LAW AND ECONOMICS SEMINAR **Professor Polinsky**
Winter Quarter 2018

Thursday, February 1, 2018
4:15 - 5:45 p.m.
Stanford Law School
Law School Room 270 (Manning Lounge)

"Informed Trading and Cybersecurity Breaches"

by

Eric Talley

(Columbia Law School)

Note: It is expected that you will have reviewed the speaker's paper before the seminar.

INFORMED TRADING AND CYBERSECURITY BREACHES[1]

Joshua Mitts[2] Eric Talley[3]

January 26, 2018
(First Draft: December 2, 2017)

PRELIMINARY DRAFT[4]

Abstract: Cybersecurity has become a significant concern in corporate and commercial settings, and for good reason: a threatened or realized cybersecurity breach can materially affect firm value for capital investors. This paper explores whether market arbitrageurs appear systematically to exploit advance knowledge of such vulnerabilities. We make use of a novel data set tracking cybersecurity breach announcements among public companies to study trading patterns in the derivatives market preceding the announcement of a breach. Using a matched sample of unaffected control firms, we find significant trading abnormalities for hacked targets, measured in terms of both open interest and volume. Our results are robust to several alternative matching techniques, as well as to both cross-sectional and longitudinal identification strategies. All told, our findings appear strongly consistent with the proposition that arbitrageurs can and do obtain early notice of impending breach disclosures, and that they are able to profit from such information. Normatively, we argue that the efficiency implications of cybersecurity trading are distinct—and generally more concerning—than those posed by garden-variety information trading within securities markets. Notwithstanding these idiosyncratic concerns, however, securities fraud doctrine in its current form appears poorly adapted to address such concerns, and it would require nontrivial re-imagining to meet the challenge (even approximately).

[1] We thank [your name here] and workshop participants at Columbia Law School, the Santa Fe Institute, and the Toulouse School of Economics for helpful comments and discussions. Kailey Flanagan and Hanna K. Song provided excellent research assistance. This draft is a companion piece to an eponymous technical manuscript offering a more detailed theoretical analysis. All errors, regrettably, are ours.
[2] Associate Professor, Columbia Law School. joshua.mitts@law.columbia.edu.
[3] Isador & Seville Sulzbacher Professor of Law, Columbia Law School; Co-Director, Millstein Center for Global Markets and Corporate Ownership. etalley@law.columbia.edu.
[4] For updated versions of this paper, please visit https://ssrn.com/abstract=3107123.

INFORMED TRADING AND CYBERSECURITY BREACHES

Joshua Mitts Eric Talley

Table of Contents

1. Introduction

The ascendancy and impact of the information economy during the last quarter century have been both dramatic and unprecedented. Fully one fifth of the preeminent Dow Jones Industrial Index in the mid-1990s was composed of Eastman Kodak, Bethlehem Steel, F.W. Woolworth, International Paper, Sears Roebuck and Union Carbide. Amazon and Google were little-known startups. Apple Computer—not on this list—was a moribund upstart from the 1980s. Facebook and Bitcoin were still a decade away from creation. How times have ever changed. The digitization of the world's economy has hastened profound changes in commerce, record-keeping, law enforcement, personnel policy, banking, insurance, securities markets, and virtually all aspects of services and manufacturing sectors.

At the same time, a key pillar of the digital economy—the ease of accessing/copying/ distributing information at scale—is also frequently its Achilles Heel, in the form of cybersecurity risk. The massive and cataclysmic data breach of Equifax in September 2017, for example, which compromised highly confidential information of tens of millions of clients (including Social Security numbers), was hardly the first of its kind (nor the last). For more than a decade, firms and organizations that store confidential data digitally have been targets (potential or actual) of similar types of attacks often with analogously cataclysmic implications for victims.

Within securities-market settings, of course, one person's catastrophe can be another's arbitrage opportunity. And so it came to be in the late summer of 2016, when Muddy Waters Capital—a well-known short hedge fund—opened a confidential line of communication with MedSec, a start-up cybersecurity firm claiming to have discovered a serious security software flaw in the pacemakers produced by St. Jude Medical, a then-public medical device company (knee-deep in the process of being acquired by Abbot Laboratories). Only after taking a substantial short position in St. Jude did Muddy Waters publicly disclose the device's vulnerability,[5] causing an immediate fall in St. Jude's stock price in excess of eight percent.[6] Similar patterns of material changes in value after disclosure of a cybersecurity event are now commonplace.[7]

[5] See http://d.muddywatersresearch.com/tou/?redirect=/content/uploads/2016/08/ MW_STJ_08252016_2.pdf
[6] See Goldstein, Matthew, Stevenson, Alexandra and Picker, Leslie, 2016. "Unusual Pairing Makes Public Bet vs. Pacemakers." New York Times (Sept. 8, 2016 at B1).
[7] To take a current example, Uber's recent disclosure of a cybersecurity loss of client payment records caused an outside investor (Softbank) to reduce its valuation assessment of Uber by nearly a third. See Financial Times, "SoftBank share purchase discounts Uber by 30%" (Nov. 27, 2017).

Muddy Waters' securities-market play around St. Jude's data breach disclosure is perhaps unsurprising—particularly when (a) cybersecurity breaches have material price effects in general; and (b) the underlying vulnerability involved potentially confidential data. Trading in the securities of compromised issuers is, after all, far safer than trafficking directly in the stolen information itself. Indeed, fencing such protected data directly is almost always a criminal offence under state and federal law. [8] In contrast, buying low and selling high (or selling high and buying low) in securities markets is a venerated capitalist ritual. At the same time, the St. Jude / Muddy Waters kerfuffle raises intriguing questions about how widespread such cybersecurity-related trading is, whether material arbitrage rents are available, and who tends to earn them. And, to the extent that appreciable arbitrage rents exist, might they directly or indirectly subsidize cyber-hacking---effectively catalyzing destructive activity solely for the purpose of trading on the basis of the harms and risks it creates? Is it possible to detect such activities by observing the footprint of trading patterns? Should such coordinated behavior be more heavily regulated by authorities?

In this paper, we consider public-company announcements of cybersecurity breaches, analyzing how they interact with securities-market trading activity. Specifically, we consider the phenomenon of securities-market trading on the basis of advanced knowledge of a cybersecurity breach ("informed cyber-trading"). Conceptually, such information arbitrage opportunities are eminently plausible, and privately informed traders can typically exploit their information so long as there is sufficient independent market activity (*e.g.*, among liquidity or noise traders) to provide "cover" for the informed arbitrageur. Thus, informed traders plausibly have a strong incentive to take short positions against the hacked firms—positions that should be observable in securities market activity. We test this proposition empirically, making use of a novel data set corporate data breaches involving publicly traded companies. Using a variety of means to match breached firms against comparators with no announced vulnerabilities, we find significant trading abnormalities in the put option market for hacked firms, measured both through open interest and trading volume. Our results, moreover, appear robust to a variety of matching techniques as well as to cross-sectional and time-series analysis. We view these results as consistent with the proposition that arbitrageurs tend to have early notice of impending cybersecurity breach disclosures, and that they trade on the basis of that information.

[8] *See, e.g.*, 18 U.S. Code §§ 1028A and 1030 (discussed *infra* in Section 4).

Although our principal focus is positive and empirical in nature, our findings also hold relevance for larger normative / prescriptive debates about whether such trading practices warrant additional legal proscription. Normatively, the debate over how (or whether) securities law *should* regulate informed trading is complex, balancing concerns over price discovery, liquidity, and allocational efficiency. Informed cyber-trading shares many of these traits; but it also tees up other efficiency concerns that are contextually unique. If significant arbitrage rents from advance knowledge of cybersecurity risks were wholly undeterred, several inefficient investment distortions plausibly follow, both by "hackers" (including cybersecurity firms) attempting to expose vulnerabilities and introduce costs that would not otherwise come to light; and by issuers themselves, anxious to expend efforts to frustrate (or divert) hackers' attention. Such expenditures represent real economic costs not present in garden variety information trading contexts. Consequently, informed cyber-trading plausibly justifies enhanced legal scrutiny of those who profit from the activity.

Under current securities law, however, several instantiations of informed cyber-trading would likely be permissible. To be sure, it is almost certainly unlawful for parties to conspire to steal proprietary information from a firm, or to spread *false* information about a cybersecurity risk in order to manipulate stock prices. That said, if such parties were simply to use publicly available investigatory tools to discover, trade upon, and then expose *bona fide* cybersecurity vulnerabilities (as Muddy Waters and MedSec were alleged to have done), they would face little scrutiny under current law. They would not run afoul of received insider trading theories, which generally require the breach of a confidential or fiduciary relationship.[9] And they would not violate market manipulation proscriptions, which require the introduction of *inaccurate* information into the market.[10] Although several federal courts have recently contemplated an extension to insider trading doctrine to reach (so-called) "outsider traders"— informed traders who are neither corporate fiduciaries nor have breached a confidential relationship[11]—no court to our knowledge has firmly embraced this expansion to date. In short, the task of redesigning securities law to address the costs of informed cyber-trading is a sizable ask, posing a difficult prospective challenge for policy makers and regulators alike.

[9] U.S. v. O'Hagan, 521 U.S. 642 (1997).
[10] See, e.g., SEC v. Masri, 523 F. Supp. 2d 361, 373 (S.D.N.Y. 2007).
[11] Some recent case law has entertained the idea that hacking into a confidential server and then trading on the information accessed might constitute a "deceptive practice" under Rule 10b-5. See, e.g., S.E.C. v. Dorozhko, 574 F.3d 42, 51 (2nd Cir. 2009) ("misrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly deceptive within the ordinary meaning of the word…. [D]epending on how the hacker gained access, it…could be, by definition, a deceptive device or contrivance that is prohibited by Section 10(b) and Rule 10b--5.") We discuss this nascent strand of case law (sometimes referred to as "outsider trading") in Section 4, *infra*.

Our analysis contributes to a growing literature on cyber-security threats in law, economics and computer science, assimilating to a larger literature on informed trading in securities markets. From a conceptual perspective, several contributions in computer science[12] have developed frameworks for analyzing self-protection decisions among firms that are potential cybersecurity risks, arguing that firms that, in a world of scarce resources, firms may optimally "triage" their self-protection efforts based on firm-level cost benefit calculus. Such calculus can often give rise to collective action problems of either under- or over-investment in protection,[13] when (say) interconnected firms within a network make individual decisions about security. Others in information sciences have analyzed the problem from the standpoint of timing,[14] asking whether targets should invest pro-actively before an attack or reactively afterward. If reactive investment is possible to mitigate an existing attack (and the information of such an attack becomes known), it is may well be optimal to under-invest in proactive technology and utilizing such mitigation efforts once attacks are detected. Although we are unaware of significant market pricing literature on informed cyber-trading *per se*, the efficiency implications of informed trading has been richly explored using seminal frameworks from information economics which demonstrate how informed traders can simultaneously catalyze price discovery and impede to market depth and liquidity.[15] Empirically, our analysis draws on a growing literature computer science identifying misconfiguration flags to predict vulnerability to hacking,[16] as well as estimating latency periods[17] for cybersecurity vulnerability breaches (of between one and twelve months before disclosure). Finally, the sub-strand of the literature closest to ours studies how stock prices react to the disclosure of cybersecurity breaches. One notable study in this area[18] presents a meta-analysis of 37

[12] See, e.g., Gordon, Lawrence A., and Martin P. Loeb. "The economics of information security investment." ACM Transactions on Information and System Security (TISSEC) 5.4 (2002): 438-457 (reviewing literature).
[13] See Lelarge, Marc. "Coordination in network security games: a monotone comparative statics approach." IEEE Journal on Selected Areas in Communications 30.11 (2012): 2210-2219. Kunreuther, Howard, & Geoffrey Heal. "Interdependent security." J. Risk & Uncertainty 26.2-3 (2003): 231-249. Making a similar point using a framework based on a terrorism scenario); Lakdawalla, Darius N. and Talley, Eric L., Optimal Liability for Terrorism (October 2006). NBER Working Paper No. w12578. Available at SSRN: https://ssrn.com/abstract=935571 (similarly applying such arguments to terrorism scenarios, and arguing that overinvestment in strategic target hardening by potential victims may justify allowing attacked parties to lodge a cause of action against non-attacked entities for over-protection).
[14] See Böhme, Rainer, and Tyler Moore. "The "iterated weakest link" model of adaptive security investment." Journal of Information Security 7.02 (2016): 81.
[15] See Kyle, Albert S. "Continuous Auctions and Insider Trading." Econometrica 53:6 (1985), pp. 1315-1335; Milgrom, Paul & Stokey, Nancy, "Information, trade and common knowledge". J. Econ. Th. 26(1): 17–27 (1982); L.R. Glosten and P.R. Milgrom. "Bid, Ask and Transaction Prices in a Specialist Market with Heterogeneously Informed Traders," Journal of Financial Economics, 14:71–100, 1985.
[16] See [cite].
[17] See Liu, Yang, et al. "Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents." USENIX Security Symposium 2015.
[18] See Spanos, Georgios, and Lefteris Angelis. "The impact of information security events to the stock market: A systematic

papers containing 45 empirical studies of the effect of information-security breaches on public-company stock prices from 2003 to 2015. The authors find that 75.6% of the studies measure statistically significant stock-price reactions to the disclosure of cybersecurity breaches. 20 out of 25 studies find negative and significant stock-price reactions for victim firms, and none of these find significant positive reactions for victim firms. Several other studies have found positive and significant stock-price reactions for information security firms, plausibly reflecting the additional demand for their services in the wake of security breaches. And, consistent with our findings, at least one significant study finds evidence of pre-announcement information leakages associated with cybersecurity vulnerabilities.[19] That said, we are unaware of any prior study measuring trading patterns in the months preceding the disclosure and central legal implications of such patterns, as we explore here.

Our analysis proceeds as follows. Section 2 presents our core empirical analysis of informed cyber-trading. Using a novel data set of publicly disclosed cybersecurity incidents, we demonstrate unusual activity in the put-option market in the weeks leading up to the disclosure, measured through "open interest" and trading volume. Section 3 discusses the normative implications of our findings, arguing that—relative to garden-variety informed trading—cyber-trading plausibly deserves greater legal scrutiny under federal securities law. Section 4 delves further into whether the current institutions of securities law are well equipped to take on the added threats of informed cyber-trading. Here we argue that as a general matter, the current state of securities law seems unfit for the challenge. The most prominent matters currently before trial courts would require the judicial embrace of theory of "outsider trading"—a novel and untested extension of existing law (which itself may be an imperfect elixir for the efficiency concerns posed by informed cyber-trading). Section 5 concludes.

2. Empirical Evidence of Informed Cyber-Trading

In this section, we dispense with the long-winded lawyerly prologue,[20] cutting directly to the chase to (a) describe our approach for detecting informed trading in advance of cybersecurity breach announcements; and (b) report on our core empirical findings.

---

literature review." Computers & Security 58 (2016): 216-229. Zhang, Jing, et al., "On the Mismanagement and Maliciousness of Networks." NDSS. 2014.

[19] See Arcuri, Maria C., Marina Brogi, and Gino Gandolfi. "The effect of information security breaches on stock returns: Is the cyber-crime a threat to firms?" Eur. Fin. Mgmt. Meeting, 2014 (finding find that the mean cumulative abnormal return to 128 cybersecurity disclosures is -.029 in the (-20,+20) window, but shrinks to -0.003 in the (-1,1) window).

[20] Dispirited lawyerly types can nonetheless savor the opportunity to luxuriate in the palaverously doctrinal *denouement* comprising Section 4, *infra.*

Data Description

Our analysis marshals a unique data set of announced corporate data breaches provided by the Identity Theft Resource Center (ITRC). Since 2005, the ITRC has collected and published an annual list of data breaches "confirmed by various media sources and/or notification lists from state governmental agencies." The ITRC's data breach report includes both exposure of personally identifying information --- i.e., any incident "in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure" --- as well as exposure of username and passwords that are not necessarily tied to an identifiable individual. One example of an ITRC data breach report—for a 2015 breach of Hyatt Hotels—is reproduced in the following Figure:

ITRC Breach ID	Company or Agency	State	Published Date	Breach Type	Breach Category	Records Exposed?	Records Reported
ITRC20151228-03	Hyatt Hotels	IL	12/27/2015	Electronic	Business	Yes - Unknown #	Unknown
	Hyatt Hotels recently detected malware on the computer system that processes payments for its hotels, The Guardian reports. It's not clear at this point whether any customer data was actually stolen, how long the malware was present on the system, or how many of the company's 627 properties in 52 countries may be affected.						
Attribution 1	Publication: esecurityplanet.com Author: Jeff Goldman Article Title: Hyatt Hotels Hit by Credit Card Breach Article URL: http://www.esecurityplanet.com/network-security/hyatt-hotels-corporation-suffers-credit-card-breach.html						

Figure 1: Specimen Identity Theft Resource Center Data Breach Report (Hyatt Hotels 2015).

The categories of information included in the report are: (1) internal ITRC identifier of the breach, (2) the company which was attacked, (3) the state in which that company is located, (4) the date the breach was published, (5) the type of the breach, (6) the category of the breach, (7) whether personal records were exposed, (8) how many records were exposed, and (9) a textual description of the breach. In addition, the ITRC provides details on the source of information about the breach, e.g., a news media report or disclosure by (or through) a governmental agency.[21]

The ITRC identified 4,580 data breaches from 2010 to 2016. While the vast majority of these incidents involve private companies, nonprofits and governmental actors, out of this group, we were

[21] State privacy laws often require companies to notify individuals whose personal information may have been compromised (see, e.g., N.H. Rev. Stat. Â§ 359-C:19). Moreover, specific federal laws sometimes require disclosure, e.g., when health concerns are implicated (HIPPA), or if the breach is sufficiently material to require disclosure by a publicly traded company under the securities laws. Although there is no general duty to disclose *all* material information under the securities laws, but cybersecurity vulnerabilities may fall into one of the enumerated categories of material event disclosure required under Form 8-K.

able to match 145 breaches to publicly traded companies.[22] To give a sense for the nature of the information contained in the textual descriptions of these 145 events, Figure 2 presents a bi-gram word cloud, which draws the most frequent consecutive word pairs in these descriptions with a size proportional to the term's frequency --- i.e., larger words appear more frequently in the textual descriptions. As Figure 2 shows, the most popular terms in these descriptions reflect the sort of information that would typically be the subject of a data breach, i.e., personal information, email address, credit cards, addresses, social security numbers, etc.

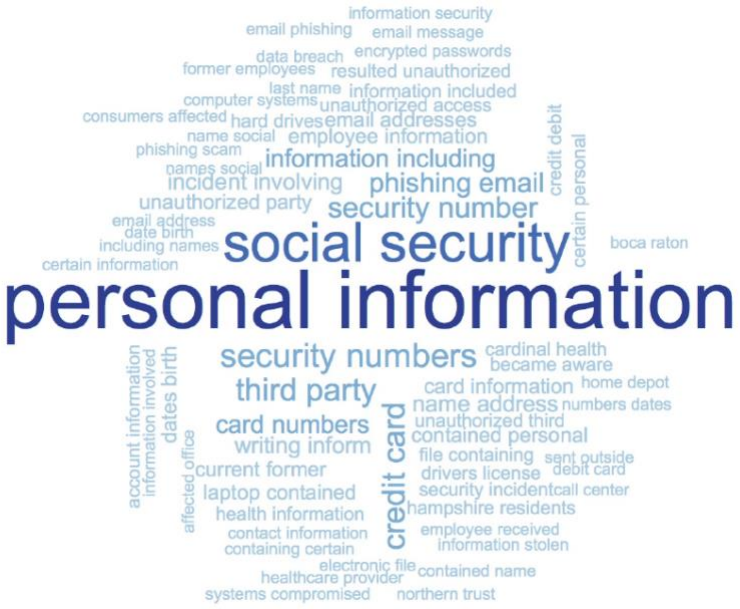

Figure 2: Bi-Gram Word Cloud for ITRC Data Breach Reports

In order to conclude that transactions involving these victims of data breaches are not due to random chance alone, it is necessary to compare these data breaches to some sort of baseline (*i.e.*, a "control" group). Even if there were no trading on corporate data breaches—for example, if we were to simply draw public companies and calendar dates at random—some firms would still experience unusually large (or small) trading activity for independent reasons. It is therefore necessary to establish a baseline group that can serve as a counterfactual, a comparison set that allows us to claim that *but for* the hacker-trader activities, target firms and the baseline group are similar in all other relevant ways, at least on average. If but-for causation in this sense appears to hold, then we are justified in concluding that observed differences attributable (at least in part) to hacker trading or tipping.

[22] For reasons detailed below, we end up using a smaller sample to ensure adequate comparability between firms and industries.

Derivatives Markets and Put Options

We examine two primary sources of data in order to measure possible hacker trading and tipping. First, we consider approximately at-the-money (ATM) equity put options written on the common stock of victim firms. An equity put option is effectively a downside bet on a firm's stock: it gives its holder the right (but not the obligation) to sell the firm's stock at a specified price (the "strike price") on a specific expiration date (also known as the "maturity" date for the option). If one denotes the strike price of a put option as K, its maturity date as T, and the firm's stock price on the maturity date as T as S_T, then the holder of a put option who acts to maximize her payoff will receive the greater of $(K - S_T)$ or zero at the time of expiry.[23] In other words, she receives the difference between the strike price and the stock price at maturity if the former exceeds the latter. If the stock price at maturity is higher than the strike price, she will rationally not exercise the put option because that would cost her money; she is better off doing nothing. [24]

Put options reflect a downside bet on the firm's stock because the value of a put option increases as the firm's stock price at maturity decreases. Put simply, the lower the stock price, the more the put option is worth: put options are thus directionally negative bets on the value of the firm. Because the directional implications of a data breach are unambiguously negative for a targeted firm --- that is, one would be hard-pressed to find an example of a successful data breach that should lead to an *increase* in the stock price of the victim firm --- put options are likely to become more valuable upon revelation of a successful data breach. This implies that market demand for put options may reflect at hackers or their "tippees" may seek to exploit information, known only to them, about a successful data breach. As noted above, we restrict our analysis to put options that are close to at the money --- that is, they have a delta between 0.4 and 0.6.[25] Put simply, that means that the strike price is likely to be relatively close to the current price of the firm's stock. We do so because a put option that is out of the money is likely to be less responsive to changes in the underlying price of the firm's stock.

---

[23] For example, suppose the stock's market price at maturity is $5 and one holds a put option with strike price of $8. The holder can profit from this contract by (a) buying the stock at market price ($5) and then exercising the option, delivering the stock to the option counterparty (for $8) and pocketing the difference ($3).

[24] The discussion in the text simplifies things a bit by presuming a "European" put option, which is exercisable only on expiration. A similar (though slightly more complicated) analysis would attend an "American" option, which is exercisable on any date up to (and including) the maturity date.

[25] The delta of a put option refers to the sensitivity of the put's value to changes in the underlying stock price, or $|\partial p_t / \partial S_t|$.

We measure market demand for put options in two ways. The first is open interest, which refers simply to the number of outstanding put-option contracts on the stock of a particular underlying firm. The second is volume, which refers to the quantity of put-option contracts that change hands between buyers and sellers over a particular window of time. Both measure the extent to which traders in the market are seeking to place downside bets on the prospects of victim firms.

In order to facilitate meaningful comparisons that are straightforward to interpret, we aggregate our dataset to the firm-event level. That is, the unit of analysis in our study is an average measure of trading in a given firm's put options over a time window relative to a data breach event. For example, we refer below to average open interest of put options for a particular firm over the two months prior to disclosure of the data breach. If, hypothetically, there were two events and two firms for each event, there would be four observations, each reflecting the average open interest for each firm in the two months prior to each event. In the following subsection, we describe how we design our empirical study to maximize the reliability of inferences as to the link between corporate data breaches and the demand for put options.

Empirical Design

We wish to evaluate empirically whether there is heightened trading in put options prior to the announcement of corporate data breaches. To do so, we rely on the well-developed literature on causal inference in empirical economics. To be sure, our hypothesis is inherently descriptive in nature---we do not suppose that data breaches *causally* increase put option trading, but rather that individuals who are aware of data breaches prior to the rest of the market may be directly trading or tipping others as to the presence of these vulnerabilities prior to disclosure. Formally speaking, this thesis requires only a correlation between the execution of corporate data breaches and market demand for put options.

Nonetheless, we are aware that an analysis of this sort is vulnerable to spurious correlations. The problem of forming a valid *counterfactual*—what level of put option trading would have emerged even in the absence of a data breach—is a vexing challenge that applies to our study just as much as with a classical causal inference project. For this reason, we employ methods to estimate the *average treatment effect* of data breaches, keeping in mind the importance of forming a valid counterfactual to evaluate whether observed put option demand can actually be attributed to data breaches.

We thus estimate two basic kinds of empirical designs, each of which relies on a different dataset. The first is a cross-sectional estimation, which simply asks: is there a heightened level of open interest and trading volume in the put options of data breach targets, *prior to* revelation of the data breach by the victim firm? To minimize the likelihood that this simple comparison between firms for each event is contaminated by other events that may give rise to put option trading, this estimation focuses on the two months immediately preceding announcement of the data breach. In this specification, we ask whether the average level of open interest and trading volume during this two-month is higher for firms who are the victims of data breaches. As described below, we employ propensity-score matching[26] to ensure that treatment and control firms are as similar as possible.

This cross-sectional specification, however, is vulnerable to the critique that firms may differ for unobserved reasons that can lead to greater overall demand for put options. To address this concern, we consider an alternative difference-in-differences design, which allows each firm-event in our dataset to have a baseline level of open interest and trading volume of put options. In this difference-in-differences specification, we compare the *change* in open interest and volume of put options from a baseline period --- eight to sixteen months prior to announcement of the data breach --- to the period of interest --- eight months prior to the day of announcement.

In our difference-in-differences design, we use this eight-month cutoff for two reasons. First, this corresponds roughly to the average period of time during which a hacker is aware of a successful data breach.[27] Moreover, a visual inspection of the data shows that this is also approximately the time when time trends begin to diverge between treatment and control firms---prior to this point, they are roughly parallel, as we show below.

We aggregate pre-post differences to the firm-event level and compare these differences between treatment and control firms. As with the cross-sectional design, we employ propensity score matching on observable covariates to ensure that similar firms are compared to each other. This heightens the plausibility of the counterfactual inference that treatment and control firms would have similar counterfactual outcomes. Along with showing that the parallel trends assumption is satisfied,

[26] See Abadie, A. and Imbens, G. W. (2006), Large sample properties of matching estimators for average treatment effects. Econometrica, 74(1):235–267.

[27] Research by Symantec has shown that hackers tend to exploit security vulnerabilities for an average of ten months prior to discovery by the affected firm (Bilge and Dumitras, 2012).

this evidence suggests that observed differences in put option trading are likely to be linked to corporate data breaches and not spuriously arising as a result of other differences between firms.

As noted previously, both of our specifications employ propensity-score matching,[28] which matches each treatment observation to one or more control observations which are similar along several covariates. We generate a propensity score and thus matching observations by estimating a logistic regression on the following covariates: (1) 4-digit SIC industry code (i.e., an indicator for each), (2) log of market capitalization, (3) log of total assets, (4) log of net income, and (5) log of total liabilities. In our view, it is essential to compare within industry because firms in different industries are very different from each other.

For these reasons, we are forced to drop those firms in industries which are too small to allow for obtaining a meaningful matched control group. Indeed, while many of these smaller industries contain several firms, many small-cap firms are too illiquid to have frequent options trading. Limiting the sample to those firms for which we have sufficient information over the relevant time periods yields 46 treatment firm-event pairs and 3,319 control firm-event pairs in the difference-in-differences dataset and 51 treatment firm-event pairs and 3,425 control firm-event pairs in the difference-in-differences dataset.[29] The following Tables present summary statistics on these datasets.

[28] See Abadie & Imbens, supra n. __

[29] The latter contains more firms than the former because it covers a longer time period.

	N	Mean	Std. Dev.	Min.	25%	Median	75%	Max.
Treatment (0/1)	3,365	0.01	0.12	0	0	0	0	1
Avg. Open Interest	3,365	496.08	2678.74	1	33.09	98.99	278.27	64,708
Log Avg. Open Interest	3,365	4.60	1.64	0	3.50	4.60	5.63	11.08
Avg. Volume	3,365	25.59	122.36	0	0.46	3.54	14.44	4212.92
Log Avg. Volume	2,853	1.62	1.94	-4.47	0.34	1.71	2.95	8.35
Market Value	3,363	10,913	37,421	3.51	445.09	1364.47	4,138	540,659
Log Market Value	3,363	7.33	1.87	1.26	6.10	7.22	8.33	13.20
Total Assets	3,365	42077	225,130	0.08	252.44	1,081	7,046	2,807,491
Log Total Assets	3,365	7.28	2.41	-2.55	5.53	6.99	8.86	14.85
Net Income	3,224	542.04	22,343	-3,347	-24.32	21.88	143.04	23,057
Log Net Income	2,021	4.70	2.02	-3.41	3.44	4.58	5.74	10.05
Total Liabilities	3,362	37,055	207,757	0.42	77.92	478.94	5,167	2,736,580
Log Total Liabilities	3,362	6.51	2.80	-0.87	4.36	6.17	8.55	14.82

Table 1: Summary Statistics: Cross-Sectional Dataset

	N	Mean	Std. Dev.	Min.	25%	Median	75%	Max.
Treatment (0/1)	3,476	0.01	0.12	0.00	0.00	0.00	0.00	1.00
Pre-Open Interest	3,476	490.75	2,130	1.00	41.89	113.96	327.79	56,933
Log Pre-Open Interest	3,476	4.79	1.54	0.00	3.74	4.74	5.79	10.95
Post-Open Interest	3,476	501.77	2,522	1.00	44.89	123.13	318.62	78,531
Log Post-Open Interest	3,476	4.82	1.50	0.00	3.80	4.81	5.76	11.27
Log O.I. (Post-Pre)	3,476	0.03	0.98	-5.87	-0.50	0.01	0.57	5.77
Pre-Volume	3,476	28.94	124.06	0.00	1.21	5.52	18.66	3,310
Log Pre-Volume	3,302	1.71	1.90	-5.83	0.47	1.83	3.00	8.10
Post-Volume	3,476	26.78	122.93	0.00	1.16	5.20	16.64	3,977
Log Post-Volume	3,268	1.67	1.86	-4.84	0.54	1.81	2.88	8.29
Log Volume (Post-Pre)	3,160	-0.07	1.22	-5.80	-0.65	-0.10	0.51	6.30
Market Value	3,474	11,260	39,095	2.59	442.99	1,390	4,195	540,659
Log Market Value	3,474	7.33	1.91	0.95	6.09	7.24	8.34	13.20
Total Assets	3,476	41,137	221,642	0.09	253.09	1,096.66	7,197	2,807,490
Log Total Assets	3,476	7.29	2.39	-2.47	5.53	7.00	8.88	14.85
Net Income	3,333	554.63	2,265	-3,347	-23.55	22.94	144.85	23,057
Log Net Income	2,078	4.75	2.00	-3.41	3.48	4.61	5.77	10.05
Total Liabilities	3,472	36,099	204,531	0.07	83.29	496.45	5,282	2,736,580
Log Total Liabilities	3,472	6.53	2.77	-2.60	4.42	6.21	8.57	14.82

Table 2: Summary Statistics: Difference-in-Differences Dataset

Balance Tests

The validity of our propensity-score matching method to estimate causal effects turns on the extent to which the treatment and control groups are balanced, that is, likely to exhibit the same

counterfactual outcomes even in the absence of treatment. Of course, there are a relatively small number of public companies with liquid options in each 4-digit SIC code industry, so any matching procedure will fall short of achieving perfect balance. Nonetheless, we perform a series of tests to verify balance in the distribution of treatment and control firms.

We begin by visually comparing the distribution of the propensity score for both the cross-sectional and difference-in-difference datasets when estimated using the full set of covariates. Figure 3 shows this distribution before and after matching for the cross-sectional and difference-in-difference datasets, respectively.[30] The similarity in the density of the two propensity scores suggests that the two groups are balanced on the propensity score.

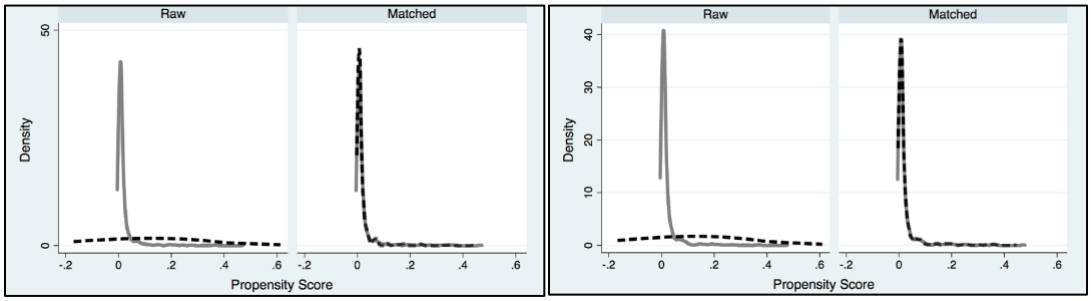

Figure 3: Propensity Score Balance Tests for Cross Sectional (Left Panel) and Difference-in-Differences Data Sets (Right Panel). In both left and right panels, the density of propensity scores is plotted for control groups (solid lines) and treatment groups (dashed lines).

Due to the relatively small number of public firms with liquid equity options in each SIC code, achieving greater balance on one covariate inevitably involves a loss of balance on another (to some extent). For this reason, in a later subsection, we present results using propensity-score matching on individual covariates, as well as all of the covariates together, to illustrate that the results do not depend on which covariates are included.

Cross Sectional Matching

	Raw Mean	(1)	(2)	(3)	(4)
Market Value	0.7782	-0.1331	-0.0094	0.2582	0.1825
Total Assets	0.5584		-0.2617	-0.1218	-0.1458
Net Income	0.6117			0.0774	0.0202
Total Liabilities	0.2611				-0.1457

Difference in Differences Matching

[30] In these figures, the propensity score is estimated on the subsample which contains nonzero open interest, but the results are virtually identical when estimating on the subsample that contains nonzero trading volume.

	Raw Mean	(1)	(2)	(3)	(4)
Market Value	0.8335	-0.0870	0.0126	0.1881	0.0426
Total Assets	0.6226		-0.2797	-0.1762	-0.2880
Net Income	0.6117			0.0613	-0.0440
Total Liabilities	0.2611				-0.2990

Table 3: Balance Test on Individual Covariates for Cross Sectional (upper panel) and Difference-in-Differences (lower panel) matched-sample specifications. The raw mean in the largest possible subsample for each covariate is given in the first column. While the matching is unable to achieve perfect balance across all of the covariates simultaneously, this table shows that each specification leads to near-perfect balance on a different covariate.

Table 3 compares covariate means in the cross-sectional and difference-in-differences dataset between the raw and matched samples. While the matching is unable to achieve perfect balance across all of the covariates simultaneously, this table shows that each specification leads to near-perfect balance on a different covariate. As shown below, the consistency of the coefficient estimates across these different specifications in significance and magnitude strongly suggests that the results are not driven by spurious variation in covariate balance.

Cross-Sectional Results

We begin by estimating the average treatment effect ("ATE") for the targeted firms by propensity score matching[31] them with non-targeted comparators over a variety of economic indicia. Normalizing the disclosure date to 0 for all breached firms, we compare (logged) open interest and (logged) volume of targeted firms to their matched counterparts over the interval [-60,0], corresponding to approximately the two-month period that precedes the first disclosure of the data breach.[32] Here, our identification strategy is based on the assumption that this interval is likely to be unknown to anyone other than the hacker (and its tippees) and corporate officers who may have become aware of the data breach. First, we estimate the difference in log open interest on outstanding put options between treatment and control firms for a variety of matching covariates. The results are shown in the following Table:

[31] See Abadie & Imbens, supra n. __

[32] We show below that the results are not driven by the choice of this interval.

This table reports the average treatment effect of corporate data breaches on the log of the average open interest of outstanding put options for target firms over the two months preceding the data breach, with propensity score matching over the following covariates: (1) an indicator for the 4-digit SIC industry code for the firm, (2) log market value as of year-end, (3) log total assets, (4) log net income, and (5) log total liabilities. In this table, the dependent variable is identical across all models, but each column reports the ATE with additional covariates included in the propensity score matching. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)
ATE	0.5528**	0.3677**	0.7539***	0.7006***
	(2.14)	(2.18)	(4.02)	(4.23)
SIC Industry	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y
Total Assets		Y	Y	Y
Net Income			Y	Y
Total Liabilities				Y
Observations	3,363	3,363	2,019	2,016

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 4: Cross Sectional Estimation; Log Open Interest

As the first row of Table 4 illustrates, there is an average increase of between .36 and .75 log points in the open interest of the put options written on target firms, and the result is consistent and statistically significant across specifications. To get an intuition behind the economic significance of the coefficients reported above, recall from Table 1 that the mean log open interest was around 4.60. Thus, an open-interest coefficient estimate of 0.7 in the full model (see Column 4) corresponds to roughly 0.70/4.60 = 15% of the mean logged open interest.

Next, we estimate differences in log trading volume of outstanding put options between treatment and control firms. The results are shown in Table 5. As the Table shows, there is an average increase of between .53 and 1.28 log points in trading volume of put options written on target firms. The result grows in both magnitude and significance as additional covariates are included in the propensity score matching, indicating that initial statistical insignificance may embody estimation noise driven by over-weighting of firms that are dissimilar.

This table reports the average treatment effect of corporate data breaches on the log trading volume in put options for target firms over the two months preceding the data breach, with propensity score matching over the following covariates: (1) an indicator for the 4-digit SIC industry code for the firm, (2) log market value as of year-end, (3) log total assets, (4) log net income, and (5) log total liabilities. In this table, the dependent variable is identical across all models, but each column reports the ATE with additional covariates included in the propensity score matching. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)
ATE	0.7980	0.5331	1.0103***	1.2798***
	(1.05)	(0.93)	(3.60)	(2.83)
SIC Industry	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y
Total Assets		Y	Y	Y
Net Income			Y	Y
Total Liabilities				Y
Observations	2,851	2,851	1,727	1,724

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 5: Cross Sectional Estimation; Log Volume

As to the economic significance of these coefficients, recall from Table 1 that the mean log volume was 1.62. Thus, the point estimate of 1.28 in the full model corresponds to roughly 79% additional trading volume of put options in the targets of corporate data breaches relative to the control group. All told, in addition to their statistical significance, our cross-sectional estimates for both open interest and volume appear to represent relatively large economic effects as well.

Although Tables 4 and 5 already perform some robustness analysis as to our matching covariates, we also conducted a robustness check on our propensity score *method*. Specifically, we re-estimated the treatment effect with all covariates across three other matching schemes for identifying treatment effects: inverse-probability weighting,[33] inverse-probability weighting with regression adjustment,[34] and regression adjustment.[35] The results are shown in the panels of the following Table, which demonstrates significant consistency across scoring methodologies.

[33] See Imbens, G. W. (2000). The role of the propensity score in estimating dose-response functions. Biometrika, 87(3):706–710.
[34] See Wooldridge, J. M. (2007). Inverse probability weighted estimation for general missing data problems. Journal of Econometrics, 141(2):1281–1301.
[35] See Lane, P. W. and Nelder, J. A. (1982). Analysis of covariance and standardization as instances of prediction. Biometrics, pages 613–621.

Log Open Interest

This table reports the average treatment effect of corporate data breaches on the log of the average open interest of outstanding put options for target firms over the two months preceding the data breach, matching on an indicator for the 4-digit SIC industry code for the firm, log market value as of year-end, log total assets, log net income, and log total liabilities. In this table, the dependent variable is identical across all models, but each column reports a different weighting scheme: (1) propensity score matching, (2) inverse probability weighting, (3) inverse probability weighting with regression adjustment, and (4) regression adjustment. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)
ATE	0.7006***	0.6347***	0.6347***	0.8998***
	(4.23)	(2.94)	(2.94)	(3.69)
Control Mean		4.5933***	4.5933***	4.5946***
		(121.56)	(121.56)	(121.70)
SIC Industry	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y
Total Assets	Y	Y	Y	Y
Net Income	Y	Y	Y	Y
Total Liabilities	Y	Y	Y	Y
Observations	2,016	2,016	2,016	2,019

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Log Volume

This table reports the average treatment effect of corporate data breaches on the log trading volume in put options for target firms over the two months preceding the data breach, matching on an indicator for the 4-digit SIC industry code for the firm, log market value as of year-end, log total assets, log net income, and log total liabilities. In this table, the dependent variable is identical across all models, but each column reports a different matching scheme: (1) propensity score matching, (2) inverse probability weighting, (3) inverse probability weighting with regression adjustment, and (4) regression adjustment. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)
ATE	1.2798***	0.9711***	0.9711***	0.7731**
	(2.83)	(4.08)	(4.08)	(2.52)
Control Mean		1.8110***	1.8110***	1.8132***
		(38.03)	(38.03)	(38.10)
SIC Industry	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y
Total Assets	Y	Y	Y	Y
Net Income	Y	Y	Y	Y
Total Liabilities	Y	Y	Y	Y
Observations	1,724	1,724	1,724	1,727

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 6: Alternative Matching Methods; Cross-Sectional Analysis; Log Open Interest (upper panel) and Log Volume (lower panel)

We also explored whether our results are an artifact of the two-month interval [-60,0], re-estimating the models matching on the full set of covariates using a variety of time event windows. The results for open interest and volume are shown in the following Table.

Log Open Interest

This table reports the average treatment effect of corporate data breaches on the log of the average open interest of outstanding put options for target firms, matching on an indicator for the 4-digit SIC industry code for the firm, log market value as of year-end, log total assets, log net income, and log total liabilities. In this table, the dependent variable is identical across all models, but each column reports a different period of sample inclusion, from one to six months prior to disclosure of the data breach. t-statistics are reported based on robust standard errors.

	1 mo.	2 mo.	3 mo.	4 mo.	5 mo.	6 mo.
ATE	0.5842	0.7006***	0.6176***	0.2816	0.0838	0.1719
	(1.50)	(4.23)	(3.62)	(1.24)	(0.35)	(0.83)
SIC Industry	Y	Y	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y	Y	Y
Total Assets	Y	Y	Y	Y	Y	Y
Net Income	Y	Y	Y	Y	Y	Y
Total Liabilities	Y	Y	Y	Y	Y	Y
Observations	1,884	2,016	2,052	2,083	2,146	2,156

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Log Volume

This table reports the average treatment effect of corporate data breaches on the log trading volume in put options for target firms, matching on an indicator for the 4-digit SIC industry code for the firm, log market value as of year-end, log total assets, log net income, and log total liabilities. In this table, the dependent variable is identical across all models, but each column reports a different period of sample inclusion, from one to six months prior to disclosure of the data breach. t-statistics are reported based on robust standard errors.

	1 mo.	2 mo.	3 mo.	4 mo.	5 mo.	6 mo.
ATE	1.1293***	1.2798***	0.7210*	0.0466	0.4916	0.5141*
	(5.79)	(2.83)	(1.82)	(0.10)	(1.22)	(1.78)
SIC Industry	Y	Y	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y	Y	Y
Total Assets	Y	Y	Y	Y	Y	Y
Net Income	Y	Y	Y	Y	Y	Y
Total Liabilities	Y	Y	Y	Y	Y	Y
Observations	1,519	1,724	1,812	1,868	1,943	1,975

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 7: Alternative Time Horizons; Cross-Sectional Analysis
Log Open Interest (upper panel) and Log Volume (lower panel)

While it is clear from Table 7 that some subsamples yield higher t-statistics than others, the point estimates are consistent in sign and magnitude regardless of the time window.

Difference-in-Differences Results

One potential concern with the results in the prior Section is that no matter how careful we are in matching treatment with control firms, our treatment firms could still differ from our controls on some durable, unobserved dimension(s). To address this concern, we estimate a difference-in-differences specification which estimates a baseline level of open interest and volume on outstanding put options of target firms over the interval [-480, -240], i.e., approximately sixteen months to eight months prior to disclosure of the data breach.[36] Our D-in-D design compares treatment-control differences during this baseline period to the analogous differences the interval [-240, 0], i.e., approximately eight months prior to disclosure up to the date of announcement. As explained previously, we aggregate the change in the log average open interest and log volume of put options between the two periods by firm-event, so there is one observation per firm-event. We then employ propensity score matching with robust standard errors to ensure that treatment and control firms are as balanced as possible on observable covariates and proceed to estimate the ATE on this outcome (i.e., the difference in log open interest and log volume).

The key identifying assumption of a difference-in-differences analysis is that treatment and control firms follow parallel trends in the matched sample. We plot these parallel trends on log open interest in the following Figure:

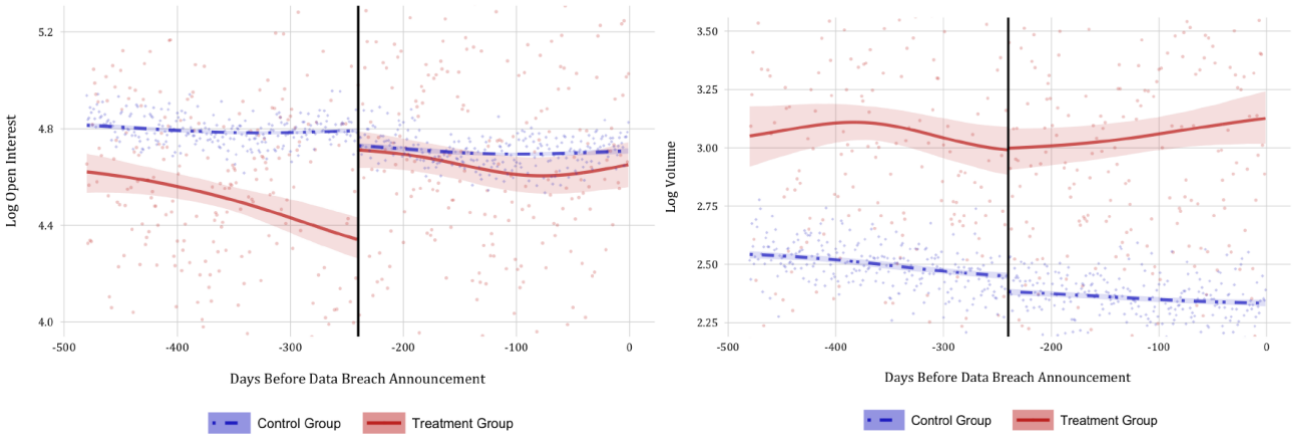

Figure 4: This figure plots time trends for log average open interest (left panel) and trading volume (right panel) on put options between treatment and control firms in the matched sample. The pre-treatment period (in days) is the interval [- 480, -240), and the post-treatment period is the interval [-240; 0].

[36] We show below that the results are not driven by the choice of this specific interval.

An eyeballing review of these parallel trends figures suggests that, indeed, the two groups appear to follow parallel trends prior to divergence during this eight-month period preceding disclosure of the data breach. This strengthens the causal interpretation of differences during this eight-month period. The parallel trend graph for open interest clearly shows the increase in the number of outstanding put options in the treatment group. Differences in volume, on the other hand, seem driven by a decrease in the control group. (We note that both represent valid identification approaches for deducing of the treatment effect in a difference-in-differences design.)

Proceeding to the statistical analysis, as before we first estimate the difference in pre-post differences of log open interest / log volume between treatment and control firms. The results of each estimation are shown in the table below. As can be seen from the upper panel of the table, for open interest we estimate an average treatment effect of between .26 and .32 log points in the pre-post difference in open interest of put options written on target firms, and the result is consistent and statistically significant across nearly every specification. The only insignificant specification has the fewest covariates included, but the point estimate is similar and thus the insignificance is likely to be driven by noise in the data. Similar results emerge from our volume estimations (bottom panel), where we find an average positive treatment effect of between .23 and .36 log points.[37] As with the cross-sectional estimation, the result is significant and increases in magnitude as additional covariates are included in the propensity score matching, indicating that initial statistical insignificance may simply reflect estimation noise driven by over-weighting of firms that are more different from each other.

[37] Comparing to the summary statistics in Table 2, the economic significance of the estimated coefficients is somewhat smaller than in the cross-sectional analysis; but it is still appreciable.

Log Open Interest

This table reports the difference-in-differences average treatment effect of corporate data breaches on the log of the average open interest of outstanding put options for target firms, with propensity score matching over the following covariates: (1) an indicator for the 4-digit SIC industry code for the firm, (2) log market value as of year-end, (3) log total assets, (4) log net income, and (5) log total liabilities. The outcome is the difference in log open interest between the periods $[t-480, t-240]$ and $(t-240, t)$ where t is the date of disclosure of the data breach. In this table, the dependent variable is identical across all models, but each column reports the ATE with additional covariates included in the propensity score matching. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)
ATE	0.3234	0.2679***	0.2793***	0.3146**
	(1.45)	(3.29)	(3.94)	(2.33)
SIC Industry	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y
Total Assets		Y	Y	Y
Net Income			Y	Y
Total Liabilities				Y
Observations	3,479	3,479	2,069	2,066

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Log Volume

This table reports the difference-in-differences average treatment effect of corporate data breaches on the log of the average trading volume of outstanding put options for target firms, with propensity score matching over the following covariates: (1) an indicator for the 4-digit SIC industry code for the firm, (2) log market value as of year-end, (3) log total assets, (4) log net income, and (5) log total liabilities. The outcome is the difference in log trading volume between the periods $[t-480, t-240]$ and $(t-240, t)$, where t is the date of disclosure of the data breach. In this table, the dependent variable is identical across all models, but each column reports the ATE with additional covariates included in the propensity score matching. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)
ATE	0.3626*	0.3044***	0.2300***	0.3425***
	(1.72)	(2.78)	(3.30)	(3.58)
SIC Industry	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y
Total Assets		Y	Y	Y
Net Income			Y	Y
Total Liabilities				Y
Observations	3,150	3,150	1,907	1,904

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 8: Difference in Differences Estimation
Log Open Interest (upper panel); Log Volume (lower panel)

As with our cross-sectional estimations, we test how sensitive these results are to using a propensity score matching method. Specifically, we re-estimate the average treatment effects from Table 8 with all covariates, again using three distinct alternative methods for matching. These sensitivity tests are

illustrated in Table 9 below. As before, we continue to find that our results are largely robust, remaining positive and significant for nearly every matching method, and similar in magnitude to the propensity-score estimation.

Log Open Interest

This table reports the difference-in-differences average treatment effect of corporate data breaches on the log of the average open interest of outstanding put options for target firms, with propensity score matching over the following covariates: (1) an indicator for the 4-digit SIC industry code for the firm, (2) log market value as of year-end, (3) log total assets, (4) log net income, and (5) log total liabilities. The outcome is the difference in log open interest between the periods $[t-480, t-240]$ and $(t-240, t)$, where t is the date of disclosure of the data breach. In this table, the dependent variable is identical across all models, but each column reports a different weighting scheme: (1) propensity score matching, (2) inverse probability weighting, (3) inverse probability weighting with regression adjustment, and (4) regression adjustment. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)
ATE	0.3146**	0.2971***	0.2971***	0.2614**
	(2.33)	(2.75)	(2.75)	(2.18)
Control Mean		-0.0028	-0.0028	-0.0040
		(-0.13)	(-0.13)	(-0.19)
SIC Industry	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y
Total Assets	Y	Y	Y	Y
Net Income	Y	Y	Y	Y
Total Liabilities	Y	Y	Y	Y
Observations	2,066	2,066	2,066	2,069

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Log Volume

This table reports the difference-in-differences average treatment effect of corporate data breaches on the log of the average trading volume of outstanding put options for target firms, with propensity score matching over the following covariates: (1) an indicator for the 4-digit SIC industry code for the firm, (2) log market value as of year-end, (3) log total assets, (4) log net income, and (5) log total liabilities. The outcome is the difference in log trading volume between the periods $[t-480, t-240]$ and $(t-240, t)$, where t is the date of disclosure of the data breach. In this table, the dependent variable is identical across all models, but each column reports a different matching scheme: (1) propensity score matching, (2) inverse probability weighting, (3) inverse probability weighting with regression adjustment, and (4) regression adjustment. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)
ATE	0.3425***	0.4060***	0.4060***	0.1551
	(3.58)	(3.21)	(3.21)	(1.57)
Control Mean		-0.0212	-0.0212	-0.0221
		(-0.80)	(-0.80)	(-0.83)
SIC Industry	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y
Total Assets	Y	Y	Y	Y
Net Income	Y	Y	Y	Y
Total Liabilities	Y	Y	Y	Y
Observations	1,909	1,909	1,909	1,912

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 9: Alternative Matching Techniques; Diff-in-Diff
Log Open Interest (upper panel) and Log Volume (lower panel)

Finally, as above, we consider whether the results are robust to our choice of the interval in the Difference-in-Differences approach, considering a variety of different "pre" and "post" treatment specifications. In Table 10, we re-estimate the models using different time horizons. The results for open interest and volume are shown in the following Table:

Log Open Interest

This table reports the difference-in-differences average treatment effect of corporate data breaches on the log of the average open interest of outstanding put options for target firms, with propensity score matching over the following covariates: (1) an indicator for the 4-digit SIC industry code for the firm, (2) log market value as of year-end, (3) log total assets, (4) log net income, and (5) log total liabilities. In this table, the dependent variable is identical across all models, but each column reports a comparison between a different period of sample inclusion: (1) $[t-360, t-180]$ vs. $(t-180, t)$, (2) $[t-420, t-210]$ vs. $(t-210, t)$, (3) $[t-480, t-240]$ vs. $(t-240, t)$, (4) $[t-540, t-270]$ vs. $(t-270, t)$, (5) $[t-600, t-300]$ vs. $(t-300, t)$ and (6) $[t-660, t-330]$ vs. $(t-330, t)$. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)	(5)	(6)
ATE	0.3165***	0.2783***	0.2679***	0.2756***	0.2361***	0.1422*
	(3.32)	(3.14)	(3.29)	(3.72)	(2.74)	(1.72)
SIC Industry	Y	Y	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y	Y	Y
Total Assets	Y	Y	Y	Y	Y	Y
Net Income	Y	Y	Y	Y	Y	Y
Total Liabilities	Y	Y	Y	Y	Y	Y
Observations	3,443	3,429	3,474	3,467	3,444	3,418

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Log Volume

This table reports the difference-in-differences average treatment effect of corporate data breaches on the log of the average trading volume of outstanding put options for target firms, with propensity score matching over the following covariates: (1) an indicator for the 4-digit SIC industry code for the firm, (2) log market value as of year-end, (3) log total assets, (4) log net income, and (5) log total liabilities. In this table, the dependent variable is identical across all models, but each column reports a comparison between a different period of sample inclusion: (1) $[t-360, t-180]$ vs. $(t-180, t)$, (2) $[t-420, t-210]$ vs. $(t-210, t)$, (3) $[t-480, t-240]$ vs. $(t-240, t)$, (4) $[t-540, t-270]$ vs. $(t-270, t)$, (5) $[t-600, t-300]$ vs. $(t-300, t)$ and (6) $[t-660, t-330]$ vs. $(t-330, t)$. t-statistics are reported based on robust standard errors.

	(1)	(2)	(3)	(4)	(5)	(6)
ATE	0.1092	0.3010*	0.3044***	0.4489***	0.4618***	0.3563***
	(0.58)	(1.88)	(2.78)	(3.83)	(3.74)	(2.67)
SIC Industry	Y	Y	Y	Y	Y	Y
Mkt. Val.	Y	Y	Y	Y	Y	Y
Total Assets	Y	Y	Y	Y	Y	Y
Net Income	Y	Y	Y	Y	Y	Y
Total Liabilities	Y	Y	Y	Y	Y	Y
Observations	3,049	3,071	3,158	3,174	3,188	3,172

t statistics in parentheses

* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$

Table 10: Alternative Time Horizons; Difference-in-Differences Analysis; Log Open Interest (upper panel) and Log Volume (lower panel)

While some subsamples yield higher t-statistics than others, all point estimates are consistent in sign and magnitude regardless of the time window.

All told, our empirical analysis uncovers relatively strong evidence of market trading abnormalities in the derivatives market prior to the public disclosure of a cybersecurity threat. While the magnitude of the effect varies (as it invariably does) on the precise estimation methodology, our results appear to be robust across the conventional alternative candidates. Although we are tempted at this stage simply to call it a day—relegating the practical details of policy responses to some unnamed future commentator—our professional duty (or our authorial zeal) impels us further to ask (a) whether the findings above pose a normative problem that securities law should address; and (b) if so, whether the tools already exist and/or are being developed for the task at hand. It is to these questions we now turn.

3. Normative Implications

Having established our empirical case that trading in advance of cybersecurity breach announcements occurs in practice, our next query concerns whether such activity poses idiosyncratic policy concerns for the efficient operation of capital markets. If it does, then there would be a *prima facie* efficiency case for tailoring securities fraud law away from its standard ground rules to account for cyber-trading concerns. In the policy debate surrounding insider trading, as well as how/whether it should be regulated, finance-minded commentators have advanced at least three dimensions of efficiency analysis for consideration: pricing efficiency, market liquidity, and allocational efficiency. We briefly discuss each in turn.

Price Discovery

Consider first pricing efficiency, the desideratum that prices in capital markets should reflect the "fundamental" value of the underlying traded securities. When satisfied (at least roughly), the accuracy of asset prices assists market participants in making portfolio choices, and it helps firms to finance value-enhancing projects. To the extent that pricing efficiency holds importance, it counsels for a permissive stance on informed trading. Indeed, if informed traders are permitted to participate in market trades, they will systematically trade up (or down) the price of a financial asset whenever it is under- (or over-) priced (Manne 1966; Macey & Haddock 1987). Although such traders will have a strong profit motive for doing so, allowing them to pursue such motives on an "unleveled" informational playing field may be a reasonable price to pay for pricing accuracy.[38]

[38] See, e.g., Chiarella v. United States, 445 U.S. 222 (1980) (rejecting the "level playing field" desideratum advanced by the SEC).

Market Liquidity

A second consideration that often embroils the insider trading debate concerns market liquidity. The price-discovery attributes that emerge from allowing informed parties to trade are practically attainable only to the extent that *uninformed* market participants are willing to participate as (losing) counterparties to such trades. In markets known to be populated with information traders, however, uninformed market participants can be understandably reluctant to trade. Indeed, in the extreme case where the *predominant* reason to trade is to exploit private information, trading among uninformed counterparties can shut down completely, leading to the collapse of a market[39] – a consequence that is antithetical to price discovery. Information traders, therefore, play simultaneously heroic and parasitic roles in their relationship with liquidity traders: They heroically contribute to price discovery; but they parasitically require liquidity-trader participation order to make information arbitrage profitable, while their very presence can systematically deter such participation.[40] Consequently, even when pricing efficiency is of vital importance, it may be efficiency enhancing for securities law to enforce an "interior solution," where information trading is rationed to a magnitude where it does not ender market dysfunction.[41]

Allocational Efficiency

Finally, informed trading in securities markets can give rise to a host of different issues related to allocational efficiency, potentially causing market participants to incur socially inefficient expenditures related to their market trading. Aspiring informed traders, for example, may overinvest in obtaining private information, or in keeping such information private, so as to protect the sanctity of their arbitrage opportunity. Uninformed traders, in turn, may overinvest in precautions, suspicious that their counterparty is an informed trader attempting to bamboozle them. Not only are such expenditures real economic costs, but they may further distort both bid-ask spreads and price discovery (Goshen 2006).

[39] Milgrom & Stokey, supra n. __
[40] See Kyle, supra n. __
[41] See Stoll, supra n. __; Glosten & Milgrom, supra n. __.

What (if Anything) Is Special about Informed Cyber-Trading?

It is worth noting that several aspects of informed cybersecurity trading share many of same traits manifested by run-of-the-mill insider trading. Informed traders seek to profit off of advanced knowledge of cybersecurity breaches, and in so doing augment pricing accuracy. Uninformed traders plausibly become cautious when transacting in settings with informed traders. And, all types of traders likely (over-) invest in information and precautions in advance of market transactions. Although there is no guarantee that securities laws have struck the precisely correct balance under the *status quo*, the aforementioned similarities *alone* would not constitute sufficient cause to treat informed cyber-trading any different from other garden variety forms of informed trading.

We submit, however, that at least two additional considerations make informed cyber-trading different—and in many respects more worrisome—than the generic case. First, the damaging nature of the information being traded on is, in a meaningful respect, a harm that is "created" by the hacker to be visited on the target. In cases where the hacker actively steals proprietary information, the imposition of harm is clear. But even when the hacker simply endeavors to expose a latent vulnerability, the underlying problem may not have attracted any attention within the hacking community (or would not have done so for some time). Once the vulnerability is announced, however, outside attention is swift. In essence, the hacker (regardless of motive) creates and imposes a harm on the targeted company—a dynamic that is not analogous to the "exogenous" forms of information possessed by garden variety information trader. In the realm of cybersecurity trading, moreover if one increases the potential arbitrage gains available from informed cyber-trading, then the incentives to hack are bound to increase as well.

Second, as the incentive of hackers to increase their activity levels grows, so too does the incentive for target firms to embrace precautionary measures to deter (or divert) a hacker's attention. In many situations, such undertakings can be considerable and costly, such as when a target's risk of hacking increases when it is identified as the "weakest link" among potential targets (Lakdawalla and Talley 2006). In such settings, a type of "arms race" to self-protect can ensue among targets, leading to significant equilibrium costs borne by each potential target.[42] In addition to being an efficiency

[42] We consider these incentives in detail in a technical companion piece. [Cite]

concern, this type of cost is once again one that is not generally manifest in generic insider trading contexts.

Consequently, although informed cyber-trading exhibits some features that are generic to informed trading environments, it also introduces certain material considerations that appear to be special to its context. Consequently, an efficiency-minded designer of securities law might well be inclined to tailor the content of the law towards greater enforcement against informed cyber-trading. In the next section, we consider whether securities laws under the status quo are up to the task.

4. Prescriptive Challenges

The previous sections have established (a) that as an empirical matter, informed cyber-trading in the securities markets occurs in advance of a data breach disclosure and (b) that it raises more idiosyncratic policy concerns in not generally present in the canonical case of informed trading (where traditional securities law has, for the most part, treaded lightly in the absence of a confidential / fiduciary relationship). In the light of these points, we now turn to the prescriptive question of whether securities fraud law can adapt to deal with cybersecurity traders, particularly when their quest for arbitrage profits would have inefficient / undesirable results. In a broad sense, our approach here is to inform the prescriptive discussion as to (a) whether current law acts to deter informed cyber-trading trading, and (b) if not, how one might go about extending current securities law to instances of informed cybersecurity trading by hedge funds. We will argue that, outside of the extreme case where hackers and traders *coordinate* for the purpose of *stealing* confidential data from targeted firms, the case for trader liability tenuous at best, and in most cases simply unavailing under the status quo. And, the most promising way to adapt current law to accommodate informed cyber-trading concerns—an extension of insider-trading law to "outsiders" who breach no fiduciary or confidentiality duty is its self far from perfect, suffering from both over- and under-inclusiveness. (The discussion below seems particularly timely in the light of the recent high-profile cybersecurity breaches, including the attack on the SEC's EDGAR website, a database of draft corporate filings – a natural goldmine for hackers seeking material nonpublic information ("MNPI") prior to public disclosure.[43])

[43] Hannah Kuchler, *Hackers Target Weakest Links for Insider Trading Gain*, FINANCIAL TIMES (Oct. 3, 2017), https://www.ft.com/content/13a317ce-a561-11e7-9e4f-7f5e6a7c98a2; Alexandra Stevenson & Carlos Tejada, *S.E.C. Says It Was a Victim of Computer Hacking Last Year*, N.Y. TIMES (Sept. 20, 2017), https://www.nytimes.com/2017/09/20/business/sec-hacking-attack.html.

To better frame our inquiry, consider Table 11 below, which subdivides the question by positing (plausibly) that the cyber-hacker and the trader may exhibit both differential interests and degrees of coordination:

		Hacker's Objective	
		Stealing Data	Detecting Vulnerabilities
Trader's Involvement	Directing / Coordinating with Hacker	Scenario I	Scenario II
	Independent from Hacker	Scenario III	Scenario IV

Table 11: Representation of Hacker's and Trader's Interaction

The columns of the Table posit that the objectives of the "hacker" (a term we use broadly to include both "white hat" and "black hat" hackers) can be either (i) to utilize target vulnerabilities in order to steal data; or (ii) merely to detect and publicize such the target's vulnerabilities. The rows, in contrast, denote the *trader's involvement* with the hacker, and can vary such that the trading entity is either (i) independent from the hacker (e.g., it learns of the hack through publicly available investigatory tools) or (ii) directs/coordinates with the hacker as part of a group with a common aim. (While intermediate interests / degrees of coordination are certainly possible, the above simplification is adequate as a first approximation for our analytic task.)

Each resulting permutation from this two-by-two matrix (denoted Scenario I through Scenario IV) entails slightly different normative and doctrinal considerations, thereby warranting slightly different analysis. Scenario I, in which the trader works actively with the hacker to steal confidential data, presents the strongest normative concerns. Scenario II, while not concerning outright data theft, also tends to entail many of the efficiency concerns of Scenario I, since the exposure of vulnerabilities can (as noted above) visit a "harm" that would not have occurred (at least probabilistically) without the incentives provided (implicitly or explicitly) through coordination with a trader. The remaining cells correspond to situations where the trader *independently* learns that of a hacker's outright theft (Scenario III) or mere detection of vulnerabilities (Scenario IV); as noted above, they present weaker normative concerns, since

the incentives to trade are (by hypothesis) unbundled from the incentives to hack. As a rough approximation, then, a tailored securities fraud doctrine in the case of informed cyber-trading would impose additional liability risk on the upper row of Table II (Scenarios I and II). As we show below, however, even in the "easiest" case for liability risk—Scenario I—the most likely form of liability for the trader may come through *criminal* liability; the levers for civil liability (brought either by the SEC or private parties) appear far more tenuous and untested under current law without courts being willing to take on a novel (and largely untested) theory of "outsider" trading. And, because criminal liability for traders is almost certainly unavailable outside Scenario I, that same untested experiment within civil liability that would have to do additional work.

Before proceeding, we note that our discussion below concentrates on *insider trading* liability, its plausible "nearby" applications and/or extension. We focus on the constellation of insider trading because it appears to be the most amenable to adaptation of major securities law applications. (Market manipulation, for example, usually would not reach informed cyber-trading, where the hacker and trader exploit information disclosures that are *truthful* in fact.)

The "Easy" Case: Coordinated Data Theft (Scenario I)

Consider first the case of Scenario I from Table 11, where a trader explicitly coordinates with and/or directs a hacker to steal confidential data from a target company; as noted above, this permutation presents the strongest case for liability under current law. Exposure appears to be particularly robust in the criminal context (which not only directly prohibits data theft, but also features criminal liability for traders in the form of mail and wire fraud, as well as aiding and abetting)[44]; interestingly, however, the case for civil liability under insider trading law remains somewhat murky—even under this "easy" scenario—given the judicially defined particulars of insider trading law under Rule 10b-5.

Many of the contours of Scenario I are literally playing out *now*—as of this writing—with parallel DOJ and SEC complaints in the high-profile *Dubovoy* case.[45] In its civil complaints filed in 2015 and

[44] Andrew Vollmer, *Computer Hacking and Securities Fraud*, CLS Blue Sky Blog (Apr. 7, 2016), http://clsbluesky.law.columbia.edu/2016/04/07/computer-hacking-and-securities-fraud/.

[45] Complaint, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015). Indictment, U.S. v. Korchevsky et al., No. 15-cr-00381 (E.D.N.Y., filed Aug. 5, 2015). Indictment, U.S. v. Turchynov et al., No. 15-cr-00390 (D.N.J., filed Aug. 6, 2015). A subsequent complaint named additional defendants. See Complaint, SEC v. Zavodchiko et al, No. 2:16-cv-00845 (D.N.J., filed Feb. 17, 2016).

2016, the SEC has charged more than 40 defendants with securities fraud and related charges stemming from an alleged international hacking-and-trading scheme organized by Ukrainian nationals Ivan Turchynov and Aleksandr Ieremenko (the "*Dubovoy* Hackers").[46] The U.S. Attorney's Offices for the District of New Jersey and the Eastern District of New York followed with criminal actions against a subset of the named defendants in the SEC case, including the *Dubovoy* Hackers and several traders (including hedge fund managers and their investment firms[47]) located both in the U.S. and abroad ("*Dubovoy* Traders").[48]

According to government documents, over a five-year period, the *Dubovoy* Hackers "used deceptive means"[49] to breach computer networks at several U.S. business newswire services (i.e., Marketwired, PR Newswire, and Business Wire)[50], stole "confidential earnings information for numerous publicly-traded companies from press releases that had not yet been released to the public," and sold such stolen material non-public information (MNPI) to the *Dubovoy* Traders.[51] The *Dubovoy* Traders, it is further alleged, as part of a coordinated plan, provided the *Dubovoy* Hackers with "shopping lists" of desired press releases, accessed the stolen MNPI through secured overseas computer servers,[52] and then "used that stolen [MNPI] to trade securities and reap over $100 million in unlawful profits."[53] The *Dubovoy* Traders used "deceptive means," including the use of multiple accounts and entities, to conceal their trading activities.[54] The case pressed against the Dubovoy Traders constitutes a veritable poster child case study for Scenario I as depicted in Table 11.

---

[46] Jonathan Stempel, *SEC Brings New Charges Over Global Press Release Hacking Scheme*, REUTERS (Feb. 18, 2016), https://www.reuters.com/article/us-trading-cyber-sec/sec-brings-new-charges-over-global-press-release-hacking-scheme-idUSKCN0VR25N.

[47] Cory Bennett, *Hackers Cash in with Insider Trading*, The Hill (Aug. 16, 2015), http://thehill.com/policy/cybersecurity/251174-hackers-cash-in-with-insider-trading; Nate Raymond, *Russia Investor, Funds Pay $18 Million to Settle U.S. Press Release Hacking Case*, Reuters (Mar. 25, 2016), https://www.reuters.com/article/us-insidertrading-cyber-sec/russia-investor-funds-pay-18-million-to-settle-u-s-press-release-hacking-case-idUSKCN0WR1A4.

[48] SEC, *SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases*, Press Release 2015-163 (Aug. 11, 2015), https://www.sec.gov/news/pressrelease/2015-163.html.

[49] Complaint ¶ 71, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015).

[50] Indictment ¶ 14, U.S. v. Turchynov et al., No. 15-cr-00390 (D.N.J., filed Aug. 6, 2015).

[51] Complaint ¶¶ 1-3, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015).

[52] U.S. Dept. of Justice, *Hacker Sentenced To 30 Months In Prison For Role In Largest Known Computer Hacking And Securities Fraud Scheme*, Press Release (May 22, 2017), https://www.justice.gov/usao-nj/pr/hacker-sentenced-30-months-prison-role-largest-known-computer-hacking-and-securities.

[53] Complaint ¶ 1, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015).

[54] *Id*. ¶ 7.

Criminal Liability

Consider first the element of criminal liability. The DOJ's indictment in the Dubovoy case charged the *Dubovoy* Traders with a series of criminal offenses that appear to be naturally teed up under federal criminal law. These include:[55]

- *Fraud and Related Activity in Connection with Computers,* in violation of 18 U.S.C. § 1830 (a.k.a., the "Computer Fraud and Abuse Act").
- *Identity Theft,* in violation of 18 U.S. Code § 1028A.
- *Money Laundering Conspiracy*, in violation of 18 U.S.C. § 1956(h) (Laundering of Monetary Instruments).
- *Wire Fraud*, in violation of 18 U.S.C. §§ 1343 and 1349 (Attempt and Conspiracy);
- *Securities Fraud*, in violation of 15 U.S.C. §§ 78j(b) (Manipulative and Deceptive Devices) and 78ff (Penalties), 17 CFR 240.10b-5 (Employment of Manipulative and Deceptive Devices), and 18 U.S.C. §2 (Principals); and

The computer fraud, identity theft and money laundering allegations are important, since they provide the predicate offenses for criminal liability required by the federal wire the fraud statute. And indeed, several of the *Dubovoy* Traders, quickly pleaded guilty to the wire fraud conspiracy charge at various times between December 2015 and August 2016.[56] Consequently, there appears to little uncertainty surrounding the application of certain criminal laws to this behavior (e.g., wire fraud, aiding and abetting),[57] they are not given further treatment herein. The more complex subject of securities fraud is discussed in detail in the context of civil liability.

Civil Liability

In contrast with the relatively straightforward application of certain criminal laws to the Scenario I trader's behavior, civil liability for traders under Scenario I tees up some interesting (and surprisingly challenging) quandaries within securities fraud jurisprudence. Specifically, if a trader enters transactions

[55] Indictment ¶¶ 112-145, U.S. v. Turchynov et al., No. 15-cr-00390 (D.N.J., filed Aug. 6, 2015). In addition to the offenses listed in association with the *Dubovoy* Traders, it may be of interest that the *Dubovoy* Hackers were also charged with crimes such as conspiracy to commit fraud and related activity in connection with computers, fraud and related activity in connection with computers, and aggravated identity theft. The Eastern District of New York charged the defendants with an overlapping set of crimes: Conspiracy to Commit Wire Fraud, Conspiracy to Commit Securities Fraud, Securities Fraud, and Money Laundering Conspiracy. Indictment ¶¶ 45-55, U.S. v. Korchevsky et al., No. 15-cr-00381 (E.D.N.Y., filed Aug. 5, 2015).

[56] U.S. Dept. of Justice, *Hacker Sentenced To 30 Months In Prison For Role In Largest Known Computer Hacking And Securities Fraud Scheme*, Press Release (May 22, 2017), https://www.justice.gov/usao-nj/pr/hacker-sentenced-30-months-prison-role-largest-known-computer-hacking-and-securities.

[57] *See, e.g.*, Vollmer, *supra* note ___ ("All this is not to say that the defendants did no wrong. They engaged in reprehensible conduct if the alleged facts can be proved, and they probably committed a variety of federal and state crimes that more neatly fit the behavior, such as laws against computer intrusions, wire fraud, and aiding and abetting primary offenses.")

on the basis of MNPI stolen through a cybersecurity hack, it remains unclear under current law whether that trader has committed insider trading in violation of Rule 10b-5. Under both the traditional and misappropriation incarnations of insider trading doctrine, liability requires the trading / tipping entity to breach a fiduciary duty to either the target firm or a third-party information generator. And in this hypothetical case, neither the hacker nor the trader is an "insider" with a fiduciary duty to the target, nor is either an appropriator of confidential information from a third party.[58] Rather, this informed cyber-trading scenario presents a "[f]ar more complex and challenging for SEC enforcement staff, the [defendants] who traded would be charged instead with 'outsider trading,' a much lesser known and barely tested legal theory of securities fraud."[59]

The SEC's complaint against the *Dubovoy* traders[60] nevertheless alleges a laundry list of civil claims for securities fraud, including:[61]

- *Section 17(a)* of the Securities Act of 1933 ("'33 Act")[62];
- *Section 10(b)* of the Securities Act of 1934 ("'34 Act") and *Rule 10b-5* thereunder[63]; and

[58] John Reed Stark, *Think the SEC EDGAR Data Breach Involved Insider Trading? Think Again.*, D&O DIARY (Oct. 2, 2017), https://www.dandodiary.com/2017/10/articles/cyber-liability/guest-post-think-sec-edgar-data-breach-involved-insider-trading-think/.

[59] *Id*.

[60] The SEC brought the same claims for relief in its complaint in the related *Zavodchiko* case.

[61] Complaint ¶¶ 222-234, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015).

[62] Complaint ¶¶ 222-224, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015) ("Defendants, by engaging in the conduct described above, knowingly or recklessly, in connection with the offer or sale of securities, by the use of the means or instruments of transportation, or communication in interstate commerce or by use of the mails, directly or indirectly: (a) employed devices, schemes or artifices to defraud; (b) obtained money or property by means of untrue statements of material facts, or omissions to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or (c) engaged in transactions, practices or courses of business which operated or would operate as a fraud or deceit upon the purchaser…By engaging in the foregoing conduct, defendants violated, and unless enjoined will continue to violate, Section 17(a) of the Securities Act.").

[63] Complaint ¶¶ 225-227, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015) ("By engaging in the conduct described above, defendants knowingly or recklessly, in connection with the purchase or sale of securities, directly or indirectly, by use the means or instrumentalities of interstate commerce, or the mails, or the facilities of a national securities exchange: (a) employed devices, schemes or artifices to defraud; (b) made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or (c) engaged in acts, practices, or courses of business which operated or would operate as a fraud or deceit upon any person in connection with the purchase or sale of any security…By engaging in the foregoing conduct defendants violated, and unless enjoined will continue to violate, Section 10(b) of the Exchange Act.").

- *Sections 20(b)*[64] *and (e)*[65] of the '34 Act.

The day after the complaint was filed, the court entered a temporary restraining order to freeze the defendants' assets and an order to show cause why a preliminary injunction should not enter.[66] A subset of the *Dubovoy* Traders (the "Amaryan Defendants") appealed this order.[67] On October 16, 2015, the court issued an opinion (the "Amaryan Opinion") granting the SEC's motion for a preliminary injunction because it had "raise[d] a strong inference that the Amaryan Defendants violated federal securities laws . . . ."[68] On February 12, 2016, hedge fund Memelland Investments Ltd. ("Memelland"), another of the *Dubovoy* Traders, filed a motion to dismiss under FRCP 12(b)(6). On September 29, 2016, the court issued a second opinion (the "Memelland Opinion") denying Memelland's motion because "the SEC particularly pled its fraud and aiding and abetting claims," giving rise to a strong inference that Memelland acted with scienter to "deceive, manipulate or defraud."[69] As of January 2018, the Amaryan and Memelland Opinions appear to be the only two opinions released in this matter. The SEC has reached settlements with several of the *Dubovoy* Traders,[70] and it appears that remaining SEC matters have been stayed until the resolution of the federal criminal actions.[71]

---

[64] Section 20(b) of the '34 Act "broadly prohibits violating federal securities law through the means of another person." William D. Roth, *The Role of Section 20(b) in Securities Litigation*, Harvard Bus. Law Rev. Online (Dec. 9, 2015), http://www.hblr.org/2015/12/the-role-of-section-20b-in-securities-litigation/. Complaint ¶¶ 232-234, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015) ("By engaging in the foregoing conduct, the trader defendants violated Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule lOb-5 [17 C.F.R. § 240.10b-5], thereunder through or by means of the hacker defendants. By engaging in the foregoing conduct, pursuant to Section 20(b) of the Exchange Act [15 U.S.C. § 78t(b)], defendants, except Ieremenko and Turchynov, violated, an unless enjoined will continue to violate Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 1 Ob-5 [17 C.F .R. § 240.1 Ob-5], thereunder.").

[65] Complaint ¶¶ 228-231, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015) ("Through their illicit trading, payments to the hacker defendants, instruction about which releases to obtain, and other means alleged in this Complaint, the trader defendants knowingly provided substantial assistance to, and thereby aided and abetted~ the hacker defendants in connection with the hacker defendants' violations of the securities laws. By engaging in the foregoing conduct, pursuant to Section 15(b) of the Securities Act and Section 20(e) of the Exchange Act, defendants, except Ieremenko and Turchynov, violated, an unless enjoined will continue to violate Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)] and Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 10b-5 [17 C.F.R. § 240.10b-5], thereunder.")

[66] SEC v. Dubovoy, No. CV 15-6076, 2016 WL 5745099, at *2 (D.N.J. Sept. 29, 2016).

[67] Id.

[68] SEC v. Dubovoy, No. CV 15-6076, 2015 WL 6122261, at *4 (D.N.J. Oct. 16, 2015).

[69] SEC v. Dubovoy, No. CV 15-6076, 2016 WL 5745099, at *1, 5 (D.N.J. Sept. 29, 2016).

[70] SEC, *Trader Agrees to Settle Claims Relating to Hacked News Release Scheme; SEC's Recovery to Date in Connection with the Scheme Exceeds $52 Million*, Litigation Release No. 23530 (May 4, 2016), https://www.sec.gov/litigation/litreleases/2016/lr23530.htm (For example, "Without admitting or denying the allegations in the SEC's complaint, Makarov agreed to be permanently enjoined from violating Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 thereunder and Section 17(a) of the Securities Act of 1933 and pay disgorgement of $100,000.").

[71] Stark, *supra* note 58.

Dubovoy has been aptly called the SEC's first major "outsider trading" case: Although initial judicial opinions were receptive to the Commission's theory, getting to that conclusion (with reasoned analysis) will likely require new precedent in this area.[72] For this reason (and given its parallels to the Scenario I fact pattern), it provides valuable context for our exploration of civil securities fraud liability for "outsider trading" by informed cyber-traders.

"Outsider Trading": A New (and Evolving) Theory of Rule 10b-5 Securities Fraud

It is important to note that despite its received formalization, the civil offense of "insider trading" is not explicitly codified in U.S. statutory securities law.[73] Instead, it has largely emerged as a judicial construction of Section 10(b) of the '34 Act and Rule 10b-5[74] thereunder, which together create "a 'catchall' aimed at fraud, requiring some sort of 'device, scheme or artifice to defraud' or some action, which would otherwise 'operate as a fraud or deceit upon a person."[75] Indeed, the U.S. Supreme Court held in *Superintendent of Ins. V. Bankers Life & Cas. Co.* that the antifraud provisions should be applied broadly, such that "Rule 10b-5 prohibit[s] all fraudulent schemes in connection with the purchase or sale of securities, whether the artifices employed involve a garden type variety of fraud, or present a unique form of deception."[76] Thus, while judicially constructed insider trading is certainly a "unique form of deception," it is not the only form of fraud covered by Rule 10b-5, which also captures general frauds such as those perpetrated by a trader who makes affirmative misrepresentations.[77] This structural lacuna seemingly leaves open a door for the SEC (assuming it can convince courts to go along) to continue shaping a new "unique form of deception," that is, the civil offense of "outsider trading."

---

[72] Stark, *supra* note 58.
[73] Stark, *supra* note 58.
[74] The text of Rule 10b-5 reads as follows:

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,
>
> (a) To employ any device, scheme, or artifice to defraud,
>
> (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
>
> (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security."
>
> 17 C.F.R. § 240.10b–5.

[75] Stark, *supra* note 58.
[76] Superintendent of Ins. of State of N. Y. v. Bankers Life & Cas. Co., 404 U.S. 6, 10 n.7 (1971); Robert Steinbuch, *Mere Thieves*, 67 MD. L. REV. 570, 574 (2008).
[77] Steinbuch, *supra* note 76 at 574.

The Dubious Fit of Conventional Insider Trading Law

Under its current construction, the prohibition of insider trading is generally understood to mean that "individuals may not purchase or sell securities based on knowledge of nonpublic information that they legally obtained or possessed as a consequence of their employment or similar circumstances."[78] Given the text of Rule 10b-5, which requires some kind of "fraud or deceit… in connection with the purchase or sale of any security," the courts developed a jurisprudential heuristic for concluding that insider trading is fraudulent or deceitful by "equating a breach of fiduciary or fiduciary-like duty [toward the information's owner] with the fraud requirement."[79] Over time, it has become accepted that a breach of a confidential or fiduciary relationship is required for traditional insider trading liability to attach.[80]

The "classical" and "misappropriation" theories of insider trading liability guide courts in applying their insider trading regime (and are, again, judicially well-trodden terrain). The classical theory—developed first—teaches that "a corporate insider[81] (with a fiduciary duty to the corporation's shareholders) may not trade in the securities of his or her corporation on the basis of material information not generally known to the investing public, and which, if made public, would substantially affect the judgment of a reasonable investor."[82] The classical theory was easily expanded to cover "tippee" outsiders who receive MNPI from "tipper" insiders (who themselves receive a personal benefit) and trade with knowledge (actual or reasonable) that the insider(s) breached their duties by tipping for personal benefit.[83] Misappropriation theory further expanded insider trading liability such that "a person violates Rule 10b-5 when he misappropriates confidential information for the purpose of securities trading, in breach of a duty owed to the source of the information, rather than to the shareholders of the [issuing] corporation."[84] The misappropriation theory thus reached certain types of corporate outsiders

[78] *Id*. at 575.
[79] *Id*.
[80] Mike Piazza, Jonathan Haray & Katie Ruffing, *Defending Against Insider Trading* Claims, Practical Law Practice Note w-000-5992 (2017).
[81] These include statutory insiders under Section 16A, as well as certain "constructive" insiders who are in a relationship of trust and confidence with the issuer. See *Dirks*, at note 14.
[82] Hagar Cohen, *Cracking Hacking: Expanding Insider Trading Liability in the Digital Age*, 17 Sw. J. Int'l L. 259, 265 (2011). *See generally* Chiarella v. United States, 445 U.S. 222 (1980).
[83] Cohen, *supra* note 82 at 266-67. *See, e.g.*, Dirks v. SEC, 463 U.S. 646 (1983); Salman v. United States, 137 S. Ct. 420 (2016).
[84] Cohen, *supra* note 82 at 267. *See generally* United States v. O'Hagan, 521 U.S. 642 (1997).

who nonetheless "deal in deception" against a third-party principal by ""pretend[ing] loyalty to the principal while secretly converting the principal's information for personal gain."[85]

Given the modest girth of judicially crafted doctrines governing insider trading, it is hard to see how Scenario I (or any other Scenario) would trigger trader liability under the conventional insider trading model, as no fiduciary relationship is breached when a hacker targets an unrelated company's MNPI and passes such information along to an unrelated trader. Thus, "[c]onventional wisdom had held that mere thieves cannot be liable for trading on stolen confidential information because they lack a fiduciary relationship to the source of the information and, therefore, do not deceive that source."[86] Nevertheless, this "conventional wisdom" could fade if the courts agree to nourish the new outsider trading theory arising out of Rule 10b-5.

Outsider Trading: A New Paradigm, or an Unwieldy Kludge?

Under several accountings, the SEC is currently developing a "new paradigm" of unlawful "outsider trading" under Section 10(b) and Rule 10b-5 to reach "a third and new category of securities miscreant — 'outsiders' — who do not work for (or with) the company, and who do not owe a duty to anyone."[87] This new category aims to capture trading on the basis of MNPI obtained via computer hacking in situations (like Scenario I) lacking the fiduciary relationship required by insider trading law. Should courts grant the SEC this liberal mandate, it could certainly bring civil securities fraud charges against a Scenario I hedge fund that coordinates with a hacker to trade on stolen information.

But what would a new theory of "outsider trading" look like? The SEC argues that trading "outsiders" are culpable under 10b-5 because they "are masquerading as company insiders and are therefore committing securities fraud."[88] In other words, the "deception" required by Rule 10b-5 "usually relates directly to the hacking or unauthorized computer access and is a bit more attenuated from the securities transaction."[89] Given this attenuation, it could be that the "in connection with the purchase or sale of any security" requirement of Rule 10b-5 is called into question. The SEC's theory

[85] *O'Hagan*, 521 U.S. at 653.
[86] Steinbuch, *supra* note 76 at 589.
[87] Stark, *supra* note 58.
[88] *Id.*
[89] *Id.*

bears a strong resemblance to Donald Langevoort's development of the idea of "intentional deception" as a trigger of fraud liability, suggesting that "[s]o long as an element of intentional deception was present in the action, the resulting trading would seem to satisfy the 'in connection with' requirement and lead to liability under Rule 10b-5." [90] Arguing for the normative desirability of this test, Langevoort concludes, "[T]here is little reason to believe that gaining a trading advantage by deceptive theft is any less deserving of proscription under Rule 10b-5 than gaining a trading advantage by a secretive breach of fiduciary duty."[91]

While the theory outsider trading triggered by deliberate deception remains relatively untested to date, the SEC has been bringing facially similar charges against outsider trading defendants since at least 2005.[92] In 2007 and 2008, *SEC v. Dorozhko*[93] gave the SEC its sole opportunity thus far to establish a beachhead of an outsider trading theory. In Dorozhko, Second Circuit confronted the question of "whether, in a civil enforcement lawsuit brought by the [SEC] under Section 10(b) of the ['34 Act], computer hacking may be 'deceptive' where the hacker did not breach a fiduciary duty in fraudulently obtaining [MNPI] used in connection with the purchase or sale of securities."[94] Dorozhko allegedly hacked into the computer network of an investor relations and web-hosting company to access unreleased earnings reports for IMS Health, Inc., which indicated that the company would miss its expected earnings, and subsequently traded on this MNPI through the purchase of put options.[95] The Southern District of New York found that Dorozhko's behavior "might be fraudulent and might violate a number of federal and state criminal statutes," but that his behavior did not violate Section 10(b) because Dorozhko did not owe a fiduciary duty to either the web-hosting company or to the hacked company.[96] Reversing the District Court, the Second Circuit answered the stated question in the affirmative, granting the SEC's application for a preliminary injunction freezing defendant Dorozhko's trading account.[97] The Second Circuit acknowledged that the SEC's claim was "not based on either of the two generally

[90] Donald C. Langevoort, *Insider Trading Regulation, Enforcement, and Prevention* § 6:14. *See also* United States v. Falcone, 257 F.3d 226, 233–34 (2d Cir. 2001) ("O'Hagan 's [sic] requirement that the misappropriated information 'ordinarily' be valuable due to 'its utility in securities trading,'…appears to be a more generally applicable factor in determining whether section 10(b)'s 'in connection with" requirement is satisfied. That requirement is met in a case where, as here, the misappropriated information is a magazine column that has a known effect on the prices of the securities of the companies it discusses.")
[91] *Id*.
[92] See e.g., SEC v. Lemus, Havel & Viiseman, et al. (2005), SEC v. Blue Bottle (2007), and SEC v. Stummer (2008), which were never contested in court. Stark, *supra* note 58.
[93] Stark, *supra* note 58.
[94] SEC v. Dorozhko, 574 F.3d 42, 43, 44 (2d Cir. 2009).
[95] Id. at 44.
[96] *Id*. at 45.
[97] *Id*. at 43, 51.

accepted theories of insider trading," but found that it was "nonetheless based on a claim of fraud" and turned its attention to "whether this fraud is 'deceptive' within the meaning of Section 10(b)."[98] In reasoning consistent with the above discussion of insider trading as a specific type of fraudulent deception, the Second Circuit explained that "what is sufficient [to establish a breach of Section 10(b)] is not always what is necessary."[99] Because Dorozhko's actions—hacking to gain access to and trade on MNPI—allegedly constituted an "affirmative misrepresentation" (as opposed to the nondisclosure that is so problematic when an insider has a duty to speak)[100], and because violation of the "affirmative obligation in commercial dealings not to mislead" is "a distinct species of fraud," the Second Circuit held that he could be liable under the antifraud rules despite the absence of a fiduciary relationship.[101]

Having made the general point that no fiduciary relationship is *necessarily required* under Section 10(b), the Second Circuit remanded the case to decide the fact-specific question of "whether the computer hacking in this case…as opposed to computer hacking in general…involved a fraudulent misrepresentation that was 'deceptive' within the ordinary meaning of Section 10(b)".[102] In doing so, the Second Circuit gave guidance regarding the ordinary meaning of "deceptive," which "covers a wide spectrum of conduct involving cheating or trading in falsehoods" and "irreducibly entails some act that gives the victim a false impression."[103] The Court introduced ambiguity to its otherwise clear opinion by stating, "In our view, misrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly 'deceptive' within the ordinary meaning of the word. It is unclear, however, that exploiting a weakness in an electronic code to gain unauthorized access is 'deceptive,' rather than being *mere theft*."[104] Thus, the Second Circuit asked the District Court to take a deeper dive into "how the hacker gained access" in order to determine whether the actions constituted "a 'deceptive device or contrivance' that is prohibited by Section 10(b) and Rule 10b– 5."[105] Unfortunately, Second Circuit panel's invitation in *Dorozhko* was never formally taken up by the District Court on remand: Dorozhko's attorney lost touch with his client and the trial court later granted summary judgment for the SEC. [106]

---

[98] *Id*. at 45.
[99] *Id*. at 49.
[100] *Id*. at 48, 49.
[101] *Id*. at 49.
[102] *Id*. at 51.
[103] *Id*. at 50.
[104] *Id*. at 51 (emphasis added).
[105] *Id*.
[106] Stark, *supra* note 58.

Nevertheless, a fair reading of the opinion suggests that trading on hacked information might constitute actionable securities fraud, but only if accompanied by deception. According to one prominent commentator "hacking might not be a securities fraud if, for instance, it was based on discovering weaknesses in software rather than, a *deception*, such as a hacker using hijacked employee credentials."[107] Thus, while negligently weak computer systems that "leav[e] a virtual door open for an online intruder" might not constitute "deception," the use of malware and the tools/processes more generally associated with the popular perception of hackers might suffice.[108] Regulators and courts will no doubt grapple with defendants about where to draw this line in the sand should outsider-trading theory gain traction.

Dorozhko's unrequited invitation is just one reason why *Dubovoy* may well represent an important moment for informed cyber-trading under federal securities law. The *Dubovoy* pleadings are instructive and show that the SEC has studied (many times over) the language in *Dorozhko*. For example, The SEC's initial complaint alleges that the *Dubovoy* Hackers used deception as follows[109].

> The hacker defendants used deceptive means to gain unauthorized access to the Newswire Services' computer systems, using tactics such as: (a) employing stolen username/password information of authorized users to pose as authorized users; (b) deploying malicious computer code designed to delete evidence of the computer attacks; (c) concealing the identity and location of the computers used to access the Newswire Services' computers; and (d) using back-door access-modules.

Moreover, the SEC's initial complaint alleges that the *Dubovoy* Traders used deception to conceal their activities through shell entities and misleading payments,[110] multiple trading accounts[111], and a secure server.[112]

---

[107] *Id*.
[108] *Id*.
[109] Complaint ¶ 71, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015). Stark, *supra* note 58.
[110] Complaint ¶ 84, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015) ("The Dubovoy Group defendants attempted to conceal the illegal payments by sending them from Tanigold Assets, one of Arkadiy Dubovoy's companies, and mislabeling them as payments for 'technological equipment' and 'building equipment.'").
[111] Complaint ¶ 91, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015) ("The Dubovoy Group defendants tried to conceal their fraud by deceptively spreading their illicit trading across numerous accounts at more than 10 brokerage firms in the names of various individuals and entities. Through this strategy, they hoped to avoid detection by brokers, regulators, and law enforcement.").
[112] Complaint ¶ 85, SEC v. Dubovoy, et al., No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015) ("Pavel Dubovoy provided instructions, which informed the reader how to log in to the server and download files and advised users to conceal the identity of the computer they used to access the server.").

Based on the preliminary opinions thus far produced in the case, it appears that courts have lent a sympathetic ear to such arguments, repeatedly using the word "fraud" to describe the *Dubovoy* Traders' actions in connection with federal securities law.[113] Moreover, in the Amaryan Opinion, without specifically elaborating on the legal standard required by Section 10(b) or Rule 10b-5, the court suggests that "the evidence submitted by the SEC raises a strong inference that the Amaryan Defendants violated federal securities laws."[114] And, even more recently, the SEC obtained a default judgment against several trading defendants on highly similar facts. In *SEC v Iat Hong, et al.*, several traders were charged with hacking into a law firm (by installing malware and compromising accounts that enabled access to law firm email accounts) and fraudulently trading on MNPI. In the default judgment, the judge concluded that the evidence "sufficiently demonstrates that Defendants directly, indirectly, or through or by means of others, hacked into the nonpublic networks of two New York-headquartered law firms and stole, through deception, confidential information covering several publicly-traded companies" and then "reaped illegal profits by trading on the stolen [MNPI]" in violation of Sections 10(b) and 20(b) of the '34 Act and Rule 10b-5 thereunder, among other securities laws.[115] While this was a default judgment rather than a litigated case, the SEC no doubt welcomes the judge's description of this hacking as deceptive.

Limits of Outsider Trading (Scenarios II through IV)

Notwithstanding its evident traction in judicial opinions, outsider-trading theory has garnered its fair share of critics decrying its many alleged infirmities. Many critics have been wary of a significant expansion of insider trading based an amorphous concept of "deception," and have instead argued that misappropriation theory can capture many of the most concerning hacker-trader conspiracies.[116] Others have lodged even stronger opposition to the concept of liability for outsiders under the antifraud

---

[113] *See, e.g.*, SEC v. Dubovoy, No. CV 15-6076, 2016 WL 5745099, at *4, 5 (D.N.J. Sept. 29, 2016) (Suggesting that: (i) "The scheme alleged in the Amended Complaint is a complex one, involving a number of individuals, entities, and straw owners who worked together to perpetrate a complex, high-tech fraud."; (ii)"These circumstances also support a strong inference that Memelland acted with scienter," where "'[s]cienter is a mental state embracing intent to deceive, manipulate or defraud, and can be established by showing recklessness."; and (iii) "Memelland's sophistication, the temporal proximity of its trades to the publication of the press releases, the similarity of its trading pattern to other Trader Defendants with conspicuous ties to the Hacker Defendants, its shared IP channels with the Dubovoy Group, and the fact that the stolen press releases contained financial information that had not yet been reported in the news all strongly support an inference that Memelland intended to participate in the fraud."

[114] SEC v. Dubovoy, No. CV 15-6076, 2015 WL 6122261, at *4 (D.N.J. Oct. 16, 2015).

[115] Default Judgment ¶ 11, SEC v. Hong et al., No. 16-cv-9947 (S.D.N.Y. filed May 5, 2017), https://regmedia.co.uk/2017/05/10/china_sec.pdf.

[116] Steinbuch, *supra* note 76 at 594-95 ("O'Hagan and its progeny should not be read as requiring a fiduciary relationship under the misappropriation theory. Both the underlying purpose of the misappropriation theory and courts' interpretation of it demonstrate that the theory encompasses the acts of nonfiduciaries.").

provisions, arguing that the new theory opens an unwieldy and unnecessary Pandora's box.[117] Andrew Vollmer, for example, has argued that "[t]he government had the ability to charge one or more reasonable and appropriate crimes against the hacker and trader defendants but reached out too far to include securities fraud."[118] And, even sympathetic judicial opinions (such as *Dorozhko*) have held that computer hackers do not typically commit insider trading, and do so only if they employ deception in their hack and such deception ultimately gives rise to trading. When either is absent, a hacker's actions are too far removed from the trading to be considered "in connection with" the purchase or sale of securities.[119]

We share some of this skepticism: it may be a bridge too far to apply the nascent doctrine of outsider-trading reliably across all hacking-trading permutations as defined above in Table 11. It seems settled that hacking through unauthorized access is reflective of "deceit," and that the "in connection with" requirement would be satisfied if the hacker and traders coordinated (such as through payments and "shopping lists" alleged in *Dubovoy*). That said, would such distinctions help in navigating the remaining scenarios, involving either the exposure of vulnerability coupled with coordinated trading (Scenario II), or the actions of a trader who simply learns that an unrelated hacker has either stolen data (Scenario III) or has found a vulnerability (Scenario IV)?

By our estimation, even if courts fully embrace the concept of outsider trading, such a move would only tend to capture *some* of Scenario II, where a vulnerability-publicizing hacker (a) uses deception to gain access and (b) coordinates with a trading party who transacts prior to any public disclosure of the breach and/or vulnerability. And even there, the requirement of *deception* would seem to exclude a host of factual situations under Scenario II where a hacker (say) makes thousands of random incursions in an effort to detect a vulnerability, but never falsely purports to be acting as an employee, customer, or other permitted party in order to gain access. Such scenarios raise roughly identical policy concerns with informed cyber-trading raised in the prior section; but they would generally not be captured by an "outsider trading" extension of current law.

[117] Vollmer, *supra* note 44 ("The recent computer hacking cases are important because they create dangers from over-zealous pursuit of securities law violations…Some bad acts are not securities fraud.").
[118] *Id.*
[119] *Id.*

In Scenarios III and IV, the link to liability under nascent outsider trading theories is even more attenuated, since there the trader is presumed unaffiliated with the hacking. This severing of coordination is particularly important for the "in connection with" requirement under the statute – particularly insofar as it pertains to the trader. A trader (such as a hedge fund) who merely discovers that a current target is being hacked and trades on that information would not appear to be liable, regardless of the motivations of the initial hacker.[120] At the same time, of course, many of the idiosyncratic concerns raised by informed cyber-trading tend to stand out when the hacker and trader *can* coordinate their actions (thereby bolstering the hacker's incentives to overinvest in hacking and the target's incentives to overinvest in precaution). Viewed thusly, the inability for outsider trading to reach Scenarios III and IV is perhaps less critical than its ill fit with efficiency concerns under Scenarios I and II.

What might be a better direction for the evolving outsider-trading doctrine? It seems relatively clear (at least to us) that courts' nascent focus on *deception* (no doubt an artifact of statutory pedigree) tends to miss the mark from an efficient markets perspective. Rather, many of the market efficiency concerns associated with cyber-trading appear to be orthogonal to deception *per se*, and instead circulate around *coordinated action* between the hacker and the trader. Such coordinated hacking and trading was clearly present in both *Dorozhko* and *Dubovoy*, and the outcomes of both could be justified on that basis. Viewed in this sense, the requirement of deception would appear to place an unattractive (and under-inclusive) limitation on the outsider-trading doctrine.

That said, if courts focused instead coordinated hacking and trading schemes for triggering liability, the result risks being wildly over-inclusive in practice, particularly when one considers how to define the amorphous boundaries of what it means to "hack". For example, does doing substantial research in a target company's activities (much of it over the Internet and targeted to information the company has made available) constitute hacking? How might one distinguish targeted research from undesirable hacking? Here, we concede that the line drawing challenge would prove difficult at a minimum. Pragmatically, then, there may be some justification in the judicial embrace *deception*, not as a desideratum grounded in first principles (of efficiency), but rather as a pragmatic mechanical governor on the undisciplined growth of outsider trading doctrine.

[120] To be sure, it is possible that outsider trading may evolve to prescribe unaffiliated third-party traders who know (or have reason to know) of the hacker's motivations. The cases thus far have stopped (far) short of this conclusion, however.

To the extent that courts continue to pursue the "deception" lever for extending 10b-5 liability, moreover, they would do well (for consistency's sake at least) to consult the rapidly-evolving jurisprudence interpreting the criminal prohibition on accessing a computer "without authorization or exceeding authorized access" under the Computer Fraud and Abuse Act (CFAA).[121] Indeed, there might be substantial benefits to unifying the tests governing criminal computer fraud and outsider-trading liability, in that defendants would have one clear standard defining the scope of prohibited conduct. Prohibiting trading on information obtained without authorized access or exceeding authorized access might serve as a useful starting point for a more expansive scope of securities fraud.

A final, alternative approach—and one that we develop in a technical companion to this paper[122]—would broadly prohibit informed cyber-trading, beyond an exempted initial arbitrage "allowance" (e.g., a monetary cap or a fraction of the firm's economic heft) which the arbitrageur would be able to pocket as a "reward" for bringing the information to light. Beyond the exemption amount, the arbitrageur would be required to adhere to a "disclose or abstain" duty, refraining from trading on the information until it has disclosed the information to the targeted issuer and the market. If the size of the exemption is calibrated at a reasonable level, this alternative approach would have the benefits of (a) preserving price discovery (at least within the limits of the exemption); (b) preserving limited incentives to uncover information about vulnerability; and (c) catalyzing communication to the issuer about the nature of the vulnerability, so as to streamline the issuer's precautionary measures. Although we see much to commend this prescriptive course from an economic policy perspective, we confess that it would be a difficult change to effect under current law (in the absence of a statutory reform).[123]

5. Conclusion

In this paper, we have considered the phenomenon of informed cyber-hacking, whereby market arbitrageurs learn of material, yet-to-be-disclosed cybersecurity breaches, executing trades in advance of the public disclosure. We have demonstrated empirically that such practices appear manifest in the derivatives market trading, where breach-disclosing firms appear to have significantly larger open

[121] 10 U.S.C. § 1030.
[122] See Mitts & Talley (2017) (technical companion).
[123] Difficult, but perhaps not impossible. The requirement of deception could be met by equating cooperation between hackers and traders as deceptive; and, much of the damages jurisprudence in insider-trading law is (and always has been) the product of precedential evolution. Our analysis excludes the possibility of common law tort claims against an informed cyber-trader, since such claims would have a difficulty establishing a duty by either the hacker or trader, and may well be preempted by federal securities law anyway.

interest and trading volume in put options (relative to a variety of control groups) in advance of the disclosure. Our results, moreover, are robust to a variety of alternative specifications and identification strategies. We have also argued that such market activity raises particular and idiosyncratic normative concerns, potentially justifying an expansion of securities fraud liability to capture such concerns. Under current law, however, it seems unlikely that such an expansion is possible without a conceptual reform to received insider trading law, which has thus far been confined to corporate fiduciaries and those who breach a duty of trust and confidence owed to the source of material non-public information. We have argued that recent endeavors to expand insider trading to outsiders (including hacker-traders) who use deception to breach a firm's cybersecurity system may be warranted, though not a perfect fit for the policy concerns in play. Nevertheless, it will prove difficult to craft an alternative doctrine that does not run the risk of being severely over- or under-inclusive. Consequently, in spite of its imperfections, the nascent theory of "outsider trading" may be a worthwhile experiment to pursue.