Stanford – Vienna
Transatlantic Technology Law Forum

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

European Union Law Working Papers

No. 26

Signed, Sealed, (Justice) Delivered? E-Signature Law and Consumer Protection Within the European Union

Jacob Lundqvist

2017

European Union Law Working Papers

edited by Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law 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 working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, 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

Jacob Lundqvist is currently pursuing a joint J.D./LL.M. degree at Stanford Law School and the University of Vienna. He received a B.A. *summa cum laude* in Ethics, Politics & Economics from Yale University in 2015, where he was a member of Phi Beta Kappa. His research interests include international trade law, corporate governance, and securities regulation.

General Note about the Content

Suggested Citation

This European Union Law Working Paper should be cited as:
Jacob Lundqvist, Signed, Sealed, (Justice) Delivered? E-Signature Law and Consumer Protection Within the European Union, Stanford-Vienna European Union Law Working Paper No. 26, http://ttlf.stanford.edu.

Copyright

Abstract

An integrated online marketplace constitutes an important step in developing the EU's internal market. But growth online requires that consumers feel confident that the technology they use for online transactions is secure. This Article identifies a missing piece in the European Union's legal framework for protecting consumers in online markets. In developing its strategy for a Digital Single Market within Europe, the European Commission has taken inadequate measures to protect consumers against online fraud. In particular, the current framework for authenticating electronic signatures provides limited protection for consumers whose e-signatures are forged by third parties. By placing the burden of proof on consumers in disputes over forged e-signatures, the law shifts the legal onus away from technology providers—the actors in the best position to identify and rectify breaches. While the recently enacted EU regulation on electronic signatures reverses the burden of proof against providers that qualify for the EU's highest certification for online security, the regulation establishes an opt-in system for this status. Providers currently have insufficient legal or economic incentives to subject themselves to more robust supervision. Instead of making stricter procedural requirements a voluntary option for provides of e-signatures technology, a new and improved EU law on electronic signatures should shift the burden of proof onto service providers to better allocate the costs of security breaches between providers and consumers.

Introduction 2

I. E-Signature Law in the European Union 6

A. The Electronic Signatures Directive 6

B. e-IDAS 9

II. Incentive Issues Under e-IDAS 12

III. Alternative Modes of Regulation 17

Conclusion 18

Introduction

Establishing the internal market counts among the greatest achievements in the European Union's sixty-year history.[1] By prohibiting quantitative and other restrictions on imports, exports, and goods in transit, the Treaty on the Functioning of the European Union (TFEU) laid the foundation for an internal €3 trillion market in goods alone.[2] So far, however, the gains in trade have largely remained offline. A vital step in furthering economic integration within the Union would be to establish a unified market for digital commerce. Currently, only seven percent of small and medium-sized enterprises within the Union engage in cross-border sales.[3] Tearing down digital borders could contribute over €400 billion annually to the EU's economy, potentially growing the bloc's GDP by up to €2.5 trillion by 2025.[4] Apart from boosting sales of goods between Member States, a more integrated digital economy could also reduce the EU's dependence on U.S.-based providers within the digital services sector.[5] Opening up new frontiers for trade in both goods and services thus promises to expand the EU's share of the worldwide digital marketplace beyond its current four percent, providing a much-needed boost to the moribund European economy.[6]

---

[1] Dominik Hanf, *Legal Concept and Meaning of the Internal Market*, *in* THE EU INTERNAL MARKET IN COMPARATIVE PERSPECTIVE: ECONOMIC, POLITICAL AND LEGAL ANALYSES (Jacques Pelkmans et al. eds., 2008) ("Whatever precise concept of the internal market one adopts, it arguably remains the European Union's main and most wide-ranging objective while forming its political, economic and legal backbone."); *Fact Sheets on the European Union: The Internal Market*, EUROPEAN PARLIAMENT (last visited Jan. 21, 2017), http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=theme3.html ("The single market is the EU's greatest achievement.").

[2] Consolidated Version of the Treaty on the Functioning of the European Union arts. 34-36, Oct. 26, 2012, 2012 O.J. (C 326) 47 [hereinafter TFEU]; *International Trade in Goods*, EUROSTAT (last visited Jan. 21, 2017), http://ec.europa.eu/eurostat/statistics-explained/index.php/International_trade_in_goods#Intra-EU_trade.

[3] *Better Access for Consumers and Business to Online Goods*, EUROPEAN COMM'N (Sept. 14, 2016), https://ec.europa.eu /digital-single-market/node/78515.

[4] *Digital Single Market*, EUROPEAN COMM'N, https://ec.europa.eu/priorities/digital-single-market_en (last visited Jan. 13, 2017); MCKINSEY, DIGITAL EUROPE: PUSHING THE FRONTIER, CAPTURING THE BENEFITS 25 (2016).

[5] MCKINSEY, *supra* note 4, at 18-19.

[6] European Commission, Why We Need a Digital Single Market 1 (2015), http://ec.europa.eu/priorities/sites/beta-political/files/dsm-factsheet_en.pdf.

Recognizing the potential benefits of an integrated online market, the European Commission introduced its plan for a "Digital Single Market" in 2015. The Commission organized its strategy around three pillars:

> (1) better access for consumers and businesses to digital goods and services across Europe (2) creating the right conditions and a level playing field for digital networks and innovative services to flourish; (3) maximising the growth potential of the digital economy.[7]

The pillars are further subdivided into sixteen "key actions" the Commission pledged to undertake before the end of 2016.[8] Key actions under the first pillar include streamlining EU rules on consumer protection across all Member States and supporting more rapid and consistent enforcement.[9] Among the key actions identified under the second pillar are "reinforc[ing] trust and security in digital services, notably concerning the handling of personal data" and collaborating with industry actors on cybersecurity.[10] The Commission mentions reviewing the e-Privacy Directive as key to fulfilling its goals on this point.[11]

Notably, however, the action plan does not identify specific legislative initiatives to enhance antifraud protection for consumers online. This omission is odd, given that electronic signatures will play a key part in the development of a well-functioning online market. E-signatures allow EU citizens to enter into agreements with the same legal force as documents signed by hand.[12] Such solutions, if implemented correctly, could reduce transaction costs between customers and vendors in the online marketplace, thereby contributing to further growth. For such gains to materialize, however, EU citizens must feel confident that their e-signature is safe and that they will not face unreasonable obstacles to getting their money back in

[7] *A Digital Single Market for Europe: Commission Sets Out 16 Initiatives to Make It Happen*, EUROPEAN COMM'N (May 6, 2015), http://europa.eu/rapid/press-release_IP-15-4919_en.htm.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *See* discussion *infra* Part I.

case their identification is forged to create fraudulent transactions. Rather than emphasizing the importance of robust protection for users of e-signatures, the Commission's strategy plan mentions e-signatures only as a technology that should become interoperable to support the third pillar's goal of maximizing growth potential.[13]

With a recently enacted regulation on e-signatures in place, the Commission may not have perceived a review of its laws in this area as a particularly urgent task in connection with developing its digital strategy. In doing so, however, the Commission left intact a regulation that places a heavy evidentiary burden on individual consumers vis-à-vis providers of e-signature technology. The "Regulation on electronic identification and trust services for electronic transactions in the internal market," commonly referred to as "e-IDAS," entered into effect on July 1, 2016.[14] Among other things, this regulation creates two categories of e-signatures technology providers. Only the providers that choose to qualify for the most secure category bear the burden of proof against a consumer who claims her identity has been fraudulently appropriated. Since compliance with the requirements of the most advanced security classification is voluntary, however, providers can design solutions that fit within less demanding categories while still advertising their services as "EU-qualified." Moreover, because the e-IDAS regulation refrained from interfering with national determinations regarding liability—including the burden of proof—it left intact a hodgepodge of national laws that frequently disadvantage consumers in disputes with providers. The lack of protection for consumers that fall victim to fraud online risks undermining consumer confidence, a factor identified by the Commission as key to developing a robust digital marketplace.[15]

---

[13] EUROPEAN COMM'N, *supra* note 7.
[14] Regulation 910/2014, O.J. (L 257) 73 [hereinafter e-IDAS].
[15] Amelia Andersdotter & Björn Lundgren, *Ändra Lagen så att Företagen Bär Risken för Lånebedrägerier*, DAGENS NYHETER (Jan. 12, 2017), http://www.dn.se/debatt/andra-lagen-sa-att-foretagen-bar-risken-for-lanebedragerier.

This Article proceeds in three parts. Part I provides an overview of the development of electronic signatures law within the European Union. Legislation in this area has come about in two rounds: First, through the Electronic Signatures Directive, enacted in 1999. Second, through e-IDAS, the Union's current set of laws that entered into effect on July 1, 2016. Part II examines the implications of e-IDAS for industry actors as well as national legislators. While some technology providers have rushed to update their services to comply with the highest standards under e-IDAS, other prominent industry actors still generate electronic signatures for their customers that provide less protection in the event of a breach. Moreover, even in countries where procedural rules are more favorable to consumers, e-IDAS permits e-signature providers to limit their liability through contractual clauses, thereby evading responsibility even where fault has been proven.

Part III identifies legislative solutions in other areas of EU law that could be incorporated in future e-signature regulations to enhance consumer protection. The EU has acted more forcefully against other service providers, for example by placing the burden of proof on digital content suppliers for showing that defects in such content arose only after delivery to the consumer.[16] The burden shifts onto consumers only if they fail to cooperate with the supplier in its investigation of the transaction.[17] Furthermore, regulations of the notary profession provide a useful alternative model for regulating providers in the e-signatures industry. In many Member States, notaries assume legal responsibility for the contents of documents they help create and face significant personal liability for breaching their duties.[18] The Article concludes by analyzing whether it would be desirable to adopt similarly strict liability standards to regulate providers of e-signatures technology across the European Union.

[16] *See infra* footnote 72 and accompanying text.
[17] *Id.*
[18] *See infra* footnote 81 and accompanying text.

I. E-Signatures Law in the European Union

The development of e-signatures law within the European Union demonstrates how the EU as an institution has different tools at its disposal to influence Member States' policies and lawmaking. Over two rounds of legislating on e-signatures, the EU went from seeking *harmony* between national laws by means of a directive to mandating *uniformity* across all Member States through the regulatory provisions in e-IDAS. But while the overall legal framework has become stronger over time, consumer protection has weakened. From a procedural perspective, EU law shifted from initially siding with consumers to later allowing providers to use significant loopholes to protect themselves in dispute scenarios. This backtracking left consumers with the burden of proving that they were not responsible for e-signatures entered in their name against industry actors that have significantly greater resources and information about risks and causes of a breach.

A. The Electronic Signatures Directive

The EU began weighing an e-signatures initiative in the late 1990s. Germany and Italy had been the first countries to develop domestic laws addressing consumer fraud related to e-identification tools, and others soon followed.[19] Because leaving Member States with the authority to craft legal solutions would lead to a plethora of standards, the Commission intervened to create a single framework that would facilitate greater cross-border commerce.[20] The drafters of the initial directive on e-signatures looked to model regulations developed by the United Nations Commission on International Trade Law (UNCITRAL).[21] In 1996, UNCITRAL developed the Model Law on Electronic Commerce to encourage greater global uniformity in the

[19] Lance C. Ching, *Electronic Signatures: A Comparison of American and European Legislation*, 25 HASTINGS INT'L & COMP. L. REV. 199, 220 (2002).
[20] Miriam A. Parmentier, *Electronic Signatures*, 6 COLUM. J. EUR. L. 251, 251 (2000).
[21] Stephen E. Blythe, *Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security*, 11 RICH. J.L. & TECH. 1, 5 (2004-2005).

regulation of e-commerce.[22] This influence is most evident in the EU directive's emphasis on striving for interoperability not only within the Union, but also with nonmember states.[23] Such a global vision forms a key component of the UNCITRAL framework.

In 1999, the EU enacted the Electronic Signatures Directive.[24] Article 1 of the Directive established as its purpose "to facilitate the use of electronic signatures and to contribute to their legal recognition."[25] The Directive made clear that e-signatures cannot be discriminated against by virtue of their electronic form.[26] An electronic signature was defined as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[27] The Directive further defined two categories of signatures: the basic and "advanced" e-signature.[28] To be recognized as "advanced," an e-signature needed to be:

> (1) uniquely linked to the signatory; (2) capable of identifying the signatory; (3) created using means that the signatory can maintain under his sole control; and (4) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.[29]

An advanced signature is created by linking a digital certificate issued by a Certificate Authority—of which there are hundreds—to a unique key held by the individual user.[30] The resulting signature contains a public key, which can authenticate the signer's identity and also prove that no changes were made to the document after it was signed.[31] Article 5 of the

---

[22] *Id.*
[23] Sarah Wood Braley, *Why Electronic Signatures Can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures*, 7 LAW & BUS. REV. AM. 417, 441 (2001) ("The most remarkable aspect of the Directive is its encouragement toward the Commission to stay on top of the law and keep the EU compatible with other third countries.").
[24] Council Directive 99/93/EC, 2000 O.J. (L 13) 12 [hereinafter E-Signatures Directive].
[25] *Id.* at 14.
[26] Jacqueline Klosek, *EU Telecom Minsters Approve Electronic Signatures Directive*, 4 CYBERSPACE L. 12, 12 (2000).
[27] E-Signatures Directive, *supra* note 24, at 14.
[28] *Id.*
[29] *Id.*
[30] Adobe, Overview of Electronic Signature Law in the EU 2 (2016), https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/overview-of-electronic-signature-law-in-the-EU.PDF.
[31] *Id.*

Electronic Signatures Directive established that advanced signatures would be admissible as evidence in legal proceedings.[32]

While the drafters foresaw that recognizing electronic signatures as legally valid would help facilitate greater adoption of paperless transactions, they also worried that insufficient consumer protection would risk undermining confidence in a new technology. Consumer protection groups had raised concerns about the consumer's burden of proof in a dispute during the consultation period preceding the Directive's enactment. Some interest groups argued that "claims of system infallibility" risked placing "an intolerable burden of proof" on the individual using a provider's system for electronic identification.[33]

The final version of the Directive sought to assuage such concerns. Article 6(2) of the Directive provided that a provider of e-signature technology "is liable for damage caused to any . . . person who reasonably relies on [a technology provider's certificate] unless [the provider] proves that he has not acted negligently."[34] This "clear statement regarding party liability" set the European legislation apart from cotemporaneous U.S. legislation, which "allow[ed] electronic commerce to develop according to rules established by the market."[35] The Directive also differed from article 13 of UNCITRAL's model law, which establishes "a presumption that under certain circumstances a data message would be considered as a message of the originator [i.e. the person signing]."[36] Thus, although it chose to enter the regulatory realm by means of the relatively weak directive tool, the EU nonetheless supported the idea that consumers should not bear the burden of proof in a dispute regarding the validity of an electronic signature.

---

[32] E-Signatures Directive, *supra* note 24, at 15.
[33] *Signature Directive Consultation Compilation*, FOUND. FOR INFO. POLICY RESEARCH (Oct. 28, 1998), http://www.fipr.org/publications/sigdirecon.html.
[34] E-Signatures Directive, *supra* note 24, at 16.
[35] Ching, *supra* note 19, at 220.
[36] UNITED NATIONS, UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT 49 (1999).

B. e-IDAS

One consequence of the EU's decision to design its initial legislation on e-signatures as a directive was that Member States kept their discretion on how to interpret and implement the EU's guidelines.[37] This gave rise to several different legal and technical standards, which undermined the EU's ambition to create more uniform legislation and, in turn, an expanded marketplace.[38] National laws differed in their allocation of procedural burdens. While some Member States adopted consumer-friendly laws, others diverted from the Directive's guidelines by enacting laws that shifted the burden of proof onto consumers.[39] At the same time, new technology was rapidly emerging, which called for more comprehensive guidelines to steer the Member States toward cohesion rather than divergence. E-signatures created through mobile applications did not fit neatly into the categories established in the Directive, and led the Commission to examine ways to update the EU's legislative framework.

On July 1, 2016, the e-IDAS regulation entered into effect across all Member States, thereby replacing the Electronic Signatures Directive.[40] Unlike directives, regulations are directly applicable in each Member State's national legal system.[41] The drafters justified their adoption of a regulation by noting that "the objectives of this Regulation" can "by reason of the scale of the action, be better achieved at Union level." Continuing to push for greater integration among Member States, e-IDAS enshrines a system of mutual recognition, requiring all Member States

---

[37] *Regulations, Directives and Other Acts*, EUROPEAN UNION (last visited Jan. 20, 2017), https://europa.eu/european-union/eu-law/legal-acts_en.
[38] Dan Puterbaugh, *Understanding eIDAS: All You Ever Wanted to Know About the New EU Electronic Signature Regulation*, LEGAL IT INSIDER (Mar. 1, 2016), http://www.legaltechnology.com/latest-news/understanding-eidas-all-you-ever-wanted-to-know-about-the-new-eu-electronic-signature-directive.
[39] *See, e.g.*, Komninos Komnios, *Electronic Signatures: Value in Law and Probative Effectiveness in Greece*, 4 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 34, 37 (2007) ("Where an electronically signed document is submitted in evidence and the authenticity of the 'qualified' signature is contested, the full onus of proof does not lie with the party adducing that evidence . . . and since it is up to the party contesting the evidence to challenge that evidence, the burden of proof must, generally speaking, turn out to be to the disadvantage of the actual or alleged signatory."); *see also infra* notes 71-72 (describing current procedural rules regarding the burden of proof in disputes between customers and e-technology providers in Sweden and Italy).
[40] e-IDAS, *supra* note 14, at 73.
[41] EUROPEAN UNION, *supra* note 37.

to "recognise and accept any means of [electronic identification] issued in another Member State which has been notified to the Commission."[42]

e-IDAS expands the signature categories established by the Electronic Signatures Directive to facilitate new technological developments. First, recognizing that many customers prefer to sign documents with mobile devices such as their phones and tablets, e-IDAS permits customers to use such devices for creating signatures that qualify for advanced status.[43] Second, e-IDAS adds the "qualified signature" as a third, and most secure, category of electronic signatures.[44] This new category is the most integrative, allowing EU citizens to use an electronic identification issued in their home state to authenticate themselves in all other Member States.[45]

The process of creating a qualified signature resembles how an advanced signature is generated.[46] Unlike an advanced signature, however, a qualified signature can be created only by using a qualified certificate. Unlike the less regulated market for public certificates, which exist in the hundreds and undergo no specific certification process, qualified certificates are issued only by entities that have been accredited by national regulators. These certificates must also be stored on a "qualified signature creation device," meaning a hardware component such as a smart card or USB token.[47]

Based on the type of signature providers supply to its customers, e-IDAS divides them into two categories: Trust Service Providers (TSPs) and Qualified Trust Service Providers (QTSPs). As the name implies, QTSPs are providers that meet the standards for issuing qualified

[42] Gavin O'Flaherty & Amy McDermott, *The eIDAS Regulation: E-Identification and Trust Services for Electronic Transactions*, LEXOLOGY (Aug. 18, 2016), http://www.lexology.com/library/detail.aspx?g=a76c61e0-c03b-4b13-b748-29cd75944e29.
[43] Michael McKee, *New EU Regulation for Electronic Signatures*, DLA PIPER (Aug. 28, 2015), https://www.dlapiper.com /en/us/insights/publications/2015/08/new-eu-regulation-for-electronic-signatures.
[44] e-IDAS, *supra* note 14, at 84.
[45] Adobe, *supra* note 30, at 2.
[46] *See* discussion *supra* Part I.A.
[47] *Easy Electronic Signatures with eIDAS*, SECCOMMERCE (last visited Jan. 29, 2017), https://seccommerce.com/en/electronic-signatures-with-eidas.

signatures. Only providers within this category are entitled to display the EU Trust Mark.[48] The Regulation further mandates that each Member State create a supervisory organization that publishes and maintains a list of QTSPs established within their jurisdiction.[49] Thus, unlike the largely unregulated market for certificate authorities that facilitate the creation of advanced signatures, the market for certificates creating qualified signatures is more closely regulated and demands greater involvement by Member States.

Depending on whether they qualify as TSPs or QTSPs, providers in the different categories must comply with different procedural requirements in disputes with customers. Article 13 of e-IDAS states that all providers, regardless of their status as either a TSP or QTSP, "shall be liable for damage caused intentionally or negligently to any natural or legal person" caused by a failure to comply with its obligations under the regulation.[50] However, the "burden of proving intention or negligence" on the TSP's part lies with the party asserting a claim against it.[51] A QTSP's intention or negligence, on the other hand, is presumed unless the QTSP demonstrates its innocence.[52]

In addition to the rules allocating the burden of proof, e-IDAS permits all providers regardless of their classification to contract out of liability "for damages arising from the use of services exceeding the indicated limitations."[53] Such contractual clauses are permitted as long as the providers "duly inform their customers in advance of the limitations on the use of the services they provide."[54] Some trust service providers have included liability caps in their terms

[48] *EU Trust Mark*, EUROPEAN COMM'N (last visited Jan. 15, 2017), https://ec.europa.eu/digital-single-market/en/eu-trust-mark.
[49] *EU Trusted Lists*, EUROPEAN COMM'N (last visited Jan. 16, 2017), https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers.
[50] e-IDAS, *supra* note 14, at 92.
[51] *Id.*
[52] *Id.*
[53] *Id.*; *see also id.* at 99 (providing the requirement that QTSPs "inform in a clear and comprehensive manner, any person seeking to use a qualified trust service of the prices terms and conditions regarding the use of that service").
[54] *Id.* at 92.

of service to limit their exposure to damage claims.[55] Such clauses are not out of the ordinary in general contract law, but they give technology providers another line of defense even if their liability for a breach has been established.

Finally, despite setting forth the two-tiered system of procedural rights described above, e-IDAS shies away from putting legal force behind its own framework. In the introductory paragraphs, the Regulation states that its provisions "should be applied in accordance with national rules on liability."[56] Therefore, e-IDAS "does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, *including the burden of proof*."[57] Although several respondents requested stronger regulation of e-signatures by the EU during public consultations leading up to e-IDAS—including with regard to liability[58]—the final enactment avoided such centralized rules. Thus, while the move from directive to regulation may have signaled a push toward uniform EU law that would facilitate greater commercial exchange, the EU's latest round of legislation leaves in place divergent national rules that affect the consumer's burden of proof in a dispute scenario. This legislative development has in effect presented consumers with a forced choice between security (through qualified signatures that rely on an additional hardware component) and comfort (through advanced signatures that can be created through devices such as smartphones).

II. Misaligned Incentives Under e-IDAS

[55] For example, The Royal Bank of Scotland limits its liability to £65,000. The Royal Bank of Scotland plc, Business Customer Agreement for the TrustAssured Service 10 (2017), http://www.rbs.co.uk/Downloads/corporate/electronic /161115_RBS_TrustAssured_%20New_TC's%20_v3%204_Final.pdf.
[56] e-IDAS, *supra* note 14, at 73.
[57] *Id.* (emphasis added).
[58] Simona Cavallini et al., STUDY ON THE SUPPLY-SIDE OF EU E-SIGNATURE MARKET 82 (2012).

As currently written, e-IDAS risks making an individual legally responsible for an act for which he bears no moral responsibility.[59] Instead of shifting the evidentiary burden to the more sophisticated party, thereby creating an incentive for high-security resolutions and greater investment in antifraud measures, the EU, through its half-measure, creates risks for users of e-signature technology that leave a conspicuous gap in the Union's consumer protection scheme. As discussed below, the e-IDAS regulation is troubling both for what it does and what it refuses to do. Its refusal to intervene forcefully to create a uniform set of liability rules means that consumers in many countries remain inadequately protected under national, pro-industry rules. Moreover, even though the e-IDAS framework is nonbinding with respect to procedural requirements, it sets a standard for future legislation in Member States that may adopt the two-tier standard in national laws. The following Part addresses both issues.

A. Industry Development

The shortcomings of e-IDAS from a consumer standpoint become evident when examining the industry for e-signatures technology on the national level. In particular, providers with relatively little cross-border business have scant reasons for becoming QTSP-compliant. Consider BankID, a Swedish provider of electronic identification services. BankID has 7.5 million active users,[60] seven million of whom reside in Sweden.[61] Having reached an impressive seventy percent of Sweden's population, BankID has recently come under criticism from competitors for monopolistic practices.[62] Nonetheless, BankID has not faced regulatory scrutiny and has gradually become the de facto standard for many businesses in Sweden.

---

[59] Andersdotter & Lundgren, *supra* note 15.
[60] *This Is BankID*, BANKID (last visited Jan. 15, 2017), https://www.bankid.com/en/om-bankid/detta-ar-bankid.
[61] Carolina Neurath, *Klarna: "Bank-Id Skapar ett Monopol,"* SVENSKA DAGBLADET (Nov. 24, 2016), http://www.svd.se/klarna-bank-id-skapar-ett-monopol.
[62] *Id.*

BankID has managed to reach its prominent market position without meeting the QTSP standards. Rather, the signatures it provides for users qualify only for the intermediate, "advanced" category.[63] It is, indeed, difficult to come up with strong incentives for providers with a large market share to voluntarily subject themselves to e-IDAS's more stringent regulation. Reputational concerns could be one. In recent months, several news outlets have revealed significant security lapses in BankID's identification system.[64] In response to such issues, BankID could have sought certification as a QTSP to shore up its reputation with users. At the same time, the existence of multiple provider categories under e-IDAS allow providers to market their technology as "EU compliant" even if their solutions do not live up to the highest EU standards.[65] Moreover, whereas qualified e-signatures require the use of an external hardware component, advanced signatures can be created using a mobile device only. Under these circumstances, competition for customers will likely sway companies to offer the most convenient technology rather than the safest one.[66]

In industries dominated by multinational providers, on the other hand, incentives should be quite strong for creating a single, integrated network for cross-border transactions. Presently, only QTSPs can provide e-signatures that facilitate such integration. In many cases, however,

---

[63] BANKID, *supra* note 60 ("According to Swedish law, and within the European Union, BankID is an advanced signature and a signature made with a BankID is legally binding.").
[64] *See, e.g.*, Hasse Eriksson, *Varnar för Bedrägerier med Mobilt Bank-Id*, DAGENS NYHETER (Dec. 1, 2016), http://www.dn.se/ekonomi/varnar-for-bedragerier-med-mobilt-bank-id; Maria Rydhagen, *Så Tar Bedragarna Över Ditt Bank-Id*, EXPRESSEN (Oct. 5, 2016), http://www.expressen.se/dinapengar/sparande/sa-tar-bedragarna-over-ditt-bank-id.
[65] *See, e.g.*, *SIGNiX's Independent E-Signature Technology Compliant with European Union's eIDAS Rules*, SIGNIX (July 1, 2016), https://www.signix.com/blog/signixs-independent-e-signature-technology-compliant-with-european-unions-eidas-rules; *see also* Liaquat Khan, *What You Need to Know About the Legality of E-signatures*, EUR. BUS. REV. (Jan. 18, 2017), http://www.businessrevieweurope.eu/technology/1212/What-you-need-to-know-about-the-legality-of-e-signatures (arguing that "businesses should opt for Advanced Electronic Signatures" because they "provide users with the evidence needed to prove their identity or that a signature has been compromised" and describing Qualified Electronic Signature technology as suitable for "businesses dealing in sensitive data"); *Juridiskt Bindande Underskrifter*, BANKID (last visited Feb. 26, 2017), https://www.bankid.com/om-bankid/juridiskt-bindande-underskrifter (describing its electronic signature technology as compliant with e-IDAS).
[66] Rahim Kaba, *How It Works: Qualified E-Signature Under eIDAS*, ESIGNLIVE (July 8, 2016), https://www.esignlive.com /blog/qualified-esignature-eidas ("[I]n serving the European market for over a decade now, many of our European clients have opted for the Advanced E-Signature in their implementations for common use cases such as signing contracts, agreements and onboarding documents."); *see also The new eIDAS regulation and SecCommerce*, SECCOMMERCE (last visited Feb. 20, 2017) ("[P]rivate customers do no longer need smart cards and card reader to perform legally binding electronic signatures.").

markets in which the use of electronic identification is widespread remain fragmented along national borders. Consider the European banking sector. Data from the European Central Bank demonstrate that domestic financial institutions predominate in many Eurozone countries.[67] Within the Eurozone, around seventy-five percent of assets are placed in domestic institutions.[68] Assuming this pattern holds true across all EU Member States, most European consumers conduct financial transactions with domestic banks. These institutions, then, have little incentive to voluntarily develop technology that meets QTSP standards. Without stronger incentives to seek QTSP certification, industry actors are unlikely to voluntarily comply with tougher procedural requirements. The result, of course, is that consumers in several Member States must carry the evidentiary burden in disputes.

B. Legislative Development

Absent voluntary industry compliance with the highest standards under e-IDAS, national legislators could act to establish more stringent demands through domestic laws. Indeed, if it could be shown that countries with more mature online markets tend to gravitate over time toward implementing more robust consumer protection initiatives, it would alleviate concerns about lacking protection imposed through EU regulations. In reality, however, a Member State's level of digital development appears to have little correlation with how pro-consumer it chooses to make its domestic legislation. Denmark, the Member State with the highest Internet use among its citizens,[69] shifts the burden of proof onto service providers in all disputes.[70] By

---

[67] EUROPEAN CENT. BANK, REPORT ON FINANCIAL STRUCTURES 21 (2015); *see also Consolidated Banking Data*, EUROPEAN CENTRAL BANK (last visited Jan. 21, 2017), https://www.ecb.europa.eu/stats/money/consolidated/html/index.en.html (defining foreign banks as "subsidiaries and branches that are controlled by either an EU or a non-EU parent that is 'foreign' from the reporting country's point of view.").

[68] FRANKLIN ALLEN ET AL., CROSS-BORDER BANKING IN EUROPE: IMPLICATIONS FOR FINANCIAL STABILITY AND MACROECONOMIC POLICIES 25 (2011). While the Eurozone contains only a subset of all EU Member States, the data is necessarily incomplete.

[69] *Use of Internet: DESI Dimension 3*, EUROPEAN COMM'N (last visited Jan. 15, 2017), https://ec.europa.eu/digital-single-market/en/use-internet-desi-dimension-3.

[70] Jan Hvarre, *Electronic Signatures in Denmark: Free for All Citizens*, 1 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 14, 17 (2004).

contrast, Sweden, the Member State with the second-highest Internet use, has a much more muddled system. In the absence of a clear position taken by the Supreme Court, lower courts have held consumers responsible for proving that their e-identification has been breached.[71] Thus, rather than conforming with the Danish principle of provider liability for its relatively mature market, Sweden's procedural framework for e-signature disputes has more in common with Italy, the EU country with the least intensity of Internet use among its citizenry.[72]

Finally, it is important to note the signaling effect e-IDAS gives to national legislatures that modernize their own legal framework to comply with EU-wide regulations. Rather than going beyond measures endorsed by the EU legislature, Member States are likely to adapt the protections afforded to consumers by e-IDAS when designing new domestic legislation. Adopting an EU regulation wholesale may provide legislators with a path of least resistance and allow them to save their powder for other fights. In December 2016, the Czech Republic enacted a new law that "adapts" its legal system to the requirements set forth in e-IDAS.[73] Rather than providing uniform liability and procedural standards for TSP and QTSPs, the Czech law reinforces the bifurcation in e-IDAS between the two categories.[74] Thus, even where e-IDAS explicitly refrains from interfering directly on the national level, the regulation has a significant impact on Member States that disclaim their liberty to develop their own procedural rule and

[71] For an overview of recent case law, see Johannes Marszalek, *Bevisbördan för Påstående om Förfalskad Namnteckning*, ZACHARIAS (Oct. 6, 2015), http://www.zacharias.se/okategoriserat/bevisbordan-for-pastaende-om-forfalskad-namnteckning; *see also* Henrik Bengtsson, *Bevisbörda och Beviskrav vid Invändning om Underskriftsförfalskning: Särskilt om Elektroniska Signaturer*, *in* ELEKTRONISK SIGNERING: EN ANTOLOGI (Jon Kihlman ed., 2013) 67, 76 (arguing that Swedish case law holds that the individual in possession of a personal authentication key for e-signatures shall be presumed to have signed any agreement bearing his signature).

[72] *Use of Internet: DESI Dimension 3*, *supra* note 69. For a description of the Italian law regarding burden of proof in fraud actions, see Aniello Merone, *Electronic Signatures in Italian Law*, 11 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 85, 96 (2014) ("[T]he use of the qualified electronic and digital signature device is assumed due to the holder, unless he proves otherwise." (citing Decreto Legislativo 7 marzo 2005, n.82, G.U. 16 May, 2005, Suppl. ordinario n.93)).

[73] *Electronic Signature*, MINISTRY OF THE INTERIOR OF THE CZECH REPUBLIC (Dec. 9, 2016), http://www.mvcr.cz/mvcren /article/electronic-signature-773488.aspx?q=Y2hudW09Mg%3D%3D.

[74] The Author recognizes the limitations in analyzing an informal translation, but confirmation of the Czech Interior Ministry's translation has been sought through various translation tools applied to the original legislative text.

instead adhere to the EU model. Thus, e-IDAS both leaves consumer-unfriendly laws in place and contributes to their further development.

III. Alternative Modes of Regulation

Having focused on the shortcomings of the existing regulatory system for e-signatures up to this point, the Article concludes by considering alternative rules that would lead to stronger consumer protection on the EU's digital market. The Commission need not look far for inspiration to enact stronger protections for consumers vis-à-vis retailers. For example, Article 9 of the Draft Digital Content Directive places the burden of proof on the supplier for showing that a defect in digital content did not exist at the time it was transferred to a consumer.[75] This rule does not apply if the supplier can establish that the consumer's "digital environment" is not compatible with the content supplied. The Directive mandates that consumers cooperate with suppliers to establish the interoperability of their digital environment.[76] Refusal to cooperate can lead to a reversal of the burden of proof in the supplier's favor.[77] Imposing a similar duty to cooperate to establish the validity of an e-signature while imposing the burden of proof on providers seems to strike a better balance than the current allocation under e-IDAS.

Another alternative would be to regulate providers of e-signature technology similarly to how several Member States regulate the notary profession. Notaries are lawyers who assist in creating many types of contracts. By participating in the formation process, notaries are in a position to reduce the likelihood of litigation at a later time.[78] Notaries fulfill similar functions in

[75] EUROPEAN COMM'N, PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON CERTAIN ASPECTS CONCERNING CONTRACTS FOR THE SUPPLY OF DIGITAL CONTENT 27-28 (2015).
[76] *Id.*
[77] *Id.*
[78] *Breaking the Seals*, ECONOMIST (Aug. 11, 2012), http://econ.st/OMtn19.

the 22 EU Member States whose legal system is based on Latin civil law.[79] Notaries who draft official documents are "responsible for the legality" of the documents and must "inform the parties of the implications and consequences of the obligations they undertake."[80] A notary who intentionally or negligently violates his duties may be subjected to "disciplinary proceedings and to civil liability for damages."[81]

While regulations of notaries are well established within the European community, applying the same model directly to the e-signatures technology providers would be misguided. Importantly, notaries are considered government officials.[82] The same level of government oversight and involvement in the e-signatures industry may well be undesirable and stymie development in a rapidly changing digital environment. On the other hand, the establishment of QTSPs and the requirement that national authorities establish and maintain lists of qualified certificate providers have already moved the needle toward more direct intervention in the market. Unfortunately, e-IDAS as currently written turns TSPs and QTSPs into a class of near-notaries, with similar authority to create contracts but much less potential liability. The inappropriate effects such a creation would have on the notary profession demonstrate why it is an equally misguided model for e-signatures law.

Conclusion

Adopting high standards for e-signature technology "will lead to more trust and confidence in the integrity of the process, which, in turn, will promote growth in e-commerce."[83]

---

[79] *Legal Professions: Notaries*, EUROPEAN E-JUSTICE PORTAL (June 28, 2016), https://e-justice.europa.eu/content_legal_professions-29-en.do#n07.
[80] *Id.*
[81] Pedro A. Malavet, *Counsel for the Situation: The Latin Notary*, 19 HASTINGS INT'L & COMP. L. REV. 389, 463 (quoting RUDOLPH B. SCHLESINGER ET AL., COMPARATIVE LAW 1 (5th ed. 1988) (footnotes omitted)).
[82] ECONOMIST, *supra* note 78.
[83] Blythe, *supra* note 21, at 19. The need for coordination likely does not end at the European Union's borders. *See* Christopher T. Poggi, *Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation*, 41 VA. J.

Notwithstanding its flaws, e-IDAS contains a laudable acknowledgement of the rapidly changing digital environment. Recognizing the "pace of technological change," e-IDAS states that "this Regulation should adopt an approach which is open to innovation."[84] Such innovation should not be limited to technological advances, but must be supplemented by legal solutions that help realize the full potential for an integrated online marketplace that encompasses all EU Member States. Legal recognition of e-signatures across the entire Union is a significant accomplishment, but constitutes only one step in promoting the use of e-signatures. Equally important is to provide consumers with adequate protection against fraudulent appropriation of their electronic identification. As citizens' concerns over fraud in online transactions continue to grow,[85] the European Union needs to reinforce protections for consumers. Holding all e-signature providers to uniform procedural and liability standards constitutes an essential step in realizing the Digital Single Market's full potential.

INT'L L. 224, 228 (2000) (arguing that coordinating electronic commerce law globally is "necessary to avoid hampering its growth").

[84] e-IDAS, *supra* note 14, at 76.

[85] EUROBAROMETER, CYBER SECURITY 61, 71 (2015) (noting that 63% of EU citizens express concern over the risks of online bank fraud and 56% express concerns over the risks of online fraud).