Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Inside The SEC's Outsider Trading Program: Part 1

By **John Reed Stark** (October 29, 2018, 10:22 AM EDT)

John Reed Stark

It was just a year or so ago when the U.S. Securities and Exchange Commission learned firsthand what it's like to experience a data breach. Like a cardiologist who suffers a heart attack and could uniquely empathize with patients, the SEC, after suffering the EDGAR data breach, could now uniquely empathize with the cybersecurity challenges faced by financial firms.

When the SEC sheepishly announced the data breach and the irony that stolen EDGAR information may have been used to profit in a securities fraud scheme perpetrated by the cyber attackers, the SEC was imparted one important lesson firsthand: Outsider trading should be a top SEC enforcement priority.

Unfortunately, the SEC appears to have ignored that powerful lesson.

By way of background, on Sept. 20, 2017, SEC Chairman Jay Clayton announced a data breach into the SEC's Electronic Data Gathering and Retrieval system, a vast database that contains information about company earnings, share dealings by top executives, and corporate activity such as mergers and acquisitions. EDGAR processes roughly 1.7 million electronic filings per year.

According to the SEC, the hacker was able to take advantage of a "software vulnerability in the test filing component" of EDGAR, which "resulted in access to nonpublic information." Once discovered, the problem was immediately patched, and two investigations began. First, the SEC initiated an internal investigation into the cause of the data breach. Second, the SEC enforcement division initiated a formal investigation into whether the cyber attackers used material, nonpublic EDGAR information in a scheme to profit unlawfully.

At the time, the SEC's EDGAR data breach announcement immediately made headlines warning of possible insider trading fraud. After all, accessing that EDGAR information before it's disclosed publicly could allow hackers to profit by trading ahead of the information's release. But the headlines perpetuated a common and oft-misunderstood misconception.

If the perpetrators of the EDGAR hack did trade on material, nonpublic information stolen from EDGAR, it was not a case of unlawful insider trading. Instead, the EDGAR hackers who traded would be charged with "outsider trading," a much more nascent and far more dangerous securities fraud variant. Outsider trading is the kind of securities fraud that threatens the integrity of the entire global financial marketplace — and it can only get worse.

Given the SEC's expertise, wherewithal, creativity and specialized resources to prosecute any kind of securities fraud, the SEC, not surprisingly, led the charge. Since 2005, when the SEC first encountered conduct involving outsider trading, and continuing through the end of 2016, prosecuting outsider trading violations evolved into a top SEC enforcement priority.

But now, a year or so after the EDGAR data breach, with four (out of five) new SEC commissioners, the SEC's interest in investigating and charging outsider trading appears to be waning and is no longer a priority. In fact, the SEC's initial outsider trading dragnet seems to have come to a screeching halt. Perhaps the SEC is referring outsider trading schemes to the U.S. Department of Justice, who has broader jurisdiction (e.g. federal prosecutors can charge outsider

Department of Justice, who has broader jurisdiction (e.g. federal prosecutors can charge outsider trading as a computer crime or theft) — but no one outside of SEC staff knows for sure.

This two-part series discusses the disappointing reality of the deafening silence of the SEC with respect to the plague of outsider trading, despite the fact that the SEC itself has been used as a pawn for an outsider trading scheme.

Part one provides a history of the SEC's outsider trading program, with a review of outsider trading case law from 2005 to 2016. Part two then discusses the legal framework the SEC adopted to charge outsider trading, concluding with an extensive analysis of the dearth of SEC outsider trading enforcement actions since 2016 as well as some suggestions going forward.

The SEC Outsider Trading Program

Consider this scenario: A Microsoft employee sneaks into the office of the company's chief financial officer, reads secret files about an upcoming positive earnings announcement, and then buys Microsoft stock before that announcement. Is the Microsoft employee guilty of unlawful insider trading? Of course. But suppose instead, a thief, who does not work at Microsoft, breaks into Microsoft headquarters via a basement window at midnight, reads the CFO's papers about an upcoming positive earnings announcement, and then buys Microsoft stock before that announcement. Is the thief guilty of insider trading? Historically, the SEC would not charge the thief with insider trading because a thief is just that, a thief, and not an insider or securities swindler.

From 2005 to 2016, however, the SEC staff changed course. The SEC began targeting the thief, because the break-in was no longer through a basement window; instead the break-in was through a virtual window, in cyberspace. Late in 2014 and early in 2015, the SEC even went so far as to issue new and novel requests and subpoenas to public companies about any and all data breaches (or attempted breaches) they have experienced. The SEC apparently selected the public companies that, according to cybersecurity firm FireEye, had experienced recent data breaches targeting inside information. FireEye had previously released a Dec. 1, 2014, report about a group of hackers called "FIN4." The report said that Fin4 was targeting the email accounts of top executives, lawyers and others in an effort to obtain nonpublic information about merger and acquisition deals and major market-moving announcements.

Ironically, the hack into the EDGAR database, which was also the subject of testimony from Clayton before the Senate Banking Committee, brought the SEC's previously quiet but steadfast outsider trading foray into the spotlight. Indeed, any enforcement actions against the perpetrators of the EDGAR hack would fall squarely within the recently chartered territory of outsider trading.

What Is Outsider Trading?

Understanding the newfangled and innovative SEC jurisprudence of outsider trading begins with a quick review of traditional notions of insider trading.

For starters, most insider trading is perfectly legal, such as when corporate executives buy stock in their own companies as an investment. Unlawful insider trading occurs when, for instance, executives buy stock in their own company based on material, nonpublic information learned on the job.

The rationale for policing unlawful insider trading is that for the markets to work efficiently and fairly, everyone needs to be working with the same basic information, or at least, that those with special access to nonpublic information are prevented from taking advantage of it before other investors. The prohibition on unlawful insider trading levels the playing field and protects the integrity of financial markets.

Some insider trading cases are straightforward, such as when a corporate executive trades stock in his or her company before the company's earnings announcement. The executive has a duty to not trade on corporate information, described in the law as a "fiduciary duty or other duty of trust and confidence."

But the outer edges of insider trading law are murky at best, especially when it is not clear whether a fiduciary duty attaches to a given person, such as when "mere thieves" or strangers, learn and trade upon confidential financial information gained through a cyberattack.

The reason for the quirks of insider trading law is that SEC statutes, rules and regulations make no explicit statutory prohibition (or even mention) of insider trading; rather, the prohibition against insider trading is actually a jumbled, garbled, judicially created concoction, which has evolved slowly over time.

Judges derive insider trading violations from Section 10(b) of the Securities and Exchange Act of 1934 and Rule 10b-5 promulgated thereunder (together known as the "SEC's anti-fraud provisions"), and are a "catchall" aimed at fraud, requiring some sort of "device, scheme or artifice to defraud" or some action, which would otherwise "operate as a fraud or deceit upon a person."

Courts have historically found that the SEC's anti-fraud provisions are not intended as a specification of particular fraudulent acts or practices, but rather are designed to tackle the infinite variety of devices by which undue advantage may be taken of investors and others. Along those lines, the U.S. Supreme Court held in 1971, in Superintendent of Insurance v. Bankers Life & Casualty Co., that the SEC's anti-fraud provisions prohibit all fraudulent schemes in connection with the purchase or sale of securities, whether the artifices employed involve a garden-variety type of fraud, or present a unique form of deception.

2005-2016: The SEC Outsider Trading Paradigm

From 2005 to 2016, the SEC extended unlawful insider trading to a third and new category of securities miscreant — "outsiders" — who do not work for (or with) the company, and who do not owe a fiduciary duty to that company, its shareholders or anyone else. Reasoning that hack-and-trade cyber thieves were masquerading as company insiders and were therefore committing securities fraud, the SEC staff filed a series of important outsider trading enforcement actions.

2005: SEC v. Lohmus Haavel & Wiseman

The first outsider trading SEC enforcement action was SEC v. Lohmus Haavel & Viisemann et al. in 2005. The SEC charged that Lohmus, an Estonian investment bank, and two of its employees, obtained more than 360 confidential, soon-to-be-released press releases of U.S. publicly traded companies by stealthily "spidering" the BusinessWire website for material, nonpublic information. BusinessWire, at the time, was a leading commercial disseminator of news releases and regulatory filings.

2007: SEC v. Blue Bottle et al.

The next outsider trading SEC enforcement action was in early 2007 in SEC v. Blue Bottle et al. Blue Bottle was a Hong Kong accounting firm that the SEC charged engaged in a fraud very similar to the 2005 Lohmus scheme. Specifically, the SEC alleged that Blue Bottle hacked into computers of a news wire service to view press releases before they were published and then repeatedly executed transactions in the securities of 12 public companies just prior to press releases by those companies, netting $2.7 million in trading profits.

On April 24, 2007, the U.S. District Court for the Southern District of New York entered a default judgment against Blue Bottle ordering $2,707,177 in disgorgement of profits from the illegal trading, $18,047 in prejudgment interest, and an $8,121,561 million penalty equal to three times the profits from the illegal trading.

2007: SEC v. Oleksandr Dorozhko

An opportunity for a judicial test of the SEC's outsider trading theory arose once again in late 2007 in what many consider to be the seminal outsider trading case of SEC v. Oleksandr Dorozhko, an SEC outsider trading action that was initially dismissed, then reinstated after an SEC appeal. This case is worthy of some further analysis.

The Dorozhko matter involved an Eastern European who bet nearly a year's worth of his income that a stock price would drop in two days, realizing profits of $280,000 (more than five times his that a stock price would drop in two days, realizing profits of $286,000 (more than five times his yearly income). The SEC alleged that Dorozhko gained access to material nonpublic information from a data breach into a third-party information dissemination computer network and made his trades based on that stolen information.

Specifically, Dorozhko opened an online trading account in which he deposited $42,500 in October 2007. Shortly thereafter, a hacker gained access to earnings data for IMS Health Inc. via the servers of Thomson Financial Inc., the company providing investor relations and web hosting services to IMS.

According to the SEC, the hacker cloaked his identity and hid his tracks, and managed to overcome the security barriers at the site and gain unauthorized access to confidential information on the secure site.

Within an hour of the hacker's obtaining this information, Dorozhko used his online trading account for the first time, purchasing almost $42,000 of IMS put options, essentially betting that IMS stock would decline significantly in the near future. Later the same day, IMS announced that its earnings were 28 percent below analysts' expectations. When the market opened the next morning, the price of IMS stock dropped by about a third and Dorozhko sold his put options, realizing a profit of approximately $286,000. The SEC alleged that the hacker was Dorozhko, and charged him with outsider trading.

Judge Naomi Reice Buchwald, the Southern District of New York judge assigned to the Dorozhko matter, then dismissed the SEC action, holding that absent a fiduciary duty, Dorozhko's conduct did not amount to any kind of securities fraud. The district court noted that Dorozhko's trading was not "deceptive" and that Dorozhko was not an officer, director, representative or agent of IMS Health, Thompson Financial or any other relevant party, so Dorozhko owed no fiduciary duty to anyone. The district court found that Dorozhko was merely a hacker, an outsider with no relationship to IMS or Thomson, so he could not be liable for unlawful insider trading.

The district court rejected the SEC's outsider trading theory and held that computer hackers who steal and use information may be criminally liable for theft and computer crime, but it was too much of a stretch to charge them with any kind of securities fraud.

The SEC appealed the Dorozhko district court decision, and the U.S. Court of Appeals for the Second Circuit overturned it. The Second Circuit noted that the SEC did not need to prove the existence of a fiduciary duty because Dorozhko affirmatively misrepresented himself in obtaining the confidential information. The Second Circuit recognized that when a cyber attacker trades on stolen, exfiltrated confidential information, the SEC could charge the cyber attacker with outsider trading.

2008: SEC v. Michael A. Stummer

Another outsider trading SEC matter was filed in 2008 and involved a rather primitive version of hacking and computer intrusion. The matter, SEC v. Michael Stummer, also dubbed by the media as the "Brother-in-law from hell: Wall Street edition," involved a day trader who: (1) snuck into his brother-in-law's bedroom during a family get-together; (2) stole his brother-in-law's computer password; (3) logged on to his brother-in-law's computer; (4) reviewed on the computer material, nonpublic information about a possible tender offer by the brother-in-law's private equity firm (CI Capital Partners) of a public company (Ryan's Restaurant Group); and 5) made profitable trades based on that information.

Like the other outsider trading matters before, the Stummer matter was also never contested. Stummer settled with the SEC without admitting or denying wrongdoing, and paid about a $46,000 penalty and $46,000 in disgorgement of his ill-gotten trading gains.

2015: SEC v. Ivan Turchynov and Oleksandr Ieremenko et al.

In August 2015, the SEC stepped up its outsider trading efforts considerably, announcing its first major outsider trading case, charging a large outsider trading ring and filing enforcement actions against 34 defendants, parallel to DOJ federal criminal cases filed in the Eastern District of New York and the District of New Jersey in Newark. In this elaborate, multifaceted and international prosecution, the SEC charged that over a five-year period, Ivan Turchynov and Oleksandr Ieremenko spearheaded a scheme to hack into two or more newswire services and steal hundreds of corporate earnings announcements before the newswires released them publicly.

The SEC further charged that Turchynov and Ieremenko created a secret web-based location to transmit the stolen data to traders in Russia, Ukraine, Malta, Cyprus, France and three U.S. states — Georgia, New York and Pennsylvania. The traders were alleged to have used this nonpublic information in a short window of opportunity to place illicit trades in stocks, options and other securities, sometimes purportedly funneling a portion of their illegal profits to the hackers.

2016: SEC v. Evegenii Zavodchiko, Andrey Bokarev, Andreevna Alepko, Anton Maslov, et al.

In February 2016, the SEC added more defendants to the mix, filing a second follow-on suit in New Jersey federal court against nine additional defendants, including several Russian traders who were also allegedly involved in the outsider trading scheme and who scored more than $19.5 million in illegal profits.

2016: SEC v. Jonathan Ly

On Dec. 5, 2016, the SEC filed another outsider trading matter alleging that Jonathan Ly, who worked in Expedia’s corporate IT services department, illegally traded in advance of nine company news announcements from 2013 to 2016 and generated nearly $350,000 in profits. According to the SEC’s complaint, Ly exploited administrative access privileges designated for IT personnel to remotely hack into computers and email accounts of senior executives and review confidential documents and pre-earnings reports. Ly particularly targeted information prepared by Expedia’s head of investor relations summarizing Expedia’s yet-to-be-announced earnings and describing how the market could react to particular announcements.

Ly settled at the time of the SEC charges, without admitting or denying wrongdoing, and agreed to pay disgorgement and interest and agreed to pay $375,000. In a parallel action, the U.S. Attorney’s Office for the Western District of Washington filed criminal charges against Ly, who concurrently pled guilty to securities fraud and was later given a 15-month sentence and three years’ supervised release.

2016: SEC v. Iat Hong et al.

On Dec. 27, 2016, the SEC filed its last outsider trading case, alleging that Iat Hong, Bo Zheng and Hung Chin executed a deceptive scheme to hack into the networks of two law firms and steal confidential information pertaining to firm clients that were considering mergers or acquisitions. According to the SEC's complaint, the alleged hacking incidents involved installing malware on the law firms' networks, compromising accounts that enabled access to all email accounts at the firms, and copying and transmitting dozens of gigabytes of emails to remote internet locations. Defendants Hong and Zheng in particular coveted the emails of attorneys involved in mergers and acquisitions, as they exchanged a list of partners who performed the work at one of the law firms prior to the hack at that firm.

According to the SEC's complaint, Hong, Zheng and Chin used the stolen confidential information contained in emails to purchase shares in at least three public companies ahead of public announcements about entering into merger agreements. The SEC alleges that they spent approximately $7.5 million in a one-month period, buying shares in semiconductor company Altera Inc. in advance of a 2015 report that it was in talks to be acquired by Intel Corp.

Within 12 hours of emails being extracted from one of the firms, Hong and Chin allegedly began purchasing shares of e-commerce company Borderfree so aggressively that they accounted for at least 25 percent of the company's trading volume on certain days in advance of the announcement of a 2015 deal. Hong and Zheng also allegedly traded in advance of a 2014 merger announcement involving InterMune, a pharmaceutical company.

In a parallel action, the U.S. Attorney's Office for the Southern District of New York filed criminal charges against Iat Hong, and he was arrested by Hong Kong law enforcement authorities. Iat Hong apparently remains in Hong Kong police custody despite a U.S. extradition request, while

Hong apparently remains in Hong Kong police custody despite a U.S. extradition request, while the whereabouts of the other defendants remain unknown.

***

This concludes part one of this two-part series. Please be sure to read part two, which will discuss: (1) the legal framework used by the SEC to charge outsider trading, and (2) some final thoughts and suggestions for the SEC going forward.

John Reed Stark is the president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as the chief of its Office of Internet Enforcement. He is the author of "The Cybersecurity Due Diligence Handbook."

Disclosure: During his tenure as chief of the SEC's Office of Internet Enforcement from 1998 to 2009, Stark played a role in assisting most outsider trading enforcement actions, including the ones discussed here.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.
