INFORMED TRADING AND CYBERSECURITY BREACHES*

JOSHUA MITTS†
ERIC TALLEY‡

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, both securities fraud and computer fraud in their current form appear poorly adapted to address such concerns, and both would require nontrivial reimagining to meet the challenge (even approximately).

TABLE OF CONTENTS

* We thank Alexander Guembel, Laurie Hodrick, Colleen Honigsberg, Gur Huberman, Bruce Johnsen, Don Langevoort, Mark Lemley, Jusin McCrary, Yaron Nili, Mitch Polinsky, Fernan Restrepo, and workshop participants at Columbia, George Mason, Georgetown, the Santa Fe Institute, the Securities & Exchange Commission, Stanford, the Toulouse School of Economics, UC Irvine and Wisconsin-Madison for helpful comments and discussions. Kailey Flanagan and Hanna K. Song provided excellent research assistance. This is a companion piece to an eponymous technical manuscript offering a more detailed theoretical analysis. All errors are ours.

†Associate Professor, Columbia Law School. joshua.mitts@law.columbia.edu.

‡Isador & Seville Sulzbacher Professor of Law, Columbia Law School; Co-Director, Millstein Center for Global Markets and Corporate Ownership. etalley@law.columbia.edu.

INTRODUCTION

The ascendancy and impact of the information economy during the last quarter century have been 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—which didn't make the cut—was a moribund upstart from the 1980s; Facebook and Bitcoin were still a decade away from inception. 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.

And yet, a key pillar of the digital economy—the ease of accessing, copying, and 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 (including Social Security numbers) of tens of millions of clients, was hardly the first of its kind, nor will it be 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).[1] Only after taking a substantial short position in St. Jude did Muddy Waters publicly disclose the device's vulnerability,[2] causing an immediate fall in St. Jude's stock price of about eight percent.[3] Similar patterns

[1] Matthew Goldstein et al., *Unusual Pairing Makes Public Bet vs. Pacemakers*, N.Y. TIMES, Sept. 9, 2016, at B1–B2.

[2] *See id.* at B1.

[3] Michelle Celarier, *Muddy Waters Ends 2016 with a Big Gain*, INSTITUTIONAL INV., Jan. 13, 2017, https://www.institutionalinvestor.com/article/b1505q7kzxzsyg/muddy-waters-ends-2016-with-a-big-gain ("St. Jude's initially dropped 8 percent on Block's August 25 short call

of material changes in value after disclosure of a cybersecurity event are now commonplace.

Muddy Waters' securities market play around St. Jude's data breach disclosure is perhaps unsurprising—particularly when: (1) cybersecurity breaches can have profound price effects in capital markets; and (2) 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.[4] In contrast, buying low and selling high (or selling high and buying low) in securities markets is a venerated ritual of capitalism. 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 cyberhacking—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 study securities market trading plausibly on the basis of advance knowledge of a cybersecurity breach ("informed cybertrading"). Conceptually, such information arbitrage opportunities are eminently possible, and privately informed traders can typically exploit their information so long as there is sufficient independent market activity (for example, among liquidity or noise traders) to provide "cover" for the informed arbitrageur.[5] Thus, informed traders can have strong incentives to take short positions against the hacked firms—positions that should be detectable in securities market activity. We test this proposition empirically, making use of a novel data set of 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 analyses. We view these results as consistent with the proposition

---

but recovered slightly as its announced deal with Abbott Laboratories looked more certain.") 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* Leslie Hook & Richard Waters, *SoftBank Share Purchase Discounts Uber by 30%*, FIN. TIMES (London), Nov. 28, 2017, https://www.ft.com/content/2a2131e0-d3ef-11e7-a303-9060cb1e5f44.

[4] *See, e.g.,* 18 U.S.C. §§ 1028A, 1030 (2018); *infra* Part IV.

[5] Albert S. Kyle, *Continuous Auctions and Insider Trading*, 56 ECONOMETRICA 1315-1335 (Nov. 1985) (showing how informed trader disguises information in noisy order flow).

that arbitrageurs tend to have early notice of impending cybersecurity breach disclosures, and that they trade on the basis of that information.

Although our principal focus is positive and empirical in nature, our findings also hold relevance for larger normative 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 allocative efficiency. Informed cyber-trading shares many of these traits, but it also tees up other idiosyncratic efficiency concerns. If significant arbitrage rents from advance knowledge of cybersecurity risks were wholly undeterred, several inefficient investment distortions plausibly follow, both by hackers[6] (including cybersecurity firms) whose efforts tend to publicize and exacerbate vulnerabilities that would otherwise remain unobserved, and by issuers themselves—anxious to expend efforts to frustrate or divert hackers' attention. Moreover, the redistributive profits obtained via these trading opportunities may incentivize hackers to exploit security vulnerabilities, leading to greater dissemination of stolen personal information, impersonation, and identity theft. These represent real economic costs, which are largely absent in garden-variety information-trading contexts. Consequently, we argue, informed cyber-trading plausibly justifies enhanced legal scrutiny of those who profit from the activity.

Nevertheless, several variations of informed cyber-trading appear to be perfectly legal under current law. 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 computer queries to access, 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 violate market manipulation proscriptions, which require the introduction of "*inaccurate* information into the market."[7] Nor would they appear to run afoul of received insider trading theories, which still require the breach of a confidential or fiduciary relationship (though courts are actively revisiting this requirement as of the date of writing).[8] Perhaps a better match on liability

---

[6] *See infra* Part IV.

[7] SEC v. Masri, 523 F. Supp. 2d 361, 372 (S.D.N.Y. 2007) (emphasis added).

[8] *See* United States v. O'Hagan, 521 U.S. 642, 652 (1997). 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, but who use deceptive means to hack into another's computer system. *See, e.g.*, SEC v. Dorozhko, 574 F.3d 42, 51 (2d Cir. 2009) ("[M]isrepresenting 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."). Nevertheless, no court to our knowledge has firmly embraced this expansion to date. We discuss this nascent strand of case law (sometimes referred to as "outsider trading"). *See infra* Part IV.

grounds would be the provisions of the Computer Fraud and Abuse Act (CFAA), which (notwithstanding its name) does not require a showing of intent to defraud in order to trigger liability.[9] But the CFAA remains relatively untested in these contexts, and its remedies provisions are generally limited to concrete remediation costs.[10] In short, the task of redesigning law to address the costs of informed cyber-trading is a sizable ask, posing a difficult prospective challenge for policy makers and regulators alike.

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[11] have developed frameworks for analyzing self-protection decisions among firms that are potential cybersecurity risks, arguing that firms, in a world of scarce resources, may optimally triage their self-protection efforts based on a cost-benefit calculus. Such calculus can often give rise to collective action problems of either under- or over-investment in protection, when (say) interconnected firms within a network make individual decisions about security.[12] Others in information sciences have analyzed the problem from the standpoint of timing, asking whether targets should invest proactively before an attack or reactively afterward.[13] If reactive investment is possible to mitigate an existing attack (and the information about such an attack becomes known), it may well be optimal to under-invest in proactive technology and utilize such mitigation efforts once attacks are detected.[14]

Although we are unaware of significant market pricing literature on informed cyber-trading *per se*, the efficiency implications of informed trading have been richly explored using seminal frameworks from information economics, which demonstrate how informed traders can simultaneously catalyze price discovery and impede market depth and liquidity.[15] Empiri-

---

[9] 18 U.S.C. § 1030 (2018).

[10] 18 U.S.C. § 1030(g) (2018).

[11] *See, e.g.*, Lawrence A. Gordon & Martin P. Loeb, *The Economics of Information Security Investment*, 5 ACM TRANSACTIONS ON INFO. & SYS. SECURITY (TISSEC) 438, 439 (Nov. 2002) (reviewing literature).

[12] *See* Marc Lelarge, *Coordination in Network Security Games: A Monotone Comparative Statics Approach*, 30 IEEE J. ON SELECTED AREAS IN COMM. 2210, 2210-2219 (Nov. 2012); Howard Kunreuther & Geoffrey Heal, *Interdependent Security*, 26 J. RISK & UNCERTAINTY 231, 231–49 (Mar. 2003) (making a similar point using a framework based on a terrorism scenario); Darius N. Lakdawalla & Eric L. Talley, *Optimal Liability for Terrorism* 1-34 (Nat'l Bureau of Econ. Research, Working Paper No. 12578, 2006), https://ssrn.com/abstract=935571 (applying, similarly, 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).

[13] *See* Rainer Böhme & Tyler Moore, *The "Iterated Weakest Link" Model of Adaptive Security Investment*, 7 J. OF INFO. SECURITY 81, 86–91 (2016).

[14] *Id.* at 91.

[15] *See, e.g.*, Albert S. Kyle, *Continuous Auctions and Insider Trading*, 53 ECONOMETRICA 1315 (Nov. 1985); Paul Milgrom & Nancy Stokey, *Information, Trade and Common Knowledge*, 26 J. ECON. THEORY 17 (1982); Lawrence R. Glosten & Paul R. Milgrom, *Bid, Ask and Transaction Prices in a Specialist Market with Heterogeneously Informed Traders*, 14 J. FIN.

cally, our analysis draws on a growing computer science literature identifying misconfiguration flags to predict vulnerability to hacking, as well as estimating latency periods for cybersecurity vulnerability breaches (of between one and twelve months before disclosure).[16] 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 presents a meta-analysis of thirty-seven papers containing forty-five empirical studies of the effect of information-security breaches on public company stock prices from 2003 to 2015.[17] The authors find that 75.6% of the studies measure statistically significant stock-price reactions to the disclosure of cybersecurity breaches.[18] Twenty out of twenty-five studies find negative and significant stock-price reactions for victim firms, and none of these find significant positive reactions for victim firms.[19] 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.[20] Consistent with our findings, at least one significant study finds evidence of pre-announcement information leakages associated with cybersecurity vulnerabilities.[21] That said, we are unaware of any prior study measuring trading patterns in the months preceding the disclosure and the central legal implications of such patterns, as we explore here.

An important caveat to our analysis warrants attention before proceeding. Although our empirical results are strongly consistent with the type of informed cyber-trading that occurred in the St. Jude-Muddy Waters episode, trading activity by other market participants could produce similar results. If, for example, employees or managers of the target firm discovered early evidence of a cybersecurity breach or a vulnerability, they might also attempt to profit from that information prior to disclosure, and their activity would similarly be observable in our data. Although many of the policy considerations highlighted earlier would apply to this type of trader too, existing law is already well equipped to deal with it—since insiders at the firm typically owe duties of "trust and confidence," the breach of which will clearly trig-

---

ECON. 71 (1985). There is also a robust literature related to options market trading in advance of general corporate news. *See, e.g.,* Patrick Agustin et al., *How Do Informed Investors Trade in the Options Market?* (June 1, 2018), http://people.stern.nyu.edu/msubrahm/papers/Informed.pdf.

[16] *See* Leyla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*, ACM CONFERENCE ON COMPUT. & COMMC'NS SEC. 833, 842 (2012); *see also* Yang Liu et al., *Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents*, USENIX SEC. SYMP. 1009, 1017 (2015).

[17] *See* Georgios Spanos & Angelis Lefteris, *The Impact of Information Security Events to the Stock Market: A Systematic Literature Review*, 58 COMPUT. & SEC. 216 (2016).

[18] *Id.* at 226.

[19] *Id.* at 227.

[20] *Id.*

[21] *See* Maria C. Arcuri et al., *The Effect of Information Security Breaches on Stock Returns: Is the Cyber Crime a Threat to Firms?*, EUR. FIN. MGMT. ASS'N. CONFERENCE (2014) (finding that the mean cumulative abnormal return to 128 cybersecurity disclosures is -.0029 in the (-20,20) window, but shrinks to -0.003 in the (-1,1) window).

ger insider trading liability under current law. In many ways, in fact, it is the curiously *distinct* legal treatment accorded insiders and outsiders in the context of informed cybertrading that makes the topic an interesting one to ponder.

Our analysis proceeds as follows. Part two 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.[22] Part three 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. Part four delves further into whether current legal institutions are equipped to take on the added threats of informed cyber-trading. Here we argue that contemporary securities fraud and computer fraud law appear, at least individually, unfit for the challenge, both suffering from distinct forms of under-inclusiveness. While long-term statutory reforms may provide a durable response, in the shorter term a more expedient elixir is likely to be maintaining the status quo, in which both doctrines play a supporting role in concert with expert regulators (such as the Securities and Exchange Commission (SEC)), who should remain involved. Part five concludes.

I. Empirical Evidence of Informed Cyber-Trading

In this Part, we dispense with the long-winded lawyerly prologue,[23] cutting directly to the chase to: (1) describe our approach for detecting informed trading in advance of cybersecurity breach announcements; and (2) report on our core empirical findings.

A. Data Sources

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."[24] The ITRC's data breach report includes both exposure of personally identifying information—for example, 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

[22] *See infra* Part II.A (defining "open interest").

[23] Dispirited lawyerly types can nonetheless savor the opportunity to luxuriate in the palaverously doctrinal *denouement* comprising. *See infra* Part IV.

[24] Identity Theft Resource Center, Data Breach Reports 3 (2015), https://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

username and passwords that are not necessarily tied to an identifiable individual.[25] One example of an ITRC data breach report—for a 2015 breach of Hyatt Hotels—is reproduced in Figure 1[26]:

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 that 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—such as a news media report or disclosure by (or through) a governmental agency.[27]

The ITRC identified 4,580 data breaches from 2010 through 2015.[28] While the vast majority of these incidents involve private companies, nonprofits and governmental actors, we were able to match 145 breaches to publicly traded companies.[29] 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—so, larger words appear more frequently in the textual descriptions. As Figure 2 shows, the most popular terms in these descriptions reflect information that would typically be the subject of a data breach—including

[25] *Id.* at 2.

[26] *Id.* at 31.

[27] State privacy laws often require companies to notify individuals whose personal information may have been compromised. *See, e.g.*, Notification of Security Breach Required, N.H. REV. STAT. ANN. § 359-C:20 (2018). Moreover, specific federal laws sometimes require disclosure, e.g., when health concerns are implicated, Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. § 164.400–414 (2000), 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, cybersecurity vulnerabilities may fall into one of the enumerated categories of material event disclosure required under Form 8-K.

[28] IDENTITY THEFT RESOURCE CENTER, *supra* note 24.

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

personal information, email addresses, credit cards, addresses, and social security numbers.

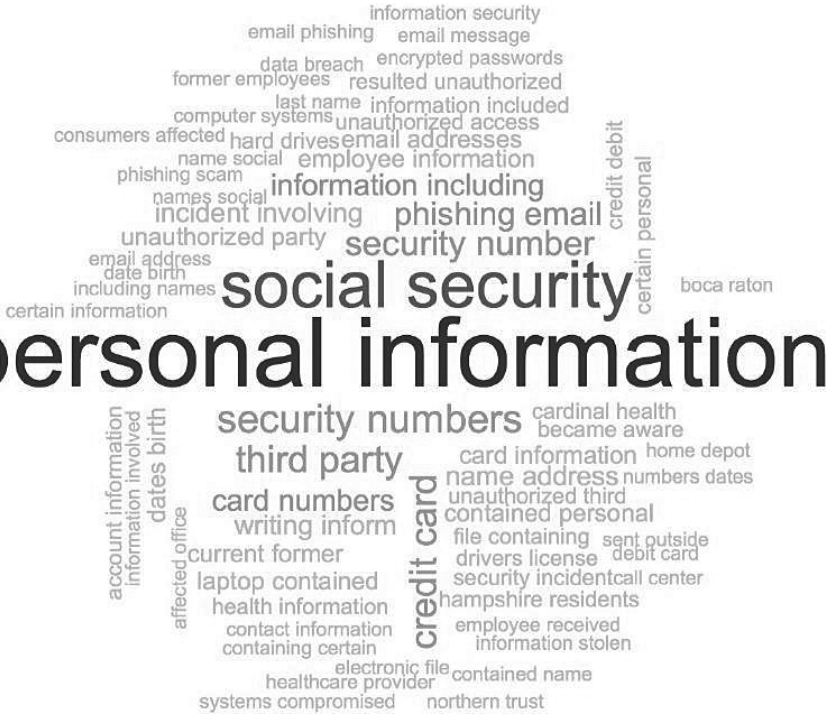

Figure 2: Bi-Gram Word Cloud for ITRC Data Breach Reports

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—a "control" group. Even if actors did not trade on corporate data breaches—for example, if we were simply to 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 to 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 appears to hold, then we are justified in concluding that the observed differences are attributable (at least in part) to hacker trading or tipping.

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 speci-

fied 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 the firm's stock price on its maturity date, then the holder of a put option who acts to maximize her payoff will receive the greater of the strike price minus the stock price or zero at the time of expiry.[30] 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.[31]

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—one would be hard-pressed to find an example of a successful data breach that would 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. Thus, market demand for put options may reflect that hackers or their "tippees" are seeking 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 ATM—so, they have a delta between 0.4 and 0.6.[32] Within this range, 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.

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 period 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 period relative to a data breach event. For example, we

---

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

[31] 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.

[32] The delta of a put option refers to the sensitivity of the put's value to changes in the underlying stock price.

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 section, 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.

B. 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.[33] 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*—defining 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 period is higher for firms that are the victims

[33] *See, e.g.*, Jonah Gelbach & Jonathan Klick, *Empirical Law and Economics*, 1 OXFORD HANDBOOK OF LAW & ECON. (Francesco Parisi ed. 2017).

of data breaches. As described below, we employ propensity score matching[34] 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.[35] 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 firm-level covariates, measured as of the year prior to the attack, 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, 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,[36] 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) four-digit Standard Industrial Classification (SIC) industry code; (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 that reason, we do not attempt to compare trading behavior between firms in different industries

---

[34] *See generally* Alberto Abadie & Guido W. Imbens, *Large Sample Properties of Matching Estimators for Average Treatment Effects*, 74 ECONOMETRICA 235 (2006).

[35] 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 & Dumitras, *supra* note 16, at 842.

[36] *See* Abadie & Imbens, *supra* note 34.

Table 1: Summary Statistics: Cross-Sectional Dataset

	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 2: Summary Statistics: Difference-in-Differences 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

For these reasons, we are forced to drop those firms in industries which are too small to allow for 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 forty-six treatment firm-event pairs and 3,319 control firm-event pairs in the difference-in-differences dataset and fifty-one treatment firm-event pairs and 3,425 control firm-event pairs in the difference-in-dif-

ferences dataset.[37] Tables 1 and 2 present summary statistics on these datasets.

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—or 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 four-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-differences 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-differences datasets, respectively.[38] The similarity in the density of the two propensity scores suggests that the two groups are balanced on the propensity score.

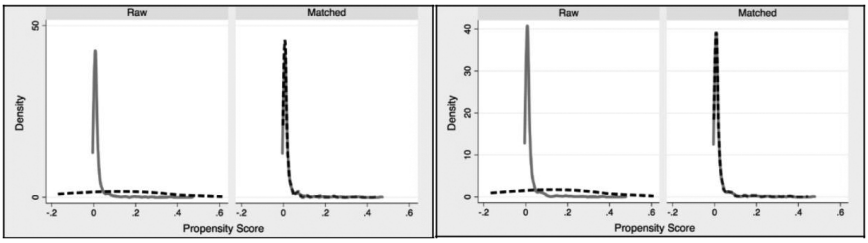

Figure 3: Propensity Score Balance Tests for Cross Sectional (left panel) and Difference-in-Differences Data Sets (right panel). In both the left and right panels, the density of propensity scores is plotted for treatment groups (solid lines) and control groups (dashed lines), comparing the raw controls with the propensity score matched observations.

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, we present the results using propensity score matching on individual covariates, as well as on all of the covariates together, to illustrate that the results do not depend on which covariates are included.[39]

Table 3 compares covariate means in the cross-sectional and difference-in-differences dataset between the raw and matched samples. While the

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

[38] 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.

[39] *See supra* Part II.B.

matching is unable to achieve perfect balance across all of the covariates simultaneously, Table 3 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 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

	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.

C. Cross-Sectional Analysis

We begin by estimating the average treatment effect ("ATE") for the targeted firms by propensity score matching[40] 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.[41] Here, our identification strategy is based on the assumption that this interval is likely to be unknown to anyone

[40] See Abadie & Imbens, *supra* note 34.
[41] We show below that the results are not driven by the choice of this interval.

other than the hacker (and any tippees) and corporate officers who may have become aware of the data breach. First, we estimate the difference in logged open interest on outstanding put options between treatment and control firms for a variety of matching covariates. The results are shown in Table 4:

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; Logged Open Interest

As the first row of Table 4 illustrates, there is an average increase of between 0.36 and 0.75 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 a sense of the economic significance of the coefficients reported above, recall from Table 1 that the mean logged 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, which shows an average increase of between 0.53 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 represent 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 provide 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,[42] inverse-probability weighting with regression adjustment,[43] and regression adjustment.[44] The results are shown in the panels of Table 6, which demonstrates significant consistency across scoring methodologies.

[42] *See* Guido W. Imbens, *The Role of the Propensity Score in Estimating Dose-Response Functions*, 87 BIOMETRIKA 706, 707–708 (2000).

[43] *See generally* Jeffrey M. Woolridge, *Inverse Probability Weighted Estimation for General Missing Data Problems*, 141 J. ECONOMETRICS 1281 (2007).

[44] *See generally* Peter W. Lane & John A. Nelder, *Analysis of Covariance and Standardization as Instances of Prediction*, 38 BIOMETRICS 613 (1982).

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.

D. Difference-in-Differences Analysis

A 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 may still differ from our controls on some important, unobserved dimension(s). To address this concern, we estimated a difference-in-differences specification, which adds to the treatment/control comparison a comparison of each firm to its prior self. Specifically, the difference-in-differences approach estimates a baseline level of open interest and volume on outstanding put options of target firms over the interval [-480, -240]— approximately sixteen months to eight months prior to disclosure of the data breach in each treatment firm.[45] We then compare differences between treatment and control firms during this baseline window to the analogous differences interval [-240, 0]—or approximately eight months prior to disclosure up to the date of announcement. As explained previously, we aggregated 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 employed 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—which equals the difference in log open interest and log volume).

It is important to emphasize that our difference-in-differences approach represents more of a robustness check of our baseline finding than it does a strict causal inference test. That is, we do not suggest that the cybersecurity vulnerability "causes" the informed trading we observe, but rather that they co-occur together. To be sure, our difference-in-differences analysis is *in the spirit* of a causal design, in that we inquire whether there is a parallel evolution prior to a certain point in time when the informed trading appears to commence. That said, we expressly embrace this approach in an exploratory fashion, so that our goal is to examine at what point informed trading appears to commence. As such, we plot trends on log open interest between the treatment and control groups in the following figure:

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

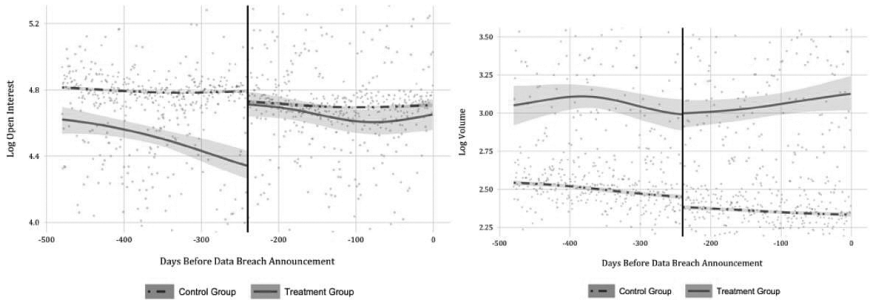

Figure 4: This figure plots time trends for log average open interest (left panel) and trading volume (right panel) on put options between treatment and control firms in the matched sample. The pre-treatment period (in days) is the interval [-480, -240), and the post-treatment period is the interval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

An eyeballing assessment of these parallel-trend figures suggests that the two groups appear to follow somewhat parallel trends prior to divergence during this eight-month period preceding disclosure of the data breach. We note that the respective trends in the open interest charts does seem to exhibit some divergence in trends as the eight-month point approaches (which may be due to the illiquid market for options with expiry longer than one year). In any event, the open interest graph suggests an 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. (While reiterating that we are not strictly estimating a causal relationship, we note that the relative movement in the difference of interest in both graphs represent valid identification approaches for inferring average treatment effects in a difference-in-differences design.)

Proceeding to the statistical analysis, as before we first estimated the difference in pre-post differences of log open interest and log volume between treatment and control firms. The results of each estimation are shown in Table 8. As can be seen from the upper panel of the table, for open interest we estimated an average treatment effect of between 0.26 and 0.32 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 0.23 and 0.36 log points.[46] As with the

[46] Compared 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. *See supra* Table 2.

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.

As with our cross-sectional estimations, we test how sensitive these results are to the 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 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)

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; Difference-in-Differences; 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, altering the pre- and post-treatment specifications. The re-estimated results using a variety of different time horizons 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 pronounced evidence of market trading abnormalities in the options 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: (1) whether the findings above pose a normative problem that securities law should address; and (2) 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.

II. Normative Implications: Is Cyber-Trading Special?

Having offered empirical evidence that informed cyber-trading appears to occur in practice, we now turn to the "so what?" question: does informed trading in advance of a cybersecurity breach disclosure raise important and idiosyncratic policy concerns for the efficient operation of capital markets? If it does, then there would be a *prima facie* efficiency case for tailoring legal rules in order to account for cyber-trading concerns. If, in contrast, the concerns raised by informed cyber-trading are largely identical to those of garden-variety information-trading contexts, then there would be no particular reason to treat the activity with any special degree of legal or regulatory skepticism.

In the familiar policy debate surrounding informed securities market trading—as well as how and whether it should be regulated legally—scholars have advanced at least four policy dimensions worthy of attention[47]: (1) price discovery; (2) distributional fairness; (3) market liquidity; and (4) allocative efficiency. We discuss each in turn below in the context of cybersecurity-related trading. Our analysis suggests that while informed cyber-trading does not seem particularly special when viewed against any of the first three dimensions on this list, it raises potentially unique efficiency concerns as to the fourth, plausibly justifying *sui-generis* regulatory scrutiny.

---

[47] *See, e.g.*, Jonathan R. Macey, Insider Trading: Economics, Politics, and Policy 21–47 (1991). Another relevant policy dimension concerns strategic incentives of corporate insiders themselves (such as whether to delay disclosure of information in order to permit informed trading). *Id.* at 37. We exclude these considerations here, since the predominant set of issues concerns non-statutory insiders.

A. Price Discovery

Consider first the desideratum of pricing efficiency—for example, the proposition that capital markets should be structured to facilitate the systematic adjustment of prices to incorporate relevant information about the "fundamentals" underlying traded securities. When satisfied (at least roughly), pricing efficiency assists market participants in making sound portfolio choices, and it helps firms to finance value-enhancing projects. Indeed, as has long been known (and celebrated) by economists, market prices are often an excellent mechanism to summarize and convey information about the underlying economic attributes of an asset (for example, its scarcity and riskiness), a benefit that frees most market participants from the costly task of having to investigate and verify such matters directly.[48] A closely related corollary to pricing efficiency follows immediately: that it is preferable for securities prices to adjust *rapidly* as market and company fundamentals change, rather than on a delayed or attenuated basis (where pricing inaccuracies persist). Such rapid price "discovery" ensures that relevant information about market fundamentals flows to individuals as quickly as possible, further enabling them to make sound portfolio choices.

To the extent one views price discovery as important (and most economists do), it typically counsels a permissive stance on informed trading. Although most securities market prices are thought to rapidly reflect relevant publicly available information (sometimes called "semi-strong" efficient), informed trading can sharpen that accuracy by hastening the incorporation of new information into market price. If informed traders are permitted to trade freely on the basis of their information, their own trading activity will systematically drive up (or down) the price of a financial asset whenever it is under- or over-priced based on the newly-arrived information.[49] Indeed, not only will the prospect of arbitraging the information be attractive to such traders, but it will also motivate at least some of them to monitor new information in the first place. The ensuing price change effectively transmits the import of that new information to other market participants, providing a public good that enhances overall pricing efficiency.

Informed cyber-trading shares many of these traits. Given a known vulnerability that will soon be disclosed, informed trading can push market prices in the direction of fundamentals. Moreover, one might argue, the ability to profit from that information helps induce aspiring arbitrageurs to discover information about such future disclosures. Thus, in our view, the

---

[48] *See, e.g.*, F.A. Hayek, *The Use of Knowledge in Society*, 35 Am. Econ. Rev. 519, 526–528 (1945). It is worth noting, of course, that when the set of underlying economic attributes at stake is sufficiently varied and rich, price—a unidimensional piece of information—may become a less reliable embodiment of such attributes. *See, e.g.*, Archishman Chakraborty & Bilge Yılmaz, *Manipulation in Market Order Models*, 7 J. Fin. Mkt.187–206 (2004).

[49] *See generally* Henry Manne, Insider Trading and the Stock Market (1966); Macey, *supra* note 47.

relative merits of informed trading for price discovery remain relatively consistent (at least on first approximation) when one compares informed cyber-trading to garden variety information trading. There does not seem to be much of a compelling argument—at least on the basis of this desideratum—that counsels for more rigorous relative scrutiny.

B. Distributional Fairness

The desideratum of pricing efficiency just discussed consciously accepts the reality that the price discovery process will—by definition—produce (informed) winners and (uninformed) losers in individual trades, and that their interactions through the market will provide a public good of price discovery. From a pure Kaldor-Hicks efficiency perspective, this outcome seems eminently defensible, since winners and losers in the trading market are largely engaged in making or receiving transfer payments from one another—activities that play a neutral role in the efficiency calculus. At the same time, to the extent that one's measure of economic welfare also places weight on distributional equity,[50] the transfer payments that facilitate price discovery may matter too—particularly if the identities of the winners and losers in this process are highly correlated across trades and over time, permitting certain traders to make systematic arbitrage rents at the expense of others. To the extent that winning and losing is systematic in information trading, the prospect of a consistently unlevel playing field in securities markets might well be a significant welfare cost of price discovery—one that attenuates the case for pursuing perfect (or near perfect) pricing efficiency.[51]

Although economic-minded commentators vary in the extent to which they value distributive equity concerns in the context of informed trading,[52] resolving this longstanding disagreement proves unnecessary here: for distributive fairness concerns—while plausibly relevant—shed little *additional* light on the problem in the context of informed cyber-trading. To be sure, given the scarcity of programming and hacking talent and access to large

---

[50] *See generally* Hal R. Varian, *Distributive Justice, Welfare Economics, and a Theory of Fairness*, 4 PHIL. PHILOSOPHY AND PUB. AFF. 223 (1975) (advancing such a theory).

[51] It should be noted that the "level playing field" rationale for securities law—a rough proxy for distributive fairness—has largely been rejected as a formal statutory goal by courts. *See, e.g.*, *Chiarella v. United States*, 445 U.S. 222, 232 (1980) (rejecting the "level playing field" desideratum advanced by the SEC). Remaining mindful of the difference between "is" and "ought," however, it is worthwhile to ponder fairness anyway, since it remains a relevant normative criterion.

[52] *See generally* Michael J. Fishman & Kathleen M. Hagerty, *Insider Trading and the Efficiency of Stock Prices*, 23 RAND J. ECON. 106 (1992); Kimberly D. Krawiec, *Fairness, Efficiency, and Insider Trading: Deconstructing the Coin of the Realm in the Information Age*, 94 NW. U. L. REV. 443 (2001). There is also a longstanding debate about whether distributional fairness concerns—even if relevant from a welfare perspective—should enter into liability standards at all, or rather should be capitalized into tax-and-transfer systems. *See generally* LOUIS KAPLOW & STEVEN SHAVELL, FAIRNESS VERSUS WELFARE (2002). This argument is particularly unhelpful here, however, since securities markets are global and many participants are beyond the taxing authority of any single governmental actor.

trading platforms, it is plausible that informed cyber-traders may enjoy systematic rents across firms, across transactions, and over time. It is also plausible that their informed trades bring information of tremendous value to the market through the pricing mechanism, tipping off not only uninformed traders but also the firms themselves about the risk of a hack. That said, a similar (if not identical) set of tradeoffs appears manifest in virtually any informed trading context. Consequently, there does not appear to be a compelling reason to accord greater (or lesser) scrutiny to informed cyber-trading than any other type of informed trading activity.

C. Market Liquidity

A third consideration that often attends the insider trading debate—and one that combines the two aforementioned concerns—concerns market liquidity. To the extent that informed parties are allowed to participate in market trading, they will typically transact their business alongside *uninformed* market participants, who may become wary of being taken advantage of when they trade with informed parties. In such settings, uninformed market participants can understandably become reluctant to provide liquidity to the market. Indeed, the very fact that a (possibly) informed trader wishes to buy or sell a financial asset may constitute a strong signal that one stands to lose by serving as counterparty to the proposed transaction. In fact, in the extreme case where the *predominant* driver of trade is private information, trading among uninformed counterparties can shut down completely, leading to the near collapse of a market[53]—a consequence that is, ironically enough, deeply antithetical to price discovery. Informed traders, therefore, play simultaneously heroic and parasitic roles in their relationship with other traders. They heroically contribute to price discovery, but they parasitically require liquidity-trader participation in order to make information arbitrage profitable, even though their very presence can systematically deter such participation.[54] Consequently, even when pricing efficiency is of vital importance and distributive equity concerns are assumed away, it may be efficiency-enhancing for market regulators to embrace a compromise where information trading is permitted, yet limited in magnitude to a level that does not engender market dysfunction or illiquidity.[55]

As above, however, the importance of depth and liquidity to capital markets *in the context of informed cyber-trading* does not seem systematically distinct from its importance in the *general context* of informed trading. In both cases, the extreme prevalence of private information can cause markets to seize up, thereby justifying (at least potentially) some outer limits on

---

[53] *See* Milgrom & Stokey, *supra* note 15, at 17.

[54] *See* Kyle, *supra* note 15, at 1315–17.

[55] *See* Hans R. Stoll, *Inferring the Components of the Bid-Ask Spread: Theory and Empirical Tests,* 44 J. FIN. 115 (1989); Glosten & Milgrom, *supra* note 15, at 72.

ability of participants to exploit information advantages. Though the precise boundary that such limits should demark is far from clear, there is also little reason to think that its location is dramatically different in the context of informed cyber-trading.

D. Allocative Efficiency

Finally, informed trading in securities markets can foment a host of different issues related to allocative efficiency, in which market participants may incur costly expenditures in order to facilitate and/or prevent the transfer payments that attend information arbitrage. Aspiring informed traders, for example, may overinvest in acquiring inside information about existing (but as-yet-undisclosed) risks, or in keeping such information proprietary, hoping to exploit it maximally for personal advantage. Potential market counterparties, in turn, may respond by overinvesting themselves, suspicious that their counterparties are informed traders attempting to exploit their ignorance. Issuers, too, might get into the mix, attempting to make their cyber-defenses effectively "bullet proof" so as to avoid the costs and embarrassment of having third parties expose latent problems or risks. Even in the presence of such costly distortions, prices could still be exceedingly accurate, reflecting (and quickly adjusting) to each new change in information. But such pricing efficiency provides little if anything in the way of public goods, since many market participants have little left to learn, having already incurred substantial, duplicative costs to acquire that information directly.[56]

As with the analysis above, informed cyber-trading shares several of the same allocative efficiency concerns as those that apply to the more general information-trading scenario. Traders and firms may have similar sorts of incentives to invest "too much" (from a social perspective) in divining latent facts. We submit, however, that at least two additional considerations make informed cyber-trading different—and in many respects more worrisome—than the general case:

- First, unlike the garden-variety case of informed trading—where the underlying new information is independent of the arbitrageur's efforts to discover it—with informed cyber-trading the new information is substantially "created" by the hacker and then visited on the firm. Where the hacker actively steals proprietary data (such as employee social security numbers), this endogeneity is obvious. But even when the hacker merely exposes an *existing* vulnerability, the hacker's actions are still akin to imposing a harm on the target. For example, the underlying vulnerability exposed might have gone undetected for the

[56] *See* Zohar Goshen & Gideon Parchomovsky, *On Insider Trading, Markets, and "Negative" Property Rights in Information*, 87 U. VA. L. REV. 1230 (2001), 1230-1270.

foreseeable future, had it not been for the prospect of extracting cyber-trading rents. Moreover, an exposed cybersecurity vulnerability can easily compound, furnishing a digital roadmap for countless nefarious—albeit less skilled—actors seeking to exploit the target's likely vulnerabilities.[57] (Even if the target is able to conjure up a quick fix for the specific hack disclosed, its software vulnerability may be far more systematic, and in any event the exposed firm often becomes target practice for other hackers in the wake of the initial disclosure, driving the cyber-trader's profits higher still.) In many respects, then, the cyber-hacker plays a role in creating and imposing a unique harm on the targeted company—one that (in our view) is qualitatively different from "exogenous" information shocks serendipitously observed by an information trader. Allowing a coordinated hacker-trader team to capture these arbitrage gains would implicitly subsidize the very harm-creating activity that is being "discovered" in the first instance.

- Second, and relatedly, when hackers have an enhanced incentive to create such harms, targets also have an enhanced incentive to undertake costly precautionary measures meant to deter (or divert) hacker activity. In many situations, such undertakings can be considerable, such as investing in added internal cyber-hacking squads, or offering attractive third-party "bounties" to those who detect and bring forward unknown vulnerabilities. These incentives are perhaps maximal in instances where a target's risk of hacking increases when it is identified as the "weakest link" among potential targets. In such settings, a type of "arms race" to self-protect can ensue among potential targets, whereby each effectively doubles down on the equilibrium influence costs borne by hackers and targets alike.[58]

Informed cyber-trading, therefore, raises unique allocative efficiency considerations relative to garden-variety information trading. Policy-minded legal actors and commentators might thus do well at least to consider whether—in the light of these sui-generis costs—informed cyber-trading warrants heightened scrutiny by courts. In the next Part, we consider whether legal institutions under the status quo are up to the task.

---

[57] Muddy Waters' research report on St. Jude, for example, contained a detailed 34-page description of how to exploit two different vulnerabilities in the St. Jude pacemakers, including step-by-step instructions detailing even what type of equipment to purchase on internet shopping sites (such as e-Bay) to consummate the hack. MUDDY WATERS CAPITAL LLC, RESEARCH REPORT ON ST. JUDE MEDICAL, INC. 2-9 (Aug. 25, 2016), http://www.muddywatersresearch.com/content/uploads/2016/08/MW_STJ_08252016_2.pdf.

[58] We consider these incentives in detail in a technical companion piece. *See* Joshua Mitts & Eric Talley, Informed Trading and Cybersecurity Breaches: Technical Companion 12–13 (unpublished manuscript 2017) (available from authors upon request).

III. Prescriptive Challenges

The previous sections have (1) presented empirical evidence that informed cyber-trading occurs at a statistically and economically significant scale, and (2) argued that such trading raises certain idiosyncratic policy concerns that are *not* generically present in the canonical case of informed trading. In light of these observations, we now turn to the prescriptive question of how legal institutions might address informed cyber-trading in circumstances where policy concerns justify special scrutiny. More concretely, our approach here is to inform the pragmatic discussion as to (1) whether current law already acts to deter informed cyber-trading trading, and (2) if not, how one might adapt current legal institutions to address more effectively informed cyber-trading activity. We will advance the thesis that under current federal law—outside of certain special contexts—informed cyber-trading faces surprisingly little legal scrutiny. Moreover, the two most promising ways to adapt current law to address informed cyber-trading—extending insider-trading liability to outsiders or expanding the reach of the Computer Fraud and Abuse Act (CFAA)—both fall short (in different ways) in addressing the distinct normative quandaries raised by the practice.[59]

To frame and situate our prescriptive discussion, consider Table 11 below, which subdivides the legal policy question by positing the possibility that the hacker and the trader may be different persons with different individual interests.

		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

[59] This discussion 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. Hannah Kuchler, *Hackers Target Weakest Links for Insider Trading Gain*, Fin. Times (Oct. 2, 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.

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 motivated either by a desire: (1) to exploit the target's vulnerabilities in order to steal data; or (2) merely to detect and publicize such the target's vulnerabilities. The rows, in contrast, denote the *trader's interaction* with the hacker, distinguishing contexts where the trading entity : (1) is independent from the hacker (that is, it learns of the hack through independent means); or (2) directs, coordinates or transacts with the hacker in pursuit of a common aim.[60] While intermediate interests and degrees of coordination are no doubt possible, Table 11 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, wherein the trader works actively with the hacker to steal confidential data, corresponds to the strongest normative policy concerns, since the breach involves the loss of confidential information and the coordinated efforts of the trader and hacker (which can in turn facilitate explicit or implicit incentive structures that exacerbate *ex ante* hacking/protection incentives). Scenario II, while stopping short of outright data theft, also tends to entail many of the policy concerns of Scenario I, since the exposure of vulnerabilities can (as noted above) impose "harms" on the target that are effectively subsidized through informed trading activities. The remaining cells correspond to situations where the trader *independently* learns of a hacker's outright theft (Scenario III) or mere detection of vulnerabilities (Scenario IV), but does not coordinate efforts with the hacker. As suggested above, these latter scenarios present weaker cases for placing liability *on the trader*, since (1) trading incentives are (by hypothesis) divorced from hacking incentives (and thus cannot subsidize the hacker's efforts), and (2) the trader's activity might even expose (via the price) the existence of the hack to the public and the target.[61] As a rough approximation, then, an efficiency-minded legal decision-maker would tend to place the greatest amount of scrutiny on the upper row of the table (Scenarios I and II). As we show below, however, current law does not appear to have the same reach. Even the "easiest" case for scrutiny—Scenario I—sometimes can prove to be a stretch in establishing liability (particularly for traders), with perhaps the most leverage coming through *criminal* sanctions; the levers for *civil* liability (brought either by government regulators or private parties) appear even more limited and untested under current

[60] In cases where the hacker and trader are the same person, of course, the degree of coordination between the two is complete, so that such situations would fit easily into the top row of Table 11.

[61] This is not to say that one would have no concerns in these permutations. For example, one could argue that when an unaffiliated trader learns of an active theft of data (Scenario III), the trader should be under a "Good Samaritan"–like duty to disclose the information. That said, such considerations do not appear to raise sui-generis normative concerns in the case of data breach when compared to other possible latent harms discovered by a trader.

law. Scenario II imposes even fewer constraints still. And, while current law could be adapted to be a better prescriptive "fit" for either scenario, doing so would require either structural statutory reform, or that courts be receptive to novel (and largely untested) innovations.

To help illustrate our claims, consider the seemingly "easy" case of Scenario I, where a trader explicitly coordinates with or directs a hacker to purloin confidential data from a target company. As noted above, this permutation presents the strongest policy case for legal or regulatory scrutiny. And, as it happens, this particular scenario has garnered disproportionate attention to date from courts and regulators. Here, it appears that courts have been open to applying both federal securities and data breach statutes to impose legal exposure on both hackers and traders.[62] Interestingly, however, the doctrinal divinations needed to impose liability risk on such actors—while admirably creative—are still an awkward fit with the type of legal oversight one might design from a blank slate to deal with informed cybertrading.

Analysis of these considerations need not be confined to abstract hypotheticals, however. The legal dimensions of Scenario I are evolving even as of this writing—in the form of governmental complaints in an interrelated cluster of high-profile actions (the "*Dubovoy* case").[63] These actions constitute, in many ways, a virtually perfect case study of Scenario I. In its civil complaints filed in 2015 and 2016, the SEC charged more than forty 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").[64] 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 traders (including hedge fund managers and their investment firms)[65] located

---

[62] *See* Andrew N. Vollmer, *Computer Hacking and Securities Fraud* (Va. Law & Econ. Research, Working Paper No. 26, 2015), https://ssrn.com/abstract=2679092.

[63] Complaint at ¶ 1, SEC v. Dubovoy, No. 2:15-cv-06076-MCA-MAH (D.N.J. Oct. 16, 2015); Indictment at ¶ 1, United States v. Turchynov, No. 2:15-cr-00390 (D.N.J., filed Aug. 6, 2015); Indictment at ¶ 1, United States v. Korchevsky, No. 1:15-cr-00381 (E.D.N.Y., Aug. 5, 2015). A subsequent complaint named additional defendants. *See* Complaint at ¶ 1, SEC v. Zavodchiko, 2016 WL 9224898 (D.N.J. Feb. 17, 2016).

[64] Indictment at ¶ 1, Turchynov, No. 2:15-cr-00390; *see* 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.

[65] Cory Bennett, *Hackers Cash in with Insider Trading*, The Hill (Aug. 16, 2015, 9:00 AM), 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, 12:45 PM), https://www.reuters.com/article/us-insidertrading-cyber-sec/russia-investor-funds-pay-18-million-to-settle-u-s-press-release-hacking-case-idUSKCN0WR1A4.

both in the U.S. and abroad ("*Dubovoy* Traders").[66]

According to government documents, the *Dubovoy* Hackers repeatedly "used deceptive means"[67] over a five-year period to breach computer networks at several U.S. business newswire services—such as Marketwired, PR Newswire, and Business Wire[68]—extracting material non-public information (MNPI) in the form of "confidential earnings information for numerous publicly traded companies from press releases that had not yet been released to the public." The *Dubovoy* Hackers then sold the purloined data to the *Dubovoy* Traders[69] as part of an orchestrated and coordinated plan. Indeed, the government asserts that the *Dubuvoy* Traders even provided the *Dubovoy* Hackers with "shopping lists" of desired press releases, accessed the stolen MNPI through secured overseas computer servers,[70] and then "used that stolen [MNPI] to trade securities and reap over $100 million in unlawful profits."[71] The *Dubovoy* Traders are further alleged to have used "deceptive means," including the use of multiple fictitious accounts and entities, to conceal their trading activities.[72]

In its criminal indictment of the *Dubovoy* Traders, the government alleged a series of transgressions under federal criminal law, including:

- *Securities Fraud under Rule 10b-5*, 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).
- *Fraud and Related Activity in Connection with Computers,* in violation of 18 U.S.C. § 1830 (also known as the Computer Fraud and Abuse Act, or "CFAA," discussed below).
- *Wire Fraud*, in violation of 18 U.S.C. §§ 1343 and 1349 (Attempt and Conspiracy).
- *Money Laundering Conspiracy*, in violation of 18 U.S.C. § 1956(h) (Laundering of Monetary Instruments).[73]

---

[66] Press Release, SEC, SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases (Aug. 11, 2015), Release 2015-163.

[67] Complaint at ¶ 71, Dubovoy, No. 2:15-cv-06076-MCA-MAH.

[68] Indictment at ¶ 14, Turchynov, No. 15-cr-00390.

[69] Complaint at ¶¶ 1–3, Dubovoy, No. 2:15-cv-06076-MCA-MAH.

[70] Press Release, U.S. Dep't of Justice, Hacker Sentenced To 30 Months In Prison For Role In Largest Known Computer Hacking and Securities Fraud Scheme (May 22, 2017).

[71] Complaint at ¶ 1, Dubovoy, No. 2:15-cv-06076-MCA-MAH.

[72] *Id.* at ¶ 7.

[73] Indictment at ¶¶ 112–45, U.S. v. Turchynov, 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 at ¶¶ 45–55, U.S. v. Korchevsky, No. 15-cr-00381 (E.D.N.Y., filed Aug. 5, 2015).

The securities fraud and CFAA charges play prominent roles here, since (1) they embody the most general-purpose charges in the informed cyber-trading context; and (2) they constitute critical predicate offenses for criminal liability under wire fraud and money-laundering statutes. The majority of individuals indicted by the DOJ reached plea agreements with federal prosecutors between December 2015 and August 2016, pleading guilty to the wire fraud conspiracy counts, with the DOJ dropping most of the predicate criminal charges.[74] Such criminal settlements are not uncommon, and in a sense deter others who would attempt similar conduct in the future. Yet, the *Dubuvoy* plea agreements also leave open whether the predicate securities fraud or CFAA charges themselves would have had traction had they been pursued to trial.[75] We thus consider each below in turn.

A. Securities Fraud Liability

Consider first the allegations of securities fraud. In pursuing its criminal claims, the government had the benefit of additional enforcement expertise; as frequently happens in securities fraud contexts,[76] the SEC coordinated with federal prosecutors and *also* filed a series of independent civil claims alleging securities fraud by the *Dubuvoy* Traders. These allegations included:

- *Section 10(b)* of the Securities Act of 1934 ("'34 Act") and *Rule 10b-5* thereunder.[77]
- *Section 17(a)* of the Securities Act of 1933 ("'33 Act").[78]

---

[74] See U.S. Dep't of Justice, *supra* note 70.

[75] It bears noting that the defendants were also charged with identity theft under federal law, which might also have carried weight as a predicate offense for wire fraud/money laundering.

[76] *See* Mary Jo White, SEC Chair, All-Encompassing Enforcement: The Robust Use of Civil and Criminal Actions to Police the Markets (March 31, 2014).

[77] Complaint at ¶¶ 225–27, SEC v. Dubovoy, 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.").

[78] *Id.* at ¶¶ 222–24. ("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.").

- *Sections 20(b)*[79] *and (e)*[80] of the '34 Act.

As with the criminal case, Rule 10b-5 plays a starring—and, indeed, central—role here, as several of the other charges effectively bootstrap to the 10b-5 allegations. Note, however, that CFAA claims are wholly absent in the SEC's complaint (since CFAA enforcement is not part of the Commission's regulatory mandate).

Several of the SEC's parallel cases remain pending as of this writing, and it appears that most have been stayed pending the resolution of remaining criminal actions.[81] That said, at least two opinions have already emanated from the civil actions, and both are relevant to our inquiry here. First, shortly after the SEC complaint was filed, the District Court in New Jersey entered a temporary restraining order freezing the defendants' assets and an order to show cause why a preliminary injunction should not be entered against all defendants.[82] A "subset" of the *Dubovoy* Traders (the "Amaryan Defendants") appealed this order.[83] 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 . . . ."[84] On February 12, 2016, hedge fund Memelland Investments Ltd. ("Memelland"), one of the *Dubovoy* Traders, filed a motion to dismiss under FRCP 12(b)(6).[85] 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

---

[79] 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*, 6 HARVARD BUS. LAW REV. 36, 36 (2015), http://www.hblr.org/2015/12/the-role-of-section-20b-in-securities-litigation/; *see* Complaint at ¶ 233–34, Dubovoy, No. 2:15-cv-06076-MCA-MAH (" 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 10b-5 [17 C.F.R. § 240.10b-5], thereunder through or by means of the hacker defendants. 234. 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[d] unless enjoined will continue to violate Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 110b-5 [17 C.F.R. § 240.10b-5], thereunder.").

[80] Complaint at ¶¶ 230–31, Dubovoy, No. 2:15-cv-06076-MCA-MAH ("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.")

[81] 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/.

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

[83] *Id.* at *1.

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

[85] Dubovoy, 2016 WL 5745099, at *1.

Memelland acted with scienter to "deceive, manipulate or defraud."[86] As of February 2018, the Amaryan and Memelland Opinions appear to be the only two opinions released in this matter, though the SEC has reached settlements with several of the *Dubovoy* Traders.[87]

But what about the underlying merit of the securities fraud allegation (whether criminal or civil)? Here, things become surprisingly opaque. The familiar 10b-5 claim for securities fraud charges turns on showing—in connection with the purchase or sale of any security—the use of a device, scheme, or artifice to defraud; an act, practice, or course of business which operates or would operate as a fraud or deceit; or, the making of any untrue statement (and in certain cases, omission) of a material fact.[88] As noted above, Rule 10b-5 is extremely general, covering both conventional fraud and insider trading claims. Both are at least *theoretically* in play in the case of informed cyber-trading. At the same time, both prove to be awkward fits in many plausible factual scenarios.

The offense of "insider trading" is not explicitly codified in Rule 10b-5, but it instead emerged as a judicial construction of Rule 10b-5 that effectively equates an informed trader's *silence* (in appropriate circumstances) with an affirmative misstatement of material fact. In this respect, the doctrine is a bit of a catch-all, broadening the application of Rule 10b-5 beyond a strict construction of its text.[89] Nevertheless, even when read in this broad fashion, insider trading has time-honored boundaries that make it a difficult fit, even in Scenario I.

---

[86] *Id.* at *1.

[87] *See* Trader Agrees to Settle Claims Relating to Hacked News Release Scheme; SEC's Recovery to Date in Connection with the Scheme Exceeds $52 Million, Release No. LR-23530, 2016 WL 2615155 (May 4, 2016) ("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.").

[88] The specific 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 (2018).

[89] Stark, *supra* note 81. This judicial construction has a long pedigree: the U.S. Supreme Court held in *Superintendent v. Bankers Life* 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." Superintendent of Ins. of State of N. Y. v. Bankers Life & Cas. Co., 404 U.S. 6, 11 n.7 (1971); *see also* Robert Steinbuch, *Mere Thieves*, 67 Md. L. Rev. 570, 574 (2008).

There are two predominant pathways to prove insider trading under Rule 10b-5, frequently referred to as the "classical" and "misappropriation" theories. The classical theory—often dubbed the "traditional" theory as it was developed first—teaches that "a corporate insider"[90] (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."[91] The classical theory was easily expanded to cover "tippee" outsiders who receive MNPI from "tipper" insiders (who themselves receive a personal benefit from tipping) and trade with knowledge (actual or reasonable) that the insider(s) breached their duties by tipping for personal benefit.[92]

Misappropriation theory—developed later—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."[93] The misappropriation theory thus reached certain types of corporate outsiders who nonetheless "deal in deception" against a third-party owner of information by "pretend[ing] loyalty to the principal while secretly converting the principal's information for personal gain."[94]

Under either the classical or misappropriation theories, then, the insider-trading prohibition has come to be 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*."[95] That is, the linchpin for deducing whether actionable insider trading has occurred under Rule 10b-5 is by "equating a breach of fiduciary or fiduciary-like duty [toward the information's rightful owner] with the fraud requirement."[96]

And therein lies the rub. As capacious as insider trading theories have become, the accepted doctrinal framework squares poorly with the canonical case of informed cyber-trading (as well as the facts of *Dubuvoy*), where the

---

[90] 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 v. SEC, 463 U.S. 646, 661 n.20 (1983).

[91] 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).

[92] Cohen, *supra* note 91, at 266–67; *see, e.g.*, *Dirks*, 463 U.S. at 659; Salman v. United States, 137 S. Ct. 420, 423 (2016). Even after *Salman,* it remains somewhat unclear what knowledge the trading tippee(s) must have about the original tipper's motives. *Salman,* 137 S. Ct. at 427.

[93] Cohen, *supra* note 91, at 267; *see generally* United States v. O'Hagan, 521 U.S. 642 (1997).

[94] *O'Hagan*, 521 U.S. at 653 (1997).

[95] Steinbuch, *supra* note 89, at 575 (emphasis added).

[96] *Id.* at 575–76.

hacker and trader are neither fiduciaries of the target, nor are they in a relationship of trust and confidence with a third party information "owner."[97] Indeed, it is hard to see how Scenario I would trigger *any* liability under the received insider trading framework, since no fiduciary relationship is breached when a hacker targets an unrelated company's MNPI, and then passes such information in a coordinated fashion to a trader. Simply (if ironically) put, "mere thieves" of MNPI—even those who profit from it through market transactions—are not insiders according to Rule 10b-5.[98]

That said, a series of recent cases have experimented with an alternative application of Rule 10b-5 to informed cyber-trading—one that characterizes the conduct not strictly as a species of insider trading, but rather as a hybrid with conventional securities fraud, in which the cyber-traders make use of a "deceptive device" in relation to securities transactions.[99] Because it leans on a conventional fraud claim, this extension dispenses with the burden of demonstrating the breach (or even the existence) of any fiduciary relationship. That said, it is a "[f]ar more complex and challenging" theory of liability for government regulators to pursue.[100] Under several accountings, the government's theory represents a new paradigm of unlawful "outsider trading" under 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."[101] This new category aims to capture trading on the basis of MNPI obtained via computer hacking in situations (like Scenarios I and II), lacking the fiduciary relationship required by insider trading law, but still reflecting the requisite degree of deception. Should courts prove receptive to this theory, it could certainly represent a bona fide threat of securities fraud exposure against a trader in Scenario I who coordinates with a hacker to detect or trade on stolen data.

But what would a new theory of outsider trading look like? While the idea is still in nascent stages of development, the SEC has theorized that cyber-trading "outsiders" can nonetheless be culpable under Rule 10b-5 when, as part of the hack, they "are masquerading as company insiders. . .."[102] In other words, under this theory, the *deception* element mandated by Rule 10b-5 relates "directly to the hacking or unauthorized computer access and is a bit more attenuated from the securities transaction."[103] Note that coordination between the hacker and trader envisaged by Scenarios I and II (in the form of a common plan, scheme, or transaction) appears to be critical to this theory as well; for without such coordinated efforts (for exam-

---

[97] *See* Stark, *supra* note 81.

[98] Steinbuch, *supra* note 89, at 589 ("Conventional 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.").

[99] SEC v. Dorozhko, 574 F.3d 42, 51 (2d Cir. 2009) (internal quotation marks omitted).

[100] *See* Stark, *supra* note 81.

[101] *See* Stark, *supra* note 81.

[102] *See* Stark, *supra* note 81.

[103] *See* Stark, *supra* note 81.

ple, the hacker and trader acting independently), it would be difficult to say that the deceptive hack was also "in connection with the purchase or sale of any security" requirement, another critical requirement of Rule 10b-5.[104]

The emerging theory of outsider trading bears a strong resemblance to Donald Langevoort's development of the idea that "intentional deception" should serve as a trigger for securities fraud liability, arguing 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."[105] Propounding 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."[106]

While the outsider trading model remains a relatively untested prototype, the SEC has asserted facially similar charges against several outsider trading defendants for years.[107] A decade ago, in *SEC v. Dorozhko,*[108] the SEC had its best (and sole) opportunity thus far to establish a beachhead for outsider trading theory. In *Dorozhko*, the 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."[109] In the case, the SEC alleged that Dorozhko 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.[110] 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.[111] Accordingly, it denied

---

[104] 17 C.F.R. § 240.10b-5 (2018).

[105] 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.") (quoting United States v. Carpenter, 791 F.2d 1024, 1033 (1986)).

[106] Langevoort, *supra* note 105.

[107] *See e.g.*, Stark, *supra* note 81 (discussing SEC v. Blue Bottle Ltd., SEC v. Lohmus Haavel & Viisemann, and SEC v. Stummer).

[108] SEC v. Dorozhko, 574 F.3d 42, 43–44 (2d Cir. 2009).

[109] *Id.*

[110] *Id.* at 44.

[111] *Id.* at 45.

the SEC's request for a preliminary injunction freezing Dorozhko's trading account.[112]

A unanimous three-judge panel on the Second Circuit reversed and remanded the case to the Southern District of New York.[113] Acknowledging that the SEC's claim was "not based on either of the two generally accepted theories of insider trading," Judge Cabranes' opinion noted that the complaint was "nonetheless based on a claim of fraud" and accorded "attention to whether this fraud is 'deceptive' within the meaning of Section 10(b)."[114] Notably, the Second Circuit explained that "what is sufficient [to establish a breach of Section 10(b)] is not always what is necessary."[115] Because Dorozhko's actions—hacking to gain access to and trade on MNPI—allegedly constituted an "affirmative misrepresentation" (as opposed to "silence or nondisclosure"),[116] and because violation of the "affirmative misrepresentation 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.[117]

Having made the general point that a fiduciary relationship is *not necessary* 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)."[118] In doing so, the opinion 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.'"[119] The Court infused ambiguity into 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*."[120] 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."[121] Unfortunately (at least for us), the Second Circuit panel's invitation in *Dorozhko* was never formally taken up by the District Court on remand: Dorozhko's attorney lost

---

[112] *Id.*
[113] *Id.* at 51.
[114] *Id.* at 45.
[115] *Id.* at 49.
[116] *Id.* at 48–49.
[117] *Id.* at 49.
[118] *Id.* at 51.
[119] *Id.* at 50 (quoting *United States v. Finnerty*, 533 F.3d 143, 148 (2d Cir. 2008)).
[120] *Id.* at 51 (emphasis added).
[121] *Id.*

contact with his client and the trial court later granted summary judgment for the SEC.[122]

A fair reading of the opinion nevertheless suggests that trading on hacked information *might* constitute actionable securities fraud, but *only if* accompanied by some manifested deception on behalf of the hacker. 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."[123] Thus, while negligently weak computer systems that "leav[e] a virtual door open for an online intruder" might not open the door to "deception," the use of malware and the tools and processes more generally associated with the popular perception of hackers might suffice.[124] Regulators and courts will no doubt grapple with defendants about where to draw this line, should outsider trading theory gain a greater jurisprudential following.

Dorozhko's unrequited invitation for doctrinal development is just one reason why *Dubovoy* represents a potential watershed moment for informed cyber-trading under federal securities law. The *Dubovoy* pleadings are instructive, and they clearly evince the government's deep familiarity with the language in *Dorozhko*, and its attempt to squeeze the underlying allegations within its ambit. For example, The SEC's complaint alleges that the *Dubovoy* Hackers used deception as follows.

> 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.[125]

Moreover, the SEC's initial complaint alleges that the *Dubovoy* Traders deceptively concealed their activities through shell entities, misleading payments,[126] multiple trading accounts,[127] and a secure server.[128]

---

[122] Stark, *supra* note 81.

[123] *Id.* (interpreting *Dorozhko*).

[124] *Id.*

[125] Complaint at ¶ 71, SEC v. Dubovoy, No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015); Stark, *supra* note 81.

[126] Complaint at ¶ 84, Dubovoy, No. 2:15-cv-06076-MCA-MAH ("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.' ").

[127] *Id.* at ¶ 91 ("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.").

Based on the preliminary opinions thus far produced in the case, it appears courts have been sympathetic to outsider-trader theory.[129] For example, in the *Amaryan* Opinion, without specifically elaborating on the legal standard required by Section 10(b) or Rule 10b-5, the district court suggests that "the evidence submitted by the SEC raises a strong inference that the Amaryan Defendants violated federal securities laws."[130] And, even more recently, the SEC obtained a default judgment against several trading defendants on highly similar facts. In *SEC v Iat Hong*, 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.[131] 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.[132]

Notwithstanding its evident traction in judicial opinions, outsider trading theory has attracted a chorus of critics decrying its many alleged infirmities. Many of them have been wary of a significant expansion of insider trading based on an amorphous concept of deception and have instead argued that misappropriation theory can capture many of the most concerning hacker-trader conspiracies.[133] Others have lodged even stronger opposition to the concept of liability for outsiders under the antifraud provisions, arguing

---

[128] *Id.* at ¶ 85 ("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.").

[129] *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.") (quoting *SEC v. Infinity Grp. Co.*, 212, F.3d 180, 192 (3d Cir. 2000).

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

[131] Default Judgment at ¶ 11, SEC v. Hong, No. 1:16-CV-09947 (S.D.N.Y. May 5, 2017) (Bloomberg Law).

[132] *Id.* (emphasis added).

[133] Steinbuch, *supra* note 89, 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.").

that the new theory opens an unwieldy and unnecessary Pandora's Box.[134] 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."[135] 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.[136] 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.[137]

More generally, whatever one's opinion is about outsider trading theory, with or without it the overall fit of securities fraud law to informed cyber-trading appears far from perfect. It is all but obvious that conventional insider trading models (classical and misappropriation) are ill-equipped to deal with cyber-traders. By requiring a fiduciary-like relationship with either the company or a third-party owner of MNPI, the classical and misappropriation theories simply fall flat by focusing on factors that have questionable normative relevance here. The emerging theory of outsider trading—to the extent it has traction—is a slightly better fit, but hardly a bespoke one. On the one hand, the theory would seem to require some type of coordination between the hacker and the trader (as in the top row of Table 11), consistent with our normative analysis. Yet, by hinging an offence on an affirmative *deception* by the hacker, outsider trading theory fails to capture an important subset of problematic informed cyber-trading, where the hacker/trader team are "merely guileless thieves," utilizing brazen (but not deceptive) means to access unauthorized information. Hence, even if outsider trading theory gains jurisprudential traction (a long-shot proposition in its own right), securities law would remain substantially under-inclusive relative to the normative challenge at issue.[138]

B. Liability Under the CFAA

If securities law stumbles in the task of addressing problematic normative issues surrounding informed cyber-trading, what might succeed? The

---

[134] Andrew Vollmer, *Computer Hacking and Securities Fraud*, THE CLS BLUE SKY BLOG (Apr. 7, 2016), http://clsbluesky.law.columbia.edu/2016/04/07/computer-hacking-and-securities-fraud/ ("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.").

[135] *Id.*

[136] SEC v. Dorozhko, 574 F.3d 42, 42 (2d Cir. 2009).

[137] Vollmer, *supra* note 134.

[138] It is certainly possible that the definition of *deceptive* may be expanded even further to entail not only affirmative misrepresentations but also "digital trespassing" (unauthorized access to data), or alternatively a violation of some other statutory fraud proscription (such as the CFAA). Such a reform, however, would be an even more profound break from existing jurisprudence.

criminal indictment of the *Dubovoy* Traders provides a possible clue, in a charge that many would find more esoteric: violation of the CFAA.[139] Although not within the regulatory remit of the SEC, the CFAA has both criminal and civil enforcement mechanisms that might, in theory, be better adapted tools for the normative task at hand.

Originally promulgated in 1986 (and expanded through amendment several times since), the CFAA prohibits essentially three categories of conduct: (1) using unauthorized access to fraudulently acquire valuable information from a computer; (2) causing damage through the unauthorized transmission of computer passwords; and (3) causing unauthorized damage to computer data or causing damage to a computer.[140] Although the liability provisions of the CFAA are quite general, they tend to concentrate actions whereby one accesses a "protected computer," either "without authorization" or in a manner that "exceeds authorized access."[141]

The term "protected computer" refers not to the level of security protocols that protect the compromised data, but rather to the intended use of the compromised computer. Under the CFAA, this definition includes any computer that is used (i) by/for the federal government, (ii) "[by/for]" a financial institution," or (iii) "in or affecting interstate or foreign commerce."[142] These categories have been interpreted broadly. For example, courts have read the "interstate commerce" flag to be triggered by the use of any computer connected to the Internet—regardless of whether the computer is located inside or outside the United States—as affecting interstate commerce.[143]

The elements of the CFAA that concern "authorization" tend to subdivide defendants into two groups: "outsiders"—third parties with no affiliation with the target and enjoying no authorization to access the protected content, and "insiders"— parties (such as employees, customers, and contractors) who, pursuant to some relationship with the target, have (or previ-

---

[139] 18 U.S.C. § 1030 (2018).

[140] *See* Audra Dial & Daniel G. Schulof, *The Computer Fraud and Abuse Act: An Underutilized Litigation Weapon*, https://www.kilpatricktownsend.com/~/media/Files/articles/ADial%20DSchulof%20Technology%20Litigation%20Desk%20Reference_The%20Computer%20Fraud%20and%20Abuse%20Act.ashx. The precise contours of the CFAA are slightly broader. 18 U.S.C. § 1030(a) (2018).

[141] Office of Legal Education Executive Office for United States Attorneys, Prosecuting Computer Crimes (June 2013).

[142] 18 U.S.C. § 1030(e)(2) (2018).

[143] 18 U.S.C. § 1030(e)(2)(B) (2018) (amending the CFAA to include Internet-connected computers outside the US); *see also* United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) ("No additional interstate nexus is required when instrumentalities or channels of interstate commerce are regulated."); United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009) ("[T]he latter two elements of the section 1030(a)(2)(C) crime [obtaining information from a protected computer] will always be met when an individual using a computer contacts or communicates with an Internet website."); Paradigm All., Inc. v. Celeritas Tech., LLC, 248 F.R.D. 598, 602 (D. Kan. 2008) ("As a practical matter, a computer providing a 'web-based' application accessible through the internet would satisfy the 'interstate communication' requirement.").

ously had) some limited authorization to access data, but transgressed that authorization on the date of the breach.[144] Interestingly, the CFAA tends to treat insiders who exceed their authorization with some degree of deference, requiring *actual* intent by the insider to damage the computer for liability to follow.[145] Outsiders are subject to less accommodation and may be found liable for intentional, reckless or other damage caused by their digital trespass.[146] In recent years, moreover, some courts have been willing to convert insiders into outsiders—stripping them of their more protected status—when the insider breaches its duty of loyalty to the target, such as when the insider pursues interests antithetical to the interests of the target.[147]

The CFAA insider/outsider distinction—augmented by the aforementioned fiduciary breach conversion—stands in stark contrast with Rule 10b-5's insider trading doctrine (as discussed above).[148] In 10b-5 actions, the liability standard aggressively scrutinizes insiders who breach a fiduciary duty to access data, but it develops a case of "alligator arms" vis-à-vis outsiders, even under the nascent outsider trading theory (which still hinges awkwardly on *deception* by the hacker). Thus, at least on this critical dimension, the CFAA seems to be a significantly better fit for addressing informed cyber-trading.

On the other hand, CFAA liability is far clunkier than securities law in engaging other challenges, such as the degree of coordination between the hacker and trader. Recall that securities fraud exposure tends to "scale down" when the hacker and trader are completely independent from one another, since the deceptive hack is remote from and thus arguably not "in connection with" the purchase and sale of securities.[149] This retrenchment seems normatively justified, since the lack of coordination substantially reduces the danger that cyber-trading activity subsidizes hacking and defensive activity. Under the CFAA, in contrast, the relevance of coordinated activity fades (at least for the hacker). Although a trader who operates independent of the hacker can probably avoid CFAA liability, the hacker's exposure does not appear to change.[150]

---

[144] 18 U.S.C. § 1030(a)(1) (2018) (establishing CFAA liability if a party "knowingly accessed a computer without authorization or exceed[ed] authorized access . . . .").

[145] United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007).

[146] *Id.* at 219 (referencing legislative history).

[147] *See e.g.,* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); Ervin & Smith Advert. & Pub. Relations, Inc. v. Ervin, 2009 WL 249998, at *8 (D. Neb. 2009); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1060 (S.D. Iowa 2009) ("[T]he determinative question is whether Artino breached his duty of loyalty to NCMIC when Artino obtained information from NCMIC's computers."); ViChip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

[148] *See supra* Part IV.A.

[149] *See supra* Part II.A.

[150] See Dial & Schulof, *supra* note 140, at 57–58 (discussing the flexibility and generality of the CFAA in going after hackers relative to other potential theories).

A second area of misfit concerns the civil provisions of the CFAA, and in particular the measure of damages available to private parties. Although the CFAA provides civil remedies (both injunctive and in damages) for persons injured by unauthorized access or computer fraud, the level of monetary damages available has historically been quite limited. Under the CFAA, monetary relief is explicitly limited to economic damages.[151] Moreover, most courts interpreting the statute have measured economic damages against the CFAA's definition of "loss," which equals "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[152] An obvious limitation to this provision is that consequential damages (including stock price fall) associated with the breach must be related to an interruption of service. In cases where a data breach simply results in the unauthorized access or downloading of data with no "service interruption," such consequential losses may be unavailable.[153] In the absence of a significant broadening of this interpretation, it seems unlikely that private parties will pursue civil CFAA litigation vigorously against informed cyber-traders; most of the work will be left to criminal enforcement.

This last observation raises a final shortcoming of CFAA liability: the relative absence of regulatory expertise for the DOJ to draw upon in pursuing CFAA claims against informed cyber-traders. As noted above, federal prosecutors have long enjoyed a secret weapon in their securities fraud prosecutions (including insider trading): a sophisticated and motivated regulator in the SEC, possessing an ample budget, years of expertise, and well-trained staff and attorneys capable of unpacking often dense and complicated transactions.[154] Indeed, the SEC and DOJ actively tout their cooperation and the latter's reliance on the former's expertise in many complicated fraud prosecutions. CFAA claims, in contrast, are outside of the SEC's remit and do not come with a built-in regulator to assist with uncovering the key facts.

---

[151] 18 U.S.C. § 1030(g) (2018).

[152] 18 U.S.C. § 1030(e)(11) (2018).

[153] *See* Nexans Wires S.A. v. Sark-USA, Inc., 166 F. App'x 559, 562–63 (2nd Cir. 2006) (holding that plaintiff's claim for lost revenue due to defendant's misappropriation of its confidential data did not constitute a cognizable loss under the CFAA "[b]ecause it is undisputed that no interruption of service occurred in this case"); John DiGiacomo, *Civil Actions Under the Computer Fraud and Abuse Act*, Revision Legal (Feb. 4, 2015), https://revisionlegal.com/internet-lawyer/civil-actions-computer-fraud-abuse-act/#_ftnref23. *But see* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001) (observing that—in an "increasingly electronic world"—the CFAA covers more than just the cost of physical damage and may also include "the value to the victim of what has been stolen and the victim's costs in shoring up its security features"). In contrast, private actions under securities law generally give a plaintiff (here, target stockholders who traded during the fraud) a full measure of loss, which—given the nature of the transaction—tends to coincide with the informed trader's gain from the trade.

[154] *See* White, *supra* note 76.

C. Synopsis

Given the discussion above, the battle between Rule 10b-5 and the CFAA as a legal theory for scrutinizing informed cyber-traders yields no clear-cut victor. On the one hand, the CFAA is far more flexible and less statutorily-ossified than Rule 10b-5—where fiduciary duty and deception requirements severely constrain enforcement modalities. That said, the CFAA appears less able to tailor itself to *coordinated* hacker-trader schemes—it has unattractive civil damages provisions, and it has no built-in regulator to lend expertise to criminal prosecutors in investigating and pursuing claims.[155]

In short, both approaches fall short, and neither appears to lend itself to an obvious and simple fix. Certain forms of tinkering around the edges might be possible, of course. Proponents of outsider trading theory, for example, may attempt to push for an even more capacious definition of *deceptive*—one that includes (say) willful and deliberate access to data that the hacker knows or has reason to know is unauthorized ("digital trespassing"). Given the tenuous state of flux that outsider trading theory finds itself in, however, this strategy carries obvious risks. Alternatively, proponents of CFAA enforcement might push courts to expand their construction of consequential damages, granting private claimants greater license to recover economic losses (including those capitalized through lower equity prices). Here too, however, the statutory definitions in the CFAA make such a construction a heavy lift in the absence of statutory amendment.

To the extent that one considers systematic statutory reform, it is necessary to remember that information trading is a complex, normative landscape. Simply because there are idiosyncratic dangers associated with informed cyber-trading, it does not follow that all such trading is undesirable. As with any other type of informed trading, cyber-trading can convey information through price, to both market participants and to the targets of hacking themselves. Any substantive reform to either securities law or the CFAA must remain mindful of this tension. One intriguing possibility—which we develop in a technical companion to this paper —would broadly prohibit informed cyber-trading (along the CFAA model), but would simultaneously exempt initial arbitrage "allowance" (that is, a monetary cap or a fraction of the firm's economic heft) shielded from both criminal fines and civil recovery.[156] This allowance would serve as a type of "bounty" for bringing the information to light. Once the exemption level is met, however, the trader 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 reasonably, this alternative approach would have the benefits of

---

[155] *See supra* Part IV.B.

[156] See Mitts & Talley, *supra* note 58.

(1) preserving price discovery (at least within the limits of the exemption); (2) preserving limited incentives to uncover information about vulnerability; and (3) catalyzing communication to the issuer about the nature of the vulnerability, so as to streamline both the hacker's offensive efforts and 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.[157]

Short of such systematic statutory reforms, however, perhaps the most expedient strategy would be to continue some version of the *status quo*, where the DOJ has nominal authority to bring enforcement actions under either Rule 10b-5 or the CFAA, but it can more effectively enlist the SEC's investigatory assistance to help develop and focus its claims. No doubt some investigations will come up dry in uncovering actionable securities fraud claims, but such cases will usually not announce themselves *ex ante*, effectively rationalizing the SEC's coordinated involvement (at least early on). Where a securities fraud claim proves viable (such as in an outsider trading case involving hacker deception), the SEC and DOJ can continue to pursue a coordinated strategy, much as they do today. Where it does not, the SEC will have to back away, leaving the government to pursue a criminal CFAA claim should it choose, but with the benefit of the SEC's past factual investigation.

Conclusion

In this paper, we have considered the phenomenon of informed cyberhacking, whereby market arbitrageurs learn of material, yet-to-be-disclosed cybersecurity breaches and execute 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 exhibit significantly larger open 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 certain idiosyncratic normative concerns, potentially justifying more capacious exposure to liability for hacker/traders in response to such concerns. Under current law, however, it seems unlikely that such an expansion is possible without substantial legal and statutory reform. 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

[157] Difficult, but perhaps not impossible. The requirement of deception could be met by labeling cooperation between hackers and traders as deceptive. 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 cybertrader, 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.

fit for the policy concerns in play. Similarly, liability under the CFAA—while not requiring deception or fraud— still suffers from deficits in investigatory expertise, monetary damages provisions, and appropriate tailoring for securities market harms. In the short term, it will likely prove difficult to nudge doctrine in a way that does not run the risk of being severely over-or under-inclusive. In the absence of a more systematic reform (which could be years away at best), the status quo (including a more developed and mature doctrine of outsider trading) may be the most expedient—even if flawed—response to informed cyber-trading.