X. Hackers Access Nonpublic Law Firm Documents: Outsider Trading and its Implications

On December 27, 2016, the Securities and Exchange Commission (SEC) filed a complaint against three Chinese citizens, Iat Hong (Hong), Bo Zheng (Zheng), and Hung Chin (Chin), who hacked into two New York City law firms' networks.[1025] The complaint alleges that Hong, Zheng, and Chin (defendants) obtained information relating to impending acquisitions in order to invest strategically before the deals went public, quickly profiting upon the announcement of the deals.[1026] This case has broad implications and raises complex questions pertaining to cybersecurity measures in law firms. How can "outsider trading" be regulated and prevented?[1027]

This article discusses the circumstances of the law firm hackings, analyzes applicable federal regulations, and broadly considers measures that law firms may take in order to prevent such data breaches from occurring in the future. First, Section A explains the law firm hackings and the subsequent trades that occurred. Second, Section B considers the SEC's analysis of the data breach, its application of the Securities Exchange Act of 1934 (SEA), and relevant precedent. Finally, Section C briefly details measures being taken by the SEC in order to prevent further breaches.

A. The Cybersecurity Hacking

This outsider-trading scheme began in early March 2014 with a PowerPoint presentation titled "Internal Information of U.S. Stock Operations," which Zheng shared with Hong.[1028] Just a few months later, on or before July 31, 2014, the defendants compromised the account of an employee at a New York law firm.[1029] Installing malware enabled them to gain access to the firm's email system, from which they

---

[1025] *See generally*, Complaint, SEC v. Hong et al., No. 16-cv-9947 (S.D.N.Y. Dec. 27, 2016), https://www.sec.gov/litigation/complaints/2016/comp-pr2016-280.pdf [perma.cc/P9N9-YV4G].

[1026] *Id.* at 2.

[1027] *See generally* John Reed Stark, *The SEC's "Outsider Trading" Dragnet*, CYBERSECURITY DOCKET (June 25, 2015), http://www.cybersecuritydocket.com/2015/06/25/the-secs-outsider-trading-dragnet/ [perma.cc/7PRU-RA-JM].

[1028] *See* Complaint, *supra* note 1, at 9.

[1029] *Id.* at 2.

were able to access non-public information.[1030] In total, the defendants managed to steal nearly six million pages of information.[1031]

The first deal the defendants exploited was one involving InterMune, a biotechnology company on the brink of being acquired.[1032] In 2014, between August 13 and 21, the defendants purchased 18,000 shares of InterMune.[1033] The deal was announced just days later on August 24, 2014.[1034] As predicted, the price of the InterMune shares surged when the deal was made public, at which point the defendants sold their shares and netted roughly $400,000 in illegal profits.[1035] The defendants continued their access to the law firm's private information into 2015.[1036] During this time, Intel and Altera began negotiating the terms of Intel's acquisition of Altera, a semiconductor company.[1037] The defendants accordingly began purchasing Altera stock on February 17, 2015, again exploiting a dramatic increase in value.[1038] The acquisition was formally announced on March 27, 2015.[1039] The defendants responded to this announcement by selling their shares for a profit of about $1.63 million.[1040]

In early April 2015, just days after the Intel/Altera transaction was made public, the defendants compromised an employee account at a second New York City law firm and gained access to its web server and email server with the use of malware.[1041] Hundreds of thousands of pages of non-public information were stolen.[1042] The major deal

---

[1030] *See id.* at 11 ("'Malware' is software that is intended to damage or disable computers and computer networks, or to circumvent installed security and access controls.").
[1031] *See id.* at 12.
[1032] *Id.* at 3.
[1033] *Id.* at 13–14.
[1034] *Id.* at 3.
[1035] *Id.*
[1036] *See id.* at 15.
[1037] *See id.* at 3, 15.
[1038] *Id.* at 16–17 ("From February17, 2015 to March 27, 2015, Defendants purchased a total of over 207,000 Altera shares for approximately $7.5 million." The announcement of the Altera deal caused a 30% increase in share price, which the Defendants turned into "illegal profits of over $1.63 million.").
[1039] *See id.* at 3.
[1040] *Id.*
[1041] *Id.* at 17–18.
[1042] *See id.* at 18.

that Hong and Chin profited from at this firm was an impending tender offer between Pitney Bowes, Inc. and Borderfree, Inc., two e-commerce companies.[1043] Between April 29, 2015 and May 5, 2015, the defendants purchased Borderfree shares so aggressively that at times their trades constituted at least 25 percent of Borderfree's trading volume.[1044] The deal, announced on May 5, 2015, caused Borderfree stock to increase by more than 105 percent, enabling the defendants to net $850,000 in illegal profits.[1045]

The two law firms the defendants exploited have remained unnamed.[1046] However, it is known that the defendants had attempted to hack into five additional law firms.[1047] The defendants attempted to hack into these five additional firms on over 100,000 occasions between March and September of 2015.[1048] Though they did not succeed at gaining access to these five additional firms, they managed to make an estimated $3 million in illegal profits from the information they stole from the two firms that they did manage to hack.[1049] Ultimately, all three men "have been criminally charged in the United States with trading on confidential corporate information obtained by hacking into networks and servers of law firms working on mergers."[1050] Specifically, they have been charged with conspiracy, insider trading, wire fraud, and computer intrusion.[1051] On May 5, 2017, U.S. District Judge Valerie E. Caproni entered default judgments against the defendants.[1052] Monetary relief was ordered in the form of

---

[1043] *Id.* at 4. *See generally* PITNEY BOWES, http://www.pitneybowes.com/us/global-ecommerce.html [perma.cc/WJP3-3EBG].

[1044] Complaint, *supra* note 1, at 4.

[1045] *Id.*

[1046] *See* Nate Raymond, *U.S. Accuses Chinese Citizens of Hacking Law Firms, Insider Trading*, REUTERS (Dec. 28, 2016), http://www.reuters.com/article/us-cyber-insidertrading-idUSKBN14G1D5 [perma.cc/WJP3-3EBG] (providing insight into which firms may have been compromised, but ultimately determining that it is inconclusive).

[1047] *See id.*

[1048] Sara Randazzo & Dave Michaels, *U.S. Charges Three Chinese Traders with Hacking Law Firms*, WALL ST. J.: MARKETS (Dec. 27, 2016, 7:52 PM), http://www.wsj.com/articles/u-s-charges-three-chinese-traders-with-hacking-law-firms-1482862000 [https://perma.cc/YRA9-WZF7].

[1049] Complaint, *supra* note 1, at 2.

[1050] *Id.*

[1051] *Id.*

[1052] Default Judgments Entered Against All Defendants In Law Firm Hacking

disgorgement, prejudgment interest, and civil penalties equal to three times disgorgement.[1053] The combined total is equal to roughly $9 million.[1054]

B. The Applicability of Current SEC Regulations

1. The Securities Exchange Act and Outsider Trading

The SEC filed its complaint "pursuant to the authority conferred by Sections 21(d) and 21A" of the SEA and claims relief as provided therein.[1055] Though obviously not drafted with cybersecurity in mind, the SEC applies the SEA to this modern issue in its claim against the defendants.[1056] In its complaint, the SEC extended traditional insider trading regulations to outsider trading.[1057] "The SEC staff's legal argument for charging unlawful outsider trading is that cyber thieves are masquerading as company insiders and are therefore committing securities fraud."[1058]

Case, Litigation Release No. 23,826 (May 9, 2017), https://www.sec.gov/litigation/litreleases/2017/lr23826.htm [perma.cc/T4TR-JKF3] ("The default judgments, entered by U.S. District Judge Valerie E. Caproni for the Southern District of New York on May 5, 2017, permanently enjoins all of the defendants from violating Sections 10(b) and 20(b) of the Securities Exchange Act of 1934 and Rule 10b-5 thereunder and defendants Hong and Chin from violating Exchange Act Section 14(e) and Rule 14e-3 thereunder.").

[1053] *Id.*

[1054] Robert Abel, *SEC orders Chinese hackers to pay $9M for hacking law firms for trade secrets*, SC MEDIA (May 9, 2017), https://www.scmagazine.com/law-firm-hackers-hit-with-9m-in-fines/article/655738/ [perma.cc/GEF6-458P].

[1055] *See* Complaint, *supra* note 1, at 5 (seeking "to enjoin such transactions, acts, practices, and courses of business, and to obtain disgorgement, prejudgment interest, civil money penalties, and such other and further relief as the Court may deem just and appropriate.").

[1056] *See generally id.* at 23–25.

[1057] *See generally id.* "Unlawful insider trading occurs when, for instance, executives buy stock in their own company based on material, nonpublic information learned at the office." Stark, *supra* note 3. This is contrasted by outsider trading, which occurs when an outsider, rather than an executive, trades strategically. *Id.*

[1058] *Id.*

The SEC first claimed the defendants violated Section 10(b) of the SEA and Rule 10b-5 promulgated thereunder,[1059] which prohibit the use of "any manipulative or deceptive device or contrivance" in connection with the purchase or sale of a security.[1060] The broad language of Section 10(b) and Rule 10b-5, particularly the inclusion of "*any* manipulative or deceptive device" and "*any* device, scheme, or artifice to defraud" allow these provisions, written well before cybersecurity was a conceivable threat, to apply to this relatively recent concern.[1061]

The SEC further alleged that the defendants were aiding and abetting violations of Section 10(b) and Rule 10b-5.[1062] By hacking into firm networks and trading strategically on the information obtained, the defendants "knowingly or recklessly provided substantial assistance in connection with violations of Section 10(b) . . . and Rule 10b-5 . . . ."[1063]

[1059] Complaint, supra note 1, at 23 (Defendants "(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 fraud or deceit upon any person in connection with the purchase or sale of any security."); *see* 15 U.S.C. § 78j(b) (2012) ("To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors."); 17 C.F.R. § 240.10b-5 (2015) ("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.").

[1060] 15 U.S.C. § 78j(b).

[1061] 15 U.S.C. § 78j(b) (emphasis added); 17 C.F.R. § 240.10b-5 (emphasis added).

[1062] Complaint, *supra* note 1, at 24.

[1063] *Id.*

Additionally, the SEC alleged that the defendants violated Section 14(e) and its corresponding Rule 14e-3, which apply to tender offers.[1064] Rule 14e-3 provides that any person who trades on material information that they know or could assume to be private is in violation of Section 14(e) of the SEA.[1065] In its complaint, the SEC contends that "[b]y April 29, 2015, substantial steps had been taken to commence a tender offer for the securities of Borderfree, including, among others: the retention of law firms to engage in confidential tender offer discussions and the exchange of draft transaction documents."[1066] At the same point in time, Hong and Chin had access to nonpublic information relating to this acquisition.[1067] According to the SEC, because the defendants traded on this information, which they "knew or had reason" to believe was nonpublic given the fact that they broke into a secured network belonging to a party involved in the tender offer, the defendants violated Section 14(e) and Rule 14e-3.[1068]

Finally, the SEC alleged that the defendants violated Section 20(b) of the SEA.[1069] Section 20 generally addresses individuals who aid and abet violations of other sections of the SEA.[1070] Section 20(b)

[1064] *Id.*

[1065] 15 U.S.C. § 78n(e) ("It shall be unlawful for any person to make any untrue statement of a material fact or omit to state any material fact necessary in order to make the statements made, in the light of the circumstances under which they are made, not misleading, or to engage in any fraudulent, deceptive, or manipulative acts or practices, in connection with any tender offer or request or invitation for tenders, or any solicitation of security holders in opposition to or in favor of any such offer, request, or invitation. The Commission shall, for the purposes of this subsection, by rules and regulations define, and prescribe means reasonably designed to prevent, such acts and practices as are fraudulent, deceptive, or manipulative."); 17 C.F.R. § 240.14e-3 ("(a) If any person has taken a substantial step or steps to commence, or has commenced, a tender offer (the 'offering person'), it shall constitute a fraudulent, deceptive or manipulative act or practice within the meaning of section 14(e) of the Act for any other person who is in possession of material information relating to such tender offer which information he knows or has reason to know is nonpublic and which he knows or has reason to know has been acquired directly or indirectly . . . .").

[1066] Complaint, *supra* note 1, at 24.

[1067] *Id.*

[1068] *Id.*

[1069] *Id.* at 25.

[1070] 15 U.S.C. § 78t ("Liability of controlling persons and persons who aid and abet violations").

states that "[i]t shall be unlawful for any person, directly or indirectly, to do any act or thing which it would be unlawful for such person to do under the provisions of this chapter or any rule or regulation thereunder through or by means of any other person."[1071] This violation is, accordingly, connected to the violation of Section 10(b) and Rule 10b-5.[1072]

The SEA also provides rules relating to penalties imposed on profits obtained by trading on nonpublic information.[1073] In its complaint, the SEC requests the court to enter damages of "up to three times the profits made pursuant to Section 21A of the Exchange Act . . . or, alternatively, to pay a civil penalty under Section 21(d) of the Exchange Act."[1074] Much like the rules that govern the conduct of traders, these rules also are broad enough to include the type of activity in which the defendants were engaged.[1075]

John Reed Stark, cybersecurity consultant and former SEC attorney, explains that there is existing case law that utilizes SEA provisions, such as those discussed above, to reach issues of outsider trading.[1076] Over time, a number of cases have been argued on the theory that outsider trading is merely insider trading in disguise.[1077] The first in this line of cases is the 2005 case, *SEC v. Lohmus, Havel & Viisemann*.[1078] In that case, the defendant, an Estonian bank, was

---

[1071] *Id.*

[1072] 15 U.S.C. § 78j(b); 17 C.F.R. § 240.10b-5; *see* Complaint, *supra* note 1, at 25.

[1073] *See, e.g.*, 15 U.S.C. § 78u(d) ("Injunction proceedings; authority of court to prohibit persons from serving as officers and directors; money penalties in civil actions"); § 78u-1(a)(2) ("The amount of the penalty which may be imposed on the person who committed such violation shall be determined by the court in light of the facts and circumstances, but shall not exceed three times the profit gained or loss avoided as a result of such unlawful purchase, sale, or communication.").

[1074] Complaint, *supra* note 1, at 28.

[1075] *See generally* 15 U.S.C. § 78u(d); 15 U.S.C. § 78u-1.

[1076] Randazzo & Michaels, *supra* note 24; *see* Stark, *supra* note 3 ("Though a bit of a leap, there are actually a few SEC enforcement actions that have already evidenced (though not truly tested) the SEC's adoption of its new outsider trading canon.").

[1077] Stark, *supra* note 3 ("The SEC staff's legal argument for charging unlawful outsider trading is that cyber thieves are masquerading as company insiders and are therefore committing securities fraud.").

[1078] *Id. See generally* Lohmus Haavel & Viisemann, Litigation Release No.

charged with obtaining nonpublic, soon-to-be published press releases of U.S. companies, which it later used to inform its trades.[1079] The legal theory that outsider trading is a form of insider trading was not tested in this case, however, since it was settled out of court.[1080]

In 2007, the SEC brought its second outsider trading action.[1081] *SEC v. Blue Bottle* involved a Hong Kong accounting firm that was engaged in a similar scheme as the bank in *SEC v. Lohmus, Havel & Viisemann*.[1082] Once again, the SEC was unable to present its outsider trading theory, this time because the court ordered a default judgment.[1083] The most promising test of the theory of outsider trading came about in another 2007 case.[1084] *SEC v. Dorozhko* involved an individual who gained access to nonpublic information through a data breach, then traded based on that information.[1085] Initially, the court dismissed the matter because Dorozhko, the defendant, did not owe the companies a fiduciary duty.[1086] At that stage, the outsider trading

---

19,810, 2006 WL 2422653 (Aug. 22, 2006).

[1079] Lohmus Haavel & Viisemann, *supra* note 54, at 1 ("In its Complaint the Commission alleged that the defendants conducted a fraudulent scheme involving the electronic theft and trading in advance of more than 360 confidential, non-public press releases issued by more than 200 U.S. public companies.").

[1080] Stark, *supra* note 3.

[1081] *Id. See generally* Blue Bottle Ltd., Litigation Release No. 20,095, 2007 WL 1238669 (Apr. 27, 2007).

[1082] *See* Blue Bottle Ltd., *supra* note 57 ("The Court found that the Defendants opened a U.S. brokerage account using false information and documents. During a six week period in January and February 2007, Defendants traded just before news releases of at least 12 different U.S. public companies and amassed profits totaling approximately $2.7 million.").

[1083] *See* Stark, *supra* note 3.

[1084] *Id.*

[1085] SEC v. Dorozhko, 606 F. Supp. 2d 321, 322 (S.D.N.Y. 2008), *vacated*, 574 F.3d 42 (2d Cir. 2009) ("On October 29, 2007, the SEC filed the instant complaint alleging that Dorozhko violated §10(b) of the Securities Exchange Act of 1934 ('Exchange Act') (15 U.S.C. § 78j (b)), and Rule 10b-5 promulgated thereunder (17 C.F.R. § 240.10b-5) by either hacking into a computer network and stealing material non-public information, or through a more traditionally-recognized means of insider trading such as receiving a tip from a corporate insider.").

[1086] *Id.* at 324.

theory was rejected.[1087] On appeal, however, the Second Circuit overturned the decision, finding that misrepresentation occurred when Dorozhko accessed the nonpublic information even though he was an outsider,[1088] thus giving some legitimacy to the outsider trading theory.[1089] Existing regulation provides a foundation for bringing securities laws claims based on cybersecurity breaches, but it is clear that the novelty of cybersecurity issues raise many questions when applying SEA and SEC rules.

2. Cyber Meets Securities Fraud: A New Spin on a Familiar Issue

Recently, there has been a wide array of targets for cybercriminals.[1090] Cyberspace is vulnerable to "a wide range of risk stemming from both physical and cyber threats and hazards."[1091] Additionally, cyberspace is difficult to secure due to the ability of cybercriminals to commit crimes anywhere in the world.[1092] Due to this vulnerability a "range of traditional crimes are now being perpetrated through cyberspace."[1093] Though the defendants in the recent law firm cybersecurity hack were exposed, it appears possible that law firms could become targets for hackers again.[1094] U.S. Attorney Preet Bharara

---

[1087] *Id.*

[1088] *See* SEC v. Dorozhko, 574 F.3d 42, 51 (2d Cir. 2009) ("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. Accordingly, depending on how the hacker gained access, it seems to us entirely possible that computer hacking could be, by definition, a 'deceptive device or contrivance' that is prohibited by Section 10(b) and Rule 10b–5.").

[1089] *See* Stark, *supra* note 3 (stating that the theory has yet to be tested fully at the trial court level).

[1090] *See* Christian Berthelsen, *Chinese Hackers Charged with Trading on Stolen Law Firm Data*, BLOOMBERG (Dec. 27, 2016), https://www.bloomberg.com/news/articles/2016-12-27/china-residents-charged-with-insider-trading-on-hacked-m-a-data [perma.cc/J4PC-PLJJ].

[1091] *Cybersecurity Overview*, DEP'T HOMELAND SEC., https://www.dhs.gov/cybersecurity-overview [perma.cc/M9ND-NX83].

[1092] *Id.*

[1093] *Id.*

[1094] Raymond, *supra* note 22 ("The case is the latest U.S. insider trading pros-

claims that "[t]he case of cyber meets securities fraud should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals."[1095] According to prosecutors, information stolen included client email attachments that had been sent to the firms.[1096] The attachments detailed confidential proposed deals—information that could then be traded on.[1097] Law firms might be particularly susceptible to such attacks because they operate as partnerships and often lack infrastructure with the degree of sophistication required to upend such attacks.[1098]

Cybersecurity adds an additional layer of investigation to traditional securities fraud.[1099] In the SEC's case against the defendants, the defendants were traced via a common IP address[1100] and a substantial money trail.[1101] These elements of the crime allowed the investigation to proceed with relative ease.[1102] Particularly, "the indictment suggests social engineering—perhaps through a phishing email—could have been one of the techniques used, and the indictment also suggests that remote system access could be a point of compromise."[1103] These

---

ecution to involve hacking, and follows warnings by U.S. officials that law firms could become prime targets for hackers.").

[1095] *Id.*

[1096] Randazzo & Michaels, *supra* note 24.

[1097] *Id.*

[1098] *Id.* (quoting John Reed Stark, stating, "Law firms are a virtual treasure trove for sensitive information that could be valuable.").

[1099] *See generally Cybersecurity Overview*, *supra* note 67 ("Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.").

[1100] Ron Cheng, *China-Based Hacking Case Against U.S. M&A Firms Illustrates Cyber Security and Enforcement Issues*, FORBES (Jan. 11, 2017), http://www.forbes.com/sites/roncheng/2017/01/11/china-based-hacking-case-against-u-s-ma-firms-illustrates-cyber-security-and-enforcement-issues/#3ea5cd1da331 [https://perma.cc/NDK4-W57J].

[1101] *Id.* ("Despite the implied sophistication of this scheme, the charges also suggest that tracing the hack back to the points of origin was not significantly more difficult than many past computer crime cases, given the use of a common IP address, not to mention the money trail from the trades.").

[1102] *See id.*

[1103] *Id.*

strategies could easily be implemented in other countries, where securities could be similarly exploited.[1104]

In terms of legal actions, the concept of outsider trading presents a new issue, as it does not fit within the realm of classical theory or misappropriation theory of insider trading.[1105] Outsider trading is unlike insider trading because no pre-existing relationship has been breached in making the trades.[1106] Unlike misappropriation theory, which involves direct access to the private information, the deception involved in outsider trading pertains to the act of hacking into the private information.[1107] The outside traders neither work for the companies whose shares they trade illegally, nor do they owe a legal duty to such companies.[1108] These circumstances put a modern twist on the old notion of insider trading.[1109] Moving forward, it is important that law firms continue to take protective measures, such as enacting cybersecurity programs and policies, hiring third parties to conduct security assessments, obtaining security certifications, using file encryption, and carrying cybersecurity insurance.[1110]

[1104] *Id.*

[1105] *See* Stark, *supra* note 3 ("Under the first, the classical theory, insider trading occurs when a corporate insider trades in the securities of his or her corporation on the basis of material, non-public information. A corporate insider is entrusted with confidential information by virtue of his or her position, and in return owes fiduciary duties to the shareholders not to use that information for personal gain. Under the second and more recently decreed 'misappropriation theory,' courts extended liability for securities violations beyond classical insiders to those who misappropriate material, nonpublic information for use in a securities transaction in violation of some fiduciary or fiduciary-like duty that they owe to a party.").

[1106] *Id.*

[1107] *Id.* ("It . . . is a bit more attenuated from the securities transaction.").

[1108] *Id.*

[1109] *See id.* ("Understanding the newfangled (and innovative) SEC jurisprudence of outsider trading begins with a quick review of traditional notions of insider trading.").

[1110] *See* Kathryn T. Allen, *Law Firm Data Breaches: Big Law, Big Data, Big Problem*, NAT'L L. REV. (Jan. 11, 2017), http://www.natlawreview.com/article/law-firm-data-breaches-big-law-big-data-big-problem [perma.cc/G8B3-Q7LG] (stating that these security measures have not yet been widely adopted).

In recent years, law firms have noted the issue of cybersecurity and have been encouraged by their clients to take efforts to tighten security measures.[1111] Additionally, firms have formed information-sharing groups so that information regarding potential threats will be shared more widely.[1112] Nevertheless, concerns remain and firms should remain vigilant.[1113]

C. Effects Moving Forward

The SEC has recognized the novelty of the cybersecurity issue and has, over the course of the last few years, developed enhanced trading surveillance and analysis tools in order to protect against such attacks.[1114] These new methods allow the SEC to better identify the scope of the scheme carried out by the defendants.[1115] Additionally, the recent litigation may help further solidify the reach of the SEC in outsider trading matters and the theory of outsider trading.[1116] Nevertheless, as the recent cybersecurity hack demonstrates, it is important for law firms to adequately protect themselves and detect potential data breaches.[1117]

D. Conclusion

The outsider trading committed by Hong, Zheng, and Chin resulted in profits totaling roughly $3 million.[1118] A default judgment entered in favor of the SEC has ordered roughly $9 million in fines.[1119] This judgment reinforces the applicability of the SEA to the relatively

---

[1111] Randazzo & Michaels, *supra* note 24.
[1112] *Id.*
[1113] *See id.* ("Matthew Fawcett, general counsel for data-management and storage company NetApp, said he is concerned about the cybersecurity and physical security of the outside law firms he hires.").
[1114] Press Release, U.S. Sec. & Exch. Comm'n, Chinese Traders Charged with Trading on Hacked Nonpublic Information Stolen from Two Law Firms (Dec. 27, 2016), https://www.sec.gov/news/pressrelease/2016-280.html [perma.cc/2KY5-6F7Z] ("This action demonstrates our commitment and effectiveness in rooting out cyber-driven schemes no matter how sophisticated.").
[1115] *Id.*
[1116] *See supra* Section B.
[1117] Randazzo & Michaels, *supra* note 24.
[1118] Complaint, *supra* note 1.
[1119] Abel, *supra* note 30.

new issue of cybersecurity, an area of the law that is still developing.[1120] However, in order to prevent such hacking from taking place, law firms must take all precautions required to adequately protect information from potential hackers.[1121]

Emily Humbert[1122]

[1120] *See generally* Stark, *supra* note 3.
[1121] *See* Raymond, *supra* note 22 ("The case is the latest U.S. insider trading prosecution to involve hacking, and follows warnings by U.S. officials that law firms could become prime targets for hackers.").
[1122] Student, Boston University School of Law (J.D. 2018).