through data aggregators acting as "electronic fund transfer service providers" under Regulation E.[539]

- "If a bank customer gives their account credentials to a [personal financial management companies (PFM)] which subsequently initiates an unauthorized transfer or an unauthorized transfer is initiated by an outside source as a result of a breach of the PFM, the transfer would be considered authorized by the bank because the client had furnished an access device (i.e. login credentials) to the PFM, leaving the customer liable for such transfers. Accordingly, the bank would not be liable for these transfers unless the customer notified them that the transfers by the person, PFM or other vendor were no longer authorized. Consumers might look to a PFM for restitution if they qualify as a "service provider" under Regulation E." - Consumer Bankers Association (CBA), Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp. 7-8.

- "It is unclear whether and when, under the terms of Regulation E: a single sign-on service provided by a Data Aggregator constitutes an "access device" because it is a "code, or other means of access to a consumer's account"; a Data Aggregator is a "financial institution" because it "issues an access device and agrees with a consumer to provide electronic fund transfer services" by providing consumers a single sign-on service and permitting the initiation of electronic funds transfers through the bank; or a Data Aggregator is a "service provider" to the consumer for purposes of Section 1005.14, and therefore subject to liability for unauthorized transfers pursuant to Comment 14(b)-1, if it does not have an agreement with the bank regarding specific access (i.e., outside the scope of any services it may provide to or on behalf of the bank)." - Financial Services Roundtable ("FSR") and the FSR's Technology Policy Division – BITS, Response to CFPB Request for Information Regarding Consumer Access to Financial Records, cit., p. 12.

- "Under federal law, banks are not liable for unauthorized transactions made by the data aggregator or its employees to whom the consumer has provided the "access device," e.g., credentials to access the account and transfer money electronically. Regulation E, which implements EFTA, provides that consumers generally are not liable for unauthorized electronic fund transfers. An "unauthorized electronic fund transfer" is a transfer by someone other than the consumer without actual authority to make the transfer and from which the consumer receives no benefit. The term

[538] See, 12 C.F.R. Section 1005.2(m)(1) (excluding from the definition of an "unauthorized electronic fund transfer" any "electronic fund transfer initiated… [by] a person who was furnished the access device to the consumer's account by the consumer…."). Comment 2(m)-2 clarifies that "[i]f a consumer furnishes an access device and grants authority to make transfers to a person (such as a family member or coworker) who exceeds the authority given, the consumer is fully liable for the transfers unless the consumer has notified the financial institution that transfers by that person are no longer authorized.").

[539] See 12 C.F.R. Section 1005.14(a)(1) ("A person that provides an electronic fund transfer service to a consumer but that does not hold the consumer's account is subject to all requirements of this part if the person: (1) Issues a debit card (or other access device) that the consumer can use to access the consumer's account held by a financial institution; and (2) Has no agreement with the account-holding institution regarding such access.").

does not include transfers "by a person who was furnished the access device to the account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized." The Official Staff Commentary further explains that if the consumer furnishes an access device and grants authority to a person who exceeds that authority, the consumer is liable unless the consumer has notified the financial institution that transfers by that person are no longer authorized. Thus, banks are not liable for unauthorized transactions made through the data aggregator. If a data aggregator is unable or unwilling to reimburse the consumer, the consumer suffers the loss … Data aggregators that permit consumers to initiate electronic fund transfers from accounts held at financial institutions that do not have an agreement with the financial institution are "service providers" under Regulation E, as they issue "access devices" that may be used to permit electronic fund transfers to and from the account. As service providers, they are liable for unauthorized transactions under Regulation E as well as certain other provisions." - American Bankers Association, Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp. 8-9.

6) Certain financial institutions warned that uncertainty about whether account providers can be held responsible for misuse of data might have the negative effect of delaying or impeding the development of industry standards for more secure and reliable access to consumer-permissioned information.

- "Uncertainty about whether account providers can be held responsible for misuse of data provided to third parties could potentially hinder development of industry standards for more secure and reliable access to consumer-permissioned information." - BBVA Compass, Response to Request for Information Regarding Consumer Access to Financial Records ("RFI"), cit., p. 5.

7) Some financial institutions and associations representing them objected to the notion that Section 1033 of Dodd-Frank mandates access to third parties.

- "[Heartland Credit Union Association does] not interpret section 1033 to require a financial institution to provide a third-party with direct access to a consumer's account — regardless of whether the consumer has authorized the third-party to do so. Since the CFPB has not directly cited section 1033 as authority to possibly require financial institutions to provide third-parties with direct account access, [Heartland Credit Union Association is] unsure which section of the Dodd-Frank Act would provide such authority." – Heartland Credit Union Association, Response to Request for Information Regarding Consumer Access to Financial Records ("RFI") Docket No. CFPB-2016-0048 (February 17, 2017), p. 3.

- "[The American Bankers Association does] not believe … that the [CFPB] can use Dodd-Frank Act §1033 to address consumer protection risks associated with data aggregation. §1033 authorizes the [CFPB] to facilitate consumer access to financial information, but that authority does not extend to regulation of third-party access to consumer financial information … Notably, §1033 only applies to consumers accessing their own information. The statute makes no mention of third party access to the information, even where the consumer has apparently granted authority. The plain language of the statute limits access to the account information to the consumer. Had Congress intended to extend access to any person to whom the consumer had provided credentials (especially without the financial institution's knowledge), it would have so provided, as allowing access under such circumstances presents risks not present when consumers are given access to their own account information." - American Bankers Association, Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp.13-14.

- "First, the Dodd-Frank Act requires banks to "make available to a consumer" the consumer's financial information – it does not require banks to provide data to third parties. The legislative history of Section 1033 similarly does not provide support for an interpretation that Congress intended the provision to require banks to allow access by third parties (on behalf of consumers or otherwise) to data, let alone potentially unsafe access. Second, the provision has limited scope … and therefore is more limited than the broad information that a data aggregator may be able to obtain when it accesses bank systems, without bank authorization, using an accountholder's log-in credentials. Finally, the provision only requires that banks "make [such information] available" to consumers, and banks already make consumer financial data available to consumers, for example, through online banking. … In short, we believe that neither Section 1033 nor any other statute requires banks to disclose consumer data to third-party data aggregators, or to otherwise engage in business with or to facilitate the business models of third-party data aggregators and, in fact, such an interpretation would run counter to established competition policy in the United States. Further, recent judicial precedent suggests that data aggregators who access computer sites without the permission of the site's owner may be in violation of the Computer Fraud and Abuse Act, subjecting them to both civil and criminal liability [See, Facebook v. Power Ventures, Inc., 13-17102 (9th Cir. 2016), citing 18 USC 1030(a)(2)(C)]." - The Clearing House Association, Request for Information Regarding Consumer Access to Financial Records, cit., pp. 15-16.

- "The entire text of Section 1033 concerns consumer access, in no place is there any language which indicates that Congress intended the Bureau to ensure permissioned third parties can access customer account data. Consumers of course must be free to use their own account data as they see fit. Consumers can download their data and upload it if they so wish. However, the CFPB simply does not have authority to require community banks to open their systems to third parties, and other entities which may have not implemented appropriate security processes or procedures." – Independent Community Bankers of America, Response to Docket No. CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records (February 21, 2017), pp. 2, 7.

8) Noting that Section 1033 standards should cover data security, authentication, and access, some financial institutions, further, argued that access to consumer financial data should be limited to those aggregators that have contractual privity with the financial institution at issue, and that the data retrieved by the aggregator must be properly identified and fully disclosed to the financial institution at issue.

- "Consumer-permissioned access by an unaffiliated third party can raise questions about the third party's data security and data sharing practices, and the level of control the common customer has to limit the access granted … When the permissioned party establishes a contractual relationship with the financial account provider, the provider can thoroughly evaluate that party's risk management, security, and privacy practices. Applying [BBVA Compass]'s third-party risk management program, these permissioned parties are subject to initial and ongoing review to ensure that the appropriate consumer safeguards and standards are maintained. [BBVA Compass] can also manage operational concerns by agreeing to activity windows that can be sustained without compromising performance of [BBVA Compass]'s other systems." - BBVA Compass, Response to Request for Information Regarding Consumer Access to Financial Records ("RFI"), cit., pp. 3, 5-7.

9) Related to the above, several financial institutions and associations representing them asked the CFPB to clarify the circumstances under which account providers are (and are not) expected to apply their third-party risk management programs when interacting with aggregators.[540]

- "[T]hrough third-party vendor requirements, banks must ensure the vendors they work with are held to the same standards as the bank … These requirements proscribe guidance to banks for assessing and managing risks associated with third-party relationships. By establishing a working relationship with banks, [personal financial management companies (PFMs)] will be checked for critical privacy and security requirements, adding an essential level of protection to consumers. Unfettered access granted to a non-contractual PFM without appropriate risk reviews and controls could run afoul of these regulatory expectations for banks. Without company-wide processes and procedures to ensure that all third parties are systematically screened to verify whether or not they will have access to a company's networks, IT systems or data, third parties can put an organization at risk of reputational impact, regulatory exposure, and revenue loss." - Consumer Bankers Association (CBA), Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp. 6-7.

[540] Prior to entering into third-party relationships, a regulated financial institution must conduct an in-depth assessment of the third party's ability to perform activities in compliance with applicable laws and regulations. Through the due diligence process, the regulated financial institution must review, among others, the third-party's business strategy and goals and must evaluate its compliance programs and risk management programs. See, e.g., Office of the Comptroller of the Currency (OCC), *OCC Bulletin 2013-29, Third-Party Relationships - Risk Management Guidance*, Office of the Comptroller of the Currency (October 30, 2013); Office of the Comptroller of the Currency (OCC), *OCC Bulletin 2017-7, Third-Party Relationships - Supplemental Examination Procedures*, Office of the Comptroller of the Currency (January 24, 2017); Office of the Comptroller of the Currency (OCC), *OCC Bulletin 2017-21, Third-Party Relationships - Frequently Asked Questions to Supplement OCC Bulletin 2013-29*, Office of the Comptroller of the Currency (June 7, 2017); Office of the Comptroller of the Currency (OCC), *Semiannual Risk Perspective - From the National Risk Committee*, Office of the Comptroller of the Currency (Spring 2017); Board of Governors of the Federal Reserve System, *Guidance on Managing Outsourcing Risk*, Board of Governors of the Federal Reserve System SR Ltr. 13-19 / CA 13-21 (December 5, 2013); Federal Deposit Insurance Corporation (FDIC), FIL-44-2008, *Guidance for Managing Third-Party Risk*, Federal Deposit Insurance Corporation (June 6, 2008); Federal Deposit Insurance Corporation (FDIC), FIL-127-2008, *Guidance on Payment Processor Relationships*, Federal Deposit Insurance Corporation (Revised July 2014); Federal Deposit Insurance Corporation (FDIC), FIL-3-2012, *Payment Processor Relationships Revised Guidance*, Federal Deposit Insurance Corporation (Revised July 2014); Federal Deposit Insurance Corporation (FDIC), FIL-43-2013, *Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities*, Federal Deposit Insurance Corporation (Revised July 2014); Consumer Financial Protection Bureau (CFPB), *Compliance Bulletin and Policy Guidance 2016-02, Service Providers*, Consumer Financial Protection Bureau (October 31, 2016); Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), *Joint Advance Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards*, Federal Reserve System Docket No. R-1550 and RIN 7100-AE-61, OCC Docket ID OCC-2016-0016 and RIN 1557-AE06, FDIC RIN 3064-AE45 (October 19, 2016).

- "Entering into bilateral agreements with selected third parties] has served [BBVA Compass] well in integrating with a relatively small number of third parties where [BBVA Compass] has a business interest in the integration. However, it cannot sensibly scale if account providers are required to grant access at no cost to any third party authorized by the consumer. Effective due diligence processes are costly where the account provider does stand to benefit from the relationship. Further, effective due diligence requires the ability for the account provider to be able to decline to enter into the relationship (or terminate the relationship, in the case of existing relationships), which is incompatible with unrestricted consumer-permissioned access to data …This tension with traditional bank third-party risk management standards provides the [CFPB] (and other regulators of account providers) with an important role to play in clarifying the circumstances under which account providers are and are not expected to apply their third party risk management programs. This could be done through amending or adding to examination manuals and/or guidance published by the Bureau and other federal banking regulators on third-party and vendor risk management. The [CFPB] and other regulators could also play a role in developing guidance on appropriate consumer disclosures and risk warnings designed to help consumers understand the implications of granting third parties access to their account data." - BBVA Compass, Response to Request for Information Regarding Consumer Access to Financial Records ("RFI"), cit., p. 5.

10) Financial institutions and associations representing them also asked whether the financial institution and/or the aggregator have to bear the costs associated with compliance. Moreover, they expressed the view that, although access to data should remain free to consumers, if aggregators are monetizing data provided by a financial institution, then some of those proceeds should be paid back to the financial institution.

- "[c]ommunity banks have a vital stake in containing any damage caused by hackers, identity thieves and breaches to third parties. Regardless of where a breach occurs, banks are the stewards of the customer financial relationship. They take measures to restore consumer confidence in the financial system and absorb any upfront costs, which may be significant, of third-party intrusions by responding to customer concerns and inquiries, protecting against fraud and any other expenses. Therefore, any costs associated with a breach or hack should be borne by the entity that incurs the breach. Firms with third-party access to a consumer's account should bear full liability for any consumer harm resulting from a breach to its system." - Independent Community Bankers of America, Response to Docket No. CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records, cit., p. 7.

11) Finally, financial institutions expressed the view that the CFPB should avoid the issuance of strict and unnecessary regulation; recommended that the CFPB coordinate its analysis and intervention with other financial and prudential regulators; and urged the CFPB to support and encourage the development of strong industry standards for account providers and third parties and risk-based security and privacy standards for consumer-permissioned providers, which would foster innovation while ensuring customer protection.

- At a minimum, development of stronger "industry standard" practices for account providers and third parties alike is likely to increase competition and consumer choice if it facilitates smaller consumer-permissioned parties with an opportunity to compete on an equal footing with more established firms. The establishment of a common set of risk-based security and privacy standards for consumer-permissioned providers would foster the flow of information needed for innovation while protecting the consumer. - BBVA Compass, Response to Request for Information Regarding Consumer Access to Financial Records ("RFI"), cit., p. 7.

- "Fidelity does not recommend regulatory action by the CFPB at this time. … [Fidelity] recommends that the CFPB encourage the rapid adoption of [models alternative to screen scraping] by both aggregators and financial services firms. … [Fidelity] recommends that the CFBP coordinate its analysis of these issues with securities regulators who are experienced in evaluating regulatory and operational requirements of securities firms."- Fidelity Investments, Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp. 6-7.

- "[G]iven the variability of approaches and the availability of new technologies, we believe that market participants are best situated to decide which authentication and access technologies should be used. Accordingly, we do not believe at this time that the CFPB should prescribe standards or guidance mandating particular access or authentication practices or technologies, as regulatory standards or guidance are invariably outpaced by technological developments. We do, however, welcome the CFPB's promulgation of guidance concerning the need to move away

from insecure practices with respect to credential sharing, in order to incentivize market participants to invest in the development of new technologies … we recommend that the CFPB formally begin consultation with Federal banking agencies (such as the OCC) and the FTC under section 1033(e) of the Dodd-Frank Act. In particular, the Federal banking agencies would be able to share their perspectives on safety and soundness, reputational risk, and trust in the banking industry with respect to practices in the consumer financial data services marketplace." - Capital One, Response to CFPB Request for Information Regarding Consumer Access to Financial Records, cit., pp. 15, 19.

- "With respect to the specific issue of data access, [Electronic Transactions Association (ETA)] believes that the best way to address these challenges is for financial institutions and the FinTech industry to continue to work together to develop solutions and standards to ensure that consumers are able to permission their financial data safely and securely rather than having the CFPB mandate requirements through rulemaking or other regulatory means. ETA is concerned that any government attempt to implement regulations governing account access information will negatively affect the incentive and ability of institutions to continue to develop new and innovative products and services that benefit consumers." - Electronic Transactions Association, Comments on Request for Information Regarding Consumer Access to Financial Records, Docket No. CFPB–2016–0048 (February 21, 2017), pp. 3-4, 6-7.

(b) Summary of Selected Responses from Data Aggregators, Fintech Companies, and their Industry Representative Groups

1) Data aggregators, fintech companies, and their industry representative groups generally argued that banks should not filter or monopolize access to consumer financial information.

- "Account providers have a significant interest in ensuring that the third parties accessing their systems are legitimate actors that have the technical and operational capacity to keep customer data safe. However, account providers must not attempt to use security concerns as a pretext for restricting access by imposing excessive requirements on third parties that will be impossible for all but the largest potential partners to accept. Similarly, account providers should not impose fees on consumer-permissioned third parties as a de facto method of restricting access to all but their most preferred partners." - Center for Financial Services Innovation (CFSI), Response to CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records (February 21, 2017), p. 7

- As holders of consumer financial account information, banks may also limit third party access to this data. Non-banks may face unreliable transaction feeds from banks. For companies whose services are premised on access to consumer account data, a faulty data feed poses a major problem. Not only is the non-bank unable to provide its service to a consumer, it does not have the ability to fix the problem. … More importantly, these types of periodic and unpredictable blockages are also problematic for consumers. They prevent consumers from being able to rely on fintech applications and in turn, prevent consumers from accessing much-needed financial management tools. Without consistent and up-to-date access to their banking information, consumers may make financial choices based on out-of-date information. … In addition, consumers may face legal uncertainty when they choose to use products and services offered by companies that do not provide transaction accounts. Some banks have adopted terms of service that prohibit a user from sharing her online credentials. Other banks impose liability on consumers for sharing their account information." - Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Record, cit., pp. 5-6.

- "It is important that any of participants not able to prevent the evolution of this ecosystem in a manner that may limit consumers' access and choice. Third-party service providers experience interoperability challenges when data is shared directly by banks and based upon contracts which set varying restrictions for how data is shared, how often and what data will be shared." - Upstart Network, Response to CFPB Docket No. CFPB-2016-0048 Requests for Information: Consumer Access to Financial Records (February 21, 2017), p. 3.

- "Personal financial information belongs to the customer. The [Marketplace Lending Association] therefore believes that although the protection and security of consumer financial inform is of the utmost importance, unnecessary and burdensome restrictions should not be placed on an individual's ability to access and share their own financial data." - Marketplace Lending Association, Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 (February 21, 2017), p.1.

2) Data aggregators, fintech companies, and their industry representative groups also expressed the view that Section 1033 of the Dodd-Frank Act codifies the consumers' right to access their personal financial data, whether directly or indirectly through technology-powered third party platforms.

- "The [Marketplace Lending Association] believes that a consumer's right to access and share their own financial data is currently codified in statute by Section 1033 of the Dodd-Frank Act. Clear guidance from regulators can help guarantee that there is no confusion that it is the consumer, and no one else, who gets to choose which pieces of their financial information can be accessed and shared." - Marketplace Lending Association, Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., p.1.

- "The members of the [Consumer Financial Data Rights Group (CFDR)] believe that the CFPB has an obligation to define and defend [the right of the consumers to access their financial data] as defined by Section 1033 of the Dodd-Frank Act." - Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., p. 1.

3) Some data aggregators and fintech companies expressed the view that the liability for unauthorized transactions under Regulation E, which may result from improper use of a consumer's access credentials, should remain with banks. Moreover, they argued that, if such liability does shift from banks, it should rest with consumers who assumed the risk involved in using their services.

- "Regulation E … limits consumers' liability for unauthorized electronic transactions from their accounts, provided they report the fraud promptly. However, if a consumer "grants authority to make transfers to a person ... who exceeds the authority given, the consumer is fully liable for the transfers unless the consumer has notified the financial institution [(i.e., her bank)] that transfers by that person are no longer authorized." In theory then, if a consumer authorizes an aggregator to check her account balance and that aggregator initiates transactions from the account, the consumer might still be liable for the transactions initiated. Not only could this potential liability deter consumers from using non-bank data aggregation services, it may also deter investment in non-banks thus slowing development of new fintech applications." - Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., p. 6.

4) Some fintech companies and representative groups argued that all ecosystem participants (including data aggregators) should comply with existing legal framework (e.g., the Gramm-Leach-Bliley Act (GLBA) regulating the proper disclosure and use of consumer financial data.

- "Additionally, financial institutions and aggregators alike must comply with the privacy provisions of the [Gramm-Leach-Bliley Act (GLBA)], which requires providing adequate notice to the customer if it wishes to share personal financial information with a third party." - Envestnet Yodlee, Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, Docket No.: CFPB-2016-0048 (February 21, 2017), p. 11.

- "An existing legal framework – the Gramm-Leach-Bliley Act (GLBA) – governs the proper disclosure and use of consumer financial data. Ecosystem participants – both traditional institutions and newer digital players – should abide by this framework, including provisions that limit the use of permissioned data to the scope of the consumer's consent. More generally, the disclosure and use of consumer data by digital products and services is subject to all applicable laws and regulations. - Plaid Technologies, Response to CFPB regarding Consumer Access to Financial Records Docket No. CFPB-2016-0048 (February 21, 2017), p. 22.

5) Some fintech companies and industry groups expressed the view that both data aggregators and fintech companies obtaining data from banks are not, in the ordinary course, "service providers" to banks and should not be subject to the regulatory burdens associated with bank vendor management programs.

- "Financial institutions often attempt to characterize permissioned parties as third party service providers to banks, which allow them to run them through the vetting procedures required by regulators. … In our view, this characterization is inappropriate for the undersigned parties, who do not help banks service their customers. Rather, the members of the CFDR Group each provide services to customers based on information hosted by banks. If banks are able to operate under a framework in which permissioned parties are defined as third party service providers, banks dictate the terms on which permissioned parties can operate and may significantly restrict third parties' ability to access and/or share data. In turn, this limits the kinds of fintech tools available to consumers that provide alternatives to traditional banking, especially for the underserved consumer." - Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., p. 13.

6) Other fintech companies and representative groups expressed the view that each permissioned party accessing data should be vetted, and such vetting process should be performed by an independent intermediary.

- "From Plaid's perspective, each permissioned party accessing data should be vetted and meet obligations around privacy, data security, and acceptable use restrictions that are commensurate with their data access. … Trusted intermediaries play a crucial role in vetting permissioned parties on behalf of consumers, account providers, and the entire ecosystem. They are uniquely well-positioned to do this, and financial institutions are not. Moreover, there are inherent conflicts of interest presented by banks vetting fintech products and services that they perceive as being potential competitors." - Plaid Technologies, Response to CFPB regarding Consumer Access to Financial Records, cit., p. 25.

7) When responding to concerns about data security, fintech companies and their industry representative groups generally argued that financial institutions, aggregators, and other permissioned parties already takes significant measures to protect the security and verification of the information being accessed in compliance with applicable requirements.

- "Banks are required to practice effective risk management by conducting third party audits, background checks, and due diligence. Additionally, financial institutions and third-parties alike must comply with the privacy provisions of the [Gramm-Leach-Bliley Act (GLBA)], which requires providing adequate notice to the customer if it wishes to share personal financial information with a third party. Aggregators that have contractual relationships with OCC-regulated financial institutions are themselves OCC supervised and examined. Banks, aggregators, and PFMs should also require explicit and informed consumer consent for third party account access to ensure that consumers understand and wish to authorize access to their account information. Enabling consumers to revoke this access provides greater flexibility and control over when and how third parties may access this data." - Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., pp. 10-11.

8) In addition, when responding to concerns about data security, fintechs companies and their industry groups argued that technology developments (e.g., APIs, authentication, and tokenization protocols) could help solve many data security problems and challenges.

- "Technology has also enabled aggregators and third party servicers to ensure that data is accessed in a secure and reliable manner. For example, tokenization provides a safe way to control third party access to banking information by allowing an aggregator to identify a consumer and their account without having to obtain their banking credentials. Read-only access is another method to ensure the safe access of account information. By providing a read-only access code to account aggregators, financial institution s may limit third-parties to viewing account balances and histories, rather than being able to initiate funds transfers." - Envestnet Yodlee, Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., p. 11.

- "Although some incumbent institutions tend to frame their concerns as related to "privacy" or "security," the members of this group believe that the objections are largely strategic and submit that it is possible as a technology matter to ensure that data can be shared safely and securely. To wit: account-level information has been shared safely and securely in the United States for the last two decades. To improve the safe and secure transmission of consumer-permissioned financial data that has served consumers in the United States well over the last two decades, this Group suggests that the financial services industry in the United States should embrace an open application program interface ("Open API") framework as a means to providing unfettered and secure access to financial data and, with this letter, urges the CFPB to join in the advocacy for the embrace of an Open API architecture for financial services as a means to improving the financial health of all Americans." - Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., pp. 1-2, 11.

9) Certain data aggregators and fintech companies also stressed the need to avoid unnecessary strict regulation and to encourage industry-led efforts aimed at creating common standards for data sharing.

- "[A]dditional coordination across the industry to establish standards and best practices for vetting will help promote trust and transparency throughout the system and create a level playing field for future innovators … [The Center for Financial Services Innovation (CFSI)] believes the industry can come together develop standards and best

practices for data sharing that enable consumer choice, are inclusive of smaller institutions and promote innovation." - Center for Financial Services Innovation (CFSI), Response to CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records, cit., p. 7.

- "[Financial Innovation Now (FIN)] believes that regulation of permissioned access to consumer financial account data is not necessary at this time. We are concerned that regulation would run the risk of creating a framework that likely would restrict market developments or innovations and not easily adapt to the pace of technological innovation and consumer expectations. This concern is particularly acute with respect to technical standards or a technology mandate … FIN believes that consumers' interests will be promoted most effectively if: … [s]tandards for permissioned access to consumer financial account data are developed by Industry, regularly reviewed and updated, and do not mandate a specific type of technology … FIN recommends that industry standards be developed and applied. Examples of such industry standards and best practices are those envisioned by the Center for Financial Services Innovation ("CFSI") or those contemplated within the Financial Services Information Sharing and Analysis Center ("FS-ISAC"). Developing industry standards, formal or informal, potentially based on the discussions at CFSI or FS-ISAC, would lead to the establishment of a data-sharing ecosystem that is open to all, not only those who bank with the financial institutions that have entered into bilateral agreements. Fundamentally, these standards must include a focus on security, reliability, and consumer consent." - Financial Innovation Now ("FIN"), Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp. 2, 5-6.

- "Interoperability and flexibility are two key considerations in evaluating the potential for a data access standard or standards to benefit the ecosystem. Interoperability for permissioned parties is essential to scale any connected solution … Flexibility empowers financial institutions to make this data available in a way that minimizes technical impact and cost — and keeps customers safe. But interoperability for developers and flexibility for institutions can conflict. Today, trusted intermediaries often play a balancing role — providing technologies that enable interoperability for developers while accommodating the preferences of, and minimizing the demands on, financial institutions." - Plaid Technologies, Response to CFPB regarding Consumer Access to Financial Records, cit., p. 25.

- "The industry should establish security best practices, while simultaneously allowing aggregators access to any data they need … CFPB should work with, and indeed rely on, industry — data aggregators, app developers, and financial institutions — to identify reasonable, effective security standards. Best security practices already exist and the fintech companies in our network have made clear that they are willing to follow any such standards in order ensure continued access to data. Identifying and implementing a meaningful, effective security standard will allow continued growth of the industry and new and better consumer products will develop as companies get access to more granular data." - Tech:NYC, Comments to the Consumer Financial Protection Bureau Docket No.: CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records (February 21, 2017), p. 2

- "There is strong support for the proposition that data obtained from consumer financial account providers, whether directly or through third-party data aggregators, would be more available and reliable if it were available through standardized tools. Consumer financial account providers and third-party data aggregators may be best positioned to determine how data should ultimately be shared provided that the ability for consumers to easily access such information and make it available to others is also adequately safeguarded." - Upstart Network, Response to CFPB Docket No. CFPB-2016-0048 Requests for Information: Consumer Access to Financial Records, cit., p. 3.

- "Kabbage fully supports the creation of broad-based and flexible industry principles to facilitate customers accessing and using the data they are generating." - Kabbage, Response to Request for Information Regarding Consumer Access to Financial Records, CFPB–2016–0048 (February 21, 2017), pp. 12-13

- "The [CFPB] should encourage stakeholders to work towards an industry-led effort to: create and standardize an approved method that would increase the number of financial institutions capable of enabling their customers to take advantage of financial account data through digitally sharing financial information; and encourage financial institutions to make financial account data available in a standardized format. Such a standardization would enhance consumers' ability to confidently access and use their financial information to their advantage, lowering the cost to serve them, decreasing friction, and ultimately allowing financial services companies to provide better products at lower costs to consumers … [Earnest] agrees with CFPB Director Richard Cordray's recent statement that "Consumers should be able to use their financial records and account information and securely share access in an electronic format….". [Earnest] believes that achieving this goal is best accomplished through industry-led standard setting processes and look forward to engaging in these stakeholder discussions." - Earnest, Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048 (February 21, 2017), p. 2.

10) On the other hand, some fintech companies warned that any attempt to impose a single standard for consumer-permissioned access to consumer financial account data could negatively affect competition and could stifle innovation.

- "Our current ecosystem for data aggregation … functions at huge scale with high security connecting 14,000 financial institutions with tens of millions of consumers. One reason it functions so well is the mix of methods used to collect the data, depending upon each circumstance. Any attempt to impose a single "standard" would disrupt the collaborative process that's been built bank-by-bank over twenty years, and rob the system of its inherent resiliency. … There are a number of secure methods for the collection of financial data in general use today. This is not a problem, it's a strength. Different approaches are feasible or optimal for different Banks and Data Hubs under different circumstances. This array of secure options is what makes near-universal data availability possible today. If a new "standard" were to be imposed, that universal access would be shattered." - Personal Capital, Response to the Consumer Financial Protection Bureau's Request for Information Regarding Consumer Access to Financial Records, cit., pp. 1, 4.

11) Finally, some fintech companies and data aggregators urged the CFPB to consider a principles-based approach to the issue of consumer-permissioned access to consumer financial account data and consumer data sharing, thus avoiding the creation of specific rules that might soon become obsolete with rapid technological advancements and market developments. They also encouraged the CFPB to coordinate its action with other regulatory agencies in order to clarify how existing rules apply to third-party services providers accessing consumer financial data and records and to examine the ways in which a principles-based guidance could help encourage more financial institutions to make the data of their customers available to them through third-party applications of their choice.

- "In furtherance of its mandate under Section 1033, Kabbage recommends that the CFPB … (2) develop principles-based standards for customer data access that foster innovation through the financial services ecosystem." - Kabbage, Response to Request for Information Regarding Consumer Access to Financial Records, cit., pp. 2-3.

- "Further coordination among all of the stakeholders in this debate – financial institutions, data aggregators, fintech providers, regulators and consumers – will be critical to achieving a secure, inclusive and innovative financial data-sharing ecosystem that supports consumer financial health- Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., p. 15.

- "[The Center for Financial Services Innovation (CFSI)] urges the CFPB to consider a principles-based approach to [data sharing ecosystem], avoiding the creation of specific rules that will soon become outdated with the quick pace of technological change and market developments. … [The] CFSI thinks the CFPB has an important and constructive role to play by providing principles-based guidance that affirms consumers' right to access their financial data. CFSI believes that such guidance from the CFPB might be the catalyst that is needed to bring all of the necessary stakeholders to the table to develop effective industry-wide solutions. CFSI's Data Sharing Principles may provide a useful starting place … CFSI encourages the CFPB to coordinate with its counterparts in the OCC and other agencies to clarify how existing rules apply to third-party data access, where applicable, and to examine the ways in which principles-based guidance can help encourage more account providers to make their consumers' data available to them in the third-party applications of their choice. In addition, given the increasingly important role that data aggregators play as intermediaries and custodians of consumers' data, the CFSI encourages the CFPB, OCC and other agencies to consider whether bringing them under more direct supervision would contribute to a more open and secure data sharing ecosystem." - Center for Financial Services Innovation (CFSI), Response to CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records, cit., pp. 2-3, 7-8.

(c) Summary of Selected Responses from Consumer Group Representatives

1) Responses from consumer groups identified safe and secure data sharing as a common goal that should be pursued by regulators, financial institutions, data aggregators, and fintech companies.

- "The growing prevalence of data aggregation may call for industry-wide guidance to ensure that consumer data is obtained and transmitted securely, that consumers using third party tools can rely on data to be accurate and timely, and that any granted permissions are clearly communicated to the consumer and can be revoked at any time. A collaborative effort to create industry standards should also ensure that a diverse set of financial service providers are included in the conversation, including financial technology (fintech) companies, nonprofits, prepaid providers, and smaller community banks and credit unions." - Commonwealth, Response to CFPB-2016-0048, Request for Information Regarding Consumer Access to Financial Records (February 21, 2017), pp. 1-2.

- "The CFPB should work with the other bank regulators, the FTC, financial institutions, data aggregators, intermediaries and other parties to address both issues – how data is shared, and what security must be in place for companies that access account data – in order to protect both consumers and institutions from the risks of inappropriate access and use of that data." - National Consumers Law Center, Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048 (February 21, 2017), pp. 1, 5-6.

2) Some consumer groups argued that core privacy, security, and transparency principles should govern the sharing of all consumer data.

- "[The National Consumers Law Center] agrees with the principles set forth in the comments of Consumer Action. Consumers need protections that include: [s]imple, clear disclosures of how consumers' personal financial information would be used and shared, and whom it would be shared with; [a]ccess to and use of consumers' financial data should be limited to the express purpose for which it is being used … unless a consumer specifically authorizes an additional purpose; [d]ata storage must be limited to the need to save individuals' data to provide an ongoing aggregation service. Otherwise providers must be required to delete consumer data as soon as it is no longer needed for the chosen purpose; [p]lain-language statements by data aggregators that they will use data provided by consumers only to fulfill customers' financial goals and that customers retain full control over data access and the ability to revoke that access." - National Consumers Law Center, Comments in Response to Requests for Information: Consumer Access to Financial Records, cit., p. 6.

3) Certain consumer group representatives, further, argued that consumers should not loose Regulation E liability protections for unauthorized transactions when sharing credentials with aggregators, because improper transactions would still be considered "unauthorized" under the regulation.

- "When consumers share their own data with third parties, they must be able to retain their Regulation E rights to be compensated for unauthorized charges. Using third-party financial management tools should not lead to fewer protections for disputed transactions." - Center for American Progress (CAP), Response to Request for Information on Consumer Access to Financial Records (Docket No. CFPB-2016-0048) (February 21, 2017), p. 2.

- "Some financial institutions take the position that consumers lose their dispute rights and liability protection under Regulation E if they give a third party permission to access their account and unauthorized charges result. That is incorrect. The CFPB should take action to stop financial institutions from misrepresenting consumers' liability rights in order to discourage use of competing services …Regulation E rights are not waivable and financial institutions may not change them by contract [Reg. E, § 1005.6(b)(6); Reg. E, Official Interpretations § 1005.6(b)-3;NCLC, Consumer Banking & Payments Law § 5.1.2a, updated online at library.nclc.org.] … [The] exception to the Regulation E liability protection [under 12 C.F.R. §1005.2(m), according to which the term unauthorized transaction does not include an electronic fund transfer initiated by a person who was furnished the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized] does not deprive consumers of error resolution or liability protection when they provide account credentials to third-party services that access account data in the course of providing services to the consumer. Even assuming that a username and password combination is an "access device" and was the device used to make the transfer, the "person" that was furnished the access device is the third-party service … not a rogue employee … Consumers need a clear single source of error resolution if they have been the subject of unauthorized charges. That source, under the mandate of Regulation E, is the account-holding institution." - National Consumers Law Center, Comments in Response to Requests for Information: Consumer Access to Financial Records, cit., pp. 3-4.

4) Consumer representative groups also expressed the view that banks should not be permitted to prevent data access for purposes of stifling competition.

- "Consumers can benefit from accessing their financial account data, and the CFPB should prevent financial institutions from blocking access to that data for the purpose of stifling competition … anti-competitive motives should never be allowed to interfere with consumers' ability to access their own data safely … The CFPB should implement [Section 1033 of the Dodd-Frank Act] by preventing financial institutions from unduly inhibiting consumers' access to their own data." - National Consumers Law Center, Comments in Response to Requests for Information: Consumer Access to Financial Records, cit., pp. 2-3.

5) Lastly, consumer group representatives warned of the need for regulation to avoid harm to consumers.

- "The CFPB should facilitate open access to one's own financial records and set standards for data sharing and security. … [F]irms may not seek to independently permit this access if it could potentially erode their competitive advantage. If industry is unwilling to develop sufficiently robust protocols, the CFPB should set standards under Section 1033 to expand access to third-party data tools and create a more competitive market." - Center for American Progress (CAP), Response to Request for Information on Consumer Access to Financial Records, cit., p. 1.

The CFPB stated that it would review the responses to the Request for Information briefly summarized above and would utilize them to: (1) help the industry develop best practices to deliver benefits to consumers and address potential consumer harms; and (2) evaluate whether to issue relevant guidance or to engage in future rulemaking.[541] At present, it remains to be seen whether the Request for Information will prompt future action by the CFPB, which could include issuance of guidance, rulemaking, and/or enforcement actions, relating to the access, sharing, and use of consumer financial data.

5.B. U.S. Federal Reserve System (Federal Reserve)

While the CFPB has been testing the waters in Open Banking and has sought to gain deeper insights on new financial services that rely on consumer-permissioned access to consumer financial data and account information, the U.S. Federal Reserve System (Federal Reserve) has increasingly focused its attention on the risks and opportunities created by fintech innovation.

In this regard, the goal of the Federal Reserve is clear: "to ensure that consumers are protected and that the safety and soundness of banks is maintained."[542] Toward this end, the Federal Reserve has acknowledged that the application of regulations and laws designed based on traditional financial and banking services / products and traditional market structures may create challenging or novel issues when applied to innovative fintech services / products or new market structures. At the same time, any new regulation and guidance would need to be crafted and implemented in a way that won't restrict future innovation for the benefits of consumers, investors, and the market as whole. Because of this, the Federal Reserve has begun to carefully analyze fintech innovations and their impacts across different areas, including supervision, community development, and financial stability. It has also committed to regularly engage with various participants in the fintech sectors to develop a shared understanding of these issues as they evolve. At the same time, it has sought to gain deeper insights in recent technology and markets developments driving the movement towards Open Banking and has begun to consider which existing guidance and regulations may be ill-suited to capture these developments and connected risks. All these efforts align directly with the Federal Reserve's role in maintaining the stability of the financial system and containing systemic risk that may arise in financial markets.[543]

---

[541] See, Consumer Financial Protection Bureau (CFPB), *Request for Information Regarding Consumer Access to Financial Records*, cit., p. 3.
[542] See, Teresa Cunnan (Executive Vice President and Division Director, Financial Institution Supervision and Credit, Federal Reserve Bank of San Francisco), *Fintech: Balancing the Promise and Risks of Innovation*, cit., pp. 2-4.
[543] Ibidem.

Significantly, in a speech delivered at the Conference on Financial Innovation in Washington in December 2016, Federal Reserve Board (FRB) Governor Lael Brainard referred to the Request for Information issued by the CFPB discussed above and noted that "fintech innovations that rely on data sharing may create security, privacy, and data ownership risks, even as they provide increased convenience to consumers."[544] FRB Governor Brainard also warned that, in the context of consumer permissioned access to consumer financial data, issues such as transparency, data privacy, and data ownership would soon become a growing concern. [545]

A few months later, in a speech delivered at the Northwestern Kellogg Public-Private Interface Conference in April 2017, FRB Governor Brainard returned on the topic suggesting that the FRB has a key role in overseeing the relationships between banks and data aggregators.[546] In particular, she described banks as one of a number of entities in "the fintech stack," and noted that fintech companies are able to build upon the core deposits and related account data, credit origination, compliance management, and payment activities of banks, much like third-party app developers are able to rely on smartphone sensors, processors, and interfaces.

On the other hand, FRB Governor Brainard acknowledged that, different from other entities, banks' activities are much more highly regulated. Regulations of banking activities are critical "to enable consumers to trust their banks to secure their funds and maintain the integrity of their transactions." [547] Because of this, she argued that "[w]hile "run fast and break things" may be a popular mantra in the technology field, it is ill suited to an arena where a serious breach could undermine confidence in the payments system." [548]

Moreover, FRB Governor Brainard recognized that some of the key underpinnings of consumer protection and safety and soundness in the banking world "sit uneasily alongside the requisites of openness, connectivity, and data access that enable today's app ecosystem." [549] These key underpinnings include, for example, regulatory provisions that regulate banks' liability for unauthorized charges and exceptions to such liability, as well as provisions that requires banks to perform extensive risk assessments and due diligence of their service providers, covering a variety of aspects including the service provider's operations and internal controls.[550]

---

[544] See, Lael Brainard (Federal Reserve Board Governor), *The Opportunities and Challenges of Fintech*, cit.
[545] Ibidem.
[546] See, Lael Brainard (Federal Reserve Board Governor), *Where Do Banks Fit in the Fintech Stack?*, Speech Delivered at the Northwestern Kellogg Public-Private Interface Conference on "New Developments in Consumer Finance: Research & Practice," Chicago (IL) (April 28, 2017).
[547] Ibidem.
[548] Ibidem.
[549] Ibidem.
[550] Ibidem (explaining that "before entering an outsourcing arrangement, a bank is expected to consider whether the service provider's internal processes or systems (or even human error at the outside party) could expose the bank and its customers to potential losses or expose the bank's customers to fraud and the bank to litigation; whether the service provider complies with applicable laws and regulation; and whether poor performance by that outside party could materially harm the bank's public reputation … banks are expected to conduct extensive risk assessments and due diligence of their service providers, extending even to operations and internal controls, among other requirements. While that helps ensure a safe and sound banking system, that also makes it more challenging for both the banks and fintech companies to harness safely the interconnectivity that has powered other parts of the digital world."). See,

FRB Governor Brainard, then, analyzed relative benefits and drawbacks of three different approaches to integrating banks into the "fintech stack":

- APIs – FRB Governor Brainard observed that a number of large banks have been developing and opening APIs to outside developers, to enable them to build new financial and banking products and services on banks' platforms.[551] She noted that the fact that API providers can require specific controls and protections over the use of their APIs might raise complex issues when applied onto the highly regulated banking sector. In particular, she argued that "the banks' terms of access may be determined in third-party service provider agreements that may offer different degrees of access. These may affect not only what types of protections and vetting are appropriate for different types of access over consumers' funds and data held at a bank in order to enable the bank to fulfill its obligations for data security and other consumer protections, but also the competitive position of the bank relative to third-party developers."[552]

- Agreements Between Banks and Data Aggregators – FRB Governor Brainard observed that a different approach would be for banks to enter into partner agreements with data aggregators, which would collect consumer financial account data from banks and, then, provide access to that data to outside fintech developers through open APIs. She argued that this approach might benefit fintech developers, which would be able to build innovative financial and banking services and products by connecting to APIs provided by selected vendors, rather than multiple APIs provided by many different banks. In addition, she noted that this approach might be well-suited for those banks that lack the necessary financial resources and/or strategic incentives to create their own open APIs. This is because, by partnering with data aggregators, these banks would have the opportunity to open their systems to thousands of developers, without the need of developing and maintaining their own open APIs. Significantly, FRB Governor Brainard expressed the view that, if the partner agreements between banks and data aggregators are structured as data aggregators performing outsourced services to banks, then banks should also be able to conduct the appropriate due diligence of their vendors.[553]

Further, she observed that some banks have adopted an even more "closed" approach to fintech developers, by entering into individual agreements with selected technology providers or data aggregators.[554] She noted that, in the context of these agreements, banks generally "negotiate for greater control over their systems by limiting who is accessing their data--often to a specific third party's suite of products … many banks use these agreements to limit what types of data will be shared."[555] She stressed the importance for banks of

---

also, Teresa Cunnan (Executive Vice President and Division Director, Financial Institution Supervision and Credit, Federal Reserve Bank of San Francisco), *Fintech: Balancing the Promise and Risks of Innovation*, cit.; Robert Canova (Senior Financial Analyst at Federal Reserve Bank of Atlanta), *Fintech Companies: Banks' Allies or Rivals?*, Federal Reserve Bank of Atlanta View Point – Banking and Finance (March 15, 2016). For further discussion on this point, see Section 5.A.iii above.

[551] See, Chapter 2 above.

[552] See, Lael Brainard (Federal Reserve Board Governor), *Where Do Banks Fit in the Fintech Stack?*, cit.

[553] On this point, see, e.g., Envestnet Yodlee, Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., p. 2. (noting that "Yodlee has been in the aggregation business for m o re than 17 years, and has complied with hundreds o f bank audits and with examinations by the Office of the Comptroller of the Currency ("OCC") throughout its history.").

[554] See, Chapter 2 above.

[555] See, Lael Brainard (Federal Reserve Board Governor), *Where Do Banks Fit in the Fintech Stack?*, cit.

vetting their third parties in order to fulfill their legal and regulatory obligations. On the other hand, she also acknowledged the concerns raised by some consumer groups that "the standards for vetting should be commonly agreed to and transparent to ensure that banks do not restrict access for competitive reasons and that consumers should be able to decide what data to make available to third-party fintech applications."[556]

- Screen Scraping – FRB Governor Brainard noted that, when banks are unable or unwilling to provide permissioned access or they decide to limit or block access, data aggregators can nevertheless collect consumer data for use by fintech developers without the permission, or even potentially without the knowledge, of the bank. This is because, data aggregators and fintech developers can directly ask consumers to give them their online banking logins and passwords; once received such credentials, they can log onto banks' online consumer websites, as if they were the actual consumers, and extract the information they need (screen scraping). FRB Governor Brainard argued that this process may create significant challenges, particularly in terms of privacy and data security. She noted that "[s]ome banks report that as much as 20 to 40 percent of online banking logins is attributable to data aggregators. They even assert that they have trouble distinguishing whether a computer system that is logging in multiple times a day is a consumer, a data aggregator, or a cyber attack."[557] On the other hand, however, she acknowledged that the use of screen scraping might also have positive outcomes. In particular, she observed that "[s]ome fintech firms argue that screen scraping … may be the most effective tool for the customers of small community banks to access the financial apps they prefer--and thereby necessary to remain competitive until more effective broader industry solutions are developed."[558]

Noting that current consumer financial data is accessed and shared through one of the described connectivity approaches, FRB Governor Brainard argued that "getting these connectivity questions right, including the need to manage the consumer protection risks, is critically important. It could make the difference between a world in which the fintech wave helps community banks become the platforms of the future, on the one hand, or, on the other hand, a world in which fintech instead further widens the gulf between community banks and the largest banks." [559]

FRB Governor Brainard recognized that the connectivity solutions discussed above pose a number of risks and may create significant tradeoffs. For example, the connectivity solutions that involve data aggregators and that rely on screen scraping create repositories of consumer credentials, which are extremely vulnerable to cyber attacks. Moreover, because no contractual relationships typically exist between screen scrapers and the banks from which the former pull consumer financial data and information, banks have very little leverage or ability to assess and vet the security of the screen scrapers' systems and methods or their overall risk. In addition, uncertainty still exists as per who – among the bank, the data aggregator, the

[556] Ibidem. See, also, Envestnet Yodlee, Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit., p. 1. (arguing that "[o]ver our almost two-decade history, Yodlee has built a client base that includes 12 of the 20 largest banks in the United States and the largest banks in more than 20 countries.").
[557] See, Lael Brainard (Federal Reserve Board Governor), *Where Do Banks Fit in the Fintech Stack?*, cit
[558] Ibidem.
[559] Ibidem.

fintech developer, or the consumer – shall bear the responsibility for any losses in the event a data aggregator or third-party developer is breached.[560] On the other side, FRB Governor Brainard acknowledged the concerns of fintech companies that banks could "use their control over consumer data access in the context of bilateral contracts with data aggregators to leverage their position in order to impede competition elsewhere in the stack."[561]

Against this background, FRB Governor Brainard remarked the objective of the Federal Reserve of supporting socially beneficial innovations, while at the same time ensuring that any related risks are appropriately managed, consistent with applicable legal requirements.[562]

FRB Governor Brainard, further, pointed to a variety of approaches to facilitate connectivity in financial services that are currently being taken by regulators around the world, with particular focus on the Open Banking frameworks currently developed in the UK and the EU/EEA. However, she expressed the view that, at least initially, the United States would likely address the issues in a different way, "given that regulatory authorities are more broadly distributed, and the relevant statutory language predates these technological developments."[563] In particular, she discussed a number of initiatives undertaken by U.S. federal agencies addressing issues surrounding consumer permissioned access to consumer financial data and information, including the CFPB's Request for Information discussed above and the Office of the Comptroller of the Currency (OCC)'s special purpose national bank charter discussed in Chapter 7.[564]

FRB Governor Brainard also stressed the relevance of existing safety and soundness regulation. For example, she suggested examining vendor risk management guidance, which could help banks connect more securely and efficiently with the fintech apps utilized by their consumers; and recommended conducting periodic assessments of whether (and how) authority under the Bank Service Company Act might pertain to developments in the fintech sector.

Finally, while noting that the industry is experimenting with innovative connectivity solutions and may it soon develop widely accepted standards, FRB Governor Brainard encouraged greater cooperation among regulators, the private sector, and other stakeholders. As the open banking ecosystem rapidly evolves, she remarked the importance for such collaborative efforts to address not only the technical challenges, but also the important policy, regulatory, and legal questions discussed above.

---

[560] Ibidem (noting that "[s]ome third-party developers have included terms and conditions that specifically limit their liability to consumers.").
[561] Ibidem.
[562] Ibidem (arguing "[w]e do not want to unnecessarily restrict innovations that can benefit consumers and small businesses through expanded access to financial services or greater efficiency, convenience, and reduced transaction costs. Nor do we want to drive these activities away from regulated banks and toward less governed spaces in the financial system.").
[563] Ibidem.
[564] Ibidem (arguing that "obtaining a special purpose charter would have the practical effect of allowing certain fintech companies (companies that make loans, make payments, or accept deposits) to potentially bypass the need for connecting to a bank for certain purposes in favor of becoming licensed as banks themselves.").

5.C. Industry-Driven Initiatives

5.C.i. Common Principles and Best Practices for Consumer Data Sharing

As previously discussed, a large number of U.S. based data aggregators, fintech companies, and their representative groups have expressed the view that regulation of permissioned access to consumer financial account data is not necessary at present.[565] The risk - they have argued - is that any such regulation would soon become obsolete and would create a framework that would restrict market developments and stifle innovation. Because of this, they have recommended increased coordination across the industry to create common standards and best practices for data sharing. These standards and best practices should enable consumer choice, be inclusive of smaller institutions, properly address privacy and data security concerns, be flexible and (to the extent possible) technology neutral. Identifying, implementing, and maintaining such standards and best practices, in turn, would: help increase privacy and data security; promote trust and transparency throughout the system; lead to the establishment of a data-sharing ecosystem that is open to all; and spur further technology and market developments, while also creating a level playing field for future innovators.

Examples of such industry standards and best practices are those identified by the Financial Services Information Sharing and Analysis Center (FS-ISAC)[566] and those envisioned by the Center for Financial Services Innovation (CFSI).[567] The standards and best practices proposed by the CFSI are discussed in detail below.

Center for Financial Services Innovation ("CFSI"). On 24 October 2016, the CFSI released a guide for the responsible sharing of consumer financial data titled "CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration" (CFSI Data-Sharing Guide).[568] The CFSI Data-Sharing Guide was developed in collaboration with numerous industry experts; it was built on CFSI's previous work to establish industry-specific principles and best practices leveraging CFSI's Compass Principles;[569] and was written taking into consideration the various initiatives undertaken by U.S. regulators discussed above.[570]

---

[565] See, Section 2.C. and Section 5.A.iii. above.

[566] See, Section 2.A.iii. above. See, also, Financial Services Information Sharing and Analysis Center (FS-ISAC), API Breaches, FS-ISAC Expert Webinar Series (May 23, 2017).

[567] The Center for Financial Services Innovation (CFSI) is a national authority on consumer financial health, which leads a network of financial services innovators (e.g., banks, fintech companies, processors, servicers, non-profits, and community-based organizations) committed to building a more robust financial services marketplace with higher quality products and services. Through its Compass Principles and a lineup of proprietary research, insights and events, CFSI informs, advises, and connects members of its network to seed the innovation that will transform the financial services landscape. Through its consulting work, its Financial Capability Innovation Funds, and its Financial Solutions Lab, the CFSI fosters innovative products and technologies that improve the financial health of consumers and nurture small businesses. More information on the CFSI and its activities is available on the CFSI's website at http://cfsinnovation.org.

[568] See, Center for Financial Services Innovation (CFSI), *CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration*, Center for Financial Services Innovation Report (October 2016).

[569] More information on the CFSI's Compass Principles is available on the CFSI's website at http://cfsinnovation.org/research/compass-principles/.

[570] See, Center for Financial Services Innovation (CFSI), *Center for Financial Services Innovation Unveils Framework for Responsible Industry-Wide Sharing of Consumer Financial Data*, Center for Financial Services Innovation (October 24, 2016) (quoting Jennifer Tescher (CFSI CEO) stating that "[a]s evidenced by Director Cordray's comments, the ownership and sharing of

The CFSI Data-Sharing Guide contains aspirational principles to guide the development and operation of the financial data sharing ecosystem and specific practices to lay the foundation for achieving those principles. Taken together, the CFSI's principles and practices are intended to serve as a roadmap helping fintech innovators, data aggregators, and financial institutions work together in support of improved consumer financial health outcomes.

In the CFSI Data-Sharing Guide, the CFSI acknowledged that consumers' ability to understand, manage, and improve their financial health requires having a full picture of their financial lives. It, then, observed that over the last two decades, the emergence of data aggregators has enabled traditional and non-traditional providers to offer innovative products and services to consumers, which give them a more complete view of their financial lives. These developments have had the positive effect of empowering consumers to more effectively manage their financial lives and improve their financial health, but they have also raised questions, and have generated concerns, around data security and privacy, consumer control, and transparency.

The CFSI noted that while a number of Open Banking regulatory and policy initiatives have been developed in the UK and in EU/EEA, no U.S. guidelines or regulatory requirements exist that govern access to consumer within the unique complexity of the U.S. financial system. Against this background, the CFSI encouraged greater industry coordination and stressed the importance of a self-regulating role that the industry can play through the development of shared principles and standards. To this end, the CFSI proposed five key principles, which can help the financial services industry establish data-sharing best practices that are secure, inclusive and innovative:

- Availability - Consumers must have the ability to view their financial information within trusted and secure third-party applications of their choice.[571]
- Reliability - Consumer financial data must be timely, consistent, accurate and complete.[572]
- Consent - Consumers must have the ability to provide explicit consent for access to and use of their data that can easily be viewed, modified and revoked.[573]

---

consumer financial data has become a crucial topic to both financial services organizations and innovators alike … We share the view that consumers' ability to understand, manage and improve their financial health requires having a full picture of their financial lives. By working with a wide range of stakeholders we have assembled a sensible, yet actionable set of principles that encourages everyone to collaborate in the best interests of the consumer - and that will help accelerate innovation in this critical space.").

[571] See, Center for Financial Services Innovation (CFSI), *CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration*, cit., pp. 4-5 (recommending that "[f]inancial institutions and data aggregators agree on audit standards for new third-party application providers intended to promote security and minimize fraud; … Financial institutions, data aggregators and third-party application providers may collaborate in the development of a centralized auditing entity that would certify the security of new entrants and be responsible for the ongoing maintenance of a single industry-wide auditing standard. To the greatest extent possible, financial institutions, data aggregators and third-party application providers exchange data under mutually agreed-upon terms.").

[572] Id., pp. 5-6 (recommending that "[f]inancial institutions, data aggregators and third-party application providers collaborate to determine what data will be shared to achieve application functionality. Financial institutions, data aggregators and third-party application providers establish a known timing and volume of data transfers to provide optimal functionality for the consumer. Financial institutions do not disrupt the flow of data unless there is significant and demonstrable security or system integrity risk to the business or a security risk for the consumer. … Data aggregators inform financial institutions of any suspicious attempts to access data and/or systems. Consumers are provided with clear, easy-to-use means to resolve data reporting errors.").

[573] Id., pp. 6-7 (suggesting that "[t]hird-party application providers seek consumer permission for the specific data access necessary to enable application functionality at the time of enrollment. … Consumers maintain their consent, either through a readily-available and clear revocation option or by renewing permission on an established timeline. … The ability to clearly view and revoke previously-

- Security - All entities must follow applicable laws and industry best practices with regard to data privacy and security.[574]

- Minimization - Only the data required for application functionality shall be collected, and stored only for the minimum amount of time needed.[575]

The CFSI, further, acknowledged that, while the principles and practices identified in the CFSI Data-Sharing Guide provide an important starting point, significant work would still need to be done in order to ensure that such principles and practices are applicable across the industry. Because of this, the CFSI encouraged further coordination among all various stakeholders involved (e.g., financial institutions, data aggregators, fintech providers, regulators and consumers themselves), as key condition for achieving a secure, inclusive, and innovative financial data-sharing ecosystem that supports consumer financial health.

In conclusion, the CFSI discussed five potential long-term solutions to ensure inclusive and secure data access for consumers, which would require significant coordination and infrastructure developments beyond those outlined in the CFSI Data-Sharing Guide:

- Industry-Wide API or Other Technical Standards – The CFSI expressed the view that implementing and maintaining a common set of data-sharing standards, implementation guidelines, and technical infrastructure solutions would significantly benefit all market participants. For example, it observed that initiatives such as the OFX Consortium[576] and the UK's Open Banking Working Group[577] could provide informative precedents for the creation of industry-wide API or other technical standards. On the other hand, the CFSI acknowledged that these initiatives would require greater coordination among industry participants, as well as substantial investment in new financial institution technology infrastructure. It also recognized that not all financial institutions can afford such investments, and, therefore, suggested that the providers of core banking services could play key role in making such technology available to the entire ecosystem.[578]

- Cooperative Development Among Financial Institutions – The CFSI observed that in past financial institutions have established jointly-owned and jointly-operated entities to provide services to the broader marketplace. A notable example of such entities is ClearXChange network for faster payments. The CFSI, thus, suggested apply a similar model to data sharing. In particular, it argued that the use of common processors by many smaller financial institutions could have significant benefits, including:

---

permissioned data access is available at any time through the third-party application. Financial institutions and data aggregators may collaborate to develop dashboards, either via the financial institutions' websites or a third-party site, which provide the consumer with the ability to view, modify and/or revoke consent for all of the third-party applications to which consent has been provided.").

[574] Id., p. 7 (recommending that "[f]inancial institutions, data aggregators and third-party application providers collaborate to define industry-wide standards and protocols for consumer data sharing. … All entities that participate in the generation, collection, transfer and storage of consumer financial data follow applicable laws and industry best practices regarding data privacy and security.").

[575] Id., pp. 7-8 (recommending that "[f]inancial institutions, aggregators and third-party application providers agree on the minimum amount of data necessary to achieve application functionality. Financial institutions, aggregators and third-party application providers agree on the maximum storage time to achieve application functionality … Data that are no longer required for the application functionality or for legal compliance are destroyed.").

[576] See, Section 2.A.ii.

[577] See, Section 4.A.

[578] See, Center for Financial Services Innovation (CFSI), *CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration*, cit., p. 9.

facilitating wider adoption of technology and data management standards across many financial institutions; helping maintain standards, build infrastructure, and provide innovative solutions, while allowing each entity to retain control over the implementation.[579]

- The "Credit Bureau" Model – The CFSI argued that a compelling solution for more secure data sharing could also involve the creation of a trusted, transparent, and accessible intermediary, which would be tasked with "collecting, monitoring, storing and sharing data; providing a centralized error-resolution process; and vetting new market entrants."[580] Because they already perform many of these tasks, the CFSI suggested that data aggregators could take a leading role in the establishment of such an entity. Relevant examples of this model that could be used as references include credit bureaus and the Vendor Security Alliance.[581]

- Complete Consumer Data Ownership – The CFSI acknowledged that in theory consumers "own" their data, but in practice such data remains "a largely intangible and widely-dispersed resource that is difficult to control or manage."[582] In particular, the CFSI observed that, at present, a model of complete financial data ownership by consumers has few systems in place to leverage and very limited examples to use as references (e.g., Personal Data Project and Handshake). Nevertheless, the CFSI argued, such model would have "the potential to fully disrupt the concept of data sharing," by enabling not only access and control for consumers, but also further monetary and service benefits yet to be defined.[583]

- Government Regulation – The CFSI warned that regulation of consumer data access could pose a challenging trade-off: on one hand, such regulation could create a level playing field for all actors and could help protect consumers' interests; on the other hand, such regulation could restrict further market developments and technology innovations. For this reason, the CFSI recommended the CFPB and other agencies carefully balance the tradeoffs between regulatory certainty and the flexibility that market participants need in order to continue innovating; and encouraged providers to proactively engage with regulators to help them gain a better understanding of the numerous challenges and opportunities involved in data sharing.[584]

5.C.ii. Fintech Industry Lobbying Groups

Following interest from several U.S. regulatory agencies on the issue of consumers' ability to access and share their financial data and information, leading fintech companies have formed lobbying groups to

[579] Ibidem.
[580] Ibidem.
[581] Vendor Security Alliance (VSA) is a coalition of leading technology companies, launched by Palantir Technologies, Twitter, Uber, Square, Atlassian, Go Daddy, Dropbox, Docker, and Airbnb in September 2016. The VSA was formed to verify the cybersecurity practices of third-party vendors and streamline vendor security compliance and vetting process. In collaboration with the VSA, experienced compliance officers and leading security experts release a yearly questionnaire to benchmark their risk. Companies can, then, use this questionnaire to qualify vendors and ensure that appropriate controls and security measures are in place. The first questionnaire was released in October 2016. More information on the VSA and its activities is available on the VSA's website at https://www.vendorsecurityalliance.org.
[582] See, Center for Financial Services Innovation (CFSI), CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration, cit., p. 10.
[583] Ibidem.
[584] Ibidem.

advocate for allowing consumers to access and share their financial data with chosen third parties. This section focuses on the activities of two of these lobbying groups, the Consumer Financial Data Rights (CFDR) and Financial Innovation Now (FIN).

Consumer Financial Data Rights (CFDR). On 19 January 2017, a group of fintech companies announced the formation of the Consumer Financial Data Rights (CFDR), an industry coalition that brings together some of the most influential and innovative companies in the fintech ecosystem, including Affirm, Betterment, Digit, Envestnet | Yodlee, Kabbage, Personal Capital, Ripple, and Varo Money, among others.[585]

The CFDR supports the consumers' right to innovative products and services that improve their financial well-being and are powered by unfettered access to their financial data. It encourages open data access and promotes the sharing of data via open APIs as the way forward. The CFDR is committed to drive financial innovation in a collaborative ecosystem by bridging the needs of consumers, banks, fintech innovators, and regulators. It also aims to improve dialogue throughout the financial industry, to actively engage the government, and to work with banks, fintech companies, and third-party platforms.

Among its initial activities, on 21 February 2017, the CFDR submitted a joint comment letter in response to the CFPB Request for Information discussed above.[586]

Prior, on 17 February 2017, the CFDR submitted a joint comment letter in response to the advanced notice of proposed rulemaking on enhanced cyber risk management standards issued by the Federal Reserve Board, the Office of the Comptroller of the Currency (OCC), and the FDIC discussed in Chapter 1.[587] In its response to the advanced notice of proposed rulemaking on enhanced cyber risk management standards, the CFDR expressed the view that the scope of the proposed rulemaking as currently drafted is overbroad in the extreme; and it warned that broad application of enhanced cyber risk management standards could be used by covered financial institutions to deny access to consumer data by third parties that refuse to assume the compliance burden of becoming service providers to those institutions. This, in turn, would stifle further innovation and, ultimately, hurt consumers. Because of this, the CFDR encouraged the Federal reserve Board, OCC and FDIC to: (1) use a risk-based framework to define the scope and application of Enhanced Cyber Risk Management Standards; (2) review the proposed rulemaking to focus more narrowly on those third-party providers to covered financial institutions whose depth of connections with and/or provided services to those institutions would pose a significant risk if attacked; and (3) in reviewing the proposed rulemaking, allow for variation by size, function, and profile of regulated institutions.[588]

---

[585] See, e.g., Envestnet Yodlee, *New Industry Group Established to Support Consumers' Right to Access their Financial Data*, Envestnet Yodlee Press Release (Redwood City (CA), January 19, 2017); Bryan Yurcan, *Fintech Companies Form Lobbying Group Focused on Data Sharing*, American Banker (January 19, 2017).
[586] See, Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, cit.
[587] See, Consumer Financial Data Rights Group (CFDR Group), CFDR Group Comment Letter to "Enhanced Cyber Risk Management Standards" Docket ID OCC-2016-0016 (February 17, 2017).
[588] See, Consumer Financial Data Rights Group (CFDR Group), CFDR Group Comment Letter to "Enhanced Cyber Risk Management Standards," cit., pp. 2-3.

Financial Innovation Now (FIN). On 3 November 2015, technology industry leaders - including Amazon, Apple, Google, Intuit and PayPal - announced the formation of Financial Innovation Now (FIN), a coalition that promotes policies to help foster greater innovation in financial services.[589]

FIN and its member companies share the belief that financial innovation: (1) empowers consumers, by improving access to financial tools and services, increasing convenience and ease of use, and helping users save money and lower costs; and (2) supports the growth of small businesses, by enabling greater access to capital for them and providing them with analytical tools to make strategic, data-driven decisions, and strengthen authentication and security solutions. In its efforts to encourage financial innovation, FIN promotes policies that aim to: realize trust and safety of new technologies; leverage technology to reduce barriers and enhance access for the underserved; enable real-time payments clearing processes; expand the online marketplace for consumer and small business lending; and unlock the power of financial applications.

Significantly, ensuring consumers have unobstructed access to their own financial information is a founding principle of FIN.[590] In this regard, FIN has acknowledged that consumers and small businesses are increasingly using innovative applications to better manage their financial lives and leverage their own financial data to qualify for better rates and services. Consumers and small business need clear access to their accounts to enable these benefits. For this reasons, FIN has encouraged policymakers to empower consumers and small businesses to securely access their own accounts via whatever application or technology they wish, without charges that could favor one application or technology over another.[591]

On October 2016, in commenting the publication by CFPB of Project Catalyst Report,[592] Brian Peters (Executive Director at FIN) praised the CFPB for recognizing the importance of consumers' ability to securely access financial information to better manage their financial lives. He, then, reaffirmed the FIN's commitment to work closely with the CFPB to achieve the mutual goal of ensuring that financial technology can "operate transparently and efficiently to facilitate access and innovation."[593]

Most recently, on 21 February 2017, FIN submitted a comment letter in response to the CFPB Request for Information discussed above.[594] In its response letter, FIN expressed the view that consumers' interests would be promoted most effectively if: (1) consumers could give permission to access their financial account data securely and easily, using any secure application or technology of their preference, without

[589] See, Financial Innovation Now (FIN), *Tech Industry Leaders Launch Coalition to Advocate for Policies to Foster Innovation in Financial Services*, Financial Innovation Now Press Release (Washington (DC) (November 3, 2015)). More information on FIN and its activities is available on FIN's website at http://financialinnovationnow.org.
[590] See, Financial Innovation Now (FIN), *Statement by Brian Peters*, Executive Director of Financial Innovation Now, Financial Innovation Now Press Release (November 17, 2016).
[591] See, Financial Innovation Now (FIN), *Financial Innovation Now | Policy Priorities*, Financial Innovation Now, p. 2. See, also, Financial Innovation Now (FIN), *Letter to the Honorable Donald J. Trump President-Elect of the United States and the Trump-Pence Transition Team*, Financial Innovation Now (November 30, 2016), p. 2.
[592] See, Section 5.A. above.
[593] See, Financial Innovation Now (FIN), *Statement by Brian Peters*, Executive Director of Financial Innovation Now, Financial Innovation Now Press Release (October 24, 2016). See, also, Financial Innovation Now (FIN), *Statement by Brian Peters*, Executive Director of Financial Innovation Now, Financial Innovation Now Press Release (November 17, 2016).
[594] See, Financial Innovation Now (FIN), Response to Request for Information Regarding Consumer Access to Financial Records, cit.

charges or restrictions that unreasonably favor any one application or technology over another; and (2) the industry developed, and regularly reviewed and updated, technology neutral standards for permissioned access to consumer financial account data."[595]

[595] Id., pp. 2, 4-6.

CHAPTER 6. TIME FOR A NEW KIND OF BANK

The path towards Open Banking driven by the forces discussed in Chapter 1, enabled by the technology advances analyzed in Chapter 2, and accelerated by the regulatory developments examined in Chapters 3 to 5, has a significant impact on banks and other established financial institutions.

In particular, Open Banking breaks a long time trend of consolidation within the banking and financial services industry, while accelerating specialization and modularization.[596] In addition, Open Banking helps drive disruptive innovation in the financial and banking services industry and offers fintech companies a chance to disintermediate banks' profitable customer-facing businesses, while avoiding capital-intensive areas. This, in turn, has the potential effect of slicing off the higher-return on equity segments of banking's value chain in origination and sales, thus leaving banks with the basics of asset and liability management.[597]

Reports by McKinsey estimate that, if banks do not take any mitigating actions, then in five major retail banking businesses (consumer finance, mortgages, SME lending, retail payments and wealth management) from 10% to 40% of revenues (depending on the business) and between 20% and 60 % of profits will be at risk by 2025, with consumer finance being the most vulnerable.[598] Similarly, a report by Accenture estimates that evolving customer preferences, advances in technology and increased competition by fintech companies and large technology companies may cause a dramatic erosion of UK banks' payment revenues, down to 43% of current payments based revenues by 2020.[599] In addition, the report by Accenture indicates that UK banks are set to see their interest-based revenue streams significantly impacted by a loss of "customer ownership," resulting from the displacement of bank-customer interactions by fintech or progressive traditional financial services companies.[600]

A more recent report by McKinsey argues that a combination of three main forces — digitization, regulation, and a weak global economy — threatens to significantly reduce profits for the global banking industry over the next three years.[601] Both developed-market banks and emerging-market banks face this challenge: the former are likely to be most affected, with nearly $90 billion (25%) of profits at risk; whilst the latter are vulnerable especially to the credit cycle. Among major developed markets, the US banking industry appears to be best positioned to successfully address the described challenge; whilst the European and UK banking industries might incur more severe losses, having nearly $35 billion (c. 31%) of profits at

[596] See, e.g., PWC, *Who Are You Calling a 'Challenger'? How Competition is Improving Customer Choice and Driving Innovation In the UK Banking Market*, cit., p. 22; McKinsey & Company, *The New Rules for Growth through Customer Engagement*, cit., pp. 32-33; Earnix, *The Role of Analytics in the Banking Age*, Earnix Report (2017), pp. 4-5.
[597] Cfr., e.g., McKinsey & Company, *A Digital Crack in Banking's Business Model*, McKinsey Quarterly Insights (April 2016); Ernst & Young, *Landscaping UK Fintech*, cit., p. 5; McKinsey & Company, *The Digital Battle that Banks Must Win*, cit.
[598] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., p. 5; McKinsey & Company, *The Fight for the Customer: Mckinsey Global Banking Annual Review 2015*, McKinsey Global Banking Report (March 2015).
[599] Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., p. 3.
[600] Id., p. 4.
[601] See, McKinsey & Company, *A Brave New World for Global Banking*, cit.

risk.[602] Digital disruption might further reduce banks' profits from current $110 billion to $50 billion in 2020 and significantly cut returns on equity by 2020, even after some mitigating actions. [603]

In addition to the foregoing (and perhaps most important), the movement towards Open Banking poses a significant risk of loss of customer insights to banks.[604] The danger is real, as banks need (at minimum) an opportunity to engage with their customers in order to build loyalty, cross-sell successfully and deliver a rewarding customer experience.[605]

A first manifestation of this threat is the "break-up" or "atomization" of banking and financial services discussed in Chapter 1, whereby customers increasingly utilize banking and financial products and services provided by various fintech companies and technology giants. This not only reduces the opportunities to cross-sell for banks, but it also causes banks to loose customer insights and data, thus, eroding a key competitive advantage that banks have long enjoyed. A second manifestation of this threat is the opening-up of access to banks' customer account data to third-party services providers discussed in Chapter 2, whereby customers can conduct their banking and financial activities (e.g., checking account balances, viewing transaction histories and initiating payments) from a third-party online portal with limited or no meaningful engagement with their banks. This creates the danger for banks of losing a direct front-end relationship with their customers (and therefore the ability to cross-sell or up-sell), because third party services providers increasingly handle everyday customer interactions. Against this scenario, if banks do not take any action, they will face the risk of becoming mere "utility-type" providers used by third-party services providers.[606]

Because of the reasons discussed above, the movement towards Open Banking ultimately forces banks to reassess their role in the banking and financial services industry.[607]

As noted in a recent report by McKinsey, to overcome the challenges and fully exploit the opportunities created by Open Banking, banks must undertake a radical transformation focused on three main themes - resilience, renewal, and reorientation:[608]

Resilience. First, banks must perpetrate and safeguard the short-term viability of their business (resilience). This requires implementing measures to protect revenues, reduce short-term costs, manage capital and risk, and protect core business assets.[609]

---

[602] Ibidem.
[603] Ibidem.
[604] See, Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., p. 9; Deloitte, *Open Banking: What Does The Future Hold?*, cit., p. 5.
[605] See, Earnix, *The Role of Analytics in the Banking Age*, cit., pp. 6-7 (surveying a total of 300 senior banking executives at UK and European banks and reporting that "73% of bankers expect Open Banking to diminish the advantage of existing customer relationships and make it more difficult for banks to cross-sell and 75% believe banks will have to significantly overhaul their pricing and value models in order to maintain market share over the next five years.").
[606] See, Contino, *An AWS Centric Solution Architecture For Open Banking*, Contino Report (March 7, 2017), p. 3.
[607] See, e.g., Deloitte, *Open Banking: What Does The Future Hold?*, cit., p. 8; Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., p. 9.
[608] See, McKinsey & Company, *A Brave New World for Global Banking*, cit.; McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., pp. 8-12.

Renewal. Second, banks need to streamline their operating models and IT structures, platforms and systems (renewal).[610] At present, the vast majority of banks have legacy IT structures, platforms and systems that are extremely articulate and complex. These legacy IT structures, platforms and systems provide the back-office operations for thousands of products and services; they must comply with stringent security and compliance requirements; and they must support rigorous risk-management standards.

Significantly, many of these legacy IT structures, platforms and systems were designed decades ago and poorly fit with today's customers' expectations to be able to engage with their banks whenever they want, wherever they are, and through any preferred channel, be it via mobile, tablets, desktop, or over the phone.[611] On top of this, many of these legacy IT structures, platforms and systems are now highly fragmented. As a result, making them work in today's environment is extremely costly: a significant part of banks' IT budget is allocated to maintenance; and IT maintenance costs are likely to rise year after year as fintech companies enter new areas of the banking value chain. Finally, by relying on poorly integrated legacy IT structures, platforms and systems, banks are also exposing themselves to significant operational risks and cyber security threats.[612]

To address these challenges, an increasing number of banks are now deploying advanced technologies, ranging from mobile to agile to cloud.[613] Boosting internal innovation will help banks modernize their infrastructures in a cost-efficient way, will give them increased agility, and will allow them to promptly and appropriately respond to rapid market changes.

Furthermore, in order to mitigate the potential cost advantage of fintech companies and to address the evolving needs of their customers, banks are rapidly transforming their systems through radical simplification, process digitization, and streamlining.[614] An increasing number of banks are now leveraging the power of new technologies to offer a holistic, secure and fully digital experience for customers. This includes, for instance: paperless know-your-customer (KYC) process that rely on the use of biometric technologies; interactive and intuitive digital financial planner services; financial robo-advisory services; electronic, fast, and simplified processes of application and approval of mortgage or loan that utilize a massive number of structured and unstructured data collected and processed within seconds to determine

---

[609] See, KPMG, *The Digital Bank of the Future. Setting Course in a Disrupted Marketplace: Becoming the Digital Bank of the Future*, KPMG Insights (April 5, 2017); KPMG, *Setting Course in a Disrupted Marketplace. The Digitally-Enabled Bank of the Future*, KPMG Report (April 2017), pp. 10-11.

[610] See, Accenture, *The Future of Fintech and Banking: Digitally Disrupted or Reimagined?*, Accenture Report (2015), pp. 4-5.

[611] See, e.g., Lael Brainard (Federal Reserve Board Governor), *Where Do Banks Fit in the Fintech Stack?*, cit. (noting that "[m]ost banks' core systems are amalgams of computing mainframes built decades ago before the Internet or cloud computing were widely available and, in many cases, stitched together over the course of mergers and consolidations. It takes a lot of investment to securely convert that infrastructure to platforms that can operate in real-time with ready access for Internet-native third-party developers.").

[612] The Economist, *The Disruption of Banking*, cit., pp. 4-5.

[613] McKinsey & Company, *Banking on the Cloud*, cit.; McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., p. 11.

[614] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., p. 10; Ernst & Young, *Revolutionary Change is Transforming the Financial Services Landscape. Financial Services Leadership Summit December 2016*, cit., pp. 7-11; McKinsey & Company, *Building a Digital-Banking Business*, cit., pp. 5-7; McKinsey & Company, *A Brave New World for Global Banking*, cit.; Massachusetts Institute of Technology (MIT), *Digital Banking Manifesto: The End of Banks?*, cit., pp. 7-8, 11-13; Microsoft, *Digital Transformation in Financial Services: From Strategy to Reality*, Microsoft Financial Services - Banking & Capital Markets Insights (April 13, 2017).

the borrower's creditworthiness and risk of default; and simplified, fast and at no-cost domestic and international wire transfers.

Reorientation. Third, in addition to resilience and renewal discussed above, banks must prepare and implement an effective reorientation agenda.

The transformation at stake goes far beyond technology. This means that, if banks want to thrive in the new Open Banking ecosystem, they cannot simply respond by establishing a digital presence and making their existing products and services available in mobile and online form. Hence, banks will need to reinvent themselves and identify and implement new and different approaches to their business to provide the flexibility that speaks to the real-world needs of their customers. Banks will also need to consider how to further develop their franchises to create and cultivate an ecosystem around their customers and form much closer relationships with them. To be relevant to their customers, banks will need to evolve their own business models, potentially reducing their short-term revenues in order to access longer-term, but larger, revenue pools.[615] At the same time, banks will need to make higher risk investments in innovation and to develop new investment assessment criteria in order to properly identify, select and execute any of such investments.[616]

To achieve these goals, banks should examine a number of critical areas, which are discussed in more detail in the following sections.

6.A. Flexible, Synchronized, and Personalized Multi-Channel Presence

The movement towards Open Banking and the related development of open API ecosystems are driving a shift from bank product-centric interactions to customer-centric interactions.[617]

At present, forward-thinking banks are increasingly seeking to orient themselves around their customers. In this context, flexible, synchronized and personalized banking is becoming the new norm. Customers want to have the flexibility to bank at all hours, anywhere, through multiple devices. Because of this, banks need to offer multiple channels with a variety of functionalities for customers to choose how they bank, whether it is in a local branch, at home, on a phone, or through a mobile device.[618]

At the same time, customers also want to pick up their banking and financial activities right where they left off and, thus, continue the journey whenever they want regardless of what channel they start with. This means that banks need to ensure continuity of services across all customer touch points and to provide customers with real-time updated and consistent information. This is necessary to deliver a customer

[615] See, Accenture, *The Future of Fintech and Banking: Digitally Disrupted or Reimagined?*, cit., p. 10.
[616] See, Accenture, *Fintech and the Evolving Landscape: Landing Points for the Industry*, Accenture Report (2016), pp. 10-11 (noting that "banks cannot wait until the return on their investments in innovation is as clear as historically demanded for ordinary 'Run' or 'Change the Bank' projects or investments. Using historical investment assessment criteria may optimise the bank, but it will not truly challenge or change the business model.").
[617] See, McKinsey & Company, *The New Rules for Growth through Customer Engagement*, cit., p. 34.
[618] See, Microsoft, *Banking as a Digital Platform*, cit.

experience that is not only secure, private, and transparent, but also seamless, contextual, and synchronized across all available channels.[619]

Finally, customers expect their banks to know and remember their preferences, needs and goals. This means that banks must deliver a truly personalized customer experience and tailor their services to better address customers' needs and objectives.[620]

6.B. Comprehensive Data Ecosystem, Data-Driven Insights and Analytics

If banks want to remain relevant in an evolving Open Banking ecosystem, they must learn to play a greater role into their customers' lives. This means being present not just at the moment a specific banking or financial transaction takes place, but also before and afterwards. It also means becoming an integral part of customers' digital lives through daily interactions with customers and the development of digital ecosystems of partners, including financial services and non-financial services providers. This, in turn, means that the future of banks will greatly depend on their ability to become an "everyday bank" trusted and indispensable to many of the everyday activities of their consumers.[621]

In a costumer-centric ecosystem such as the one empowered by the movement towards Open Banking, costumer engagement increasingly centers around the customer's next action, and critically relies on knowing what behaviors will enhance the customer-bank relationship.[622] To develop this knowledge, banks will need to build a comprehensive data ecosystem to include customer data from within and beyond the bank, relating to all interactions and transactions across digital and physical channels. A comprehensive data ecosystem will give banks the ability to look at their customers holistically and will yield deeper and more meaningful insights about their financial lives, preferences and needs. This understanding, in turn, will help banks refine their business strategy, properly assess their risks, improve decision-making, and ultimately strengthen their relationships with their customers.[623]

---

[619] See, Microsoft, *Banking on Technology: Enabling an Omnichannel Approach in Financial Services*, cit.; McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., pp. 9-10.
[620] See, Massachusetts Institute of Technology (MIT), *Digital Banking Manifesto: The End of Banks?*, cit., p. 7.
[621] See, Accenture, *Becoming the Indispensable Everyday Bank*, Accenture Insights – Video Transcript (2014); Accenture, *Everyday Bank: The Digital Revolution*, Accenture Insights (2014); Accenture, *The Everyday Bank -– Infographics*, Accenture Report (2014); Microsoft, *Empowering the Digital Bank: The API Economy: Helping Financial Services Companies to Build Better Products*, Microsoft Financial Services - Banking & Capital Markets Insights (May 27, 2015).
[622] See, McKinsey & Company, *The New Rules for Growth through Customer Engagement*, cit., pp. 35-36.
[623] See, e.g., Microsoft, *Data-Driven Organizations Will Lead The Digital Revolution. Part 1 of 3: The Opportunity of Big Data*, Microsoft Financial Services - Banking & Capital Markets Insights (September 22, 2016); Microsoft, *Data-Driven Organizations Will Lead The Digital Revolution. Part 2 of 3: Getting Business Value Out of Big Data is Hard*, Microsoft Financial Services - Banking & Capital Markets Insights (September 26, 2016); Microsoft, *Data-Driven Organizations Will Lead The Digital Revolution. Part 3 of 3: Key Enablers for Successful Transformation*, Microsoft Financial Services - Banking & Capital Markets Insights (September 27, 2016); Microsoft, *Empowering Banking & Capital Markets: A Data-Driven Business*, Microsoft Financial Services - Banking & Capital Markets Insights (December 1, 2016); Microsoft, *Thriving in an Age of Radical Uncertainty*, Microsoft Financial Services - Banking & Capital Markets Insights (December 13, 2016); Microsoft, *The Financial Services Industry Is Banking on Digital Transformation*, Microsoft Financial Services - Banking & Capital Markets Insights (January 9, 2017); Microsoft, *Intelligent Digital Insights or Fabricated Financial Data?*, Microsoft Financial Services - Banking & Capital Markets Insights (April 3, 2017); McKinsey & Company, *Citigroup on Engaging the Digital Customer*, McKinsey Interview Series – Transcript of the Interview of Michael L. Corbat (Citigroup CEO) (June 2015); Center for Financial Services Innovation (CFSI), *Big Data, Big Potential: Harnessing Data Technology for the Underserved Market*, Center for Financial Services Innovation Report (March 2015) (discussing four key trends and exploring how real-life companies are leveraging big data in financial services).

Over time, banks have accumulated masses of valuable data about their customers, services, products, supply chains, operations and more, but they have long missed the opportunity to leverage and effectively utilize such data. It is now imperative for banks to tackle this challenge. In today's rapidly evolving Open Banking ecosystem, business is increasingly driven by getting information to the right people at the right time, while contextual data has become the most valuable currency. In this context, banks should follow the example of tech giants and consider consolidating data across transactions to gain a more unified view of their customers' activities (e.g., information regarding customers' in-store payments and geospatial mobility).[624] This, in turn, will enable banks to provide more personalized and contextual customer experience and to better predict customers' future financial activities and credit worthiness.

In addition to the foregoing, it is critical for banks to process and evaluate customer data in real time and to connect them to create a 360-degree view of their customers' activities by leveraging predictive analytics, deep learning, probabilistic algorithms and other advanced technologies. This will help banks anticipate customer behavior and needs, predict relevant interaction opportunities, and provide a more holistic, instant, contextual, and personalized banking customer experience.[625] Establishing a robust analytics and data infrastructure will also allow banks to launch creative services and drive scientific decisions across a broad range of activities from credit underwriting to customer acquisition, from servicing to collections and many more.[626]

6.C. Renewed Organizational Structure and Internal Culture

As the path towards Open Banking accelerates, it becomes imperative for banks to evolve their organizational structures to effectively support a data and insight driven operating model, enable speedier decision-making, deliver a distinctive customer experience, and ensure faster adaptability to external and internal changes.

To deliver banking and financial services using a constantly iterative approach, banks will also need to optimize cross-team collaboration and to nurture a working environment that supports a frenetic pace of innovation and allows compliance and risk-management teams to take on the roles of enablers and problem solvers, instead of mere gatekeepers. Moreover, banks will need to foster a culture that fuels innovation and makes it possible for banks to attract professionals at all organizational levels with the skillset needed to succeed in a Open Banking ecosystem, including engineers and data scientists. Finally, it is critical for banks to establish and cultivate a shared vision and common values across their entire organizations to motivate, support, and enable this profound transformation.[627]

---

[624] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., pp. 8-10; Accenture, *Fintech and the Evolving Landscape: Landing Points for the Industry*, cit., pp. 8-9.
[625] See, Microsoft, *Will Consumers Build Digital Banking Products?*, Microsoft Financial Services - Banking & Capital Markets Insights (March 27, 2017).
[626] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., pp. 8-9.
[627] Id., p. 12. See, also, McKinsey & Company, *Banking on the Cloud*, cit; Ernst & Young, *Revolutionary Change is Transforming the Financial Services Landscape. Financial Services Leadership Summit December 2016*, cit., pp. 12-13; McKinsey & Company, *Building a Digital-Banking Business*, cit., pp. 6-8; Massachusetts Institute of Technology (MIT), *Digital Banking Manifesto: The End*

6.D. Active Participation in the Fintech Ecosystem

In today's rapidly evolving banking and financial services industry, active participation by banks in the fintech sector is of critical relevance. To this end, banks can deploy a number of fintech-related strategies, including collaborations, business partnerships, investments, M&As, and creation of innovation labs. These strategies are analyzed in detail below.

6.D.i. Collaborations and Partnerships

The structure of the fintech sector is rapidly evolving and a new spirit of collaboration between fintech companies and banks is developing across a variety of banking and financial products and services. While the use of open APIs previously discussed is facilitating this collaboration, the new Open Banking ecosystem is making collaboration (almost) a necessity.[628]

Banks are now taking bold steps to engage with promising fintech companies. The synergies between banks and fintech companies are significant: they can leverage each other's strengths and capabilities and can make up for each other's shortfalls.

More in detail, on one hand, there are significant benefits for banks that partner and collaborate with fintech companies:

- First, collaborations and partnerships between banks and fintech companies present a great opportunity for banks to drive revenue growth. According to a report by UBS bank management, fintech companies could contribute up to a 3.8% bank revenue increase in the next three years.[629] This is important as fintech companies are progressively taking large bites out of every part of banks' product portfolios, are disaggregating their offerings service-by-service, and are growing stronger across various segments of the banking and financial services industry. By collaborating with fintech companies, banks will have an opportunity to successfully address these challenges.[630]

- Second, through collaborations and partnerships with fintech companies, banks gain access to new interesting and compelling banking and financial products and services, which they can use to complement their existing offerings. As discussed in Chapter 1, successful fintech companies have demonstrated the ability to maintain a "laser-like focus" on specific banking and financial products and services, building

---

of Banks?, cit., p. 9; McKinsey & Company, *Voices on Bank Transformation: Insights on Creating Lasting Change*, McKinsey Global Banking Report (March 2015); Ron Van Wezel, *The Programmable Bank: Opportunities for Open Banking*, The Financial Brand (December 12, 2016).

[628] See, e.g., Accenture, *The Future of Fintech and Banking: Digitally Disrupted or Reimagined?*, cit., pp. 4, 8; McKinsey & Company, *Fintechs Can Help Incumbents, Not Just Disrupt Them*, McKinsey Financial Services Report (July 2016); McKinsey & Company, *A Digital Crack in Banking's Business Model*, cit.; KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, cit., p. 46, 62; Robert Canova (Senior Financial Analyst at Federal Reserve Bank of Atlanta), *Fintech Companies: Banks' Allies or Rivals?*, cit.

[629] See, UBS, *Global Banks: Is FinTech a Threat or an Opportunity?*, UBS Evidence Labs, UBS Global Research Q-Series (July 2016).

[630] See, Currencycloud, *Banks and the FinTech Challenge: How Disruption Has Been a Catalyst for Collaboration and Innovation*, Currencycloud White Paper (2016), pp. 6-8.

excellence into both the technology and the customer experience.[631] Because of this, by partnering and collaborating with fintech companies, banks have the opportunity to create targeted and more personalized products and services for their clients. Furthermore, fintech companies can help banks create a seamless customer banking experience, whereby all aspects of a customer's interactions with a bank are unified and synchronized.[632]

- Third, successful fintech companies offer powerful data-driven services and products and have strong and trusting relationships with their customers. Banks have realized the enormous potential of fintech companies' innovative customer interactions and are increasingly willing to partner with fintech companies to enrich and complete their customer relationship propositions.[633]

- Fourth, through collaborations and partnerships, banks can exploit the agility, speed, and technological openness of fintech companies. They can leverage fintech companies' unique ability to move fast, to take risks, and to innovate.[634]

- Fifth, stringent regulatory environment in banking and finance coupled with legacy systems and cultures do not always allow banks to experiment and jump into uncharted waters. Yet, by collaborating with fintech companies, banks have the opportunity to boost their innovative capabilities and access latest advancements in technology. In addition, by cooperating with fintech companies, banks can accelerate their plans for innovation, can increase their rate of execution, and can bring to the market innovative solutions with the highest level of security, controls, and resiliency. This process of "fintech co-innovation" or "startup driven fintech innovation" is becoming increasingly important in the banking and financial services industry.[635]

- Finally, in order to evolve from being product-centric to customer-centric, banks will need to leverage data analytics technologies and use contextual data more effectively. Fintech companies can help banks mine their data and better understand customers' specific needs, problems, and goals. This, in turn, can help banks offer more compelling and customer valuable propositions.[636]

On the other hand, fintech companies can themselves benefit from partnering and collaborating with banks in a number of ways:

---

[631] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., p. 8 (noting that "banks should be less preoccupied with individual fintech attackers and more focused on what these attackers represent—and build or buy the capabilities that matter for a digital future.").
[632] See, KPMG, *Five Ways Banks Can Use Fintech to Build Trust*, KPMG Insights (April 12, 2016).
[633] See, e.g., PWC, *PSD2 – Redrawing the Lines: FinTech's Growing Influence on Financial Services*, PWC Global Fintech Report (2017), p. 6; Accenture, *Payments APIs: Too Compelling To Ignore*, cit. (noting that "[b]y providing services at the center of the digital ecosystem with broader, more open business partnerships, banks could increase their operating income up to 30 percent, their customer base up to 10 percent and their customer interactions up to 250 percent.").
[634] See, e.g., McKinsey & Company, *A Brave New World for Global Banking*, cit.; The Economist, *The Disruption of Banking*, cit., pp. 8-9; Robert Barba, *Tech, Love and Understanding*, American Banker (October 5, 2016).
[635] See, Accenture, *The Future of Fintech and Banking: Digitally Disrupted or Reimagined?*, cit., p. 9; KPMG, *Should Banks Nurture Internal Innovation or Invest in FinTech?*, KPMG Insights (February 4, 2016).
[636] See, KPMG, *Five Ways Banks Can Use Fintech to Build Trust*, cit.

- First, banks can help fintech companies build a global and much deeper customer base. This is important because, as the fintech sector matures, customer acquisition gets trickier and more expensive and earning the trust of customers as a banking and financial partner becomes an even greater challenge for fintech companies. Against this background, fintech companies that partner with banks gain the opportunity to tap into the banks' well-established and large customer bases, gain customer trust beyond their early adopters and acquire new customers faster, efficiently and at lower acquisition costs.[637]

- Second, banks can help fintech companies deal with regulations. There are significant challenges for fintech companies seeking to scale their activities, and these challenges may slow down the continued development of their technologies. In particular, as they growth their activities, fintech companies may face increasingly complex financial and banking regulatory challenges and may have to comply with stricter risk management and compliance requirements. Thus, to compete head on with traditional and non-traditional players, fintech companies need to build strong teams of tech-savvy compliance and regulatory experts, who can help them navigate legal and compliance issues; they also need to become proficient in the art of cyber security and risk management and to build the teams and technology to support these capabilities. By collaborating with banks, fintech companies gain the opportunity to leverage banks' leading industry expertise in banking and financial regulatory compliance and risk management.[638]

- Third, increasing collaboration between fintech companies and banks is also driven by the need to enhance capabilities and products. This is in part attributable to the fact that fintech companies still utilize traditional financial infrastructure (e.g., credit cards or ACH payment rails) and often rely on banks to provide the back-end transactions and the compliance support needed for their services and products to work.[639]

- Finally, growing the operations can be resource-intensive for fintech companies and requires them to properly assess their liquidity and credit needs.[640] Banks have the financing capabilities to invest in

[637] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., p. 5; The Economist, *The Disruption of Banking*, cit., p. 9; Currencycloud, *Banks and the FinTech Challenge: How Disruption Has Been a Catalyst for Collaboration and Innovation*, cit., p. 7.

[638] See, e.g., JPMorgan Chase & Co. (Stephen Markwell - Head of Treasury Services Product Investments (author) and Karen Larsen, CTO and Head of Fintech Payments Strategy (author)), *How FinTech and Banks are Partnering*, JPMorgan Chase & Co. Insights (February 6, 2017); The Economist, *The Disruption of Banking*, cit., pp. 6, 9; McKinsey & Company, *The Future of Bank Risk Management*, McKinsey Risk Report (July 2016).

[639] See, e.g., Lael Brainard (Federal Reserve Board Governor), *Where Do Banks Fit in the Fintech Stack?*, cit. (noting that "More often than not, there is a banking organization somewhere in the fintech stack. Just as third-party app developers rely on smartphone sensors, processors, and interfaces, fintech developers need banks somewhere in the stack for such things as: (a) access to consumer deposits or related account data, (b) access to payment systems, (c) credit origination, or (d) compliance management. For instance, account comparison services rely on access to data from consumers' bank accounts. Savings and investment apps analyze transactions data from bank accounts to understand how to optimize performance and manage the funds consumers hold in those accounts. Digital wallets draw funds from payment cards or bank accounts. Marketplace loans most often depend on loan origination by a bank partner. And payment innovations often "settle up" over legacy payment rails, like the automated clearinghouse system. In short, the software stacks of almost all fintech apps point to a bank at one layer or another."); JP Morgan Chase & Co. (Tim Sandel - Managing Director (author)), *The FinTech Revolution*, JPMorgan Chase & Co. Insights (December 21, 2016).

[640] See, JP Morgan Chase & Co. (Tim Sandel - Managing Director (author)), *4 Key Considerations for Tech Companies When Going Global*, JPMorgan Chase & Co. Insights (February 17, 2017).

fintech companies and, thus, support the development of their technologies and the growth of their activities.[641]

For the reasons discussed above, banks are now positioning themselves for a new era of mutually beneficial partnerships and collaborations with fintech companies and the appetite for cooperation, on both sides, is growing significantly. There are already many examples of these partnerships and collaborations. For instance, JP Morgan Chase has partnered with a number of leading fintech companies to improve its consumer offerings,[642] including: On Deck, to use its online technology platform to process loan applications;[643] InvestCloud, to offer digital wealth advice to its clients;[644] TrueCar, to create a platform that allows it to play a more central role in car buying;[645] Roostify, to deliver digital mortgage platform;[646] Symphony, for communication;[647] and Digital Asset Holdings, on a trial blockchain initiative.[648] Similarly, Bank of America Merrill Lynch has entered into strategic partnerships with fintech companies, including: ModoPayments, to power digital payments;[649] and ViewPost, to provide online invoicing and payment services.[650] Barclays has partnered with many leading fintech companies, including: Safello, to explore financial applications of blockchain;[651] and Circle Internet Financial, to boost its digital currency capabilities.[652] In a similar fashion, Santander has teamed up with many leading fintech companies to empower its offerings, including: Tradeshift, to support the growth of its supply chain finance digital platform and the ecosystem surrounding its B2B marketplace;[653] Sigfig, to provide high-quality wealth management and robo-advisory platform solutions;[654] and Kabbage, to offer fast loans to SMEs.[655] Likewise, Morgan Stanley has been collaborating with fintech companies like: Addepar, to automate administrative tasks;[656] Zelle, to enhance P2P digital payment solutions;[657] and Twillio, to help enhance client communications.[658]

---

[641] See, The Economist, *The Disruption of Banking*, cit., p. 5, 9.
[642] See, JP Morgan Chase & Co., Jamie Dimon (Chairman and Chief Executive Officer), *Letter to Shareholders*, (April 4, 2017).
[643] See, JP Morgan Chase & Co. (Stephen Markwell - Head of Treasury Services Product Investments (author) and Karen Larsen, CTO and Head of Fintech Payments Strategy (author)), *How FinTech and Banks are Partnering*, cit.; Peter Renton, *An In Depth Look at the OnDeck/JPMorgan Chase Deal*, Lend Academy (December 4, 2015); Peter Rudegeair, Emily Glazer, and Ruth Simon, *Inside J.P. Morgan's Deal With On Deck Capital*, The Wall Street Journal (December 30, 2015).
[644] See, JP Morgan Chase & Co., *JPMorgan Chase Partners With InvestCloud for Digital Wealth Management*, JP Morgan Chase & Co. Press Release (September 20, 2016). See, also, Finextra, *JPMorgan Chase Partners with InvestCloud for Digital Wealth Management*, Finextra (September 21, 2016); Tanaya Macheel, *JPMorgan Buys Stake in InvestCloud to Speed Digital Revamp*, American Banker (September 21, 2016).
[645] See, Suzanne Woolley, *JPMorgan Courts Millennials by Putting the Whole Car-Buying Nightmare Online*, Bloomberg (August 26, 2016); Emily Glazer, *J.P. Morgan in a Car-Lending Chase*, The Wall Street Journal (August 25, 2016); Robert Barba, *How JPM Makes Tech Partnerships Work*, American Banker (November 28, 2016).
[646] See, Jacob Passy, *JPM Teams with Fintech to Deliver Digital Mortgage Platform*, American Banker (February 16, 2017).
[647] See, Ron Miller, *Wall Street-Backed Symphony Wants To Revolutionize Financial Services Communication*, Techcrunch (February 21, 2015).
[648] See, Ben McLannahan, *Blythe Masters and JPMorgan Trial Blockchain Project*, Financial Times (January 31, 2016).
[649] See, Bryan Yurcan, *Bank of America Partners with Digital Payments Firm*, American Banker (October 20, 2016).
[650] See, BI Intelligence, *Bank Of America Strengthens Digital Business-To-Business Offerings*, BI Intelligence (August 19, 2016).
[651] See, Shona Ghosh, *Barclays Becomes First UK High Street Bank to Explore the Blockchain*, Haymarket (June 24, 2015); Grace Caffyn, *Barclays Trials Bitcoin Tech With Pilot Program*, CoinDesk (June 22, 2015).
[652] See, Aime Williams, *Barclays Partners with Goldman-Backed Bitcoin Payments App*, Bloomberg (April 5, 2016).
[653] See, Anna Irrera, *Santander Partners with Supply Chain Finance Startup Tradeshift*, Reuters (July 11, 2017).
[654] See, Jonathan Shieber, *Sigfig Locks in Big Banking Partners for its Tech-Enhanced Advisory Services with $40M Round*, TechCrunch (May 24, 2016).
[655] See, Kabbage, *Kabbage and Santander UK Partner to Accelerate SMB Growth*, Kabbage News (April 3, 2016).
[656] See, Hugh Son, *Morgan Stanley Signs with Asset-Gobbling Startup Backed by Thiel*, Bloomberg (January 10, 2017).

In addition to the foregoing, fintech companies have the opportunity to engage with banks through a number of summits, symposia, and conferences. These events typically take place in fintech centers, like Silicon Valley / Bay Area, New York, and London; and they gather representatives of prominent venture capital firms, hundred of fintech companies, alongside executives and senior management of the bank(s) organizing the event at hand. Notable examples include: the Bank of America Merrill Lynch annual Technology Innovation Summit in the Bay Area; the JP Morgan Chase annual Fintech & Specialty Finance Forum in New York and annual Technology Symposium in Menlo Park; Goldman Sachs annual Financial Technology Conference in New York; and many more. At these events, banks' executives and senior management typically laid out their firm's wide goals and priorities for the coming years, while attending fintech startups have the opportunity to pitch their products and services, and leading fintech companies often receive innovation awards.

Notwithstanding the benefits and the synergies discussed above, it is important to understand that partnerships and collaborations between banks and fintech companies may also create complexities and challenges, which include the following:

- First, an initial challenge is technology integration, as banks' IT legacy and outdated infrastructures may cause disharmony.

- Second, when fintech companies and banks combine their forces there may be an even bigger risk of clashing distinctly different cultures.

- Third, challenges may arise as banks and fintech companies seek to combine diverse approaches to working and innovating, as well as substantially different risk tolerances.

- Fourth, further complexities are created by the need of integrating fintech company's agility and innovation, while marrying it to the controls and assets of the banks.

- Finally, an additional challenge that fintech companies often face when partnering with incumbents is the complexity in navigating these established institutions. Banks may drag fintech companies through numerous meetings before doing anything and sometimes the process of just getting to the right person is difficult and takes several months.

Addressing the described challenges will require banks to: undertake an internal reorganization to encourage effective collaboration among far-flung parts of their organization; and evolve their engagement model to be more accessible, efficient, and nimble. On the other hand, fintech companies will need to improve the way they work and engage with banks. This is a thoughtful process particularly when it comes to compliance with financial and banking regulatory requirements, as well as security and risk management processes. To this end, fintech companies will need to gain a keen understanding of both the types of

---

[657] See, Brena Swanson, *Big Banks Band together to Introduce Digital Payment App Zelle*, HousingWire (June 12, 2017); Sarah Perez, *Zelle, The Real-Time Venmo Competitor Backed by Over 30 U.S. Banks, Arrives this Month*, TechCrunch (June 12, 2017).
[658] See, Morgan Stanley, *Management Partners with Twilio to Help Enhance Client Communications*, Morgan Stanley Press Release (June 13, 2017).

controls they need to satisfy in order to work with banks and key enterprise features like ability to scale, security, and resiliency.

6.D.ii. Investments and Acquisitions

Investments in Fintech Companies. Banks have been actively investing in fintech startups and emerging companies for a few years. Some of them have created dedicated corporate venture arms, investment vehicles or bespoke fintech funds, whilst others plan to launch one in the next few years.[659]

There are abundant examples of banks investing in fintech startups. For instance:

- Citi through its Global Corporate Venturing Arm - Citi Ventures - has invested across more than 50 deals, including a Series D investment in Blue Vine, a Series C investment and a Series E investment in Betterment, and a Series C investment in Chain.

- Bank of America Merrill Lynch has been reported to have being setting aside $3 billion from its annual budget for investing in fintech innovation.[660]

- JP Morgan Chase is another incumbent bank particularly active in supporting fintech innovation. In his annual shareholder letter, JP Morgan Chase CEO Jamie Dimon offered details on the bank's fintech approach and projects: he indicated that the bank spent more than $9.5 billion on technology in 2016, of which about $3 billion went toward new initiatives; of this amount, $600 million was spent on emerging fintech solutions in areas including big data, machine learning, cybersecurity, and electronic trading.[661] Among JP Morgan Chase's most notable investments in fintech companies are a Series B investment in Square, a Series B investment in OpenFin, a Series E investment in Avant, and a Series D investment in Motif Investing.

- Goldman Sachs has become a tech-investing powerhouse in recent years. To date, it has invested in a number of leading fintech companies, including Square, Circle Internet Financial, and Plaid.

- Santander has been investing in fintech startups through Santander InnoVentures, its London-based fintech venture fund. Its investments include a Series C investment and a Series D investment in iZettle, a Series A investment and a Series B investment in Ripple, a Series E investment in Kabbage, and a Series D investment in Sigfig.

[659] See, Accenture, *The Future of Fintech and Banking: Digitally Disrupted or Reimagined?*, cit., p. 10.
[660] See, e.g., Let's Talk Payment, *BofA Has $3 Billion to Pour Into Innovation as Banks Are Swarming Around FinTech Startups*, Lets Talk Payment (January 8, 2016); Penny Crosman, How B of A's Billion-Dollar Tech Cuts Could Fuel Startups, American Banker (June 28, 2016).
[661] See, JPMorgan Chase & Co., Jamie Dimon (Chairman and Chief Executive Officer), Letter to Shareholders (2017), cit.

- BBVA has been particularly active in investing in fintech companies. For instance, in 2015 it invested US$68 million in the online bank Atom Bank for a c. 29.5% stake,[662] and in 2017 made a follow up investment of Euro 34.1 million to maintain its stake of c. 29.5%.[663]

Over the past couple of years, banks and established financial institutions have progressively oriented their investments towards fintech companies that are open to collaborate with incumbents.[664] However, the ratio of competitive versus collaborative fintech investments still differs significantly across geographic areas. For instance, in Europe most investments have moved towards competitive fintech startups; whilst in the United States most investments have concentrated in collaborative fintech startups.[665]

Acquisitions of Fintech Companies. As the fintech sector matures, banks and established financial institutions are increasingly attracted to the prospect of acquiring fintech companies that best fit their organizations, cultures and activities.[666] For example, Spanish bank BBVA has placed M&A at the center of its fintech and Open Banking strategies: its acquisition deals include a notable US$117 million acquisition of digital banking startup Simple.[667]

Acquiring a fintech company is not an easy task for a bank. The ultimate goal of the acquisition is to preserve the acquired fintech company's agility and innovation, while marrying it to the controls and assets of the bank. This process of "fintegration" poses significant technical and non-technical challenges:[668]

- First, technology-related challenges. The acquiring bank will need to include IT in the due diligence and integration planning. It is critical for the acquiring bank and the fintech company being acquired to develop an efficient and effective plan that maps the current state, the transformation strategy, and the future state of the combined entities' technologies.

- Second, data integration-related challenges. The IT plan will need to include a roadmap for the integration of data covering a variety of technical aspects, including the establishment of a primary data

[662] See, Atom Bank, *Atom and BBVA - Capital Raise Over and £135m Raised, We're One Step Closer to Launch*, Atom Bank Press Release (November 24, 2015). See, also, Ingrid Lunden, *UK Mobile-Only Atom Bank Picks Up $128M Led by BBVA, Owner of Simple in the U.S.*, TechCrunch (November 24, 2015).
[663] See, BBVA, *BBVA Strengthens its Commitment to UK's Atom Bank*, BBVA Press Release (March 3, 2017). See, also, Bryan Yurcan, BBVA Increases Investment in UK Digital Bank Atom, American Banker (March 3, 2017).
[664] The level of investment into fintech companies that collaborate with incumbents increased by 138% in 2015, representing 44% of all fintech investment, while investments into fintech companies that compete with incumbents only increased by 23%. See, Accenture, *Fintech and the Evolving Landscape: Landing Points for the Industry*, cit., pp. 5-6; Ernst & Young, *Revolutionary Change is Transforming the Financial Services Landscape. Financial Services Leadership Summit December 2016*, cit., p. 6; Penny Crosman, *Fintech's Goals are Changing, VC's Appetite is Not*, American Banker (April 16, 2016).
[665] The shift towards collaboration is more pronounced in North America, where the proportion of investment in collaborative fintech companies has grown from 40% in 2010 to 60% in 2015. In particular, in New York the proportion of investment in collaborative fintech companies has grown from 33% in 2010 to 56% in 2015, while in California the proportion of investment in collaborative fintech companies has grown from 29% in 2010 to 37% in 2015. This trend is reversed in Europe, where the proportion of investment directed to collaborative fintech companies has decline from 38% in 2010 to 14% in 2015. This can be partially attribute to Europe's regulatory environment that has helped lower the barriers to entry and is supportive of fintech startups looking to compete directly with established players in the banking and financial industry. See, Accenture and the Partnership Fund for the New York City, *Fintech's Golden Age*, Accenture Report (2016), pp. 3-4. See also, Ernst & Young, *Landscaping UK Fintech*, cit., pp. 4-8.
[666] See, Accenture, *Fintech and the Evolving Landscape: Landing Points for the Industry*, cit., p. 6.
[667] See, BBVA, *BBVA Acquires Simple to Accelerate Digital Banking Expansion*, BBVA Press Release (February 20, 2014). See, also, William Alden, *BBVA Buys Banking Start-Up Simple for $117 Million*, DealBook (February 20, 2014); Bradley Leimer, *Lessons from BBVA's Simple Acquisition: It's Time to Build Better Banks*, American Banker (February 28, 2014).
[668] See, The Economist, *The Disruption of Banking*, cit., pp. 11-12.

management system to allow an integrated, seamless and common view of customers and the utilization of flexible or hybrid cloud technologies to accelerate the data integration process.

- Third, regulatory challenges. The acquiring bank will need to make regulatory integration (covering policies, contracts, guidelines, protocols, procedures, processes, and training) an early priority and will need to ensure constant and ongoing compliance oversight post closing.

- Fourth, data security-related challenges. Alongside regulatory integration, the acquiring bank will need to make data security an early priority. A security audit should take part during the due diligence process, and immediately after the closing of the transaction the acquiring bank's and the fintech company's protocols and networks will need to be integrated at the highest standard of the two entities.

- Fifth, cultural challenges. The acquiring bank may have a risk appetite and a process-focused culture that significantly differ from the agility and customer-centric culture of the fintech company being acquired. To preserve the fintech company's innovative mindset and culture, the acquiring bank may consider "ring-fencing" the fintech company being acquired and allow it to maintain its own leadership, organizational rules, and physical location.

- Sixth, enterprise infrastructures-related challenges. To complete the fintegration process, the acquiring bank and the fintech company being acquired will need to integrate their enterprise infrastructures, including data centers, data networks, network and application architectures.

6.D.iii. Incubator and Accelerator Programs

Over the past five years, a number of leading banks have built incubator and accelerator programs dedicated to fintech startups. Through these programs, banks provide participating startups with co-working spaces, mentorship, seed and early-stage funding and the opportunity to tap into their vast networks of partners and customers. On the other hand, through incubator and accelerator programs banks gain the opportunity to: collaborate with talented teams bringing to the market disruptive ideas; transfer to newcomers knowledge and expertise accumulated through years of experience in the financial and banking services industry; and financially support the development of groundbreaking banking and financial solutions and harvest the results thereof.

Examples of fintech incubator and accelerator programs launched by banks are numerous. For instance:

- In the United States, Wells Fargo operates an in-house fintech labs and innovation center to help fintech startups and entrepreneurs work more closely with the bank. Similarly, Citi has a global network of labs strategically located around the world, including in the United States, Ireland, Israel, and Singapore. The labs pioneer the exploration of disruptive trends and emerging technologies to build the capabilities for future Citi solutions, including blockchain and cryptocurrencies, biometric authentication, the internet of things, artificial intelligence, among others. Another banking giant, JPMorgan Chase, is a founding partner at the Financial Solutions Lab, a $30-million, five-year initiative managed by the Center for Financial

Services Innovation (CFSI). Financial Solutions Lab launched its first competition in February 2015 and currently seeks to identify, test and bring to scale promising innovations that help Americans increase savings, improve credit, and build assets.

- In Europe, the Barclays Accelerator program, powered by Techstars, provides a wide range of advising, mentoring, and financing resources to fintech companies that pushes innovation across the financial and banking services industry, covering areas such as cyber security, artificial intelligence wealth management, investment banking, big data, and crytocurrency. Similarly, Deutsche Bank operates bank labs in New York, Silicon Valley, Berlin, and London with three principal goals: to help the bank evaluate and adopt emerging technologies; to develop a culture of innovation; and to contribute to the bank's digital strategy.

An alternative approach to incubator and accelerator programs established by individual banks involves the creation of innovation labs and creative think-tanks that partner with multiple banks and other established financial institutions. One prominent example is FinTech Innovation Lab. Now in its seventh year, the FinTech Innovation Lab is an annual mentorship programme for entrepreneurs and early-stage companies that are developing cutting-edge technologies for the financial services sector. The FinTech Innovation Lab began in New York in 2010, founded by the Partnership Fund for New York City and Accenture. In 2012, it launched a programme in London, and then in Hong Kong and Dublin in 2014. Major global and domestic banks support the FinTech Innovation Lab's initiatives, including Bank of America Merrill Lynch, Barclays, Citi, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Lloyds Banking Group, Morgan Stanley, Nationwide, RBS, BBVA, Santander, and UBS.

6.E. Openness

6.E.i. Open Banking Strategies

Openness is at the heart of today's banking and financial revolution. As discussed in Chapters 3 and 4, legislative/regulatory reforms and policy initiatives in Europe and the UK are accelerating the movement toward Open Banking. Yet, this movement has undoubtedly a global nature and holds the potential to spark a competitive race that goes far beyond Europe and the UK to impact global financial and banking markets.[669] Moreover, while EU and UK regulators are paving the way, banking and financial regulators in other countries are expected to follow with similar Open Banking-related regulations and standards in the upcoming years. For these reasons, the medium-to-long term impacts of EU and UK Open Banking legislative/regulatory reforms and policy initiatives will likely be felt across the operating models of banks all around the world. This impact will vary in intensity and scale depending on each individual bank's strategic approach to openness.

[669] See, Finextra, *PSD2 and Open Banking: Defining Your Role in the Digital Ecosystem*, cit., p. 7, 18, 22, and 32 (explaining that Open Banking is what global banking markets are moving to and what clients all around the world are demanding).

When defying their approach to openness, banks will first need to appraise the ongoing viability of their business model and clarify what their core business and value drivers are. Further, they will need to identify their customer base and what their customers' needs and goals are; they will also need to understand what will drive customer acquisition and retention and what capabilities will need to be deployed to differentiate from traditional and new competitors. Building on this understanding, banks will, then, have to decide how far they want to go with "openness." To this end, banks will need to identify available strategic options, properly assess the relative advantages and challenges, and determine how to evolve their existing organizations, culture and technical architectures to support their new role in the Open Banking ecosystem.[670]

As policy and regulatory frameworks remain fluid, the early phase of Open Banking will likely see a variety of firms compete and experiment with different types of models, processes, and designs for Open Banking.[671] Examples of available Open Banking strategies are laid out below.

Open Banking Strategy #1. As a first approach to openness, banks subject to PSD2 requirements may seek to achieve basic compliance without implementing further measures.[672] While this is likely to be a relative cheaper and easier approach, it could also create the risks for banks of disintermediation and loss of volume and quality of customer interactions.[673]

That said, it is important to understand that, as competition by traditional and non-traditional players intensifies, banks must have a clear strategy for developing and maintaining their core business, optimize the use of their resources and prioritize their investments. Because of this, for certain (small) banks limiting the approach to openness to mere compliance may still be optimal. The banks that adopt this first Open Banking strategy may decide to narrow the focus of their business model towards the provision of liquidity and infrastructure services to third-party services providers (e.g., other banks or fintech companies). In this scenario, the bank operates as a "utility" that manages underlying customer accounts, processes payment transactions, and provides liquidity and credit services to third-party providers that own the customer experience. Increasing regulatory and compliance costs could make this model compelling in the eyes of third-party services providers: third-party services providers could rely on the bank/utility provider to

[670] See, Deloitte, *Open Banking: What Does The Future Hold?*, Deloitte Digital Report (April 2017), p. 8.
[671] See, e.g., Euro Banking Association (EBA), *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, cit., pp. 17-21; Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., pp. 11-17 (analyzing four primary strategic options are available to banks to respond effectively to the threats and opportunities of PSD2 and Open Banking); Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit. (discussing where opportunities for innovation may develop in the short, medium and long term and how PSD2 and Open Banking initiatives can act as a catalyst to digital transformation in banking); IBM, *Open Banking: Everything You Need to Know*, A presentation by Bharat Bhushan (Industry Technical Leader, Banking and Financial Markets - IBM), Technology Innovation Exchange (2017), slides 17-20; McKinsey & Company, *Digital Banking: Winning the Beachhead*, cit., pp. 6-9; Strategy&, *Catalyst or Threat? The Strategic Implications of PSD2 for Europe's Banks*, Strategy& Report (July 2016); Chris Skinner, *Four Banking Business Models for the Digital Age*, Chris Skinner's Blog (October 24, 2016); Deloitte, *PSD2 Opens the Door to New Market Entrants. Agility Will Be Key to Keeping Market Position*, Deloitte Report (2016), pp. 7-10; PWC, *PSD2 – A Game Changing Regulation. What Challenges and Opportunities Could the New Directive Provide?*, PWC Insights (2017).
[672] Similarly, banks that are not subject to PSD2 requirements may decide to adopt a conservative approach to Open Banking by implementing limited measures consistent with PSD2 requirements, without taking any further action.
[673] See, e.g., Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., p. 12.

perform heavily regulated activities and take on the related compliance burden and, in some circumstances, they may even avoid the costs and procedural hurdles of applying for a banking license. How many banks will be able to successfully operate this model, in turn, will depend on a number of factors, including economies of scale and regulatory restrictions.

Open Banking Strategy #2. A different approach to openness would be for a bank to go beyond mere compliance with PSD2 and to utilize the regulatory-driven base API level as a catalyst for more disruptive transformation.

Significantly, since the beginning of 2017, banks subject to PSD2 requirements have begun to evolve their approach to PSD2 to be more strategic.[674] Although at the date of writing there are still a number of technical areas where the debate on how PSD2 will be practically implemented is open, banks appear generally more comfortable with the evolving Open Banking ecosystem and are increasingly considering ways to leverage PSD2 to create new business opportunities and offer better and more comprehensive services to their customers.

As previously discussed, PSD2 mandates are mainly restricted to payment account transaction, credit transfer initiation, and account identity verification. This means that banks could extend the development of their APIs beyond mere compliance and could allow a customer to retrieve additional data sets, as well as enriched and calculated data. Examples may include customer data from non-payment accounts, identity documentation, account activities categorization, customer demographics, liquidity forecasts, credit scores and much more. In addition, banks could extend the development of their APIs to integrate standing orders and direct debit mandates or the completion of product applications via API. When extending the development of APIs beyond mere compliance, banks will gain the opportunity: to monetize additional APIs, by charging third-party providers for the use of the described additional customer data set; and to collaborate with third parties to create new personalized products and services that leverage such data sets. This, in turn, will enable banks to provide richer customer experience and to drive customer acquisition and retention.[675]

Open Banking Strategy #3. Banks that want to capitalize on regulatory pressures as drivers for change could also seek to monetize customer insights and offer services through APIs, such as account information services (AISs) and/or payment initiation services (PISs).[676]

A bank could operate an AIS and offer a "one-stop" banking portal for customers to view their accounts and transaction details. This service could, then, be enriched through the provision of financial management tools that allow customers to compare bank products, review credit scoring across multiple credit providers, automatically categorize their transactions, and enable budgeting, goal-setting and data visualization. By

[674] See, e.g., Finextra, *PSD2 and Open Banking: Defining Your Role in the Digital Ecosystem*, cit.; Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., pp. 6-9.
[675] See, Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., p. 12.
[676] Id., pp. 12-15. See, also, KPMG, *European PSD2 Open Banking Standards Provide the Opportunity for Payments Innovation*, KPMG Insights (February 15, 2017).

operating an AIS, the bank will gain a unified view of its customers' activities and will be able to improve the engagement and interactions with them. This, in turn, will give the bank the opportunity to better understand its customers' behavior and goals and to develop products and services that better meet its customers' (existing and anticipated) needs. Moreover, the bank will have the possibility of monetizing additional features, including integration with accounting/ERP systems and cash-flow management driven by predictive analytics. Finally, subject to receiving the necessary consent from the customer, the bank will be able to tap into additional customer data and insights from third-party services providers and, then, leverage them to deliver innovative and more-targeted products and services.

In addition to the foregoing, a bank could operate a PIS and combine it with instant and faster payment services. In this context, consumers would be routed to their bank portal for payment authorization and the payment would, then, be executed in real time to the merchant's account. By operating this service, a bank will have the opportunity to increase its revenues, to consolidate its customer base, and to enhance customer loyalty. Yet, the successful provision of PISs by banks will be heavily dependent on merchants' preferences. As hinted above, merchants will likely select and partner with one or more PISPs based on beneficial fee structures and/or ancillary services. Large online merchants may also decide to offer PISs themselves and then encourage their customers to use such services through discounts or other loyalty schemes at the point of sale.

Open Banking Strategy #4. As the path towards Open Banking accelerates, banking becomes increasingly collaborative, open, and nimble.[677] In addition to monetizing APIs and customer insights as discussed above, a bank could also leverage open API integration to establish more dynamic, integrated, and mutually beneficial inter- and cross-industry partnerships and relationships. In deploying this Open Banking strategy, the bank should seek to position itself at the center of an intelligent and connected ecosystem and to deliver a more personalized, contextual, seamless, and flexible customer experience across all products and services offered throughout its ecosystem.[678]

Successful execution of this Open Banking strategy can open up new revenue streams for the bank and third parties operating throughout its ecosystem.[679] Moreover, this Open Banking strategy can help the bank increase its competitive differentiation, deeper its customer base, and drive customer retention. Finally, by deploying this Open Banking strategy, the bank gains the unique opportunity to become a customer's

[677] See, Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., p. 12 (arguing that "the future of banking is agile, collaborative, 'exposed' and designed to encourage new business models – using 'systems of intelligence' in this transformation").

[678] See, Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, cit., pp. 16-17; Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., pp. 5, 7 (arguing that "[t]he ultimate goal here is the provision of a single experience for customers through one interface that combines the best of third party prediction, recommendation, analytics, payment, product choice, delivery and ongoing support services into one seamless end-to-end journey to the desired customer outcome – in which payment or purchase is a fundamental component.").

[679] See, Accenture, *Platform Economy: It's Time for Banks to Join in and Welcome Others*, Accenture Technology Vision for Banking Report (2016), p. 5 (noting that the majority of the surveyed banks believes that adopting a platform-based business would be "the most important growth strategy for the next three years; indeed, the digital-powered platform economy and open banking could drive drive up return on equity by more than five percent for both mature or emerging market banks.").

preferred digital point of entry into both financial and non-financial services and, ultimately, a trusted and pivotal part of the customer's daily life.

There are a number of ways in which a bank could create an intelligent and connected ecosystem by leveraging the power of APIs.[680] At the time of writing there is undoubtedly a lot of movement in this area and a dominant model has yet to emerge. Among available models are the following:

- First, a bank could operate as an *aggregator* and a *distributor* of banking and financial products and services. In this scenario, the bank does not develop or deliver its own banking or financial products or services; rather it researches, aggregates and distributes financial and banking products and services from an ecosystem of partners. One way to monetize this service would be for the bank to take a small fee on all of the products and services the customer uses. This model has the benefits of potentially reducing development and compliance costs for the bank and broadening the offer of products and services to the costumers. However, it also creates the risk of reducing the bank's ability to differentiate, its relevance to the customers, and its knowledge of customers' everyday needs and transactions. To address these challenges, the bank may consider providing complementary services (e.g., advisory, aggregator and/or access facilitator services).

- Second, a bank could operate as a *marketplace*, whereby its customers can manage their finances and have access to third parties' financial and non-financial products and services, alongside the bank's core product(s), such as a current account. In this scenario, the bank enters into, and curates, a number of relationships and partnerships with selected and trusted third-party service providers, which agree to offer their services and products throughout the bank's marketplace as either white-labeled or co-branded services and products.[681]

- Third, a bank could operate as a *platform*.[682] In this scenario, the bank develops an open set of APIs that any third-party can use to build products and services. Different from the marketplace model, banking as a platform has the potential advantage of providing customers with a more comprehensive set of capabilities. However, unlike the marketplace model, banking as a platform comes with some lack of centralized control of quality on the part of the bank.[683]

The following section will discuss banking as a marketplace and banking as a platform in greater detail.

---

[680] Id., p. 6.
[681] See, Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., pp. 12-13.
[682] There are many and divergent definitions of "platform." Among others, platform is defined as a "a plug-and-play business model that allows multiple participants (producers and consumers) to connect to it, interact with each other and create and exchange value." See, Ron Shevlin, *The Platformification of Banking*, The Financial Brand (July 19, 2016); Sangeet Paul Choudary, *The Platform Stack: For Everyone Building a Platform… and for Everyone Else. A Unifying Framework for Digital Business Models*, Platform Thinking Labs (2016). See, also, David Brear and Pascal Bouvier, *Exploring Banking as a Platform (BaaP) Model*, The Financial Brand (March 4, 2016); David Brear and Pascal Bouvier, *Making Banking as a Platform (BaaP) a Reality*, The Financial Brand (March 25, 2016).
[683] See, Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., pp. 12-13.

6.E.ii. Banking as a Marketplace and Banking as a Platform

Among the described models, banking as a marketplace and banking as a platform have been attracting significant attention from various market participants.[684] In this regard, it is worth noting that, although marketplace and platform strategies have contributed to revolutionize many industries, they are still at a very early stage of development in the banking and financial services industry – with the sole exceptions being perhaps Visa and MasterCard.[685] This is in part attributable to the fact that banks' traditional business models have not typically lend themselves to network effects, banks have long focused on "customer ownership," and up until recently they haven't faced a serious risk of substantial disintermediation.[686] Furthermore, it is important to understand that being a marketplace or a platform is very different from, and much more complex than, becoming a "digital" bank. In fact, for a bank being a marketplace or a platform is about learning how to reinvent itself in the Open Banking era to form new and much closer and valuable relationships with customers and partners.[687]

As observed by Mark Bonchek and Sangeet Paul Choudary,[688] three key elements must be considered when implementing a marketplace / platform strategy: connection (how easily third-parties can plug into the platform to share and transact); gravity (how effective is the platform in attracting participants); and flow (how well the platform fosters the exchange and co-creation of value). According to the authors, successful platforms achieve these goals with three building blocks: a "toolbox" that enables interactions between participants and facilitates the connection by making it easy for third-party to "plug into the platform and play";[689] a "magnet" to attract to the platform a critical mass of participants (on both side of the transactions executed throughout the platform) with a kind of social gravity;[690] and a "matchmaker" that captures and processes data about the platform's participants and then leverages such data to facilitate value-creating connections between producers and consumers.[691]

---

[684] See, Accenture, *Platform Economy: It's Time for Banks to Join in and Welcome Others*, cit., p. 5 (noting that "of bank executives surveyed, nearly 50% believe that adopting a platform based business model and engaging in ecosystems of digital partners to create value are very critical to their business success; … 59% are already investing in a competitive digital technology program as part of their business strategy; … 83% percent believe platforms will be the 'glue' that brings organizations together in the digital economy; 52% expect to be working with new digital partners within their industry in the next two years while 42% expect to be working with new digital partners outside the industry.").

[685] For an interesting discussion, see John Hagel, *The Power of Platforms*. Part of the Business Trends Series, Deloitte University Press (April 15, 2015); John Hagel, *The Power of Platforms to Create New Value*, Deloitte CIO - WSJ Insights (April 15, 2015); Geoffrey G. Parker and Marshall W. Van Alstyne, *Platform Revolution: How Networked Markets Are Transforming the Economy — And How to Make Them Work for You*, W. W. Norton & Company, Ed. 1st (2016); Apigee, *The State of APIs - 2017 Report: How APIs Power Digital Ecosystems*, cit.

[686] See, Euro Banking Association (EBA), *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, cit., p. 15 (noting that "[a]s customers drive the actual uptake of such innovations, the concept of 'customer ownership' is changing towards a concept of 'customer sharing' between banks and third party developers.").

[687] See, Ron Shevlin, *The Foolish Fantasies of Fintech/Bank Partnerships*, The Financial Brand (May 23, 2016); Ron Shevlin, *The Platformification of Banking*, cit.

[688] See, Mark Bonchek and Sangeet Paul Choudary, *Three Elements of a Successful Platform Strategy*, Harvard Business Review (January 31, 2013).

[689] Ibidem (noting that "[f]or example, Apple provides developers with the OS and underlying code libraries; YouTube provides hosting infrastructure to creators; Wikipedia provides writers with the tools to collaborate on an article; and JC Penney provides stores to its boutique partners").

[690] Ibidem (noting that "[a]pple needed to attract both developers and users. Similarly, eBay needed both buyers and sellers.").

[691] Ibidem (noting that "For example, Google matches the supply and demand of online content, while marketplaces like eBay match buyers to relevant products.").

Taking the above thesis into an Open Banking context means that well-developed APIs (the "toolbox") will be critical for banks pursuing a marketplace strategy or a platform strategy as they facilitate richness and ease of integration with third-party providers of financial and non-financial services and products.[692] It also means that banks will need to become a "magnet" and develop the ability to attract a meaningful number of "right" participants to their marketplace/platform. Finally, the above suggests that a successful marketplace strategy / platform strategy will heavily rely on access to customer data and insights (the "matchmaker") that can be processed and contextualized to drive higher level analytic and provide competitive predictive services.[693] By leveraging such data and insights (subject to the required consents and authorizations), banks will be able to match participants to their marketplace / platform, thus enabling third-party providers of financial and non-financial services and products to engage the "right" costumers and customers to reach the "right" providers.

To successfully deliver on its marketplace strategy or platform strategy, a bank must take a number of actions, which include the following:

(1) First, the bank will need to identify the focus of its business and its core capabilities and then decide what capabilities may be ceded to partners. This preliminary analysis will help the bank embrace new propositions coming from traditional and non-traditional players (e.g., fintech companies and tech giants).[694]

(2) Second, a following step will be for the bank to choose its partners and define an effective strategy to attract them to its marketplace / platform.[695] By bringing the best of the fintech products and services (as well as non-financial products and services) under the umbrella of a trusted bank relationship and formulating them into efficient customer solutions that complement its existing offerings, the bank will gain the opportunity to embed itself more deeply into its customers' daily lives. To this end, the bank will need to get scrappy with smarter digital marketing tools (including social media) and to pay particular attention to the design of incentives schemes, reputation systems, and pricing models.

(3) Third, the bank will need to assess its existing architecture and IT systems and rethink them to support its marketplace strategy / platform strategy.[696] This will require investments in a variety of additional and enhanced architectural, technical, and operational capabilities, including at minimum API

[692] See, Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., p. 12.
[693] See, Earnix, *The Role of Analytics in the Banking Age*, cit.; Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., pp. 8, 12.
[694] See, McKinsey & Company, *Building a Digital-Banking Business*, cit., p. 4.
[695] See, Ernst & Young, *Revolutionary Change is Transforming the Financial Services Landscape. Financial Services Leadership Summit December 2016*, cit., pp. 6-8.
[696] See, e.g., Deloitte, *Open Banking: What Does The Future Hold?*, cit., pp. 9-10; Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit., p. 20 (explaining that "[t]here are a set of supporting technologies, as part of a broader API ecosystem, that are essential for connectivity, scalability, security, management and intelligence, which create an initial platform. But equally important are the tools, processes and mindset needed to evolve the platform at the new pace required to maintain currency in a highly competitive market."); McKinsey & Company, *The Bank of the Future*, McKinsey Interview Series – Transcript of the Interview of Somesh Khanna (McKinsey Director (NY)) (November 2014); PWC, *PSD2 – Are You Ready to Embrace the Change? Key Areas of Focus*, PWC Report (February 2017), pp. 3-5; Contino, *Accelerating Compliance & the API Economy With Open Banking & PSD2*, Contino Report (2017), pp. 7-12; Gartner, *Use PSD2 to Accelerate Open Banking*, Gartner Report (February 19, 2016).

management capabilities (developed internally and/or in collaboration with API management solutions providers)[697] integrated across all architectural layers, application service governance, and application of security protocols in accordance with applicable standards.

(4) APIs are a key building block of a successful Open Banking marketplace / platform.[698] As the API economy takes off,[699] the bank will need to adopt and deploy an effective API strategy. Towards this end, the bank should consider taking a number of concrete steps, which include the following:

- The bank should view its API strategy as first and foremost an ongoing evolving business strategy, not a mere technical product selection strategy. Furthermore, the bank should consider APIs as an independent business, set up to encourage financial innovation.[700]

- APIs will increasingly be responsible for customer engagement and revenue generation. Therefore, when it comes to APIs, the bank should take the same approach as when delivering new customer products and services. This means that the bank will need to view and manage APIs as products themselves, with all the inherent backing and support that this requires.[701]

---

[697] New breeds of companies are rapidly emerging out of the API economy, creating a new ecosystem of interconnected services surrounding the API lifecycles. Examples include companies that support APIs throughout their lifecycles with comprehensive management solutions, companies that provide security tools for access management and identity control, companies that specialize in API testing and monitoring, companies specializing in API discovery or marketing, and many more. Other critical players in the API economy are cloud hosting providers and cloud computing providers. See, Microsoft, *Empowering the Digital Bank: The API Economy: Helping Financial Services Companies to Build Better Products*, cit. (noting that the API economy "is based around four building blocks: social, mobile, analytics and cloud."); Gartner, *Magic Quadrant for Full Life Cycle API Management*, Gartner Report (October 27, 2016) (providing a detailed analysis of 19 vendors and explaining that "[i]t is impossible to provide the platform for any digital strategy, and run an effective API program to benefit from the API economy, without full life cycle API management.").

[698] See, e.g., Forrester Research, *Four Ways APIs Are Changing Banking. How Financial Services Firms Are Exploiting the API Economy*, cit., pp. 7-9, 11 note 4 (explaining that "[t]he problem that application development and delivery professionals must solve — what "well-designed" means — applies not only to open web APIs but also to B2B APIs, internal APIs, and product APIs. The answer starts with clear consideration of each API's business context and intent, then moves on to the API's functionality, technology, and future agility.); Forrester Research, *Establish Your API Design Strategy APIs Are a Key Embodiment of Your Digital Business*, Forrester Research Report (June 2013) (providing structured guidance on how to use business model, purpose, and architectural context as key pillars of an API design strategy).

[699] API economy is a general term that describes the way APIs can positively affect an organization's profitability. See, Gartner, *Welcome to the API Economy - Enterprises Need to Create an Industry Vision for Digital Business*, Gartner Report (June 9, 2016) (quoting Kristin R. Moyer, vice president and distinguished analyst at Gartner, explaining that "[t]he API economy is an enabler for turning a business or organization into a platform. Platforms multiply value creation because they enable business ecosystems inside and outside of the enterprise to consummate matches among users and facilitate the creation and/or exchange of goods, services and social currency so that all participants are able to capture value.").

[700] See, e.g., IBM, *Open Banking: Everything You Need to Know*, cit.; KPMG, *Banking is a Software Industry: Time to Walk the Walk*, KPMG Insights (February 10, 2017).

[701] See, Deloitte, *Tech Trends 2015 - The Fusion of Business and IT*, cit., pp. 24, 27, 29 (explaining that "[a]s traditional business models decline, APIs can be a vehicle to spur growth, and even create new paths to revenue. Viewing APIs in this way requires a shift in thinking. The new integration mindset focuses less on just connecting applications than on exposing information within and beyond your organizational boundaries. It's concerned less with how IT runs, and more with how the business runs."); Forrester Research, *Four Ways APIs Are Changing Banking. How Financial Services Firms Are Exploiting The API Economy*, cit., p. 9 (explaining that "[i]n much the same way that loans or mobile banking platforms are "products," so too are APIs. Like any product, APIs are a business endeavor and require adequate funding and a planned order of development."); Apigee, *The State of APIs - 2017 Report: How APIs Power Digital Ecosystems*, cit., slides 17-18 (arguing that "[t]reating APIs as products enables companies to package APIs with quota limits and pricing models. Organizations can iterate on a variety of business models to optimize on the right offerings. Successful platforms clearly define and measure a combination of business metrics like direct or indirect revenue and API consumption metrics like API traffic, the number of apps, and the number of active developers."); MuleSoft, *Open Banking and the Future of Financial Services. Are You a Survivor or Thriver?*, MuleSoft WhitePaper (2016), p. 3 (explaining that "[i]n this new ecosystem, APIs are a new channel for doing business and need to be given that importance. The monetization of the API economy presents a new source of revenue, but only if a bank's APIs are adopted and used by other organizations and developers. APIs should be productized and marketed as a source of competitive advantage, like any other traditional product.").

- The bank should design its APIs and implement its API strategy with the outside in mind from the outset, regardless of whether it plans to be open or not. Investing in this mindset can give the bank a significant competitive edge.[702]

- Successful APIs require healthy internal and external developer communities. Because of this, the bank should build APIs that can be easily found, understood, and used. In addition, the bank will need to foster a thriving, enthusiastic, and well-engaged ecosystem of developers and partners, as this will be essential for the bank to flourish its marketplace/platform on the back of its APIs.[703]

- The bank's API should have the user experience and engagement at the center of the decision-making process. To this end, the bank should carefully collect feedbacks and insights from developers and end-users of its API-based services (including individual and corporate customers) and, then, review and leverage such feedbacks and insights to inform the design process. In addition, the bank should seek to create a strong sense of community, by regular interacting with developers and users and actively seeking their comments and input.

- The bank should ensure that both customer experience professionals and technologists are engaged in API-driven business strategy discussions. In addition, it will be critical for the business model, customer experience, and technology design to happen in parallel and to coordinate seamlessly. The bank will also need to create and deploy a new combined technology and business support model to timely and effectively assist both customers and third party developers using the bank's APIs.

- The bank should invest in a robust API management platform.[704] To this end, a number of key platform requirements should be considered, including stability,[705] analytics and usage tracking,[706] API lifecycle and documentation, developer portals, hosting, and security.[707]

---

[702] See, Forrester Research, *Four Ways APIs Are Changing Banking. How Financial Services Firms Are Exploiting The API Economy*, cit., p. 9 (noting that "[b]ack in 2002, an internal policy compelled Amazon developers to use APIs for all software — and they had to design those APIs with the outside world in mind. If you design with an external use case in mind from the outset, you will save considerable effort should you wish to make those APIs open in the future.").

[703] See, e.g., Apigee, *The State of APIs - 2017 Report: How APIs Power Digital Ecosystems*, cit., slides 15-16 ("[s]uccessful organizations make it easy for developers to discover, consume and use their APIs. These organizations run developer outreach programs (hackathons, for example), deploy developer portals for easy API discovery and secure self-service access, and publish interactive documentation " … "[s]uccessful organizations have open developer programs that provide self-service developer registration, interactive documentation, and developer communities to foster sharing."); Accenture, *Payments APIs: Too Compelling to Ignore*, cit. (noting that "APIs exist for developers' use; without this, an API has no value. Recognizable, easy-to-use, documented APIs have the most uptake among developers."); Forrester Research, *Four Ways APIs Are Changing Banking. How Financial Services Firms Are Exploiting the API Economy*, cit., p. 9 ("[h]owever, to drive maximum value from APIs, you must support developers, whether internal or external. A developer portal that provides comprehensive documentation, monitoring services, as well as a sandbox for testing and that also promotes the ready discovery of APIs is the bare minimum — this is, after all, a shop window for your latest products."); Deloitte, *Tech Trends 2015 - The Fusion of Business and IT*, cit., p. 30 (noting that "[i]f you are trying to launch external-facing APIs or platforms for the first time, you should ready yourself for a sustained campaign to drive awareness, subscriptions, and support. Beyond readying the core APIs and surrounding management services, companies shouldn't forget about the required ancillary components: documentation, code samples, testing and certification tools, support models, monitoring, maintenance, and upkeep. Incentives and attempts to influence stakeholders should be tied to the target audiences and framed accordingly.

[704] See, Contino, *Accelerating Compliance & the API Economy With Open Banking & PSD2*, cit., pp. 8-10 (analyzing critical technical challenges involved in the process of developing and managing high-quality APIs); Deloitte, *Tech Trends 2015 - The Fusion of Business and IT*, cit., p. 23 (describing an API management backbone as "a platform to: 1) Create, govern, and deploy APIs: versioning, discoverability, and clarity of scope and purpose; 2) Secure, monitor, and optimize usage: access control, security policy

- APIs expose data, products, services, and transactions, thus creating assets that can be shared and reused. However, in so doing, APIs also increase potential points of vulnerability, open new potential attack vectors for fraudsters and thieves, and bring a host of new privacy, cyber, and security-related challenges. To address these concerns, the bank will need to develop an API strategy with a clear security and privacy focus from the start. At the highest level, this will command the adoption of scalable and efficient governance control models, API-level authentication and access management systems, real-time tracing and monitoring systems, API automated testing systems, as well as management tools to measure API performance and traffic volume.[708] In addition, the bank will need to implement a number of related initiatives, including updating existing security and compliance capabilities (e.g., fraud detection and KYC) and implementing new controls and security measures (e.g., machine learning and AI anti-fraud technologies, encryption, and strong customer authentication).

- Finally, reliance on APIs may intensify the bank's operational, business, reputational, and liquidity risks. To monitor, reduce, and mitigate these risks within an Open Banking ecosystem, the bank will need to build and deploy renewed and effective risk management and compliance capabilities. This point is further discussed below.[709]

(5) Fifth, the bank will need to define a new business and organizational architecture to ensure the long-term success of its marketplace strategy / platform strategy. To this end, it is critical for the bank to develop an API-based platform mindset of innovating, building, and delivering services and products. Developing and cultivating this mindset will require a complete transformation within the bank's organization. The bank should start looking at its organization through marketplace/platform lens and

---

enforcement, routing, caching, throttling (rate limits and quotas), instrumentation, and analytics; and 3) Market, support, and monetize assets: manage sales, pricing, metering, billing, and key or token provisioning."); Accenture, *Payments APIs: Too Compelling To Ignore*, cit. (explaining that selecting and operating a robust API management platform is critical "as the number of database calls to and from banks' back-end systems through APIs could be enormous … 35 percent of mobile banking app consumers access the app once a day or more; 84 percent check once a week or more. Banks will need a robust API platform to manage the volume of traffic traversing APIs and also provide the analytics for optimum usability, efficiency and effectiveness. Most banks will need to build or buy an API management gateway to facilitate secure access with partners and developers while also providing strong security controls.").

[705] See, Accenture, *Driving Innovation in Payments— Powered by APIs & Open Banking*, cit., p. 6 (noting that "[t]his is an evolving market and vendor landscape that is changing rapidly as larger traditional technology organizations are acquiring API management platforms to make their overall integration offerings more appealing. Navigating this environment can be complex.").

[706] Ibidem (explaining that "[a] good API enablement platform helps monitor API usage, run-time performance and traffic, API adoption, API economics and other measures that point to return on investment performance.").

[707] Ibidem (noting that "[r]emaining secure while enabling APIs is essential. Many platforms provide security features, such as Payment Card Industry compliance. A provider should also use platforms that can monitor access to data via APIs and can revoke or change access rights if required.").

[708] See, Contino, *Accelerating Compliance & The API Economy With Open Banking & PSD2*, cit., pp. 10-12; Deloitte, *Tech Trends 2015 - The Fusion of Business and IT*, cit., p. 28 (noting that "[s]ystem event monitoring should be extended to the API layer, allowing unexpected interface calls to be flagged for investigation. Depending on the nature of the underlying business data and transactions, responses may need to be prepared in case the underlying APIs are compromised—for example, moving a retailer's online order processing to local backup systems.").

[709] See, Contino, *Accelerating Compliance & The API Economy With Open Banking & PSD2*, cit., pp. 11-12.

viewing APIs as key business assets that the bank can leverage to reframe the way it builds and delivers new products and services and interacts with its customers and partners.[710]

(6) Sixth, to successfully establish and grow its marketplace / platform, the bank will need additional competencies and capabilities. The development of these competencies and capabilities will likely require new technology partners, revised training, and new recruitment across a number of existing and newly established teams. At the same time, the bank may need to implement corporate initiatives to create an organizational culture that supports and encourages the creation of an Open Banking marketplace / platform.

(7) Finally, and related to the above, the bank will need to protect its marketplace / platform. This is paramount for the bank in order to earn the trust and drive loyalty among customers and the various partners in its ecosystem. This means that the bank will need to address its Open Banking marketplace strategy / Open Banking platform strategy not only from a technology and business points of view, but also through legal and compliance lens. A solid legal and compliance strategy is critical to foster innovation and grow a new collaborative ecosystem, while maintaining security, safety, and transparency.

As a key priority, the bank will need to establish a solid and independent legal and compliance team(s) to oversee its marketplace / platform activities. To this end, the bank will need to clearly identify and document available compliance resources and the way in which such resources are deployed. A constant process of compliance monitor and review will need to be implemented through the testing, launching, and operating stages of new products, services, and business models. Regular legal and compliance review meetings shall be organized and the deliberations and findings of such meetings shall be carefully documented. Furthermore, a clear record of how senior management oversight is achieved will need to be maintained, including how the senior management periodically review and evaluate the effectiveness of compliance policies, guidelines, and procedures, set a top-down compliance tone, and take appropriate measures to address any compliance deficiencies.

In addition to the above, the legal and compliance team(s) will also need to consider a number of risks that a Open Banking marketplace strategy / Open Banking platform strategy may create and/or exacerbate. Among them, money laundering (ML), financial crimes, and terrorist financing (TF) will demand particular attention. The relevant regimes in the United States, EU and the UK are rapidly evolving and over the past year relevant regulatory authorities have been aggressively stepping up their enforcement actions. Given this background, it is critical for the bank's legal and compliance team(s) to establish and enforce adequate policies, guidelines, and procedures for assessing the level of financial crime, ML, and TF risks posed by

[710] See, Forrester Research, *Four Ways APIs Are Changing Banking. How Financial Services Firms Are Exploiting The API Economy*, cit., pp. 7-9; Forrester Research, *APIs Underpin A Digital Business Platform - Prepare For Digital Transformation's Constant, Unpredictable Change*, Forrester Research Report (January 2016); Forrester Research, *How APIs Reframe Business Strategy - Craft an API Strategy to Enable Digital Business Transformation*, Forrester Research Report (June 2015); Deloitte, *Tech Trends 2015 - The Fusion of Business and IT*, cit., p. 31 (arguing that in the context of an API economy "the bigger opportunity is to help educate, provoke, and harvest how business services and their underlying APIs may reshape how work gets done and how organizations compete. This opportunity represents the micro and macro versions of the same vision: moving from systems through data to the new reality of the API economy.").

prospective and existing customers. Towards this end, the legal and compliance team(s) will need to (at minimum):

- Conduct adequate customer due diligence (CDD) and enhanced due diligence (EDD) in relation to higher risk customers and shall undertake regular reviews of its assessments and analyses.

- Carry out periodic testing and reviews of its anti-money laundering (AML) and counter terrorist financing (CTF) systems and controls and maintain accurate and well-organized records of the testing and reviews undertaken.

- Ensure that relevant policies, guidelines, and procedures are current with new legislative and regulatory developments and enforcement cases.

- Promote AML, financial crime, and CTF compliance awareness across the entire bank by providing guidance and periodic training (and shall maintain accurate and well-organized records of staff completion of such trainings).

- Implement and enforce financial crime, AML, and CTF policies, guidelines, and procedures seamlessly across the entire bank's marketplace / platform. This means that, as the bank deploys its Open Banking strategy, the legal and compliance team(s) will need to broaden the scope of its(their) compliance activities to assess financial crimes, ML, and TF risk exposure across its entire ecosystem of third-party counterparties, affiliates, and partners and coordinate its compliance efforts with the compliance activities performed by such third parties with regard to the products and services offered throughout the bank's marketplace / platform.

- Consider deploying new technologies, including machine learning and AI, biometric verification, big data analytics, and cloud-based data sharing systems.

Furthermore, additional areas of risk that a Open Banking marketplace strategy / Open Banking platform strategy may create and/or exacerbate include data protection, security, and privacy. Balancing transparency and openness with data security and privacy is key to building an open API-driven ecosystem. The bank's marketplace / platform will rely heavily on: (1) well-defined APIs to facilitate richness and ease of integration with third parties' services and products; and (2) access to customer data and insights, which can be processed and contextualized to drive analytics and provide competitive predictive services.[711] Significant quantities of customer data (including personal data embedded within data relating to a customer's transaction) will likely concentrate around the bank's marketplace / platform. Because of this, monitoring and protecting costumer data though each stage of the costumer's journey across the services provided on the marketplace / platform will be a key priority. In particular, the legal and compliance team(s) will need to ensure that the testing, launching, and operating stages of any new business models,

[711] Cfr., e.g., Earnix, *The Role of Analytics in the Banking Age*, cit.; Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, cit.

products, and services are in line with applicable data protection rules and Open Banking regulatory and policy frameworks.

Open Banking and data protection compliance must address the underlying data and the mechanisms through which such data is accessed, shared, utilized, and stored. To this purpose, a number of complementary initiatives can be considered:

- First, IT and other relevant systems will need to be designed with data privacy at their core. Adequate controls must be put in place to verify the identity of the customer or third-party seeking access to the bank's APIs or customer data, and systems for rapid detection and reporting of costumer data breaches/misuses must be implemented across the bank's marketplace / platform. As the bank grows its ecosystem, limiting the amount of costumer data collected, the number of locations where costumer data is stored, and the length of time during which costumer data is stored can help mitigate the risk of data breach/misuse and minimize damages in the event a breach/misuse of costumer data occurs.

- Second, adequate mechanisms will need to be implemented to allow customers to give explicit and informed consent to the access and use of their data, to promptly and easily revoke or amend their consents, and to correct inaccurate or incomplete data. For customers to give informed consent, they must be aware of their rights and responsibilities when sharing or handling data and must be able to understand (and control) what data are collected, who has access to their data, for how long, and for what purposes. This means that the bank building a marketplace or a platform must be transparent and proactive in how it (and the third parties operating through its ecosystem) accesses, uses, shares, and stores customer data. To this purpose, the bank's website terms and conditions of use agreement, cookie policy, privacy policy and security policy, as well the agreements governing the provision of products and services across the entire marketplace / platform must be complete, accurate, and updated. Moreover, the legal and compliance team(s) may consider collaborate with third-parties operating across the bank's marketplace to develop dashboards, which will display all the applications to which a customer has provided consent to access and use his/her/its data and will allow the costumer to easily and promptly revoke or amend his/her/its consent.

- Third, the legal and compliance team(s) will need to help create a culture of data protection and privacy across the bank's marketplace / platform: communication between the legal and compliance team(s) and the various teams at the bank must be continuous (and properly documented), and periodic mandatory training will need to be organized to allow employees to better understand how the requirements of data security and privacy regulation impact their particular roles and activities.

- As the bank scales its operations, a combination of network effects, network security, and distribution power will fuel increasing value within the bank's marketplace / platform. Over time, the bank will have to negotiate new (and re-negotiate existing) inter- and cross-industry partnerships and other arrangements with a variety of third-party service providers and developers. The legal and compliance team(s) at the bank will need to be involved early in the process and its(their) insights will need to be

leveraged to create a sound integration plan. The early involvement of the legal and compliance team(s) will be critical to develop a key roadmap for risk management and regulatory compliance integration. Moreover, the early involvement of the legal and compliance team(s) in the due diligence and audit process for new third-party service providers and developers will be vital to minimize fraud, fight financial crimes, and ensure that data security and privacy remain key priorities. In performing these functions, the legal and compliance team(s) will need to consider a number of regulatory requirements and guidance, including risk management and outsourcing requirements and guidance.

Following the integration phase, the legal and compliance team(s) will need to provide ongoing and proactive oversight of the relationships between the bank and its third-parties across a number of areas, including partner assessment, rules of engagement and governance, contract and commercial management and performance management. Continuous involvement by the legal and compliance team(s) will help ensure that the management and governance of the partners are fully integrated with the bank's compliance structures, processes, and technologies; this, in turn, will enable consistent and reliable service delivery and rapid decision-making throughout the bank's entire marketplace / platform.

Based on the analysis of the above 7 points, it appears quite clear that the task of creating a marketplace / platform will be no mean feat for a bank. In implementing a marketplace strategy or a platform strategy, a bank faces a number of challenges. A first challenge is created by the fact that the bank may tend to embrace the entire value chain and view it as core. The inability to ascertain its true competence(s), in turn, makes it extremely difficult to identify areas where the bank would be better off engaging with other banks/fintech companies and offering banking and financial services or products via a third-party provider throughout its marketplace / platform. As it brings non-core offerings to the market, the bank incurs increasing costs and may have a very hard time being competitive and attracting potential partners.

Second, successful execution of the marketplace strategy and the platform strategy requires flexible open IT platform(s) capable of integrating with external platforms. The ability to connect to, and integrate with, other platforms, as well as the ability to extract, process and leverage structured and unstructured data, command a level of agility, flexibility and speed that the majority of banking legacy IT systems don't have. How challenging it is for a bank to keep up with the demand for open APIs depends on the bank and the state of its legacy core systems and technology architecture. It is practically difficult (if not impossible) for a bank (especially a national or multinational bank) to transform and update existing systems and architectures from one month to the next. This transformation is likely to be gradual and phased in over a (long) period of time.

Third, what may be even more complex for a bank than setting up an API framework is to expose it successfully. The majority of banking legacy IT systems are far from open and banks with such systems

find it more challenging to open up via APIs compared to new market participants, whose state-of-art systems and infrastructures are built for an API-driven world.[712]

[712] See Finextra, *PSD2 and Open Banking: Defining Your Role in the Digital Ecosystem*, cit., p. 23 (quoting Tom Blomfield, CEO and Founder at Monzo "[t]he irony is that the banks all have APIs already," he says. "If you use a mobile application to access your bank account, it's fetching your account data from your bank's existing API. "A2A" is just about publicly documenting those APIs and enabling third-party access.").

CHAPTER 7. THE FUTURE OF BANKING IS NOW: CHALLENGER BANKING

As early as 1994, Bill Gates made the provocative statement that "banking is necessary, banks are not," perhaps suggesting the idea that in the future, banking would be needed, but banks themselves would not. Fast-forward two decades and in 2014 venture capitalist Marc Andreessen tweeted about reinventing banking with better software:

"@cdixon @JackGavigan @Kwdmiller @aweissman I am dying to fund a disruptive bank."

— Marc Andreessen (@pmarca) February 9, 2014

With a subsequent tweet, Andreessen ignited the debated around the use of APIs to access customer financial and banking data and, then, build services on top of it.[713]

"@maxrogo @rabois @cdixon I want the pure software bank w/no physical infrastructure, + a full API for financial apps on top."

— Marc Andreessen (@pmarca) February 10, 2014

More than three years later, a steady stream of fintech companies is making this vision a reality. Challenger banks -– as these players are commonly referred to -– are now challenging the very idea of what it means to do banking. They understand the impact of Open Banking and the innovative power of APIs discussed in prior chapters; and they are actively designing the role they will play in a new open and interconnected financial and banking ecosystem.

Challenger banks recognize that, although banking is an essential part of our lives, the way people and businesses do banking hasn't changed much over time. So they take on a challenge of building something completely different from scratch. Their goals are bold and ambitious: by creating a new banking paradigm, they aim at changing the lives of million of customers; they seek to empower customers and to give them control over their finances with increased transparency and fairness of terms; they engage with customers at a new and deeper level and want them to be part of the change, helping shape the direction of the bank as it builds.

This chapter focuses on challenger banks. Specifically, it discusses major drivers behind the raise of challenger banks, examines how challenger banks are redefining the way people and businesses do banking, and identifies a number of opportunities (and challenges) that challenger banks may exploit (may face) as they scale their operations and grow their activities.

7.A. The Challenger Landscape

The umbrella of "challenger banks" covers a variety of entities with different target markets and service models. To analyze them, it is useful to group challenger banks into distinct categories, with the

[713] See, Kevin J. Delaney, *To Disrupt Banking, Do You Need to Own the Bank?*, Quartz (February 10, 2014) (noting that other "[v]alley heavyweights chimed in, including Chris Dixon (a colleague at Andreessen Horowitz), Keith Rabois (Khosla Ventures), and Mo Kofyman (Spark Capital).").

understanding that there are (and will be) hybrid challengers that do not (and won't) fit neatly into a single category.

A number of categorizations have been suggested. For instance, a recent report by PWC, which analyzes challenger banks operating in the UK banking market, distinguishes among four broad groups of challenger banks:[714]

- Mid-size Full Service Banks - Banks with well−known brands, single-digit millions of customers and between 2,000 and 9,000 employees. They generally offer a full set of standard product and services. They have increased their digital capabilities, but still rely on a well-established physical network of branches. They typically have a regional focus. At present, they are undertaking a process of transformation and modernization of their operations and IT systems, and are investing in scalable platforms to do so. Many of these mid-size full service banks are also facing profitability pressures, and are seeking to improve ROE that are currently negative or below 10%, and cost-to-income ratios that are in between 70% and 350%. Examples include CYBG, Co-operative Bank, and TSB.

- Specialist Banks – Banks that typically focus on providing lending and saving services to under-banked customer segments. They have limited or no physical presence and increasingly rely on digital channels. They often work with intermediaries to source new business. They have between 500 and 1,000 employees and a few hundred thousand customers, but tend to be profitable, with ROE between 10% and 40% and cost-to-income ratios in a range of 20% and 40%. They have growth opportunities in their target markets and the flexibility to broaden their areas of focus. Examples include OneSavings, Shawbrook and Secure Trust.

- Non-Bank Brands – Banks whose parent companies are strong players in other industries, such as Tesco, Sainsbury's, and Virgin. These banks have strong and trusted brands, and generally seek to serve the needs of customers loyal to the parent group as a whole. These banks typically have a large scale, with customer bases in a range of 1 million and 8 million and 1,000 to 3,000 employees. They have limited (but flexible) physical presence and generally focus on digital channels. They have very focused (but growing) propositions targeted at their parent companies' customers. They are relatively profitable, with ROE of between 2% and 15% and cost-to-income ratios in a range of 65% and 70%. They can tap into their parent companies' large customer base and data.

- Digital-Only Banks – Many of these banks have been founded very recently. They focus on digital channels (web and mobile apps) and have a small (but growing) scale, with between 10 to 150 employees and few hundred thousand users or less. They are positioning themselves to lead in the evolving Open Banking ecosystem. Toward this end, they tend to leverage innovative API-driven technology platforms to

[714] See, PWC, *Who Are You Calling a 'Challenger'? How Competition is Improving Customer Choice and Driving Innovation In the UK Banking* Market, cit.

deliver personalized, flexible, unified and digital customer experience and engagement. This category is discussed in more detail below.

A further study by Burnmark classifies challenger banks in three main categories:[715]

- Pseudo Challengers – Digital subsidiaries, digital partners (neo-banks) and digital startups of existing banks. Examples include Hello bank! (digital subsidiary of BNP Paribas), Moven and Simple (acquired by BBVA).

- Real Challengers – Digital-only banks that have obtained a banking license in the last 3 to 5 years or are in the process of obtaining one. Examples include Atom Bank, Monzo, and Fidor Bank. This category is discussed in greater detail below.

- Embryonic Challengers – Fintech innovators on the banking value chain that operate only through mobile apps in collaboration/partnership with established banks or other (bigger) challenger banks. Examples include Pockit and Loot.

Finally, a recent report by KPMG, analyzing the challenger landscape in the UK, distinguished among three main categories of challenger banks:[716]

- Larger Challengers – Long established banks or banks that have inherited relatively large portfolios of loans and advances to customers. Examples include Clydesdale and Yorkshire Banking Group, Handelsbanken (UK division), Paragon, TSB, Virgin Money, and Williams & Glyn.

- Small Challengers – Banks typically incorporated in the past 5 to 10 years and backed by private equity through their initial growth phase. A few of them are now listed banks. Examples include AIB (UK division), Aldermore, Close Brothers, Metro Bank, OneSavings Bank, Shawbrook Group, and Secure Trust Bank.

- Digitally-Focused Challenger – Digitally-focused banks that leverage new technologies and offer personalized services as key differentiators. They often collaborate with other businesses and enter into a variety of inter and cross-industry partnerships. Some of them have even used customer crowdfunding to consolidate the engagement with their community and advance their expansion. Examples include Atom Bank, Fidor Bank, Monzo, Starling Bank, and Tandem. This category is discussed in greater detail below.

7.B. Regulation as Driving Force Behind the Raise of Challenger Banks

The raise of challenger banks is certainly dependent on characteristics and problems specific to particular geographic areas. In developed markets, the unsatisfactory state of affairs with existing banks has created the opportunity for challenger banks to enter the banking and financial services industry and gain market

[715] See, Burnmark, *Challenger Banking*, cit.
[716] See, KPMG, *A New Landscape. Challenger Banking Annual Results*, KPMG Report (May 2016).

share by offering superior services.[717] By contrast, in emerging markets, where mobile penetration is rapidly increasing, challenger banks are best positioned to accelerate banking innovation, financial inclusion and wellness.[718]

In addition to characteristics and problems specific to particular geographic areas, a number of driving forces have also combined to facilitate the emergence of challenger banks, including evolving customer preferences, technological advances, and regulation changes. These forces have contributed in lowering the barriers of entry and removing many conditions that had been unique to the banking and financial services industry and had long protected its incumbents.[719]

Chapter 1 and Chapter 2 have already analyzed evolving customer preferences, technology advances, and fintech-related regulatory reforms and policy initiatives. This section digs a little deeper into regulatory developments that have facilitated the emergence of challenger banks – with focus on digital-only (digitally-focused) challenger banks – in the UK, Europe, and the United States. As further discussed below, while challenger banks has become an increasingly relevant and valuable component of the global financial and banking system, regulation has emerged as a key differentiator across these three geographic regions.[720]

7.B.i The United Kingdom (UK) – Banking License

In 2013, upon request by the HM Treasury,[721] the UK's Financial Service Authority (FSA) and the Bank of England published a review of the authorization process for acquiring a banking license[722] and the prudential and conduct requirements that apply to new entrant banks.[723] The review set out a number of

---

[717] Id., pp. 4-5 (noting that in the UK market the challengers outperform the big five banks (Barclays, HSBC, Lloyds Bank, Royal Bank of Scotland and Santander) in terms of return on equity (ROE), with the average ROE for challenger banks between 9.5 % for larger challengers and 17% for smaller challenger as opposed to the big five banks at 4.6%. Key factors behind the outperformance include lower legacy IT costs, a simple business model, as well as a simplified product portfolio. Significantly, challengers recorded an average cost-to-income (CTI) ratio of c. 59.6% compared to 80% CTI ratio for their incumbent counterparts.).

[718] See, Burnmark, *Challenger Banking*, cit., pp. 6-7.

[719] See, David Brear and Pascal Bouvier, *Exploring Banking as a Platform (BaaP) Model*, cit.

[720] See, McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives For Banks*, cit., p. 7 (noting that "[t]he impact [of regulation] could also vary significantly by country, given different regulatory stances, e.g., Anglo-Saxon regulation on data usage versus other EU countries; payments system directives in Europe that cause banks to open up their Application Programming Interfaces (APIs) to nonbanks.").

[721] In the aftermaths of the financial crisis of 2008-2009, the Office of Fair Trading (OFT) and the Independent Commission on Banking (ICB) published reports discussing competition and barriers to entry in the UK banking sector. See, Office of Fair Trading (OFT), *Review of Barriers to Entry, Expansion and Exit in Retail Banking*, Office of Fair Trading Report (November 2010); Independent Commission on Banking (ICB), *Final Report Recommendations*, Independent Commission on Banking Report (September 2011). Following the publication of these reports, the HM Treasury asked the Financial Conduct Authority (FSA) and the Bank of England to review the prudential and conduct requirements for new entrants to the banking sector. See, HM Treasury, *Banking Reform: Delivering Stability and Supporting a Sustainable Economy*, HM Treasury (June 2012).

[722] In the UK, a company needs a "Part 4A permission" to carry on the regulated activity of accepting deposits and it is this permission which is often termed as a "banking license." Part 4A permission refers to Part 4A of the Financial Services and Markets Act 2000 (FSMA), which together with Schedule 6 to FSMA set out the procedure for applying for permission to undertake regulated activities, the requirements for new firm authorizations and the Prudential Regulation Authority (PRA)'s and Financial Conduct Authority (FCA)'s statutory threshold conditions that must be met by a firm at authorization and on an ongoing basis. The PRA's threshold conditions are designed to promote the safety and soundness of PRA-authorized persons, whilst the FCA's threshold conditions are designed to protect consumers, protect and enhance the integrity of the UK financial system and promote effective competition in the interests of consumers. For further details, see the PRA approach documents available at http://www.bankofengland.co.uk/publications/Pages/other/pra/supervisoryapproach.aspx and Financial Conduct Authority (FCA) Handbook, Threshold Conditions available at https://www.handbook.fca.org.uk/handbook/COND/2/.

[723] See, Financial Service Authority (FSA) and the Bank of England, *A Review of Requirements for Firms Entering into or Expanding in the Banking Sector*, Financial Service Authority and the Bank of England Report (March 2013); Financial Conduct Authority

critical changes that the FSA's successor bodies, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA), were to implement, including the following: reduced capital requirements at authorization; reduced liquidity requirements for all new entrant banks; removal of barriers to expansion; improvements to the existing authorization process; introduction of an additional option for the authorization process (referred to as "mobilization"); streamlining and simplification of information requirements; and additional measures relating to the introduction of the Capital Requirements Directive (2013/36EU)(CRD) and the Capital Requirements Regulation (575/2013)(CRR) (jointly, the 'CRD IV').[724]

The described changes were specifically designed to achieve two main goals: (1) reducing the barriers to entry and expansion in the UK banking sector; and (2) enabling increased competitive challenge to existing banks.

Further, in January 2016,[725] the PRA and the FCA launched the New Bank Start-up Unit, a joint initiative aiming at giving information and support to newly authorized banks and those thinking of becoming a new bank in the UK.[726]

(FCA), *A Review of Requirements for Firms Entering into or Expanding in the Banking Sector: One Year On*, Financial Conduct Authority Report (July 2014).

[724] Both the PRA and the FCA have responsibility for the supervision of banks. The two authorities work closely together and coordinate their activities though a single authorization process. The process is separated into two or three distinct stages depending on the applicant's circumstances: (1) pre-application; (2) assessment; and (3) for some applicants mobilisation. The pre-application process is designed to increase the likelihood of submission of successful applications of required quality. The process starts with an initial meeting, which provides an opportunity for the firm to discuss its business plan and ask questions to the PRA and the FCA about the authorization process. A feedback meeting, then, takes place after the applicant has submitted, and the PRA and the FCA have reviewed, its updated business plan, including feedback from the initial meeting. An optional Mobilisation and/or IT/outsourcing meeting may also be arranged, if the applicant is considering taking a mobilisation route and/or its proposed business heavily relies on IT or outsourcing arrangements. Finally, a challenge session is arranged just before the submission of the application to discuss the proposals in depth and give the PRA and the FCA the opportunity to provide detailed challenge on the contents of the business plan being finalized. All the described meetings are typically held at either the PRA's or FCA's offices in London. Materials for the meeting must be submitted to the two authorities at minimum 10 working days (15 working days for a challenge session) before the meeting. After each meeting, the PRA and the FCA will provide formal written feedback, which will need to be included in the final application.

Once an application has been submitted, the PRA and the FCA will have a statutory deadline of either 6 (for complete applications) or 12 (for incomplete applications) months to reach a decision on the application. If the applicant takes the mobilisation route, the mobilisation period will last a maximum of 12 months. The PRA will make the final decision on the application and, if successful, it will authorize the applicant. However, the PRA can only authorize a new bank with the FCA's consent. If the FCA does not provide its consent, the PRA will be unable to authorize the applicant. The two regulators will make their own decision independently.

If the application is approved, the applicant will receive an authorization letter from the PRA and FCA (including the details of any applicable restrictions), a scope of permission notice (the Part 4A permission setting out the date from which the permission has effect, which regulated activities are allowed and any requirements or limitations), and a welcome pack. The bank's details will be published on the Financial Services Register from the authorization date as shown in the authorization letter. Contrary, if the PRA and FCA are considering refusing a submitted application, the will first let the applicant know both orally and in writing and will give the time to address their concerns. If the applicant is unable to address these concerns, the PRA and FCA will issue a "minded to refuse" letter, which will set out their concerns and will state in detail which threshold conditions and/or specific rules have not been satisfied. If the applicant is unable these deficiencies, it can withdraw the application and will have the opportunity to reapply later. However, if the applicant decides to proceed, the case will be escalated for a decision by senior management at both regulators. If the senior management at the PRA or the FCA do not agree with the case team's recommendation, the case will be referred back to the original case officers for further analysis. If instead the senior management agrees with the case team's recommendation, the PRA or the FCA will issue a "warning notice." At this point, the applicant will still be able to either withdraw the application or make representations (orally and/or in writing) to the relevant PRA or FCA decision makers. In the latter case, after hearing the representations, the decision makers can decide either not to issue a "decision notice," (in which case, the application will be referred back to the original case officers who will resume the application assessment) or refuse the application (in which case, a "decision notice" will be issued notifying the applicant of its right to refer the decision to the Upper Tribunal (Tax and Chancery Chamber)). If the application is refused and the applicant decide not to refer the "decision notice" to the Upper Tribunal, the PRA will issue a "final notice" and details of this may be published on the PRA's website.

[725] The HM Treasury originally announced the creation of the unit in November 2015. See, HM Treasury, *A Better Deal: Boosting Competition to Bring Down Bills for Families and Firms*, HM Treasury Report (November 2015).

Following the implementation of the described changes and, later, the establishment of the New Bank Start-up Unit, there has been a remarkable increase in the number of players seeking to enter the UK banking market. In particular, since January 2016, 13 banking license applications have been submitted to the Prudential Regulation Authority (PRA) in the U.K, while many new players have announced their interest in applying for a banking license in the upcoming months.[727]

The advantages of having a full banking license are significant. In addition to gaining new revenue sources (deposits and overdraft income), licensed challenger banks benefit from increased independence. Indeed, different from incumbent initiated challengers and challenger banks that partner with incumbents, licensed challenger banks can operate independently as full-fledged banks. This, in turn, gives them the opportunity to improve the quality of their services, accelerate the path of innovation, and retain their agility, without having an incumbent bank's intricate terms and conditions and outdate legacy technologies interfering.[728]

7.B.ii European Union (EU) - Banking License and Passporting

European Commission. Over the past 12 months, EU regulatory and policy discussions around fintech have significantly intensified at the European Commission.[729] In this respect, the stated objective of the European Commission is to ensure that the EU policy and regulatory framework enables the EU's financial sector to take full advantage of fintech technologies, while remaining financially sound and safe for consumers and investors. To this end, the European Commission has committed to adhere to three core principles: technological neutrality,[730] proportionality,[731] and market integrity.[732]

Acknowledging the growing relevance of fintech innovation, on 14 November 2016, the European Commission established an internal Financial Technology Task Force (FTTF).[733] Most recently, on 23

---

[726] See, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), *New Bank Start-up Unit Launched by the Financial Regulators*, Prudential Regulation Authority and Financial Conduct Authority Press Release (January 21, 2016); Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), *New Bank Start-Up Unit. What You Need to Know From the UK's Financial Regulator*, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) Guide (March 2017). For further details on the New Bank Start-up Unit visit: http://www.bankofengland.co.uk/pra/nbsu/Pages/updates-and-resources.aspx.

[727] See, Tom Belger, *PRA Receives 13 Banking Licence Applications*, Bridging & Commercial (February 16, 2017). Information on the number of banks authorized by the PRA are available in the Prudential Regulation Authority (PRA) section on the Bank of England's website. More details on newly authorized banks can be found in the Financial Services Register at https://register.fca.org.uk.

[728] See, Mary Wisniewski, *Why U.K. Fintech Firms Are Becoming (Not Partnering with) Banks*, American Banker (September 16, 2015) (quoting Tom Blomfield, CEO and Founder at Monzo explaining that by partnering with a bank "[y]ou just end up limited in a number of a different ways" … whilst having a full banking license "puts you in control of your own destiny"). See, also, Standard Treasury, *Series A Pitch Deck*, Standard Treasury Presentation (2015) (discussing relative advantages and disadvantages of starting a bank, buying a bank and acquiring a bank in the UK and the United States).

[729] Beyond the European Commission, EU regulatory and policy discussions around fintech are also taking place in the European Parliament, at the European Economic and Social Committee, at the European Supervisory Authorities (ESAs) (the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA)) and within the European Central Bank (ECB) and the European System of Central Banks.

[730] Technology neutrality is seen as a necessary condition to ensure that the same activity is subject to the same regulation irrespective of the way the service is delivered, so that innovation is enabled and level-playing field preserved.

[731] Proportionality is assessed in relation to a number of factors, including the business model, size, systemic significance, as well as the complexity and cross-border activity of the regulated entities.

[732] Application of technologies to financial and banking products and services should promote more market transparency to the benefit of consumers and businesses, without creating unwarranted risks such as market abuse, cyber security issues, and systemic risks.

[733] See, European Commission, *European Commission Sets Up an Internal Task Force on Financial Technology*, European Commission Digital Single Market Blog Post (November 14, 2016).

March 2017, the European Commission published a Consumer Financial Services Action Plan,[734] together with a consultation on the challenges and opportunities that fintech can create in the European financial sector.[735] Both documents aim at outlining and further developing the European Commission's strategy to strengthen the EU single market and its approach towards the creation of a unified European policy and regulatory framework for fintech.

With the public consultation, the European Commission has sought input from a broad spectrum of stakeholders on: (1) new technologies' impact on the European financial services sector, both from the perspective of providers of financial services and consumers; and (2) whether the regulatory and supervisory framework fosters technological innovation in line with its three core principles of technologic neutrality, proportionality and integrity. The public consultation run until 15 June 2017. The feedback so collected will help the European Commission's FTTF assess how fintech can make the EU Single Market for financial services more competitive, inclusive, and efficient, and will serve as input for the European Commission to draft the EU strategy on fintech.

More in detail, the consultation has revolved around four key policy objectives that reflect, according to the European Commission, the main opportunities (as well as the relevant challenges) created by fintech: (1) fostering access to financial services for consumers and businesses; (2) bringing down operational costs and increasing efficiency for the industry; (3) making the single market more competitive by lowering barriers to entry; and (4) balancing greater data sharing and transparency with data security and protection needs.[736]

With respect to the third objective, the public consultation has addressed two key issues - the proposed establishment of new licensing categories for fintech activities and related passporting of these activities across borders.[737] In this respect, the European Commission has noted that innovation has already reduced some of the barriers to entry onto the financial services sector by disrupting traditional distribution channels, lowering production costs, providing more advanced data analytics, and promoting the mobility of customers.[738] However, the European Commission acknowledged, there remain some barriers that technology alone cannot address. In particular, there still exist very different approaches across Member

[734] See, European Commission, *Consumer Financial Services Action Plan: Better Products and More Choice for European Consumers*, European Commission Press Release (March 23, 2017); European Commission, Consumer Financial Services Action Plan: Better Products, More Choice, COM(2017) 139 final, Brussels (March 23, 2017); European Commission, *Consumer Financial Services Action Plan: Better Products, More Choice, Greater Opportunities - Frequently Asked Questions*, European Commission (March 23, 2017); European Commission, *Consumer Financial Services Action Plan: Better Products, More Choice*, Greater Opportunities - Factsheet, European Commission (March 23, 2017).

[735] See, European Commission, *Public Consultation on FinTech: A More Competitive and Innovative European Financial Sector*, European Commission (March 23, 2017); European Commission, *Consultation Document Fintech: A More Competitive And Innovative European Financial Sector*, European Commission (March 23, 2017); European Commission, *Specific Privacy Statement FinTech: A More Competitive and Innovative European Financial Sector Referred as "Consultation" in the Text*, European Commission (March 23, 2017).

[736] See, European Commission, *Consultation Document Fintech: A More Competitive And Innovative European Financial Sector*, cit., p. 6.

[737] Id., pp. 14-15.

[738] Id., p. 14 (noting that "[i]n the past, any successful large scale provision of financial services has been characterized by unique in-house expertise, extensive distribution channels and hold large amounts of proprietary data, making it hard for challengers to compete. In addition, the compliance costs to meet the regulatory and prudential requirements are high and consumers face switching costs when leaving existing service providers.").

States to licensing requirements for services that are challenging traditional business models. The heterogeneity of these requirements, in turn, precludes the creation of a EU's thriving and globally competitive market for financial services, because innovative solutions developed in one Member State are not allowed to expand easily and freely in other markets. Against this fragmented background, the European Commission has stated its commitment to ensuring that any unjustified legal and practical barriers to setting up and scaling up fintech services across the Single Market be removed, whilst protecting consumers and monitoring the potential impact on financial stability. To this end, the European Commission has decided to investigate two initiatives: (i) giving fintech companies passporting rights to expand across borders and operate anywhere within the EU's single market; and (ii) granting "customized" licenses for fintech companies.

Commenting on recent fintech developments, European Commission Vice President Valdis Dombrovskis stated that "[i]f harnessed well, the new technologies have the potential to change for the better the financial industry, and the way people access financial services."[739] The impact of cross-border access to new financial and banking products and services on consumer was particularly in focus in his speech. He added that "[o]ur challenge is to make sure that Europe's financial sector can contribute to the digital revolution, while ensuring it remains safe and works for consumers. This is why Europe needs a coherent approach to fintech."[740] This approach is viewed as a necessary condition to foster innovation and competitiveness. These goals, in turn, can be achieved through the creation of a true technology-enabled Single Market, where consumers don't have to distinguish between domestic and foreign providers and firms can easily scale up and offer their services across the EU. As the European Commission Vice President Dombrovskis envisaged, in an integrated Single Market "from the comfort of their home, a Belgian consumer can easily open a savings account in a Dutch bank with a better interest rate; a Spanish consumer can get a loan from a company with the lowest fees, regardless of whether it's from a Latvian or a German lender, and so on." [741]

European Banking Authority (EBA). Alongside the European Commission, the European Banking Authority (EBA) has also intensified its scrutiny on fintech innovation. In spring 2017, the EBA launched the first EU-wide fintech mapping exercise in order to gain a better insight into the financial services offered and financial innovations applied by fintech companies in the EU, as well as their regulatory treatment. The EBA received responses from 22 Member States and 2 EEA States, providing estimates on the current number and expected growth of fintech companies established in their respective jurisdictions and detailed information on a sample of fintech companies.

Building on this fintech mapping exercise, existing EBA's work, and the work done by other intergovernmental and EU bodies related to fintech, the EBA published a discussion paper on August 4,

[739] See, Valdis Dombrovskis (European Commission Vice President), *Keynote Speech* at the Conference #FINTECHEU "Is EU Regulation Fit for New Financial Technologies?," (Brussels (BE), March 23, 2017).
[740] Ibidem.
[741] Ibidem.

2017 (EBA Fintech Discussion Paper).[742] In the EBA Fintech Discussion Paper, the EBA has identified proposals for future work in six areas: (i) authorization and sandboxing regimes; (ii) the impact on prudential and operational risks for credit institutions, electronic money institutions and payment institutions; (iii) the impact of fintech on the business models of these institutions; (iv) consumer protection and retail conduct of business issues; (v) the impact of fintech on the resolution of financial firms; and (vi) the impact of fintech on anti-money laundering and countering the financing of terrorism. For each of these six areas, the EBA has indicated a number of issues, summarizes the work that the EBA has done to address them up to date, identifies possible gaps and outlines the additional work that the EBA may consider pursuing.

The EBA has invited views from stakeholders on the scope of its proposed work. The consultation period will run until 6 November 2017. After the three-month consultation period, the EBA will assess the responses with a view to deciding what further steps to take during 2018.

7.B.iii The United States (U.S.) - Special Purpose National Bank Charter for Fintech Companies

While the UK holds a leading position as home of a large number of challenger banks, the United States are gaining ground with increased support from government, regulators, and industry.

At present the U.S. banking regulatory regime is highly decentralized, with multiple federal and state regulators. Within each state, there are typically separate licensing and chartering regimes for payment, money transmission, lending, and insurance, among others. In an effort to reduce regulatory complexities and optimize the use of the resources devoted to regulatory compliance, fintech companies entering the U.S. financial and banking services industry have often partnered with banks, which already have charters that authorize engaging in a range of financial and banking activities. However, over the last couple of years, the appetite of fintech companies for increased autonomy has grown significantly.

Against this scenario, the Office of the Comptroller of the Currency (OCC) - the primary regulator for all national banks and federal savings and loan associations - has been one the most proactive among U.S. regulators in addressing the concern of supporting innovation throughout the banking system and ensuring a right balance and coherence in regulating financial institutions.

The OCC first addressed the issue of fintech and related regulatory reform in August 2015, when the Comptroller of the Currency Thomas J. Curry announced that the OCC would begin an initiative to better understand innovation occurring in the financial services industry and to develop a framework aimed at supporting responsible innovation in the federal banking system.[743]

---

[742] See, European Banking Authority (EBA), *EBA publishes a Discussion Paper on Its Approach to FinTech*, European Banking Authority Press Release (August 4, 2017); European Banking Authority (EBA), *Discussion Paper on the EBA's Approach to Financial Technology (FinTech)*, EBA/DP/2017/02 (August 4, 2017).

[743] See, Thomas J. Curry (Then Comptroller of the Currency), *Remarks* Before the Federal Home Loan Bank of Chicago (Chicago (IL), August 7, 2015).

To gain a broad perspective, the OCC conducted extensive researches and held several discussions with banks, community and consumer groups, fintech companies, academics, and other regulators. This work led to the publication by the OCC of a white paper in March 2016 (OCC March 2016 White Paper).[744] In the OCC March 2016 White Paper, the OCC provided its perspective on responsible innovation in the financial services industry,[745] outlined principles guiding its approach to financial innovation,[746] and solicited feedback on 9 questions and other topics discussed therein. In response, the OCC received 63 comments from a broad cross section of stakeholders, including some comments suggesting that the OCC should consider issuing federal charters to fintech companies.[747]

Charter discussions continued at the OCC's fintech forum on responsible innovation in June 2016, which saw the participation of representatives from the banking industry, fintech companies, academia, and community and consumer groups.[748]

In June 2016, the OCC also launched the Innovation Framework Development Team, a dedicated team to develop recommendations for implementing a framework for responsible innovation.[749] The Innovation Framework Development Team combined the eight guiding principles set forth in the OCC March 2016 White Paper into five objectives covering outreach, awareness and education, timely and transparent processes, interagency communication, and organizational structure. It conducted extensive information gathering and analysis, including: interviews with key internal stakeholders; a detailed analysis of the comments received on the OCC March 2016 White Paper; a review of the research completed previously; and a careful analysis of the feedback from ongoing meetings with external stakeholders and from the OCC Forum on Responsible Innovation held in June 2016.[750]

The Innovation Framework Development Team, then, incorporated the information gathered into an assessment of relevant existing programs and processes, which ultimately led to the development of a

---

[744] See, Office of the Comptroller of the Currency (OCC), *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*, Office of the Comptroller of the Currency White Paper (March 2016). See, also, Thomas J. Curry (Then Comptroller of the Currency), *Remarks* Before the Harvard Kennedy School's New Directions in Regulation Seminar (Cambridge (MA), March 31, 2016); Thomas J. Curry (Then Comptroller of the Currency), *Remarks* Before the American Banker Retail Banking Conference (Las Vegas (NV), April 7, 2016).

[745] See, Office of the Comptroller of the Currency (OCC), *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*, cit., p. 5. (The OCC's white paper defines "responsible innovation" to mean "[t]he use of new or improved financial products, services, and processes to meet the evolving needs of consumers, businesses, and communities in a manner consistent with sound risk management and aligned with the bank's overall business strategy.").

[746] Id., pp. 5-10. The OCC's white paper identifies the following guiding principles: support responsible innovation; foster an internal culture receptive to responsible innovation; leverage agency experience and expertise; encourage responsible innovation that provides fair access to financial services and fair treatment of consumers; further safe and sound operations through effective risk management; encourage banks of all sizes to integrate responsible innovation into their strategic planning; promote ongoing dialogue through formal outreach; and collaborate with other regulators.

[747] Comments on the OCC's white paper are accessible on the OCC's website at https://www.occ.gov/topics/responsible-innovation/innovation-comments.html.

[748] See, Office of the Comptroller of the Currency (OCC), *OCC Forum on Responsible Innovation in the Federal Banking System – Videos of the Forum*, Office of the Comptroller of the Currency (June 23, 2016).

[749] The Innovation Framework Development Team includes representatives from Midsize and Community Bank Supervision, Large Bank Supervision, the Office of the Chief National Bank Examiner, the Chief Counsel's Office, and Compliance and Community Affairs.

[750] See, Thomas J. Curry (Then Comptroller of the Currency), *Remarks* Before the Marketplace Lending Policy Summit 2016 (Washington (DC), September 13, 2016).

comprehensive set of recommendations that the Comptroller of the Currency and Executive Committee accepted in early October 2016.

On 26 October 2016, the OCC announced the decisions to: (1) establish an Office of Innovation, headed by a chief innovation officer, and regional innovation offices in New York, San Francisco, and Washington DC to facilitate industry outreach efforts; and (2) implement a framework supporting responsible innovation.[751] Since its establishment, the OCC's Office of Innovation has served as the OCC's main contact and clearinghouse for requests and information related to innovation. Its staff conducts outreach to a variety of financial services stakeholders and provides technical assistance and other resources for banks and nonbanks on the OCC's expectations and guiding principles regarding responsible innovation. The OCC's Office of Innovation also promotes awareness of industry developments and training among OCC staff, monitors the evolving financial services landscape, and leads the OCC's collaboration with domestic and international regulators.[752]

On 2 December 2016, the Comptroller of the Currency Thomas J. Curry announced that fintech companies may qualify for Special Purpose National Bank (SPNB) charters under certain circumstances.[753] Accompanying his decision, the OCC published a paper discussing issues related to chartering special purpose national banks and solicited public comment to help inform its path forward (SPNB Paper).[754] In the SPNB Paper, the OCC: discussed its legal authority to grant a national bank charter to companies with limited purposes;[755] articulated the requirements for obtaining a charter;[756] and examined the chartering process.[757] Significantly, in the SPNB Paper the OCC indicated that, if a national charter were to be granted to a particular fintech company, the OCC would hold that institution to the same high standards of safety and soundness, fair access, and fair treatment of customers that all federally chartered institutions must meet.[758]

[751] See, Office of the Comptroller of the Currency (OCC), *OCC Issues Responsible Innovation Framework*, Office of the Comptroller of the Currency Press Release (Washington (DC), October 26, 2016); Office of the Comptroller of the Currency (OCC), *Recommendations and Decisions for Implementing a Responsible Innovation Framework*, Office of the Comptroller of the Currency White Paper (October 2016).
[752] See, Office of the Comptroller of the Currency (OCC), *Recommendations and Decisions for Implementing a Responsible Innovation Framework*, cit., pp. 4-6. See, also, Thomas J. Curry (Then Comptroller of the Currency), *Remarks* Before Chatham House 'City Series' Conference "The Banking Revolution: Innovation, Regulation & Consumer Choice" (London (UK), November 3, 2016).
[753] See, Thomas J. Curry (Then Comptroller of the Currency), *Remarks* Regarding Special Purpose National Bank Charters for Fintech Companies Georgetown University Law Center (Washington (DC), December 2, 2016).
[754] See, Office of the Comptroller of the Currency (OCC), *OCC To Consider Fintech Charter Applications, Seeks Comment*, Office of the Comptroller of the Currency Press Release (Washington (DC), December 2, 2016); Office of the Comptroller of the Currency (OCC), *Exploring Special Purpose National Bank Charters for Fintech Companies*, Office of the Comptroller of the Currency White Paper (December 2016).
[755] See, Office of the Comptroller of the Currency (OCC), *Exploring Special Purpose National Bank Charters for Fintech Companies*, cit., pp. 3-4.
[756] Id., pp. 4-12.
[757] Id., pp. 13-16.
[758] Id., pp. 1, 8.

The OCC carefully considered the comments received on its SPNB Paper.[759] In March 2017, it published a summary of comments and explanatory statement, in which it addressed key issues raised by commenters in response to its SPNB Paper.[760]

In the summary of comments and explanatory statement, the OCC also discussed its decision to issue for public comment a draft supplement to the Comptroller's Licensing Manual. The draft supplement (the draft Supplement) was issued in March 2017, providing guidance to any fintech company that may wish to file a charter application.[761] In the draft Supplement, the OCC explained how it would apply the licensing standards and requirements in existing regulations and policies to fintech companies applying for SPNB charters. It also described unique factors that it would consider in evaluating applications from fintech companies; expectations for promoting fair access, fair treatment, and financial inclusion; and its approach to supervising those fintech companies that become national banks. The OCC accepted comments on the draft Supplement until 14 April 2017.[762]

Significantly, in the SPNB Paper, in the response to comments on that paper, and again in the draft Supplement, the OCC has made clear that in evaluating applications from fintech companies for a SPNB charter, the OCC would be guided by the following key threshold principles: (1) the OCC will not allow the inappropriate commingling of banking and commerce; (2) the OCC will not allow products with predatory features nor will it allow unfair or deceptive acts or practices; and (3) there will be no "light-touch" supervision of companies that have an SPNB charter. Any fintech companies granted such charters will be held to the same high standards that all federally chartered banks must meet.[763]

Aligned with these principles, the OCC has expressed its belief that making SPNB charters available to qualified fintech companies would be in the public interest.[764]

---

[759] The OCC received more than 100 comment letters on the SPNB Paper. Comments on the SPNB Paper are accessible on the OCC's website at https://www.occ.gov/topics/responsible-innovation/fintech-charter-comments.html. See, also, Thomas J. Curry (Then Comptroller of the Currency), *Remarks* at LendIt USA 2017 (New York (NY), March 6, 2017); Lalita Clozel, *Fintech Charter Q&A: OCC Answers Skeptics*, American Banker (January 3, 2017).

[760] See, Office of the Comptroller of the Currency (OCC), *OCC Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies*, Office of the Comptroller of the Currency Paper (March 2017).

[761] See, Office of the Comptroller of the Currency (OCC), *OCC Issues Draft Licensing Manual Supplement for Evaluating Charter Applications From Financial Technology Companies, Will Accept Comments Through April 14*, Office of the Comptroller of the Currency Press Release (Washington (DC), March 15, 2017); Office of the Comptroller of the Currency (OCC), *Evaluating Charter Applications From Financial Technology Companies*, *Office of the Comptroller of the Currency's Licensing Manual Draft Supplemental*, Office of the Comptroller of the Currency (March 2017).

[762] Comments on the draft Supplement are accessible on the OCC's website at https://www.occ.gov/topics/responsible-innovation/public-comments-on-comptroller-licensing-manual-draft-supplement.html.

[763] See, Office of the Comptroller of the Currency (OCC), *OCC Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies*, cit., pp. 2-3.

[764] See, Office of the Comptroller of the Currency (OCC), *Evaluating Charter Applications From Financial Technology Companies*, cit., p. 1 (explaining that "[t]he OCC has reached this decision for a number of reasons. First, … an SPNB charter provides a framework of uniform standards and supervision for companies that qualify. Applying this framework to fintech companies will help ensure that these companies, like other banks that operate under federal charters, conduct business in a safe and sound manner while effectively serving the needs of consumers, businesses, and communities. Second, an SPNB charter supports the dual banking system by providing fintech companies the option of offering banking products and services under a federal charter and operating under federal law, while ensuring essential consumer protections. This is the same choice available to companies that deliver banking products and services in traditional ways. Third, providing a path for fintech companies to become national banks can make the financial system stronger by promoting growth, modernization, and competition. Moreover, the OCC's supervision of fintech companies will deepen the expertise the OCC already has acquired in emerging technologies for banking services … This enhanced "window" into developing technologies and financial innovations positions the OCC to better evaluate and respond to the risks that

Following the issuance of the draft Supplement, the Office of Innovation held office hours for national banks, federal savings associations, and fintech companies interested in discussing the OCC's perspective on responsible innovation at the OCC's San Francisco Field Office, on May 16 and 17, 2017,[765] and at the OCC's District Office in New York, on July 26 and 27, 2017.[766]

In a July 2017 speech, Acting Comptroller of the Currency Keith A. Noreika noted with enthusiasm that "[i]n May, the team's first office hours in San Francisco were "sold out," … The office has already become a valuable resource for national banks and thrifts, and its utility will only increase over time."[767] He, then, re-affirmed the OCC's commitment to support innovation within the federal banking system and stated that he "will champion the value of the national charter and the federal banking system."[768] Acting Comptroller of the Currency Noreika further expressed the belief that "the nation's banking needs are best served by a robust, vibrant dual banking system. That requires a strong federal banking system as well as a diverse system of state banks."[769] Because of this, he explained that he will "seek opportunities to amend regulations and recommend changes to legislation to promote the health and vitality of the federal banking system."[770] Then, he expressed the belief that "[w]e all need the federal banking system to be more inclusive, to accommodate new banks, and to adapt to the changing needs of the marketplace, customers, and communities. We have all complained too long about the dearth of de novo institutions as we have watched the industry consolidate. Now, we need to remove unnecessary barriers to becoming banks."[771]

In his remarks, Acting Comptroller of the Currency Noreika also said that the OCC would "vigorously" defend itself in the lawsuits challenging the proposed SPNB charter brought by the Conference of State Bank Supervisors (CSBS)[772] and the New York Department of Financial Services.[773] However, he was very careful in clarifying that "at this point, the OCC has not determined whether it will actually accept or act upon applications from nondepository fintech companies for special purpose national bank charters that rely on this regulation."[774] He further stated that "to be clear, we have not received, nor are we evaluating, any such applications from nondepository fintech companies. The OCC will continue to hold discussions with interested companies while we evaluate our options."[775]

---

accompany the delivery of those technologies. Finally, … the chartering process will enable the OCC to encourage fintech companies to use innovative ways to promote financial inclusion.").

[765] See, Office of the Comptroller of the Currency (OCC), *OCC Announces One-on-One Industry Meetings as Part of Office of Innovation Office Hours*, Office of the Comptroller of the Currency Press Release (Washington (DC), April 13, 2017).

[766] See, Office of the Comptroller of the Currency (OCC), *OCC to Hold Innovation Office Hours in New York*, Office of the Comptroller of the Currency Press Release (Washington (DC), June 19, 2017).

[767] See, Keith A. Noreika (Acting Comptroller of the Currency), *Remarks* before the Exchequer Club (Washington (DC), July 19, 2017).

[768] Ibidem.

[769] Ibidem.

[770] Ibidem.

[771] Ibidem.

[772] See, Conference of State Bank Supervisors (CSBS) v. Office of the Comptroller of the Currency and Thomas J. Curry in his official capacity as Comptroller of the Currency, Complaint for Declaratory and Injunctive Relief, Civil Action No. 1:17-CV-00763 (JEB) (April 26, 2017).

[773] See, Maria T. Vullo, in her official capacity as Superintendent of the New York State Department of Financial Services, v. Office of the Comptroller of the Currency and Keith A. Noreika, in his official capacity as Acting Comptroller of the Currency, Complaint for Declaratory and Injunctive Relief, Civil Action No. 1:17-CV-03574 (NRB) (May 12, 2017).

[774] See, Keith A. Noreika (Acting Comptroller of the Currency), Remarks before the Exchequer Club cit., p. 9.

[775] Ibidem.

A few days after the above remarks, the OCC filed a motion to dismiss the CSBS action, arguing that the complaint failed to present either a justiciable case or controversy or a reviewable final agency action, and that the group lacks standing because the OCC has yet to take any relevant action that could have a concrete effect on CSBS or its members.[776]

7.C. Digital-Only (Digitally-Focused) Challenger Banks

Among the categories of challenger banks mentioned above, digital-only (digitally-focused) challenger banks have been attracting significant attention from market participants, consumers, and regulators. The past 12 months have seen a steady stream of digitally-only (digitally-focused) challenger banks entering the market and a growing queue are planning their debuts for 2018.

This section provides a brief overview of leading digital-only (digitally-focused) challenger banks in the UK, EU, and the United States; it, then, discusses common features of leading digital-only (digitally-focused) challenger banks; and it examines a number of challenges that going forward they will need to address in order to successfully deliver on their growth strategies.

7.C.i. Notable Examples

Below are a few notable examples of digital-only (digitally-focused) challenger banks.

The United Kingdom

- *Monzo* (formerly Mondo)[777] is a UK-based, mobile-only challenger bank. Founded in 2015, Monzo was granted an unrestricted banking license in April 2017. The company offers a pre-paid Mastercard connected to a money-tracking app and has recently begun to roll out current accounts to existing users. Monzo provides 24/7 customer support and has launched innovative features, including real-time spending notifications, intelligent spending reports, and budgeting tools. Monzo charges no fees (even when traveling abroad) and pushes to be as open and transparent as it possibly can. Monzo has demonstrated a strong commitment to financial education and customer empowerment;[778] and, over time, it has built a dynamic community of users, which it actively engages in the innovation process (e.g., through blogs, social networks, community forums).

Monzo supports the Open Banking movement through a number of initiatives. For example, it has released a prototype API and actively supports a rapidly growing community of developers working on the platform through hackathons and community forums. In addition, it partners with leading fintech companies and

[776] The OCC filed its motion to dismiss on July 28, 2017. However thereafter, a federal judge ordered that the OCC's motion to dismiss be stricken based on excessive footnoting. On August 2, the OCC filed a renewed motion to dismiss. See, Conference of State Bank Supervisors (CSBS) v. Office of the Comptroller of the Currency and Keith A. Noreika, in his official capacity as Acting Comptroller of the Currency, Defendants' Motion to Dismiss for Lack of Jurisdiction and Failure to State a Claim, Civil Action No. 1:17-CV-00763 (JEB) (August 2, 2017); Conference of State Bank Supervisors (CSBS) v. Office of the Comptroller of the Currency and Keith A. Noreika, in his official capacity as Acting Comptroller of the Currency, Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss for Lack of Jurisdiction and Failure to State a Claim, Civil Action No. 1:17-CV-00763 (JEB) (August 2, 2017).

[777] For more information, visit Monzo's website at https://monzo.com.

[778] See, Monzo, *The Class of 2017: Launching Monzo University*, Monzo Blog (July 13, 2017).

technology companies to deliver innovative financial services and products. Tom Blomfield, CEO and Co-Founder at Monzo, wrote in an early blog post, "[t]he bank of the future will be a marketplace … This is why [Monzo] has a singular focus – to build the best current account in the world – rather than selling dozens of different financial products. We can focus on what we know best, whilst offering our customers access to the best products and services from across the market."[779]

To date, Monzo has raised financing from leading VC investors - including Passion Capital, Thrive, and Orange Digital Ventures - and Crowdcube investors.[780]

- *Atom Bank*[781] is a UK-based, digital-only challenger bank. It was the first of the big four UK digital-only bank challengers (Starling Bank, Monzo, Atom Bank, and Tandem Money) to launch, having received a restricted UK banking license in 2015.[782] The company now holds a full banking license and currently offers fixed savers and digital mortgage services, with current accounts expected to launch in 2018. Atom Bank uses biometric authentication to verify user identities in the bank app and provides 24/7 customer service. To date, the company has raised c. $268.14M in capital and counts among its notable investors BBVA, Woodford Investment Management, and Toscafund Asset Management.

- *Starling Bank*[783] is a UK-based, digital-only challenger bank, founded by former Allied Irish Bank COO Anne Boden. The company is a full-service standalone bank, having received a UK banking license in July 2016. Starling Bank was built from the ground up and it started accepting beta customers to open current accounts through its app in March 2017. In addition to instant account opening, Starling Bank also offers real-time account activity updates, biometric authentication, and 24/7 customer support.

Starling is committed to the Open Banking movement and gives its customers access to a mobile market of services and products that best fit their financial needs. As Anne Boden, Founder and CEO at Starling Bank, explained, Starling's aim "is to make sure consumers buy the best products for their needs." They "believe financial services is an ecosystem" and they seek to position themselves "at the heart of people's financial lives."[784] To that end, in April 2017, Starling Bank held a hackathon to launch the Starling Developer Platform. Starling Bank's Open Banking platform enables the company to seamlessly integrate with other financial services to provide a fair, transparent, and innovative banking experience for consumers. In this regard, the company has partnered with: TransferWise, to enable its customers to make cheap, easy international money transfers; Moneybox, to enable its customers to round up their purchases to the nearest pound and invest the change in companies such as Netflix, Unilever and Disney; and Tail, to give its account holders cash-back offers from retailers without the fuss of loyalty cards or codes.

---

[779] See, Tom Blomfield, *The Bank of the Future Will Be a Marketplace*, Monzo Blog (February 4, 2016).
[780] In March 2016, Monzo raised £1m in 96 seconds, making this the fastest crowdfunding raise in history at more than £10,000/second. See, Monzo, *Fastest Crowdfunding Ever: £1M in 96 Seconds*, Monzo Blog (March 3, 2016). In February 2017, Monzo surpassed its new crowdfunding round target raise of £2.5 million within four hours of opening for pre-registration. See, Monzo, *£12 Million Later: Our Crowdfunding Pre-Registration is Closed*, Monzo Blog (March 14, 2017).
[781] For more information, visit Atom Bank's website at https://www.atombank.co.uk.
[782] See, Mary Wisniewski, *Mobile-First Bank Gets U.K. Charter — Could It Happen Here?*, American Banker (July 7, 2015) (quoting Jonathan Davis, FIS' EMEA Managing Director discussing the drivers and mutual benefits of FIS's partnership with Atom Bank).
[783] For more information, visit Starling Bank's website at https://www.starlingbank.com.
[784] See, KPMG, *A New Landscape. Challenger Banking Annual Results*, cit., p.19]

While building its own marketplace, Starling Bank has been expanding its operations to Europe, receiving its banking passport into Ireland in June 2017. Starling has raised c. £70m to date, led by angel investor Harald McPike.

- *Tandem Money* (formerly, Tandem Bank)[785] is a UK-based, digital-only challenger bank. Tandem received FCA and PRA accreditation in November 2015, but received a setback in March 2017 when its banking license was suspended after investor House of Fraser pulled out of supplying a proposed £29 million of funding over concerns about whether China's State Administration of Foreign Exchange would approve the transaction. This, in turn, led Tandem to delay the launch of its savings accounts, although the company is still going forward with the launch of its credit card product.

At present, Tandem focuses on proactive approach to money management by: helping customers with budgeting; providing customers with notifications when their bills increase or a payment comes in; and helping customers reduce their bills by finding better deals to save them money.

To date Tandem has raised c. $77.8M from a number of investors, including e.ventures and Route 66 Ventures.

- *Monese*[786] is a UK-based digital-only challenger bank with a unique purpose. Founded in 2013 by Estonian serial entrepreneur Norris Koppel, Monese is dedicated to helping immigrants and expats, who might otherwise find it difficult to open a bank account outside of their home country and access core banking services. The company provides an instant mobile current account, low-cost international money transfers, a debit card, budgeting tools, and most recently a direct debit functionality.

Unlike other challengers operating as full-service banks, Monese has not a banking license; instead the company is registered as an electronic money institution under the Financial Conduct Authority (FCA)'s Electronic Money Regulations. In June 2017, Monese announced its expansion into 19 countries across Europe, allowing users to open local accounts even if they are not currently residing in that country.

To date, Monese has raised $16M from various investors, including Seedcamp, Korea Investment Partners, and Anthemis Exponential Ventures.

Europe

- *N26*[787] is a Berlin-based, mobile-only challenger bank with an ambition plan to become a mobile-only European borderless bank. Founded in 2013 (as Number26), the company received its banking license in 2016. Since then, N26 has evolved to become a fully-licensed bank operating across 17 markets in Europe.

N26 offers two types of customer accounts: a free standard N26 account; and N26 Black account, a higher-tier account that costs Euro 5.90 per month. Both accounts come with a Mastercard, but the N26 Black

[785] For more information, visit Tandem Money's website at https://www.tandem.co.uk.
[786] For more information, visit Monese's website at https://www.monese.com.
[787] For more information, visit N26's website at https://n26.com.

account gives customers additional perks, such as insurance coverage for trips abroad, mobile phone theft coverage, extended warranty of up to one additional year for qualified purchases, and fee-free foreign currency ATM withdrawals. N26 customers can monitor and control all account and card functions through the N26 mobile app, including ordering a new card, blocking or unblocking a card, changing a PIN, applying for an instant overdraft, setting purchase and withdrawal limits, or instantly transfering money to other N26 customers. In addition, Monese offers investment tools, real-time personalized updates, automatically categorized spending reports, and customizable notifications, as well as instant MoneyBeam transfers (a Venmo-like instant money transfer service).

Like Starling Bank and Monzo, N26 works with industry-leading fintech partners to bring innovative financial and banking services and features to its customers, including foreign currency transfers at competitive rates through a partnership with TransferWise.

The company has raised c. $52.73M from renowned VC investors, including Battery Ventures, Horizons Ventures, and Valar Ventures.

- *SolarisBank*[788] is a Berlin-based, digital-only and fully-licensed bank. Founded in 2016, SolarisBank leverages a banking as a platform approach to offer modular API-powered banking platforms, which enable digital partners to build and deliver state-of-the-art financial products and services. The company's three platform services - Escrow and E-money, Rapid Credit, and Digital Banking Engine - provide easy-to-integrate, scalable, and customizable solutions to most regulatory and technical challenges across industries. Thus, by acting as both a regulatory banking entity and technology firm, SolarisBank empowers its partners to create innovative financial solutions and allows them to focus on their core business.[789] Some of the company's partners include, Fashioncheque, Cringle, Hufsy, Savedo, and AutoScout24.

To date, SolarisBank has raised $41.65M from a number of investors, including FinLeap, SoftBank, and UniCredit Group.

- *Fidor Bank*[790] is a Munich-based digital-only bank. Founded in Germany in 2009, Fidor Bank is often referred to as the "world's oldest fintech bank." The company was acquired by France's Groupe BPCE in July 2016, and, since then, it has continued to operate under its own branding.

Fidor Bank's current portfolio of products in Germany covers retail and business banking, ranging from basic bank accounts and savings bonds, to various lending offers. In 2015 Fidor Bank launched in the UK, where it offers a current account called the "Smart Current Account," a Mastercard debit card, and savings bonds.[791]

---

[788] For more information, visit SolarisBank's website at https://www.solarisbank.de.
[789] See, Bryan Yurcan, *"Banking as a Service" for Fintechs Seeking Scale*, American Banker (March 21, 2016).
[790] For more information, visit Fidor Bank's website at https://www.fidor.com and https://www.fidorbank.uk.
[791] See, Oscar Williams-Grut, *A New Challenger Bank Built Like an App Store Just Launched in the UK* — We Spoke to the CEO, Business Insider (September 17, 2015); Emily Reynolds, *Inside Fidor, the Fintech Bank Run by its Customers*, Wired (June 23, 2016).

- *Klarna*[792] is a Swedish fintech company, which was granted a full banking license in Sweden in June 2017.[793] Different from the digital-only challenger banks discussed above, Klarna was founded in Sweden 2005 with the goal to make online payments safe, simple, and smooth. Over time the company has evolved and broaden its offering to become one of today's Europe's largest banks, with 60 million consumers across 70.000 merchants and working seamlessly across borders. When the company acquired SOFORT in 2014, the Klarna Group was formed.

Klarna is backed by leading VC investors such as Sequoia Capital, Bestseller, Atomico and General Atlantic.

The United States

- *Simple*[794] is an American mobile-only challenger bank based in Portland, Oregon. Founded in 2009 (as BankSimple), in 2012 the company launched as a limited beta and in 2014 it was acquired by BBVA for $117 million.[795]

Simple is not a fully licensed, standalone bank; rather it provides customers FDIC insured checking accounts through its banking partners, Bancorp and BBVA Compass. Simple also provides sleek and intuitive online and mobile app interfaces and a Simple Visa Card issued by its partner banks. Simple's costumers can make purchases both in stores and online, deposit checks using their smartphone, set up direct deposit, earn interest via Simple's partner banks, pay bills, transfer money, and withdraw cash from ATMs. In addition, Simple offers a rich set of expense tracking, financial planning, and budgeting tools, a well as a shared accounts feature that allows any two people easily manage their finances together.

- *BankMobile*[796] is a US-based, digital-only challenger bank. Founded in 2015 under parent company Customers Bank, BankMobile was acquired by Flagship Community Bank in March 2017. It targets specific customer segments, such as millennials, the underbanked, and middle-income households.

BankMobile offers a number of financial products and services, including: checking and savings accounts without any fees, lines of credit, joint accounts, access to over 55,000 surcharge-free ATMs, and a higher savings rate than the top 4 banks in the country, a personal banker for all customers, and a free financial advisor for VIP customers.[797]

- *Chime*[798] is a US-based, digital-only challenger bank. Founded in 2013, the company aims to be "the bank account that has your back". Chime is not a full-fledged bank; rather it has partnered with Bancorp to provide accounts and card services.

[792] For more information, visit Klarna's website at https://www.klarna.com.
[793] See, Klarna, *Global: Klarna - Europe's Newest Bank is Born*, Klarna Press Release (June 19, 2017).
[794] For more information, visit Simple's website at https://www.simple.com.
[795] See, Penny Crosman, *BBVA's Simple Purchase Reflects Mobile Banking's Sizzle*, American Banker (February 21, 2014).
[796] For more information, visit BankMobile's website at https://www.bankmobile.com.
[797] See, Mary Wisniewski, *BankMobile Aims to Become the Uber of Banking*, American Banker (January 20, 2015).
[798] For more information, visit Chime's website at https://www.chimebank.com.

Chime gives customers a Visa debit card, a spending account, and a savings account with an automatic savings feature that rounds up every transaction to the nearest dollar and transfers the extra change to savings. Chime requires no minimum balance to open an account and charges no monthly, overdraft, or foreign transaction fees. In addition, ATMs are fee-free at over 24,000 MoneyPass locations and Chime's customers can locate 30,000 fee-free cash back locations using the ATM Finder in the Chime app. The Chime app also sends customers daily balance updates, instant transaction alerts, and real-time deposit notifications.

To date, the company has raised $24.53M from a number of leading VC investors, including Forerunner Ventures, Aspect Ventures, and Crosslink Capital.

- *Moven*[799] is a US-based, digital-only challenger bank. Founded in 2011, Moven is not a full-service, standalone bank.[800] Instead, it provides digital banking services in partnership with the following established financial institutions: CBW Bank of Kansas; Westpac in New Zeland;[801] and TD bank in Canada.[802]

In particular, Moven provides a digital FDIC-insured bank account, with no monthly fees or minimum balances. The account is paired with an innovative mobile banking app, money management and spending visualization tools, and seamless peer-to-peer payments features. In addition, Moven leverages a network of over 42,000 ATMs, where Moven's customers can withdraw cash without any fees. Similar to other digital-only challenger banks discussed above, Moven has also teamed up with leading fintech companies to provide innovative financial service and products. For instance, it entered into partnerships with marketplace lender CommonBond and credit card consolidator Payoff.[803]

---

[799] For more information, visit Moven's website at https://moven.com.

[800] A Moven blog post from 2012 spelled out why Moven didn't want a license. See, Moven, *When Is a Bank Not a Bank?*, Moven Blog Post (November 20, 2012) (explaining that "[w]e don't have a charter because it gets incredibly complicated and expensive, which is the reason hardly any new banks have launched globally in the last few decades … In the last three decades, very few new banks have launched globally because the barriers to entry are extremely high: you have to start with lots of capital to comply with regulations; you have to have even more upfront money to get FDIC insurance licenses; you then need to jump through another bunch of hoops to get approval to start up; and once you get going, you have to heap another layer of cost into the process to ensure compliance with all the regulatory controls … You only need a charter if you are going to keep deposits which we will not, to start off with. That part may come later, but to begin with we just want to make it easy to save, spend and live smarter. That means making it easy to move your money in a good way, like Starbucks do with their Starbucks Card, like Dwolla and Venmo do for moving cash around, like PayPal and the mobile network operators do when they take deposits in the form of pre-paid telephone contracts, like the NYC Metro system and others do. …[B]y not having a charter, Movenbank will be a better banking experience for our customers. Not owning a bank charter – like the 7,000 other "banks" in the United States – means we will not think or act like a bank. 99% of these banks think that banking is all about fees, charges, overdrafts, interest rates, branches, signature cards and checkbooks. We think it is about making it simpler to save, spend and live smarter. That is why we've outsourced our bank charter to some great partners who really get this stuff, and then we've built something truly different on top of that. So you get the protection of a licensed, FDIC insured bank partner, and you get a revolutionary re-think of the way banking should work.").

[801] See, Penny Crosman, *Digitally Minded Bank Goes All-In on Responsive Design, Moven*, American Banker (February 11, 2015) (quoting Simon Pomeroy, Westpac Chief Digital Officer, explaining the drivers behind the decision of Westpac to collaborate with Movem, including creation of a consistent banking experience across any device and consolidation of digital teams and capacities"); Evan Nemeroff, *Moven Expands Globally, Forming Partnership with Westpac New Zealand*, American Banker (August 25, 2014).

[802] See, TD Bank Group, *TD and Moven Announce Exclusive Canadian Agreement*, TD Bank Group Press Release (December 2, 2014). See, also, Bryan Yurcan, *TD and Moven Extend Partnership to U.S.*, American Banker (March 28, 2017).

[803] See, Mary Wisniewski, *Fintechs Team Up to Become More Banklike*, American Banker (January 27, 2016); Finextra, *Moven Teams up with Loan Refinancers CommonBond and Payoff*, Finextra (January 28, 2016).

7.C.ii. Common Features

Although digital-only (digitally-focused) challenger banks have each a different model or approach, they all share some common features in addition to being mobile-only. Among these common features are the following:

- Technology – Different from incumbents, digital-only (digitally-focused) challenger banks are not burned by high costs of maintaining legacy IT systems vast in scale and complexity. In fact, they typically have innovative, flexible, state of the art technology platforms, which offer differentiating functionality in a personalized, user-friendly, and flexible way. Such technology platforms are either developed in-house or using best-of-breed applications and software from well-established banking system services providers and vendors. They are designed to be agile and scalable, so that the challenger banks can grow their activities rapidly and efficiently. They are also generally built in a modular way, which facilitates readily integration of functionality and data from other sources. This, in turn, helps challenger banks increase their relevance in open API-driven ecosystems and better position themselves to lead in the era of Open Banking.[804]

- Team - Digital-only (digitally-focused) challenger banks have been able to attract (and are increasingly attracting) highly skilled employees, experts, and consultants. The majority of them have still a small size team, with between 100 to 200 employees. Their employees work closely together and efficiently coordinate across functions to actively re-imagine how banking could be transformed and then execute on the plan.

- Offerings – Digital-only (digitally-focused) challenger banks now offer the opportunity to: open a bank account in a few second just using a mobile phone; send money and split bills with a single swipe; make and receive instant payments; use a card abroad without the need to place a travel notification and without being charged any fees; receive exceptional customer support in matter of seconds; and much more. They use advanced technologies - including AI, machine learning, biometrics, and distributed ledgers - to streamline customer onboarding and reduce frictions through the customer's journey, while at the same time ensuring security and full compliance with all applicable legislative and regulatory requirements.

Moreover, digital-only (digitally-focused) challenger banks push personalization as a key differentiator and offer highly personalized services and bespoke products. They tend to include social interactions at the core of their functionalities, while also growing the use of visual content and developing new technologies to create a rich and dynamic visual experience. Their services are typically available both on IOS and Android, so that almost anyone can use them.

In addition to the foregoing, digital-only (digitally-focused) challenger banks tend to employ a variety of technologies to analyze, process, and contextualize customer data and insights, including customers' transaction and spending history, channel preferences, and geo-locational information. They, then, leverage

[804] See, KPMG, *A New Landscape. Challenger Banking Annual Results*, cit., pp. 16-17; Burnmark, *Challenger Banking*, cit., p.16; PWC, *Who Are You Calling a 'Challenger'? How Competition is Improving Customer Choice and Driving Innovation In the UK Banking Market*, cit., p. 10, 28-29.

the insights and data to provide real-time recommendations to their customers, which can help them improve their ability to save money and budgeting, increase financial knowledge, and achieve specific financial goals. By evolving their interaction with customers through the use of advance data analytics technologies, digital-only (digitally-focused) challenger banks have the opportunity to improve customer experience, encourage customer loyalty, and drive profitability.

- Inclusion - Digital-only (digitally-focused) challenger banks tend to be more inclusive than incumbent banks, both in term of the services that they offer and the technology that they utilize. By leveraging their open API-driven technologies, they are developing a better understanding of unbanked and underbanked consumers and are offering really targeted propositions for underserved segments.

- Marketplace/Platform Strategies – An increasing number of digital-only (digitally-focused) challenger banks are deploying marketplace and platform strategies discussed in the prior chapter. They are now trying to pull together the offerings of non-financial and financial services and products from a growing variety of players and, then, organize them through their own marketplace / platform in a way that is coherent, efficient, and cohesive. As a result, customers of digital-only (digitally-focused) challenger banks can access multiple standalone non-financial and financial services and products, all integrated with their account, data and functionality; and they can stay easily updated on the latest technology and market trends. Significantly, as digital-only (digitally-focused) challenger banks build their own marketplace / platform, they seek to establish themselves at the center of an intelligent and connected ecosystem and to deliver a unified, personalized, seamless, flexible, and synchronized customer experience across all services and products offered throughout their marketplace / platform.

As previously discussed, two elements are critical to the success of a marketplace strategy and a platform strategy: (1) well-defined APIs, to facilitate richness and ease of integration with third parties' services and products; and (2) access to customer data and insights that can be processed and contextualized to drive analytics and provide competitive predictive services. Different from incumbents, most digital-only (digitally-focused) challenger banks are building their propositions exactly around these two elements. As a result, they are uniquely positioned to become a customer's preferred digital point of entry into financial and non-financial services and products and, ultimately, a trusted and pivotal part of their customers' daily lives.

- API and Co-Innovation Process - Digital-only (digitally-focused) challenger banks tend to adopt an "openness-based approach" to their activities, which is radically different from the way incumbents typically operate. In particular, unlike traditional banks, digital-only (digitally-focused) challenger banks shift the center of gravity from the core to their API layer. This is important because it: (1) gives digital-only (digitally-focused) challenger banks the agility and flexibility necessary to expand their offerings through inter- and cross-industry strategic partnerships and to constantly evolve their technology; (2) helps digital-only (digitally-focused) challenger banks bolsters their reach; and (3) opens up new sources of revenue for digital-only (digitally-focused) challengers and third-party providers that work with them.

Moreover, by opening up to their ecosystem, digital-only (digitally-focused) challengers revolutionize the innovation process: as they work closely with their developer community and strategic partners, digital-only (digitally-focused) challengers co-create with them. Because of this, the ability of digital-only (digitally-focused) challenger banks to attract, integrate, and establish an ongoing and constructive dialogue with their developer community and strategic partners is critical.

Digital-only (digitally-focused) challengers extend their "openness-based approach" to customers, as well. They tend to orient themselves around their customers and constantly innovate with focus on their customers' needs and goals. Their early adopters are typically tech-savvy customers, who want flexibility, simplicity, transparency and useful services.[805] As they scale their operations and grow their customer base, digital-only (digitally-focused) challenger banks search new ways to improve customer experience, support and engagement.

Furthermore, digital-only (digitally-focused) challenger banks tend to involve their customers across the various stages of the innovation process. Their online communities are extremely important as digital-only (digitally-focused) challenger banks leverage them to gather new ideas, collect comments and feedback from their customers and share their plans. By building active, well-engaged and transparent online communities, digital-only (digitally-focused) challenger banks transform banking from a one-way conversation to a two-way conversation: it is the active and constructive conversation between the digital-only (digitally-focused) challenger banks and their online community that drives new products and services creation. In addition, growing global online communities also gives digital-only (digitally-focused) challenger banks the opportunity to create and consolidate their global identity.

Finally, some digitally-only (digitally-focused) challenger banks have also opened to their customers and engaged with them at a even deeper level by inviting them to invest in the company through crowdfunding platforms.

- Transparency – When it comes to costumers, complete transparency is the norm for digitally-only (digitally-focused) challenger banks. Fees and interest rates are clearly communicated to customers, while transaction history and balance information are easily accessible and searchable through mobile apps. In addition to building online communities of customers discussed above, digital-only (digitally-focused) challenger banks often invite customers to their offices to test early versions of their app and to collect critical feedback.

Moreover, digitally-only (digitally-focused) challenger banks tend to release their product roadmap to the public; they share details of our investment ethics with their communities; and, when things go wrong, they remain fully transparent to their customers. While bringing as much as possible transparency into the open, digital-only (digitally-focused) challenger banks also focus on transparency internally, through initiatives such as default email transparency policies and weekly company-wide meetings.

[805] See, PWC, *Who Are You Calling a 'Challenger'? How Competition is Improving Customer Choice and Driving Innovation In the UK Banking Market*, cit., pp. 27-28.

7.C.iii. Looking Ahead – Key Challenges and Opportunities

Most popular digital-only (digitally-focused) challenger banks are rapidly growing their capabilities and scaling their activities across countries. To successfully deliver on their growth strategies, they must address a number of key challenges and exploit new opportunities, which include the following:

- As discussed in previous chapters, new fintech-related regulatory and policy initiatives currently developed and implemented across various geographic regions (including new Open Banking frameworks in the EU/EEA and the UK) are creating the opportunity for many new players to participate in a market that has previously not been open to them. Against this dynamic and rapidly evolving background, digital-only (digitally-focused) challenger banks are faced with a very exciting challenge: on one hand, they are finally able to enter the market without (or with very limited) access restrictions; on the other hand, they are required to comply with increasingly rigorous legislative and regulatory requirements and to bear the burden of being able to actively demonstrate such compliance.

Those digital-only (digitally-focused) challenger banks that ignore (or underestimate) the legal and compliance dimension of the above challenge when building their activities do so at their own peril. Regulatory tolerance for lapses on issues such as capital requirements, risk management, KYC, AML, antifraud, security, privacy, and regulatory compliance will be very low. This means that those digital-only (digitally-focused) challenger banks that build and efficiently integrate legal and compliance capabilities within their organization and operations will be better positioned to succeed than those that do not. This, also, means that going forward the ability of digital-only (digitally-focused) challenger banks to innovate while remaining agile in responding to evolving regulatory frameworks will be key for them to gain and strengthen their market position.

- While at present in the United States there are only few digital-only (digitally-focused) challenger banks, the number is expected to increase over the next 12-18 months. On the other hand, in Europe and the UK there is already a relevant number of digital-only (digitally-focused) challenge banks, and many more are expected to come over the next 12 to 24 months. Overall, existing digital-only (digitally-focused) challenge banks have fairly similar offerings and tend to target similar segments of the population. This means that, going forward, digital-only (digitally-focused) challenge banks will increasingly compete both with established banks and with each other for customers. Increased competition, in turn, will make customer acquisition trickier (and perhaps more expensive). This also means that any market share that a digital-only (digitally-focused) challenger bank looses now will be much harder to recover later, as the industry becomes more competitive and crowded.

- Digital-only (digitally-focused) challenge banks may also struggle with customer acquisition amid competition by large technology companies. As previously discussed, Google, Facebook, Apple, Uber, Alipay and so on are increasingly providing financial and banking services underneath their core offerings. These tech giants can count on established, active, global communities of users and are way ahead of many

players in the fintech space in utilizing consumer data and insights to offer well segmented services. Because of this, their further expansion could have a significant impact on digital-only (digitally-focused) challenger banks' growth strategies.

Given the above challenges and opportunities, digital-only (digitally-focused) challenge banks will likely have to increase customer awareness[806] and leverage their active community of users and developers in order to acquire a critical mass of customers and drive customer loyalty. Moreover, going forward, it will be increasingly important for digital-only (digitally-focused) challenge banks to clearly differentiate themselves on services, products, and customer experience from other digital players and incumbents, which are intensifying their transformative efforts. Digital-only (digitally-focused) challenge banks will also need to offer functionally rich propositions that are significantly better than those offered by their competitors.[807] Finally, digital-only (digitally-focused) challenge banks that decide to deploy marketplace and platform strategies will have to cultivate their ecosystem, strengthen their engagement with both inter-industry partners and cross-industry partners,[808] and capitalize on network effects across their marketplaces and platforms.

[806] See, PWC, *Who Are You Calling a 'Challenger'? How Competition is Improving Customer Choice and Driving Innovation In the UK Banking Market*, cit., p. 29 (reporting that "[a]s these banks are still in their infancy, they face very low levels of consumer awareness. Only 9% of our survey respondents were aware of any of the digital players … Moreover, only 9% of consumers said they would consider opening a financial product with the digital players in the next three years, in addition to the 9% of respondents which already bank with them.").

[807] Ibidem (noting that "[c]ritically, the proposition must be more than a better app, as our survey revealed that only 4% of customers who changed banking arrangements in the last three years did so because their previous provider's mobile app didn't meet their needs.").

[808] Id., p. 30. For example, digital-only (digitally-focused) challenge banks may consider partnering with players from industries with large amounts of digital customers (e.g., travel, e-commerce, social media, consumer products, and telecommunications).

CONCLUSION

Open Banking is an evolution of banking that focuses on how banks share their data, products/services, and functionality, and how they enable consumers to share their financial data, account information, and functionality for access and use by authorized third parties. This evolution is expected to increase transparency, promote competition, and foster innovation in the banking and financial services industry. These positive outcomes, in turn, will help empower consumers and businesses by giving them greater control over their data and finances.

The evolution prompted by Open Banking goes far beyond technology. Open Banking represents a defining moment at which banks are forced to re-think their role and the approach they take to their business. Open Banking focuses on the way banks innovate through partnerships and collaborations with various participants within and outside the financial and banking services industry. It is about the way banks and third parties (co)-create the value and flexibility that speaks to the real-world needs of consumers and businesses by making their financial data and account information more available and widely shared than ever before.

At present, a number of interconnected forces are driving the movement towards Open Banking. These forces include a substantial demographic shift, evolving costumer preferences and expectations, technology advances, and increased competition by new entrants such as fintech companies and large tech giants.

Alongside the described forces, legislative and regulatory reforms in Europe and the United Kingdom are acting both as a catalyst for change and an accelerator of openness in the financial and banking services industry. In parallel to these reforms, governmental authorities and regulators in the United States are starting testing the waters in Open Banking by gathering more information about current practices and potential market developments and improving their engagement with various industry participants and consumer representative groups.

Regulators have certainly an important and constructive role to play in creating and promoting the openness needed for a new paradigm of banking to flourish. In determining whether, and to what extent, to take regulatory actions with respect to Open

Banking and consumer-permissioned access to consumer financial data and account information, regulators should be mindful of the global nature of the issues at stake. In fact, overly prescriptive rules regarding access to consumer data will have the negative effects of: depriving consumers of innovative products and services which could help them (re)-gain control over their finances and materially improve their financial health; placing companies subject to any such rules at a significant disadvantage vis-à-vis their competitors in other jurisdictions; creating a fractured regulatory framework to the extent any such rule diverges substantially from international access standards or conventions; and stifling innovation by precluding fintech companies and other new entrants from accessing consumer data and/or scaling internationally. Furthermore, any regulatory action aiming at promoting Open Banking and facilitating consumer-permissioned access to consumer financial data and account information should coordinate with ongoing industry initiatives and should be subject to public comments to ensure that a measured and effective approach is developed to the benefit of all interested parties.

In addition to enabling consumers to access and share their financial records with trusted third parties without undue restrictions, Open Banking-related regulatory reforms should also provide for the establishment and enforcement of adequate safeguards. This is important because the value of Open Banking can only be realized when openness is nurtured and delivered in a responsible manner, which: maintains the trust critical to the functioning of the banking and the financial system; promotes transparency, privacy, and security in the use and disclosure of consumer financial data and account information by consumers who can control how to begin, manage, and terminate access thereof; and ensures the continue safety and soundness of the banking and financial system as a whole.

There are real tensions around many of the issues discussed above. Nevertheless, there is a promising path forward.

In particular, banks that want to gain (and maintain) a leading position in a rapidly evolving Open Banking ecosystem could consider adopting a marketplace strategy or a platform strategy. In the former scenario (banking-as-a-marketplace), the bank's customers can manage their finances and have access to third parties' financial and non-

financial products and services, alongside the bank's core product(s) (e.g., a current account). In this context, the bank enters into, and curates, a number of business partnerships with selected and trusted third-party service providers, which agree to offer their services and products throughout the bank's marketplace as either white-labeled or co-branded services and products. By contrast, in the latter scenario (banking-as-a-platform), the bank develops an open set of APIs that any third-party can use to build products and services. Different from the marketplace model, banking-as-a-platform has the potential advantage of providing customers with a greater variety of products and services and a more comprehensive set of capabilities. However, unlike the marketplace model, banking-as-a-platform may come with some lack of centralized control of quality and security on the part of the bank.

At present, fintech companies and other new entrants – particularly challenger banks – appear to be better positioned to deliver on these strategies, relatively to legacy players.

When a bank (be it an incumbent bank or a challenger bank) adopts a marketplace strategy or a platform strategy, the offering by the bank will be defined by the customer's journey (or customer's flow) as the customer searches, buys, and utilizes the products and services offered throughout the bank's marketplace or platform. In this context, differentiation will be based on a number of factors, including: seamless integration, reduced friction throughout the customer's journey, simplicity, personalized user experience, proactive and compelling customer engagement, ongoing support services, insightful predictions of customers' needs and goals, as well as governance, privacy and security checks. A bank that successfully delivers on these critical areas will be able to position itself as a customer's preferred digital point of entry into integrated non–financial and financial products and services and to acquire a central role at the heart of the customer's daily life.

Importantly, both a banking-as-a-marketplace strategy and a banking-as-a-platform strategy rely heavily on two key elements: first, well-defined APIs to facilitate richness and ease of integration with third parties' services and products; and second, access to customer data and insights, which can be processed and contextualized to drive analytics and provide competitive predictive services. Relevant quantities of customer data

(including personal data embedded within customers' transaction information) will likely concentrate around the bank's marketplace / platform. Because of this, monitoring and protecting costumer data throughout each stage of the costumer's journey across the services and products provided on the marketplace / platform will be a key priority.

Finally, when deploying a successful banking-as-a-marketplace strategy or banking-as-a-platform strategy, the bank and the various participants to its ecosystem will be able to leverage network effects generated across the marketplace / platform to scale and grow in value much more efficiently.

REFERENCES

A. Industry Reports

Accenture, *Becoming the Indispensable Everyday Bank*, Accenture Insights – Video Transcript (2014).

Accenture, *Everyday Bank: The Digital Revolution*, Accenture Insights (2014).

Accenture, *The Everyday Bank – Infographics*, Accenture Report (2014).

Accenture, *The Future of Fintech and Banking: Digitally Disrupted or Reimagined?*, Accenture Report (2015).

Accenture, *Driving Innovation in Payments — Powered by APIs & Open Banking*, Accenture Payments Report (2016).

Accenture, *Fintech and the Evolving Landscape: Landing Points for the Industry*, Accenture Report (2016).

Accenture, *Payments APIs: Too Compelling To Ignore, Accenture Perspectives - Interview at Accenture's Jeremy Light*, Accenture Report (2016).

Accenture, *Platform Economy: It's Time for Banks to Join in and Welcome Others*, Accenture Technology Vision for Banking Report (2016).

Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*, Accenture Payment Services Report (2016).

Accenture and the Partnership Fund for the New York City, *Fintech's Golden Age*, Accenture Report (2016).

Accenture, Microsoft and Avanade, *PSD2 and Open Banking Using Regulation to Kick-Start the Transformation of Banking*, White Paper (2017).

American Bankers Association, *Millenians and Banking. The Fastest Growing Customer Base is Changing the Way Banks Do Business*, American Bankers Association Report (January 2017).

Apigee, *The State of APIs - 2016 Report on Impact of APIs on Digital Business*, Apigee Report (2016).

Apigee, *The State of APIs - 2017 Report: How APIs Power Digital Ecosystems*, Apigee Report (2017).

Burnmark, *Challenger Banking*, Burnmark Report (October 2016).

CB Insights, *The Global Fintech Report: 2016 In Review. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, CB Insights Reports (February 15, 2017).

CB Insights, *The Global Fintech Report: Q2'17. A Comprehensive, Data-Driven Look at Global Financial Technology Investment Trends, Top Deals, Active Investors, and Corporate Activity*, CB Insights Reports (July 2017).

Center for Financial Services Innovation (CFSI), *Big Data, Big Potential: Harnessing Data Technology for the Underserved Market*, Center for Financial Services Innovation Report (March 2015).

Center for Financial Services Innovation (CFSI), *Center for Financial Services Innovation Unveils Framework for Responsible Industry-Wide Sharing of Consumer Financial Data*, Center for Financial Services Innovation (October 24, 2016).

Center for Financial Services Innovation (CFSI), *CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration*, Center for Financial Services Innovation Report (October 2016).

Contino, *Accelerating Compliance & the API Economy With Open Banking & PSD2*, Contino Report (2017).

Contino, *An AWS Centric Solution Architecture For Open Banking*, Contino Report (March 7, 2017).

Currencycloud, *Banks and the FinTech Challenge: How Disruption Has Been a Catalyst for Collaboration and Innovation*, Currencycloud White Paper (2016).

Deloitte, *Tech Trends 2015 - The Fusion of Business and IT*, Deloitte University Press (2015).

Deloitte, *PSD2 Opens the Door to New Market Entrants. Agility Will Be Key to Keeping Market Position*, Deloitte Report (2016).

Deloitte, *Open Banking: What Does The Future Hold?*, Deloitte Digital Report (April 2017).

Earnix, *The Role of Analytics in the Banking Age*, Earnix Report (2017).

Ernst & Young, *Landscaping UK Fintech*, Ernst & Young Report Commissioned by UK Trade & Investment (2014).

Ernst & Young, *UK FinTech on the Cutting Edge. An Evaluation of the International FinTech Sector*, Ernst & Young Report Commissioned by UK HM Treasury (2014).

Ernst & Young, *Revolutionary Change is Transforming the Financial Services Landscape*, Financial Services Leadership Summit December 2016, Ernst & Young View Points (2016).

Euro Banking Association (EBA), *Understanding the Business Relevance of Open APIs and Open Banking for Banks*, EBA Working Group on Electronic Alternative Payments and Innopay Information Paper (May 2016).

Euro Banking Association (EBA), *Open Banking: Advancing Customer-Centricity. Analysis and Overview*, Euro Banking Association Report, EBA Open Banking Working Group and Innopay Report (March 2017).

Financial Services Information Sharing and Analysis Center (FS-ISAC), *API Breaches*, FS-ISAC Expert Webinar Series (May 23, 2017).

Financial Solutions Lab, *FinLab Consumer Impact Report*, Financial Solutions Lab (November 16, 2016).

Finextra, *PSD2 and Open Banking: Defining Your Role in the Digital Ecosystem*, Finextra White Paper (September 2016).

Fjord and Accenture, *The Era of Living Services*, Fjord and Accenture Report (2015).

Forrester Research, *Establish Your API Design Strategy APIs Are a Key Embodiment of Your Digital Business*, Forrester Research Report (June 2013).

Forrester Research, *Drive Business Agility and Value by Increasing Your API and SOA Maturity - Forrester's Eight Central Elements of Service-Based Maturity Provide a Foundation for Achieving Business Agility Via APIs and SOA*, Forrester Research Report (September 2013).

Forrester Research, *Best Practices for Agile-Plus-Architecture - Enterprises Need Sustainable Business Agility, Not Just Agile Development*, Forrester Research Report (February 2015).

Forrester Research, *How APIs Reframe Business Strategy - Craft an API Strategy to Enable Digital Business Transformation*, Forrester Research Report (June 2015).

Forrester Research, *APIs Underpin A Digital Business Platform - Prepare For Digital Transformation's Constant, Unpredictable Change*, Forrester Research Report (January 2016).

Forrester Research, *Four Ways APIs Are Changing Banking. How Financial Services Firms Are Exploiting the API Economy*, Forrester Research Report (May 2016).

Gartner, *Use PSD2 to Accelerate Open Banking*, Gartner Report (February 19, 2016).

Gartner, *Welcome to the API Economy - Enterprises Need to Create an Industry Vision for Digital Business*, Gartner Report (June 9, 2016)

Gartner, *Magic Quadrant for Full Life Cycle API Management*, Gartner Report (October 27, 2016).

IBM, *Open Banking: Everything You Need to Know*, A presentation by Bharat Bhushan (Industry Technical Leader, Banking and Financial Markets - IBM), Technology Innovation Exchange (2017).

Independent Commission on Banking (ICB), *Final Report Recommendations*, Independent Commission on Banking Report (September 2011).

JP Morgan Chase & Co. (Tim Sandel - Managing Director (author)), *The FinTech Revolution*, JPMorgan Chase & Co. Insights (December 21, 2016).

JP Morgan Chase & Co. (Stephen Markwell - Head of Treasury Services Product Investments (author) and Karen Larsen, CTO and Head of Fintech Payments Strategy (author)), *How FinTech and Banks are Partnering*, JP Morgan Chase & Co. Insights (February 6, 2017).

JP Morgan Chase & Co. (Tim Sandel - Managing Director (author)), *4 Key Considerations for Tech Companies When Going Global*, JPMorgan Chase & Co. Insights (February 17, 2017).

KPMG, *Should Banks Nurture Internal Innovation or Invest in FinTech?*, KPMG Insights (February 4, 2016).

KPMG, *Five Ways Banks Can Use Fintech to Build Trust*, KPMG Insights (April 12, 2016).

KPMG, *A New Landscape. Challenger Banking Annual Results*, KPMG Report (May 2016).

KPMG, *Banking is a Software Industry: Time to Walk the Walk*, KPMG Insights (February 10, 2017).

KPMG, *European PSD2 Open Banking Standards Provide the Opportunity for Payments Innovation*, KPMG Insights (February 15, 2017).

KPMG, *Global Fintech Investment Sees Sharp Decline in 2016 Despite Record VC Funding: KPMG Q4'16 Pulse of Fintech Report*, KPMG Insights (February 20, 2017).

KPMG, *The Pulse of Fintech Q4 2016. Global Analysis of Investment in Fintech*, KPMG Report (February 21, 2017).

KPMG, *Setting Course in a Disrupted Marketplace. The Digitally-Enabled Bank of the Future*, KPMG Report (April 2017).

KPMG, *Setting Course in a Disrupted Marketplace. The Digitally-Enabled Bank of the Future*, KPMG Report (April 2017).

KPMG, *The Digital Bank of the Future. Setting Course in a Disrupted Marketplace: Becoming the Digital Bank of the Future*, KPMG Insights (April 5, 2017).

Massachusetts Institute of Technology (MIT), *Digital Banking Manifesto: The End of Banks?*, Massachusetts Institute of Technology Report (2016).

McKinsey & Company, *Digital Banking: Winning the Beachhead*, McKinsey on Payments, pp. 3-10 (May 2014).

McKinsey & Company, *The Digital Battle that Banks Must Win*, McKinsey Financial Services Report (August 2014).

McKinsey & Company, *The Bank of the Future*, McKinsey Interview Series – Transcript of the Interview of Somesh Khanna (McKinsey Director (NY)) (November 2014).

McKinsey & Company, *The Fight for the Customer: Mckinsey Global Banking Annual Review 2015*, McKinsey Global Banking Report (March 2015).

McKinsey & Company, *Voices on Bank Transformation: Insights on Creating Lasting Change*, McKinsey Global Banking Report (March 2015)

McKinsey & Company, *Gauging the Disruptive Potential of Digital Wallets*, McKinsey on Payments, Vol. 8, No. 21, pp. 3-10 (May 2015).

McKinsey & Company, *Faster Payments: Building a Business, Not Just an Infrastructure*, McKinsey on Payments, Vol. 8, No. 21, pp. 23-29 (May 2015).

McKinsey & Company, *Citigroup on Engaging the Digital Customer*, McKinsey Interview Series – Transcript of the Interview of Michael L. Corbat (Citigroup CEO) (June 2015).

McKinsey & Company, *The New Rules for Growth through Customer Engagement*, McKinsey on Payments, Vol. 8, No. 22, pp. 32-38 (October 2015).

McKinsey & Company, *Cutting Through the FinTech Noise: Markers of Success, Imperatives for Banks*, McKinsey Global Banking Report (December 2015).

McKinsey & Company, *A Digital Crack in Banking's Business Model*, McKinsey Quarterly Insights (April 2016).

McKinsey & Company, *Banking on the Cloud*, McKinsey Digital Report (April 2016).

McKinsey & Company, *Building a Digital-Banking Business*, McKinsey Financial Services Report (April 2016).

McKinsey & Company, *Fintechs Can Help Incumbents, Not Just Disrupt Them*, McKinsey Financial Services Report (July 2016).

McKinsey & Company, *The Future of Bank Risk Management*, McKinsey Risk Report (July 2016).

McKinsey & Company, *A Brave New World for Global Banking*, McKinsey Financial Services Report (January 2017).

Microsoft, *Empowering the Digital Bank: The API Economy: Helping Financial Services Companies to Build Better Products*, Microsoft Financial Services - Banking & Capital Markets Insights (May 27, 2015).

Microsoft, *Cracking the Millennial Code: Building Better Banking Relationships with Digital Natives*, Microsoft Financial Services - Banking & Capital Markets Insights (August 25, 2016).

Microsoft, *Banking on Technology: Enabling an Omnichannel Approach in Financial Services*, Microsoft Financial Services - Banking & Capital Markets Insights (August 30, 2016).

Microsoft, *Data-Driven Organizations Will Lead The Digital Revolution. Part 1 of 3: The Opportunity of Big Data*, Microsoft Financial Services - Banking & Capital Markets Insights (September 22, 2016).

Microsoft, *Data-Driven Organizations Will Lead The Digital Revolution. Part 2 of 3: Getting Business Value Out of Big Data is Hard*, Microsoft Financial Services - Banking & Capital Markets Insights (September 26, 2016).

Microsoft, *Data-Driven Organizations Will Lead The Digital Revolution. Part 3 of 3: Key Enablers for Successful Transformation*, Microsoft Financial Services - Banking & Capital Markets Insights (September 27, 2016).

Microsoft, *Enabling Mobile Banking While Keeping Customers' Safe*, Microsoft Financial Services - Banking & Capital Markets Insights (October 18, 2016).

Microsoft, *Empowering Banking & Capital Markets: A Data-Driven Business*, Microsoft Financial Services - Banking & Capital Markets Insights (December 1, 2016).

Microsoft, *Thriving in an Age of Radical Uncertainty*, Microsoft Financial Services - Banking & Capital Markets Insights (December 13, 2016).

Microsoft, *The Financial Services Industry Is Banking on Digital Transformation*, Microsoft Financial Services - Banking & Capital Markets Insights (January 9, 2017).

Microsoft, *Banking as a Digital Platform*, Microsoft Financial Services - Banking & Capital Markets Insights (January 26, 2017).

Microsoft, *Will Consumers Build Digital Banking Products?*, Microsoft Financial Services - Banking & Capital Markets Insights (March 27, 2017).

Microsoft, *Intelligent Digital Insights or Fabricated Financial Data?*, Microsoft Financial Services - Banking & Capital Markets Insights (April 3, 2017);

Microsoft, *Banking on the Cloud: Financial Institutions Reach the Stratosphere of Efficienc*y, Microsoft Financial Services - Banking & Capital Markets Insights (April 6, 2017).

Microsoft, *Digital Transformation in Financial Services: From Strategy to Reality*, Microsoft Financial Services - Banking & Capital Markets Insights (April 13, 2017).

Microsoft, *Will Digital Acceleration Simplify Banking?*, Microsoft Financial Services - Banking & Capital Markets Insights (April 17, 2017).

MuleSoft, *Open Banking and the Future of Financial Services. Are You a Survivor or Thriver?*, MuleSoft WhitePaper (2016).

MuleSoft, *Connectivity Benchmark Report - The State of Digital Transformation and APIs*, MuleSoft Report (May 2016).

Nadig, Deepak (Head of API Platform Engineering at Paypal), *Evolution of the Paypal API: Platform & Culture*, Presentation at Craft Conference (April 23, 2015).

Office of Fair Trading (OFT), *Review of Barriers to Entry, Expansion and Exit in Retail Banking*, Office of Fair Trading Report (November 2010).

PWC, *Global Economic Crime Survey 2016 - Adjusting the Lens on Economic Crime: Preparation Brings Opportunity Back Into Focus*, PWC Report (2016).

PWC, *Who Are You Calling a 'Challenger'? How Competition is Improving Customer Choice and Driving Innovation in the UK Banking Market*, PWC Report (2017).

PWC, *PSD2 – Redrawing the Lines: FinTech's Growing Influence on Financial Services*, PWC Global Fintech Report (2017).

PWC, *PSD2 – A Game Changing Regulation. What Challenges and Opportunities Could the New Directive Provide?*, PWC Insights (2017).

PWC, *PSD2 – Are You Ready to Embrace the Change? Key Areas of Focus*, PWC Report (February 2017).

Renton, Peter, *An In Depth Look at the OnDeck/JPMorgan Chase Deal*, Lend Academy (December 4, 2015).

Scratch, *Millennial Disruption Index*, Scratch Report (2013).

Strategy&, *Catalyst or Threat? The Strategic Implications of PSD2 for Europe's Banks*, Strategy& Report (July 2016).

The Atlantic, *How Connectivity is Moving Banks Forward*, The Atlantic Report (2016).

The Economist, *The Disruption of Banking*, The Economist Intelligence Unit Report (2015)

The Economist, *Retail Banking - In Tech We Trust*, The Economist Intelligence Unit Report (2016).

UBS, *Global Banks: Is FinTech a Threat or an Opportunity?*, UBS Evidence Labs, UBS Global Research Q-Series (July 2016).

B. Articles, Blog Posts and Press Releases

Alden, William, *BBVA Buys Banking Start-Up Simple for $117 Million*, DealBook (February 20, 2014).

American Banker, *Eight Illuminating Data Points on Millennials and Banking*, American Banker (May 12, 2016).

Atom Bank, A*tom and BBVA - Capital Raise Over and £135m Raised, We're One Step Closer to Launch*, Atom Bank Press Release (November 24, 2015).

Barba, Robert, *Tech, Love and Understanding*, American Banker (October 5, 2016).

Barba, Robert, *How JPM Makes Tech Partnerships Work*, American Banker (November 28, 2016).

Barba, Robert, *Why the JPM-Intuit Partnership Is a Big Step for Data Sharing*, American Banker (January 25, 2017).

BBVA, *BBVA Acquires Simple to Accelerate Digital Banking Expansion*, BBVA Press Release (February 20, 2014).

BBVA, *BBVA Strengthens its Commitment to UK's Atom Bank*, BBVA Press Release (March 3, 2017).

Belger, Tom, *PRA Receives 13 Banking Licence Applications*, Bridging & Commercial (February 16, 2017).

Berlind, David, *How 200-Year-Old Citibank Totally Nailed Its Hackathon*, ProgrammableWeb (December 15, 2014).

BI Intelligence, *Bank Of America Strengthens Digital Business-To-Business Offerings*, BI Intelligence (August 19, 2016).

Bills, Steve, *OFX Proposal to Make Aggregation Easier*, American Banker (December 6, 2004).

Blomfield, Tom, *The Bank of the Future Will Be a Marketplace*, Monzo Blog (February 4, 2016).

Bogleheads Community Forum, *Chase No Longer Works with Quicken?*, Bogleheads Community Forum (Oct. 21, 2015).

Bonchek, Mark and Sangeet Paul Choudary, *Three Elements of a Successful Platform Strategy*, Harvard Business Review (January 31, 2013).

Brear, David, and Pascal Bouvier, *Exploring Banking as a Platform (BaaP) Model*, The Financial Brand (March 4, 2016).

Brear, David, and Pascal Bouvier, *Making Banking as a Platform (BaaP) a Reality*, The Financial Brand (March 25, 2016).

Busch, Wayne, and Juan Pedro Moreno, *Banks' New Competitors: Starbucks, Google, and Alibaba*, Harvard Business Review (February 20, 2014).

Caffyn, Grace, *Barclays Trials Bitcoin Tech With Pilot Program*, CoinDesk (June 22, 2015).

Choudary, Sangeet Paul, *The Platform Stack: For Everyone Building a Platform… and for Everyone Else. A Unifying Framework for Digital Business Models*, Platform Thinking Labs (2016).

Clozel, Lalita, *Cordray Reignites Bank-Fintech Fight After Comments on Data Sharing*, American Banker (October 25, 2016).

Clozel, Lalita, *Fintech Charter Q&A: OCC Answers Skeptics*, American Banker (January 3, 2017).

Crosman, Penny, *BBVA's Simple Purchase Reflects Mobile Banking's Sizzle*, American Banker (February 21, 2014).

Crosman, Penny, *Digitally Minded Bank Goes All-In on Responsive Design, Moven*, American Banker (February 11, 2015)

Crosman, Penny, *Fintech Glasnost: Why U.S. Banks Are Opening Up APIs to Outsiders*, American Banker (July 8, 2015).

Crosman, Penny, *The Truth Behind the Hubbub Over Screen Scraping*, American Banker (November 12, 2015).

Crosman, Penny, *Fintech's Goals are Changing, VC's Appetite is Not*, American Banker (April 16, 2016).

Crosman, Penny, *Wells Fargo's Bid to Vanquish Screen Scraping*, American Banker (June 7, 2016).

Crosman, Penny, *"Banks Don't Want to Give Access to Everything: Yodlee Exec*," American Banker (June 7, 2016).

Crosman, Penny, "Data Wants to Be Free": Why Banks Should Open APIs to Others, American Banker (June 23, 2016).

Crosman, Penny, *How B of A's Billion-Dollar Tech Cuts Could Fuel Startups*, American Banker (June 28, 2016).

Crosman, Penny, *Wells-Finicity Deal Furthers Data Détente*, American Banker (April 4, 2017).

Delaney, Kevin J., *To Disrupt Banking, Do You Need to Own the Bank?*, Quartz (February 10, 2014).

Envestnet Yodlee, *New Industry Group Established to Support Consumers' Right to Access their Financial Data*, Envestnet Yodlee Press Release (Redwood City (CA), January 19, 2017).

European Banking Federation, *EBF Asks Commission to Support Ban on Screen Scraping*, European Banking Federation Statement (Brussels, 16 May 2017).

Financial Innovation Now (FIN), *Tech Industry Leaders Launch Coalition to Advocate for Policies to Foster Innovation in Financial Services*, Financial Innovation Now Press Release (Washington (DC) (November 3, 2015)).

Financial Innovation Now (FIN), *Statement by Brian Peters*, Executive Director of Financial Innovation Now, Financial Innovation Now Press Release (November 17, 2016).

Financial Innovation Now (FIN), Statement by Brian Peters, Executive Director of Financial Innovation Now, Financial Innovation Now Press Release (October 24, 2016).

Financial Innovation Now (FIN), Statement by Brian Peters, Executive Director of Financial Innovation Now, Financial Innovation Now Press Release (November 17, 2016).

Financial Innovation Now (FIN), *Letter to the Honorable Donald J. Trump President-Elect of the United States and the Trump-Pence Transition Team*, Financial Innovation Now (November 30, 2016).

Finextra, *Moven Teams up with Loan Refinancers CommonBond and Payoff*, Finextra (January 28, 2016).

Finextra, *JPMorgan Chase Partners with InvestCloud for Digital Wealth Management*, Finextra (September 21, 2016).

Finicity, *Finicity and Wells Fargo Ink Data Exchange Deal*, Finicity Press Release (April 4, 2017).

Finnegan, Matthew, *How Technology Will Transform Banking in 2017: Blockchain, Cloud Computing and Digital Challenger Banks*, Computerworld UK (December 16, 2016).

Future of the European Fintech, *PSD2-Compliant Access not Subject to an Alleged "Screen Scraping Ban,"* Future of the European Fintech Alliance (2017).

Future of the European Fintech, *Manifesto for the Impact of PSD2 on the Future of European Fintech*, Future of the European Fintech Alliance (2017).

Ghosh, Shona, *Barclays Becomes First UK High Street Bank to Explore the Blockchain*, Haymarket (June 24, 2015).

Glazer, Emily, *J.P. Morgan in a Car-Lending Chase*, The Wall Street Journal (August 25, 2016).

Hagel, John, *The Power of Platforms*. Part of the Business Trends Series, Deloitte University Press (April 15, 2015).

Hagel, John, *The Power of Platforms to Create New Value*, Deloitte CIO, The Wall Street Journal Insights (April 15, 2015).

Hope, Bradley, *Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors*, The Wall Street Journal (August 6, 2015)

Huang, Daniel, and Peter Rudegeair, *Bank of America Cut Off Finance Sites from its Data*, The Wall Street Journal (November 9, 2015).

Intuit, *Chase, Intuit to Give Customers Greater Control of their Information*, Intuit Press Release (January 25, 2017).

Irrera, Anna, *Santander Partners with Supply Chain Finance Startup Tradeshift*, Reuters (July 11, 2017).

JP Morgan Chase & Co., Jamie Dimon (Chairman and Chief Executive Officer), *Letter to Shareholders*, JP Morgan Chase & Co. (April 6, 2016).

JP Morgan Chase & Co., *JPMorgan Chase Partners With InvestCloud for Digital Wealth Management*, JP Morgan Chase & Co. Press Release (September 20, 2016).

JP Morgan Chase & Co., Jamie Dimon (Chairman and Chief Executive Officer), *Letter to Shareholders*, JP Morgan Chase & Co. (April 4, 2017).

Kabbage, *Kabbage and Santander UK Partner to Accelerate SMB Growth*, Kabbage News (April 3, 2016).

Karakas, Cemal, and Carla Stamegna, *Financial Technology (FinTech): Prospects and Challenges for the EU*, European Parliamentary Research Service (March 2017).

Klarna, *Global: Klarna - Europe's Newest Bank is Born*, Klarna Press Release (June 19, 2017).

Lane, Kin, *History of APIs*, API Evangelist Blog (December 20, 2012).

Leimer, Bradley, *Lessons from BBVA's Simple Acquisition: It's Time to Build Better Banks*, American Banker (February 28, 2014).

Let's Talk Payment, *BofA Has $3 Billion to Pour Into Innovation as Banks Are Swarming Around FinTech Startups*, Lets Talk Payment (January 8, 2016).

Let's Talk Payment (LTP), *Community Banks Call Regulators to Toughen up on FinTech for the Common Good*, LTP (June 7, 2016).

Lunden, Ingrid, *UK Mobile-Only Atom Bank Picks Up $128M Led by BBVA, Owner of Simple in the U.S.*, TechCrunch (November 24, 2015).

Macheel, Tanaya, *JPMorgan Buys Stake in InvestCloud to Speed Digital Revamp*, American Banker (September 21, 2016).

McLannahan, Ben, *Blythe Masters and JPMorgan Trial Blockchain Project*, Financial Times (January 31, 2016).

Miller, Ron, *Wall Street-Backed Symphony Wants To Revolutionize Financial Services Communication*, Techcrunch (February 21, 2015).

Monzo, *Fastest Crowdfunding Ever: £1M in 96 Seconds*, Monzo Blog (March 3, 2016).

Monzo, *£12 Million Later: Our Crowdfunding Pre-Registration is Closed*, Monzo Blog (March 14, 2017).

Monzo, *The Class of 2017: Launching Monzo University*, Monzo Blog (July 13, 2017)

Moreno, Juan Pedro, *Banking at a Digital Crossroads*, The Financial Times (January 28, 2014).

Morgan Stanley, *Management Partners with Twilio to Help Enhance Client Communications*, Morgan Stanley Press Release (June 13, 2017).

Moven, *When Is a Bank Not a Bank?*, Moven Blog Post (November 20, 2012).

Nemeroff, Evan, *Moven Expands Globally, Forming Partnership with Westpac New Zealand*, American Banker (August 25, 2014).

Open Financial Exchange (OFX), *Open Financial Exchange 2.2 [OFX2.2]*, OFX (2016).

Open Financial Exchange (OFX), *About OFX – Background Summary*, Open Financial Exchange (to date).

Open Financial Exchange (OFX), *FAQ*, Open Financial Exchange (to date).

Perez, Sarah, *Zelle, The Real-Time Venmo Competitor Backed by Over 30 U.S. Banks, Arrives this Month*, TechCrunch (June 12, 2017).

Plaid Technologies, *Plaid Announces $44 Million Series B Led by Goldman Sachs Investment Partners*, Plaid Technologies Press Release (June 20, 2016).

Plaid Technologies, *Plaid Unveils Investments by Citi Ventures and American Express Ventures*, Plaid Technologies Press Release (February 6, 2017).

Passy, Jacob, *JPM Teams with Fintech to Deliver Digital Mortgage Platform*, American Banker (February 16, 2017).

Reynolds, Emily, *Inside Fidor, the Fintech Bank Run by its Customers*, Wired (June 23, 2016).

Rudegeair, Peter, *J.P. Morgan Warns It Could Unplug Quicken and Quickbooks Users*, Wall Street Journal (November 24, 2015).

Rudegeair, Peter, Emily Glazer, and Ruth Simon, *Inside J.P. Morgan's Deal With On Deck Capital*, The Wall Street Journal (December 30, 2015).

Shevlin, Ron, *The Foolish Fantasies of Fintech/Bank Partnerships*, The Financial Brand (May 23, 2016).

Shevlin, Ron, *The Platformification of Banking*, The Financial Brand (July 19, 2016).

Shieber, Jonathan, *Sigfig Locks in Big Banking Partners for its Tech-Enhanced Advisory Services with $40M Round*, TechCrunch (May 24, 2016).

Sidel, Robin, *Big Banks Lock Horns with Personal-Finance Web Portals*, The Wall Street Journal (November 4, 2015).

Silicon Valley Bank, *Xero and Silicon Valley Bank Partner to Offer Innovative Companies Next-Generation Financial Management*, Silicon Valley Bank Press Release (July 16, 2014).

Skinner, Chris, *Four Banking Business Models for the Digital Age*, Chris Skinner's Blog (October 24, 2016).

Son, Hugh, *Morgan Stanley Signs with Asset-Gobbling Startup Backed by Thiel*, Bloomberg (January 10, 2017).

Standard Treasury, *Series A Pitch Deck*, Standard Treasury Presentation (2015).

Swanson, Brena, *Big Banks Band together to Introduce Digital Payment App Zelle*, HousingWire (June 12, 2017).

TD Bank Group, *TD and Moven Announce Exclusive Canadian Agreement*, TD Bank Group Press Release (December 2, 2014).

Tescher, Jennifer, and Beth Brockland, One-Off Data-Sharing Deals Aren't Enough, American Banker (January 27, 2017).

The Economist, *The Fintech Revolution: A Wave of Startups is Changing Finance — For the Better*, The Economist (May 9, 2015).

Todd, Sarah, *Banks' Real Fight with Fintech: Who Owns the Customer?*, American Banker (June 19, 2015).

Van Wezel, Ron, *The Programmable Bank: Opportunities for Open Banking*, The Financial Brand (December 12, 2016).

Wells Fargo & Co., *Wells Fargo, Xero Agree on New Data-Exchange Method*, Wells Fargo Press Release (June 7, 2016).

Wells Fargo & Co., *Intuit Signs New Data-Exchange Agreement with Wells Fargo*, Press Release (February 3, 2017).

Williams, Aime, *Barclays Partners with Goldman-Backed Bitcoin Payments App*, Bloomberg (April 5, 2016).

Williams-Grut, Oscar, *A New Challenger Bank Built Like an App Store Just Launched in the UK — We Spoke to the CEO*, Business Insider (September 17, 2015).

Wisniewski, Mary, *BankMobile Aims to Become the Uber of Banking*, American Banker (January 20, 2015).

Wisniewski, Mary, *Mobile-First Bank Gets U.K. Charter — Could It Happen Here?*, American Banker (July 7, 2015).

Wisniewski, Mary, *Why U.K. Fintech Firms Are Becoming (Not Partnering with) Banks*, American Banker (September 16, 2015).

Wisniewski, Mary, *Fintechs Team Up to Become More Banklike*, American Banker (January 27, 2016).

Wisniewski, Mary, *JPMorgan Chase and Intuit Partner to Share Data via API*, American Banker (January 25, 2017).

Wisniewski, Mary, *The Data Access Debate Is About to Get a Lot More Interesting*, American Banker (January 27, 2017).

Wolff-Mann, Ethan, *Big Banks Are Attacking Personal Finance Apps Like Mint*, Time (November 9, 2015).

Woolley, Suzanne, *JPMorgan Courts Millennials by Putting the Whole Car-Buying Nightmare Online*, Bloomberg (August 26, 2016).

Xero and Capital One, *Xero and Capital One Partner to Automate Small Business Accounting and Transform Banking*, Xero and Capital One Joint Press Release (May 10, 2017).

Yurcan, Bryan, *"Banking as a Service" for Fintechs Seeking Scale*, American Banker (March 21, 2016).

Yurcan, Bryan, *Bank of America Partners with Digital Payments Firm*, American Banker (October 20, 2016).

Yurcan, Bryan, *Will 2017 Be a Breakthrough Year for Data Portability?*, American Banker (December 12, 2016).

Yurcan, Bryan, *Fintech Companies Form Lobbying Group Focused on Data Sharing*, American Banker (January 19, 2017).

Yurcan, Bryan, *BBVA Increases Investment in UK Digital Bank Atom*, American Banker (March 3, 2017).

Yurcan, Bryan, *TD and Moven Extend Partnership to U.S.*, American Banker (March 28, 2017).

C. Books

Parker, Geoffrey G. and Marshall W. Van Alstyne, *Platform Revolution: How Networked Markets Are Transforming the Economy — And How to Make Them Work for You*, W. W. Norton & Company, Ed. 1st (2016).

D. Regulations and Policy Initiatives - European Union

European Banking Authority (EBA)

Enria, Andrea (Chairperson of the European Banking Authority (EBA)), *Introductory Statement* of the Chairperson of the European Banking Authority at the Committee on Economic and Monetary Affairs (ECON) of the European Parliament (Brussels (BE), March 27, 2017).

European Banking Authority (EBA), *Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication under the Revised Payment Services Directive (PSD2)*, EBA/DP/2015/03 (December 8, 2015).

European Banking Authority (EBA), *Regulatory Technical Standards on Strong Customer Authentication And Secure Communication Under PSD2, Discussion Paper – Responses*, available at https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/discussion-paper#responses_1303933.

European Banking Authority (EBA), *Consultation Paper on the Draft Regulatory Technical Standards Specifying the Requirements on Strong Customer Authentication and Common and Secure Communication under PSD2*, EBA/CP/2016/11 (August 12, 2016).

European Banking Authority (EBA), *Regulatory Technical Standards on Strong Customer Authentication And Secure Communication Under PSD2, Consultation Paper – Responses*, available at https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper#responses_1548180.

European Banking Authority (EBA), *Public Hearing on Strong Customer Authentication & Secure Communication (SCA & CSC) under Article 97 PSD2*, Presentation by Dirk Haubrich, Geoffroy Goffinet, Consumer Protection, Financial Innovation and Payments (London (UK), 23 September 2016).

European Banking Authority (EBA), *EBA Paves the Way for Open and Secure Electronic Payments for Consumers Under the PSD2*, European Banking Authority Press Release (February 23, 2017).

European Banking Authority (EBA), *Final Report - Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive* 2015/2366 (PSD2), EBA/RTS/2017/02 (February 23, 2017).

European Banking Authority (EBA), *EBA Publishes its Opinion In Response to the European Commission Intention to Amend the EBA Technical Standards for Open and Secure Electronic Payments under the PSD2*, European Banking Authority Press Release (June 29, 2017).

European Banking Authority (EBA), *Opinion of the European Banking Authority on the European Commission's Intention to Partially Endorse and Amend the EBA's Final Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication Under PSD*, European Banking Authority (EBA) Opinion (June 29, 2017).

European Banking Authority (EBA), *EBA publishes a Discussion Paper on its approach to FinTech*, European Banking Authority Press Release (August 4, 2017).

European Banking Authority (EBA), *Discussion Paper on the EBA's approach to financial technology (FinTech)*, EBA/DP/2017/02 (August 4, 2017).

European Central Bank

Wacket, Helmut (Head of Market Integration Division, European Central Bank), *Provision of Integrated Payment Initiation Services – The Role of the ERPB*, slides 9-12, in Open Forum on Open Banking, Meeting Presentation, Open Forum on Open Banking (Brussels (BE), March 20, 2017).

European Commission

Dombrovskis, Valdis (European Commission Vice President), *Keynote Speech* at the Conference #FINTECHEU "Is EU Regulation Fit for New Financial Technologies?," (Brussels (BE), March 23, 2017).

European Commission, *European Commission Sets Up an Internal Task Force on Financial Technology*, European Commission Digital Single Market Blog Post (November 14, 2016).

European Commission, *Consumer Financial Services Action Plan: Better Products and More Choice for European Consumers*, European Commission Press Release (March 23, 2017).

European Commission, Consumer Financial Services Action Plan: Better Products, More Choice, COM(2017) 139 final, Brussels (March 23, 2017).

European Commission, *Consumer Financial Services Action Plan: Better Products, More Choice, Greater Opportunities - Frequently Asked Questions*, European Commission (March 23, 2017).

European Commission, *Consumer Financial Services Action Plan: Better Products, More Choice, Greater Opportunities - Factsheet*, European Commission (March 23, 2017).

European Commission, *Public Consultation on FinTech: A More Competitive and Innovative European Financial Sector*, European Commission (March 23, 2017).

European Commission, *Consultation Document Fintech: A More Competitive And Innovative European Financial Sector*, European Commission (March 23, 2017).

European Commission, *Specific Privacy Statement FinTech: A More Competitive and Innovative European Financial Sector Referred as "Consultation" in the Text*, European Commission (March 23, 2017).

European Commission, *European Commission Letter Addressed to the EBA regarding the European Commission Intention to Amend the Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Open Standards of Communication Submitted by the EBA in Accordance with Article 98(4) PSD2*, European Commission Letter (May 24, 2017).

European Parliament

European Parliament, *The Influence of Technology on the Future of the Financial Sector*, European Parliament Resolution on FinTech, TA-PROV(2017) 0211 (May 17, 2017).

European Parliament's Committee on Economic and Monetary Affairs (ECON), *EU Needs to Accelerate FinTech Development*, European Parliament's Committee on Economic and Monetary Affairs Press Release (April 25, 2017).

European Parliament's Committee on Economic and Monetary Affairs (ECON), *Report on FinTech: The Influence of Technology on the Future of the Financial Sector*, Report prepared by Cora van Nieuwenhuizen, European Parliament's Committee on Economic and Monetary Affairs (April 28, 2017).

European Parliament's Negotiation Team, *Letter from Markus Ferber and Antonio Tajani (on Behalf of the European Parliament's Negotiation Team) to the European Banking Authority on the Draft Regulatory Technical Standard under PSD2* (Brussels (BE), October 24, 2016).

E. Regulations and Policy Initiatives – The United Kingdom

Bank of England

Carney, Mark (Governor of the Bank of England), *Enabling the FinTech Transformation: Revolution, Restoration, or Reformation?*, Speech at the Lord Mayor's Banquet for Bankers and Merchants of the City of London at the Mansion House (London (UK), June 16, 2016).

Carney, Mark (Governor of the Bank of England), *The Promise of FinTech – Something New Under the Sun?*, Speech at the Deutsche Bundesbank G20 Conference on "Digitising finance, financial inclusion and financial literacy" (Wiesbaden (DE), January 25, 2017).

Carney, Mark (Governor of the Bank of England), *Building the Infrastructure to Realise FinTech's Promise*, Speech at the International FinTech Conference 2017, Old Billingsgate (London (UK), April 12, 2017).

Financial Service Authority (FSA) and the Bank of England, *A Review of Requirements for Firms Entering into or Expanding in the Banking Sector*, Financial Service Authority and the Bank of England Report (March 2013).

Competition and Markets Authority (CMA)

Competition and Markets Authority (CMA), *CMA Paves the Way for Open Banking Revolution*, Competition and Markets Authority Press Release (August 9, 2016).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Final Report*, Competition and Markets Authority (August 9, 2016).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Summary of Final Report*, Competition and Markets Authority (August 9, 2016).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Overview*, Competition and Markets Authority Press Release (August 9, 2016).

Competition and Markets Authority (CMA), *Making Banks Work Harder for You*, Competition and Markets Authority (August 9, 2016).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Final Report Corrigendum*, Competition and Markets Authority (August 11, 2016).

Competition and Markets Authority (CMA), *What Is Open Banking?*, Competition and Markets Authority Retail Banking Market Investigation: Infographics (2016).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation – Retail Banking Market Investigation Order 2017. Notice of Intention to Make an Order under Sections 161 And 165 of, and Schedule 10 to, the Enterprise Act 2002 and Public Consultation on the Draft Order*, Competition and Markets Authority (November 23, 2016).

Competition and Markets Authority (CMA), *Open Banking Transformation Moves a Step Closer*, Competition and Markets Authority Press Release (November 23, 2016).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Draft Order – Consultation. The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (November 23, 2016).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Draft Explanatory Note. The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (November 23, 2016).

Competition and Markets Authority (CMA), *Open Banking Revolution Moves Closer*, Competition and Markets Authority Press Release (February 2, 2017).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation - Retail Banking Market Investigation Order 2017. Notice of Making an Order Under Sections 138 and 161 of the Enterprise Act 2002 Issued under Section 165 of, and Schedule 10 to, the Enterprise Act 2002*, Competition and Markets Authority (February 2, 2017).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (February 2, 2017).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Explanatory Note. The Retail Banking Market Investigation Order 2017*, Competition and Markets Authority (February 2, 2017).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Summary of Responses to the Consultation on the Draft Retail Banking Market Investigation Order and Explanatory Note*, Competition and Markets Authority (February 2, 2017).

Competition and Markets Authority (CMA), *Retail Banking Market Investigation: Final Order Corrigendum*, Competition and Markets Authority (February 28, 2017).

Competition and Markets Authority (CMA), *Imran Gulamhuseinwala appointed Open Banking Implementation Trustee*, Competition and Markets Authority Press Release (April 13, 2017).

Financial Conduct Authority (FCA)

Financial Conduct Authority (FCA), *The FCA's Role under the Payment Services Regulations 2009 - Our Approach*, Financial Conduct Authority (June 2013).

Financial Conduct Authority (FCA), FCA Handbook - The Perimeter Guidance Manual (PERG) (to date).

Financial Conduct Authority (FCA), *A Review of Requirements for Firms Entering into or Expanding in the Banking Sector: One Year On*, Financial Conduct Authority Report (July 2014).

Financial Conduct Authority (FCA), *Project Innovate: Call for Input*, Financial Conduct Authority (July 2014).

Financial Conduct Authority (FCA), *Project Innovate: Call for Input - Feedback Statement*, Financial Conduct Authority (October 2014).

Financial Conduct Authority (FCA), *Innovation Hub Now Open for Business*, Financial Conduct Authority Press Release (October 28, 2014).

Financial Conduct Authority (FCA), *Call For Input: The FCA's Approach to the Current Payment Services Regime*, Financial Conduct Authority (February 2016).

Financial Conduct Authority (FCA), *Call For Input: The FCA's Approach to the Current Payment Services Regime*, Financial Conduct Authority Press Release (February 10, 2016).

Financial Conduct Authority (FCA), *Financial Conduct Authority's Regulatory Sandbox Opens to Applications*, Financial Conduct Authority Press Release (May 9, 2016).

Financial Conduct Authority (FCA), *Call For Input: The FCA's Approach to the Current Payment Services Regime – Feedback Statement*, Financial Conduct Authority Press Release (November 15, 2016).

Financial Conduct Authority (FCA), *Call For Input: The FCA's Approach to the Current Payment Services Regime – Feedback Statement*, Financial Conduct Authority (November 2016).

Financial Conduct Authority (FCA), *Implementation of the Revised Payment Services Directive (PSD2)*, Financial Conduct Authority Press Release (April 13, 2017).

Financial Conduct Authority (FCA), *Consultation Paper - Implementation of the Revised Payment Services Directive (PSD2): Draft Approach Document and Draft Handbook Changes*, Financial Conduct Authority CP 17/11 (April 2017).

Financial Conduct Authority (FCA), *Draft For Consultation: Payment Services and Electronic Money – Our Approach. The FCA's Role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011*, Financial Conduct Authority (April 2017).

Financial Conduct Authority (FCA), *The Payment Systems Regulator (PSR)'s Proposed Approach to Monitoring and Enforcing the Revised Payment Services Directive (PSD2)*, Financial Conduct Authority (April 2017).

HM Treasury (HM Treasury)

HM Treasury, *Banking Reform: Delivering Stability and Supporting a Sustainable Economy*, HM Treasury (June 2012).

HM Treasury (HMT), *Data Sharing and Open Data for Banks*, HM Treasury Press Release (December 3, 2014)

HM Treasury (HTM), *Data Sharing and Open Data in Banking: Call for Evidence*, HM Treasury Press Release (January 28, 2015).

HM Treasury (HTM), *Call for Evidence on Data Sharing and Open Data in Banking*, HM Treasury (January 28, 2015 – updated March 18, 2015).

HM Treasury (HTM), *Data Sharing and Open Data in Banking: Response to the Call for Evidence*, HM Treasury (March 18, 2015).

HM Treasury, *A Better Deal: Boosting Competition to Bring Down Bills for Families and Firms*, HM Treasury Report (November 2015).

HM Treasury (HMT), *Implementation of the Revised EU Payment Services Directive (PSDII)*, HM Treasury Press Release (February 2, 2017).

HM Treasury (HMT), *Draft Impact Assessment on the Implementation of the EU Payment Services Directive II*, HM Treasury (February 2017).

HM Treasury (HMT), *Implementation of the Revised EU Payment Services Directive II (and Draft Regulations (Annex B))*, HM Treasury (February 2017).

Implementation Entity Steering Group (IESG)

Implementation Entity Steering Group (IESG), *Stakeholder Event: Developing An Open API Standard, Open Data and Data Sharing Out of the CMA Market Investigation – An Early Opportunity to Share Views, Thinking and Progress to Date. Event Summary*, Implementation Entity Steering Group (September 7, 2016).

Implementation Entity Steering Group (IESG), *Update to CMA – Executive Summary*, Implementation Entity Steering Group (October 2016).

Open Banking Development Group (OBDG)

Open Banking Development Group (OBDG), *Open Banking Development Group Membership Details*, Open Banking Development Group (2016).

Open Banking Development Group (OBDG), *Vision and Values*, Open Banking Development Group (2016).

Open Banking Limited (Open Banking Implementation Entity (OBIE))

Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Implementation Trustee Appointed to Lead Open Banking Revolution*, Open Banking Limited Press Release (October 31, 2016).

Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Open Banking Advisory Group Heads Named*, Open Banking Limited Press Release (December 15, 2016).

Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Platform for Distributing Bank Product, Branch & ATM Data Available*, Open Banking Limited Press Release (March 13, 2017).

Open Banking Limited (Open Banking Implementation Entity (OBIE)), *CMA Appoints New Trustee for Open Banking Implementation Entity*, Open Banking Limited Press Release (April 13, 2017).

Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Open Banking Forms Collaboration With OpenID Foundation*, Open Banking Limited Press Release (May 17, 2017).

Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Atom Bank CEO Joins Open Banking Initiative as Challenger Bank Representative*, Open Banking Limited Press Release (June 30, 2017).

Open Banking Limited (Open Banking Implementation Entity (OBIE)), *Open Banking Launches Account Information and Payment Initiation API Specifications*, Open Banking Limited Press Release (July 5, 2017).

Open Banking Working Group (OBWG)

Open Banking Working Group (OBWG), *Open Banking Working Group (OBWG) Terms of Reference*, Open Banking Working Group (September 2015).

Open Banking Working Group (OBWG), *The Open Banking Standard. Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation*, Open Banking Working Group (February 2016).

Open Data Institute (ODI)

Open Data Institute (ODI) and Fingleton Associates, *Data Sharing and Open Data for Banks - A Report for HM Treasury and Cabinet Office*, Open Data Institute (ODI) and Fingleton Associates (September 2014).

Open Data Institute (ODI), *Introducing the Open Banking Standard. Helping Customers, Banks and Regulators Take Banking into a Truly 21st-Century, Connected Digital Economy*, Open Data Institute (2016).

Open Data Institute (ODI), *Announcing the Open Banking Development Group*, Open Data Institute Press Release (August 2, 2016).

Payment Systems Regulator (PSR)

Payment Systems Regulator (PSR), *The PSR's Proposed Approach to Monitoring and Enforcing the Revised Payment Services Directive (PSD2)*, Payment Systems Regulator (April 2017).

Prudential Regulation Authority (PRA)

Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), *New Bank Start-up Unit Launched by the Financial Regulators*, Prudential Regulation Authority and Financial Conduct Authority Press Release (January 21, 2016).

Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), *New Bank Start-Up Unit. What You Need to Know From the UK's Financial Regulator*, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) Guide (March 2017).

F. Regulations and Policy Initiatives – The United States

Consumer Financial Protection Bureau (CFPB)

Consumer Financial Protection Bureau (CFPB), *CFPB Launches Project Catalyst to Spur Consumer-Friendly Innovation*, Consumer Financial Protection Bureau Press Release (November 14, 2012).

Consumer Financial Protection Bureau (CFPB), Policy on No-Action Letters; Information Collection, 81 Fed. Reg. 8,686 (February 2, 2016).

Consumer Financial Protection Bureau (CFPB), *CFPB Finalizes Policy to Facilitate Consumer-Friendly Innovation*, Consumer Financial Protection Bureau Press Release (Washington (DC), February 18, 2016).

Consumer Financial Protection Bureau (CFPB), *Project Catalyst Report: Promoting Consumer-Friendly Innovation*, Consumer Financial Protection Bureau Press Release (October 24, 2016).

Consumer Financial Protection Bureau (CFPB), *Compliance Bulletin and Policy Guidance 2016-02, Service Providers*, Consumer Financial Protection Bureau (October 31, 2016).

Consumer Financial Protection Bureau (CFPB), *Project Catalyst Report: Promoting Consumer-Friendly Innovation*, Consumer Financial Protection Bureau Innovation Insights (October 2016).

Consumer Financial Protection Bureau (CFPB), Request for Information Regarding Consumer Access to Financial Records, Docket No. CFPB 2016-0048 (November 14, 2016).

Consumer Financial Protection Bureau (CFPB), Comments Received in Response to the Request for Information Regarding Consumer Access to Financial Records are available at https://www.regulations.gov/docketBrowser?rpp=50&so=DESC&sb=commentDueDate&po=0&D=CFPB-2016-0048.

Selected Responses:

American Bankers Association, Response to Request for Information Regarding Consumer Access to Financial Records, Docket No.: CFPB-2016-0048 (February 21, 2017).

BBVA Compass, Response to Request for Information Regarding Consumer Access to Financial Records ("RFI") Docket No. CFPB-2016-0048 (February 17, 2017).

Capital One, Response to CFPB Request for Information Regarding Consumer Access to Financial Records, Docket No. Bureau-2016-0048 (February 21, 2017).

Center for American Progress (CAP), Response to Request for Information on Consumer Access to Financial Records (Docket No. CFPB-2016-0048) (February 21, 2017).

Center for Financial Services Innovation (CFSI), Response to CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records (February 21, 2017).

Commonwealth, Response to CFPB-2016-0048, Request for Information Regarding Consumer Access to Financial Records (February 21, 2017).

Consumer Bankers Association (CBA), Response to Request for Information Regarding Consumer Access to Financial Records, Docket No.: CFPB-2016-0048 / Document No.: 2016-28086 (February 21, 2017).

Consumer Financial Data Rights Group (CFDR Group), CFDR Group Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 (February 21, 2017).

Earnest, Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048 (February 21, 2017).

Electronic Transactions Association, Comments on Request for Information Regarding Consumer Access to Financial Records, Docket No. CFPB–2016–0048 (February 21, 2017).

Envestnet Yodlee, Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records, Docket No.: CFPB-2016-0048 (February 21, 2017).

Fidelity Investments, Response to Request for Information Regarding Consumer Access to Financial Records; Docket No. CFPB-2016-0048 (February 21, 2017).

Financial Innovation Now (FIN), Response to Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 (February 21, 2017).

Financial Services Roundtable ("FSR") and the FSR's Technology Policy Division – BITS, Response to CFPB Request for Information Regarding Consumer Access to Financial Records, Docket No. CFPB-2016-0048 (February 21, 2017).

Heartland Credit Union Association, Response to Request for Information Regarding Consumer Access to Financial Records ("RFI") Docket No. CFPB-2016-0048 (February 17, 2017).

Independent Community Bankers of America, Response to Docket No. CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records (February 21, 2017).

Kabbage, Response to Request for Information Regarding Consumer Access to Financial Records, CFPB–2016–0048 (February 21, 2017).

Marketplace Lending Association, Response to Consumer Financial Protection Bureau Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048 (February 21, 2017).

National Consumers Law Center, Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048 (February 21, 2017).

Personal Capital, Response to the Consumer Financial Protection Bureau's Request for Information Regarding Consumer Access to Financial Records, Personal Capital (February 21, 2017).

Plaid Technologies, Response to CFPB regarding Consumer Access to Financial Records Docket No. CFPB-2016-0048 (February 21, 2017).

The Clearing House Association, Request for Information Regarding Consumer Access to Financial Records, Docket No. Bureau–2016–0048 (February 21, 2017).

Tech:NYC, Comments to the Consumer Financial Protection Bureau Docket No.: CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records (February 21, 2017).

Upstart Network, Response to CFPB Docket No. CFPB-2016-0048 Requests for Information: Consumer Access to Financial Records (February 21, 2017).

Cordray, Richard (CFPB Director), *Prepared Remarks* of CFPB Director Richard Cordray at Money 20/20 (Las Vegas (NV), October 23, 2016).

Cordray, Richard (CFPB Director), *Prepared Remarks* to Be Delivered at the Field Hearing on Consumer Access to Financial Records Salt Lake City (Salt Lake City (UT), November 17, 2016).

Commodity Futures Trading Commission (CFTC)

Bowen, Sharon Y. (CFTC Commissioner), Statement on the Launch of LabCFTC (May 17, 2017).

Commodity Futures Trading Commission (CFTC), *CFTC Launches LabCFTC as Major FinTech Initiative*, Commodity Futures Trading Commission Press Release (Washington (DC), May 17, 2017).

Giancarlo, Christopher (CFTC Acting Chairman), *Announcing Launch of LabCFTC*, Acting Chairman's Keynote Remarks at the New York FinTech Innovation Lab Annual Reception (New York (NY), May 17, 2017).

Department of the Treasury

Department of the Treasury, *Opportunities and Challenges in Online Marketplace Lending*, Department of the Treasury White Paper (May 10, 2016).

Federal Deposit Insurance Corporation (FDIC)

Federal Deposit Insurance Corporation (FDIC), FIL-44-2008, *Guidance for Managing Third-Party Risk*, Federal Deposit Insurance Corporation (June 6, 2008).

Federal Deposit Insurance Corporation (FDIC), FIL-127-2008, *Guidance on Payment Processor Relationships*, Federal Deposit Insurance Corporation (Revised July 2014).

Federal Deposit Insurance Corporation (FDIC), FIL-3-2012, *Payment Processor Relationships Revised Guidance*, Federal Deposit Insurance Corporation (Revised July 2014).

Federal Deposit Insurance Corporation (FDIC), FIL-43-2013, *Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities*, Federal Deposit Insurance Corporation (Revised July 2014).

Federal Reserve System

Basinger, Tracy (Group VP of Financial Institution Supervision and Credit (FISC) Federal Reserve Bank of San Francisco), *Is Fintech Changing Banking Supervision?*, San Francisco Fed Blog (July 29, 2016).

Board of Governors of the Federal Reserve System, *Guidance on Managing Outsourcing Risk*, Board of Governors of the Federal Reserve System SR Ltr. 13-19 / CA 13-21 (December 5, 2013).

Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), Joint Advance Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards, Federal Reserve System Docket No. R-1550 and RIN 7100-AE-61, OCC Docket ID OCC-2016-0016 and RIN 1557-AE06, FDIC RIN 3064-AE45 (October 19, 2016).

Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), Comments Submitted in Response to the Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards are available at https://www.federalreserve.gov/apps/foia/ViewComments.aspx?doc_id=R%2D1550&doc_ver=1.

Selected Responses:

Amazon Web Services, Commentary to the Advance Notice of Proposed Rulemaking (ANPR) on Enhanced Cyber Risk Management Standards (February 17, 2017).

American Bankers Association, Response to Enhanced Cyber Risk Management Standards, (Fed) Docket No. R- 1550 and RIN 7100-AE61, (OCC) Docket ID OCC-2016-0016, (FDIC) RIN 3064- AE45 (February 17, 2017).

BSA I The Software Alliance (BSA), Comments on the Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (February 17, 2017).

Business Roundtable, Comments on the Enhanced Cyber Risk Management Standards Joint Advance Notice of Proposed Rule Making, Dkt. R 1550, RIN 7100- AE- 61 (Federal Reserve System), Dkt. ID OCC-2016-0016, RIN 1557- AE06 (OCC), RIN 3064-AE45 (FDIC) (February 13, 2017).

CME Group, Depository Trust & Clearing Corporation and Options Clearing Corporation, Joint Comment on the Enhanced Cyber Risk Management Standards Advance Notice of Proposed Rulemaking, Docket No. R-1550 RIN 7100-AE-61 (January 17, 2017).

Consumer Financial Data Rights Group (CFDR Group), CFDR Group Comment Letter to “Enhanced Cyber Risk Management Standards” Docket ID OCC-2016-0016 (February 17, 2017).

Envestnet Yodlee, Comment Letter to "Enhanced Cyber Risk Management Standards' Docket ID OCC-2016-0016 (February 17, 2017).

Financial Services Roundtable/BITS (FSR/BITS), Comments on Joint Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (February 16, 2017).

Information Technology Industry Council (ITI), Comments in Response to Banking Agencies' Advanced Notice of Proposed Rulemaking regarding Enhanced Cyber Risk Management Standards (February 17, 2017).

Institute of International Bankers (IIB), Comments on Joint Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (February 17, 2017).

MasterCard, Response to Request of Comments on the Joint Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards - Federal Reserve System Docket No. R-1550 and RIN 7100-AE-61, OCC Docket ID OCC-2016-0016 and RIN 1557-AE06, FDIC RIN 3064-AE45 (January 17, 2017).

Microsoft, Comments on Joint Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk Management Standards (February 17, 2017).

North American Chief Risk Officers Council, Comments on Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (January 17, 2017).

The Clearing House Association and The Clearing House Payments Company, Comments on the Joint Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (Federal Reserve Docket No. R- 1550 and RIN 7100-AE 61; OCC Docket ID OCC-2016-0016; FDIC RIN 3064-AE45) (February 17, 2017).

The Risk Management Association, Response to Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards (the "ANPR"): Office of the Comptroller of the Currency 12 CFR Part

30, Docket No. OCC-2016-0016, RIN 1557-AE06; Federal Reserve System, 12 CFR Chapter II, Docket No. R-1550, RIN 7100 AE-61; Federal Deposit Insurance Corporation, 12 CFR Part 364, RIN 3064-AE45 (January 13, 2017).

VivoSecurity, Comments on Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards; Federal Reserve Docket No. R-1550, RIN 7100-AE-61; OCC Docket ID OCC-2016-0016; FDIC RIN 3064- AE45 (February 17, 2017).

Board of Governors of the Federal Reserve System (FED), Office of the Comptroller of the Currency (OCC), and Federal Deposit Insurance Corporation (FDIC), Proposed Rulemaking on Enhanced Cyber Risk Management Standards – Extension of Comment Period, Joint Press Release (January 13, 2017).

Brainard, Lael (Federal Reserve Board Governor), *The Opportunities and Challenges of Fintech*, Remarks at the Conference on Financial Innovation at the Board of Governors of the Federal Reserve System (Washington (D.C.), December 2, 2016).

Brainard, Lael (Federal Reserve Board Governor), *Where Do Banks Fit in the Fintech Stack?*, Speech Delivered at the Northwestern Kellogg Public-Private Interface Conference on "New Developments in Consumer Finance: Research & Practice," Chicago (IL) (April 28, 2017).

Canova, Robert (Senior Financial Analyst at Federal Reserve Bank of Atlanta), *Fintech Companies: Banks' Allies or Rivals?*, Federal Reserve Bank of Atlanta View Point – Banking and Finance (March 15, 2016).

Consumer Compliance Outlook, *Perspectives on Fintech: A Conversation with Governor Lael Brainard*, Consumer Compliance Outlook - Federal Reserve System Publication, Issue No. 3, pp. 1, 12-14 (2016).

Curran, Teresa (Then Executive Vice President and Division Director, Financial Institution Supervision and Credit, Federal Reserve Bank of San Francisco), *Tailoring, Fintech, and Risk Culture: The Talk of the (Community Banking) Town*, Speech Delivered at the Western Independent Bankers Annual Conference for Bank Presidents, Senior Officers & Directors (Waikoloa (HI), April 4, 2016).

Cunnan, Teresa (Executive Vice President and Division Director, Financial Institution Supervision and Credit, Federal Reserve Bank of San Francisco), *Fintech: Balancing the Promise and Risks of Innovation*, Consumer Compliance Outlook - Federal Reserve System Publication, Issue No. 3, pp. 2-4 (2016).

Harker, Patrick T. (President and Chief Executive Officer Federal Reserve Bank of Philadelphia), *Fintech: Revolution or Evolution?*, Remarks at the University of Pennsylvania School of Engineering and Applied Science (Philadelphia (PA), April 3, 2017).

Marder, Tim (Fintech Senior Supervisory Analyst, Financial Institution Supervision and Credit Division, Federal Reserve Bank of San Francisco), *Fintech for the Consumer Market: An Overview, Consumer Compliance Outlook* - Federal Reserve System Publication, Issue No. 3, pp. 4-5 (2016).

Williams, John C. (President and CEO, Federal Reserve Bank of San Francisco), *Fintech: The Power of the Possible and Potential Pitfalls*, Presentation Delivered at the LendIt USA 2016 Conference (San Francisco (CA), April 12, 2016).

Federal Trade Commission (FTC)

Federal Trade Commission, *Paper, Plastic ... or Mobile? An FTC Workshop on Mobile Payments*, Federal Trade Commission Report (March 2013).

Federal Trade Commission, *Mobile Cramming*, Federal Trade Commission Report (July 2014).

Federal Trade Commission, *What's The Deal? An FTC Study on Mobile Shopping Apps*, Federal Trade Commission Report (August 2014).

Federal Trade Commission, *Internet of Things. Privacy & Security in a Connected World*, Federal Trade Commission (January 2015).

Federal Trade Commission, *Big Data. A Tool for Inclusion or Exclusion? Understanding the Issues*, Federal Trade Commission Report (January 2016).

Office of the Comptroller of the Currency (OCC)

Conference of State Bank Supervisors (CSBS) v. Office of the Comptroller of the Currency and Thomas J. Curry in his official capacity as Comptroller of the Currency, Complaint for Declaratory and Injunctive Relief, Civil Action No. 1:17-CV-00763 (JEB) (April 26, 2017).

Conference of State Bank Supervisors (CSBS) v. Office of the Comptroller of the Currency and Keith A. Noreika, in his official capacity as Acting Comptroller of the Currency, Defendants' Motion to Dismiss for Lack of Jurisdiction and Failure to State a Claim, Civil Action No. 1:17-CV-00763 (JEB) (August 2, 2017).

Conference of State Bank Supervisors (CSBS) v. Office of the Comptroller of the Currency and Keith A. Noreika, in his official capacity as Acting Comptroller of the Currency, Memorandum of Points and Authorities in Support of Defendants' Motion to Dismiss for Lack of Jurisdiction and Failure to State a Claim, Civil Action No. 1:17-CV-00763 (JEB) (August 2, 2017).

Curry, Thomas J. (Then Comptroller of the Currency), *Remarks* Before the Federal Home Loan Bank of Chicago (Chicago (IL), August 7, 2015).

Curry, Thomas J. (Then Comptroller of the Currency), *Remarks* Before the Harvard Kennedy School's New Directions in Regulation Seminar (Cambridge (MA), March 31, 2016).

Curry, Thomas J. (Then Comptroller of the Currency), *Remarks* Before the American Banker Retail Banking Conference (Las Vegas (NV), April 7, 2016).

Curry, Thomas J. (Then Comptroller of the Currency), *Remarks* Before the Marketplace Lending Policy Summit 2016 (Washington (DC), September 13, 2016).

Curry, Thomas J. (Then Comptroller of the Currency), *Remarks* Before Chatham House 'City Series' Conference "The Banking Revolution: Innovation, Regulation & Consumer Choice" (London (UK), November 3, 2016).

Curry, Thomas J. (Then Comptroller of the Currency), *Remarks* Regarding Special Purpose National Bank Charters for Fintech Companies Georgetown University Law Center (Washington (DC), December 2, 2016).

Curry, Thomas J. (Then Comptroller of the Currency), *Remarks* at LendIt USA 2017 (New York (NY), March 6, 2017).

Maria T. Vullo, in her official capacity as Superintendent of the New York State Department of Financial Services, v. Office of the Comptroller of the Currency and Keith A. Noreika, in his official capacity as Acting Comptroller of the Currency, Complaint for Declaratory and Injunctive Relief, Civil Action No. 1:17-CV-03574 (NRB) (May 12, 2017).

Noreika, Keith A. (Acting Comptroller of the Currency), *Remarks* before the Exchequer Club (Washington (DC), July 19, 2017).

Office of the Comptroller of Currency (OCC), OCC Bulletin 2001-12, Bank-Provided Account Aggregation Services (February 28, 2001).

Office of the Comptroller of the Currency (OCC), *OCC Bulletin 2013-29, Third-Party Relationships - Risk Management Guidance*, Office of the Comptroller of the Currency (October 30, 2013).

Office of the Comptroller of the Currency (OCC), *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*, Office of the Comptroller of the Currency White Paper (March 2016).

Office of the Comptroller of the Currency (OCC), *OCC Forum on Responsible Innovation in the Federal Banking System – Videos of the Forum*, Office of the Comptroller of the Currency (June 23, 2016).

Office of the Comptroller of the Currency (OCC), *OCC Issues Responsible Innovation Framework*, Office of the Comptroller of the Currency Press Release (Washington (DC), October 26, 2016).

Office of the Comptroller of the Currency (OCC), *Recommendations and Decisions for Implementing a Responsible Innovation Framework*, Office of the Comptroller of the Currency White Paper (October 2016).

Office of the Comptroller of the Currency (OCC), *OCC To Consider Fintech Charter Applications, Seeks Comment*, Office of the Comptroller of the Currency Press Release (Washington (DC), December 2, 2016).

Office of the Comptroller of the Currency (OCC), *Exploring Special Purpose National Bank Charters for Fintech Companies*, Office of the Comptroller of the Currency White Paper (December 2016).

Office of the Comptroller of the Currency (OCC), *OCC Bulletin 2017-7, Third-Party Relationships - Supplemental Examination Procedures*, Office of the Comptroller of the Currency (January 24, 2017).

Office of the Comptroller of the Currency (OCC), *Semiannual Risk Perspective - From the National Risk Committee*, Office of the Comptroller of the Currency (Spring 2017).

Office of the Comptroller of the Currency (OCC), *OCC Issues Draft Licensing Manual Supplement for Evaluating Charter Applications From Financial Technology Companies, Will Accept Comments Through April 14*, Office of the Comptroller of the Currency Press Release (Washington (DC), March 15, 2017).

Office of the Comptroller of the Currency (OCC), *Evaluating Charter Applications From Financial Technology Companies*, *Office of the Comptroller of the Currency's Licensing Manual Draft Supplemental,* Office of the Comptroller of the Currency (March 2017).

Office of the Comptroller of the Currency (OCC), *OCC Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies*, Office of the Comptroller of the Currency Paper (March 2017).

Office of the Comptroller of the Currency (OCC), *OCC Announces One-on-One Industry Meetings as Part of Office of Innovation Office Hours*, Office of the Comptroller of the Currency Press Release (Washington (DC), April 13, 2017).

Office of the Comptroller of the Currency (OCC), *OCC Bulletin 2017-21, Third-Party Relationships - Frequently Asked Questions to Supplement OCC Bulletin 2013-29*, Office of the Comptroller of the Currency (June 7, 2017).

Office of the Comptroller of the Currency (OCC), *OCC to Hold Innovation Office Hours in New York*, Office of the Comptroller of the Currency Press Release (Washington (DC), June 19, 2017).

Securities and Exchange Commission (SEC)

Piwowar, Michael (Then SEC Commissioner), *Statement* at the Financial Technology Forum (Washington (DC), November 14, 2016).

Piwowar, Michael (SEC Acting Chairman), *Remarks* before the 27th International Institute for Securities Market Growth and Development (Washington (DC), March 27, 2017).

Securities and Exchange Commission (SEC), *SEC to Hold Forum to Discuss Fintech Innovation in the Financial Services Industry. Forum to be Held on November 14 at SEC Headquarters*, Securities and Exchange Commission Press Release (Washington (DC), September 27, 2016).

Securities and Exchange Commission (SEC), *SEC Announces Agenda, Panelists for Nov. 14 Fintech Forum*, Securities and Exchange Commission Press Release (Washington (D.C.), November 3, 2016).

Securities and Exchange Commission (SEC), *Fintech Forum - The Evolving Financial Marketplace*, Fintech Forum Transcript (Washington (DC), November 14, 2016).

Securities and Exchange Commission (SEC), *SEC Announces 2017 Examination Priorities. New Areas of Focus Include Electronic Investment Advice, Money Market Funds, and Senior Investors*, Securities and Exchange Commission Press Release (Washington (DC), January 12, 2017).

Securities and Exchange Commission (SEC), *Examination Priorities for 2017*, Office of Compliance Inspections and Examinations (OCIE) of the Securities and Exchange Commission (SEC) (January 12, 2017).

White, Mary Jo (Then SEC Chairperson), *Keynote* Address at the SEC-Rock Center on Corporate Governance Silicon Valley Initiative (Stanford (CA), March 31, 2016).

White, Mary Jo (Then SEC Chairperson), *Opening Remarks* at the Fintech Forum (Washington (DC), November 14, 2016).