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 2

By **John Reed Stark** (October 30, 2018, 1:25 PM EDT)


John Reed Stark

The U.S. Securities and Exchange Commission's outsider trading program has gone dark since 2016 — which is a shame and completely unnecessary.

As **set forth in part one of this two-part series**, from 2005 to 2016, the SEC's outsider trading dragnet evolved into a fully sophisticated and powerful enforcement program, with parallel criminal prosecutions becoming the norm. Kudos to the SEC for stepping up to protect the integrity of the global financial marketplace from outsider trading, a hi-tech category of wrongdoing that the SEC staff is best-suited to scrutinize, appreciate, understand and bring to justice.

But apparently, in 2016, the outsider trading music died, and an SEC school of thought emerged that outsider trading frauds were not securities frauds at all and did not fall within SEC jurisdiction. Regrettably, since the EDGAR data breach, the SEC has not brought any outsider trading enforcement actions, and the topic of outsider trading seems to have vanished from SEC priority lists.

Part two of this series now tackles this misguided SEC school of thought head-on by first analyzing the legal framework the SEC adopted to charge outsider trading and then challenging the SEC to reconsider its unfortunate abandonment of outsider trading prosecutions.

Outsider Trading and Malware Reverse Engineering

Though some might argue that SEC v. Oleksandr Dorozhko, **discussed in part one**, was the first formal judicial recognition of outsider trading, there was a slight snag to the Second Circuit's reversal — which could impact the SEC's prosecution of the outsider trading ring. The Second Circuit remanded the case to the district court for further proceedings as to the nature of Dorozhko's hacking process — noting that 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.

The new Dorozhko trial result could have perhaps hardened outsider trading theory but, alas, after Dorozhko's attorney confirmed he was unable to get in touch with Dorozhko, the district court granted summary judgment to the SEC and, among other relief, ordered Dorozhko to pay a civil penalty of approximately $286,000, Dorozhko's net profit from trading the IMS Health put options.

Thus, the theory of outsider trading, while partially vetted by the Second Circuit, still remains somewhat untested, i.e. the question remains whether exploiting a weakness in securities code is a mere theft or is instead a "deception" and therefore unlawful outsider trading.

Therein lies the rub: For the SEC staff to charge an outsider trading violation, the SEC must "reverse-engineer" the malware involved in the cyberattack and confirm that it involved a "deception." This is what may be causing the consternation among current SEC officials and led Andrew Vollmer, former SEC deputy general counsel, to write:

> The recent computer hacking cases [like Dorozhko] are important because they create dangers from over-zealous pursuit of securities law violations. The government had the ability to charge one or more reasonable and appropriate crimes against the hacker and

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. Success on the securities fraud claims will require enlarging current law. When the government uses untested and broadened legal theories in an enforcement case, it disserves the legal system. It treats the defendants unfairly, expands the law to catch future conduct that might not be blameworthy, and encourages the SEC and criminal prosecutors to threaten arbitrary claims in the future. The securities laws and the SEC do not police the world. Some bad acts are not securities fraud.

Malware: (Oh Lord) Please Don't Let Me Be Misunderstood

The term "malware" is often misunderstood. It is often defined as software designed to interfere with a computer's normal functioning, such as viruses (which can wreak havoc on a system by deleting files or directory information), spyware (which can gather data from a user's system without the user knowing it), worms (which can replicate themselves independently to spread to other computers), or Trojan horses (which are non-self-replicating programs containing malicious code that, when executed, can carry out an attacker's actions).

The definition of malware is actually far broader. In the context of a cyberattack, malware means any program or file used by attackers to infiltrate a computer system. Like the screwdriver a burglar uses to gain unlawful entry into a company's headquarters, legitimate software can actually be malware. For example, during an advanced persistent threat, or APT, cyberattack, attackers might use "RAR" files as containers for transporting exfiltrated information, yet RAR files have a wide range of legitimate uses.

The SEC's "Malware Pleading"

Post-Dhorozko, buried quietly within the SEC's outsider trading complaints, lies the gist of how the SEC pleads malware-related facts necessary to meet the "deception" requirement of Dorozhko. For instance, in paragraph 71 of the SEC Dubovoy outsider trading ring complaint and paragraph 79 of the SEC Zavodchiko outsider trading complaint, the SEC states:

> 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.

Similarly, in the SEC's Ly complaint, the SEC made an even more specific attempt at pleading that the outsider trading ring perpetrated a fraud, and not a theft, stating:

> In or about July 2013, [Jonathan] Ly discovered that he could electronically intrude without authorization ("hack") into Expedia senior executives' company computers by using Expedia's IT administrative access privileges. Through his hacks, Ly repeatedly viewed the contents of Electronic documents maintained by Expedia executives on their company computers, including the files of the Chief Financial Officer ("CFO") and the Head of Investor Relations, without anyone's knowledge or permission. Ly's hacking soon expanded and relied on several deceptive means to access both company computers and email accounts of Expedia's senior executives, including the following:
>
> (a) misusing Expedia's IT administrative access privileges to conceal his identity and access of Expedia computers;
>
> (b) hacking, by method (a) above, into a senior IT employee's computer and stealing a "passwords" file, which contained elevated credentials associated with an IT administrative service account ("IT Service Credentials"). The IT Service Credentials, which Ly did not have permission to use, gave him even greater levels of access to Expedia employees' corporate accounts, including employee emails; and
>
> (c) misappropriating the network credentials of innocent Expedia employees to access certain Expedia email accounts (in particular, accounts for the CFO and Head of Investor

Relations) while evading detection.

Finally, in the SEC's Hong prosecution, the SEC expanded its pleading even further, making the defendants' alleged deception crystal clear in a tour de force of outsider trading pleading:

> Defendants directly, indirectly, or through or by means of others hacked into Law Firm 1's nonpublic network through deceptive means that included:
>
> a. Installing malware on servers in Law Firm 1's network. "Malware" is software that is intended to damage or disable computers and computer networks, or to circumvent installed security and access controls.
>
> b. Using the malware to obtain broad access to nonpublic aspects of Law Firm 1's network, including broad access to Law Firm 1's nonpublic email systems.
>
> c. Compromising the user account of a Law Firm 1 Information Technology employee (hereinafter "Law Firm l IT employee"). Law Firm 1 IT employee had exceptional credentials that provided access to all other email accounts within Law Firm 1's nonpublic network.
>
> d. Posing as Law Firm 1 IT employee and using his Expedia credentials to gain access to all of Law Firm 1's nonpublic email accounts, including the email accounts of Law Firm 1 merger and acquisition partners (such as Partner A).
>
> e. Engaging in additional deceptive acts to conceal the breach of the nonpublic network including disguising the activity as typical network traffic. As a result, Law Firm l's security systems did not recognize the deceptive breach.

Undoubtedly, by the end of 2016, the SEC had mastered the art of pleading deception in outsider trading cases and the SEC's outsider trading program flourished, slowly becoming implanted in the SEC enforcement program. But regrettably, the SEC's outsider training program has apparently disappeared, shifting dramatically from one of bold proclamations to one of resounding radio silence.

The SEC's Outsider Trading Enforcement Program Since the EDGAR Data Breach

Since the EDGAR data breach, the SEC has not brought any outsider trading cases — zero, zilch, nada — and the topic of outsider trading seems markedly absent from the current laundry list of SEC enforcement priorities and concerns.

Indeed, a recent New York Times op-ed piece by SEC Commissioner Robert J. Jackson Jr. and former Southern District of New York U.S. Attorney Preet Bharara, "**Insider Trading Laws Haven't Kept Up With the Crooks**," hinted at a significant rift within the SEC commissioners about outsider trading, raising questions of whether the SEC will file any future outsider trading cases ever again.

The authors write:

> [W]hat if a hacker finds his way into a corporate computer system and trades on the sensitive information he uncovers? Will that hacker face charges of insider trading? This time, the answer depends on whether the information was obtained through sufficiently "deceptive" practices, like misrepresenting one's identity to gain access to information, rather than just mere theft, like exploiting a weakness in computer code. Again, we think ordinary investors would be deeply concerned that any trading on the basis of hacked information might evade punishment. Insider trading law should not allow the possibility that profits obtained through illicit trading could fund the cyberattacks that the American government and companies are constantly facing ... The uncertainty in insider trading law invites debate over the legality of misconduct that has no place in our markets.

The SEC Should Restore its Robust and Vigorous Outsider Trading Enforcement Program

Empowered by the latest malware and online intrusion weaponry, cyberattackers engaging in outsider trading schemes like the EDGAR hack pose a serious threat to the integrity and security

outsider trading schemes like the EDGAR hack pose a serious threat to the integrity and security of the global financial marketplace — a threat that must be stopped dead in its tracks.

No longer are social security numbers, credit card information and the like the primary focuses of hackers. Information is the target — and public companies and the SEC in its EDGAR database have a lot of it. Indeed, crooks from anywhere in the world can now use their cyber wares to orchestrate corporate espionage and remotely trade stock based on stolen secrets.

Of all the regulators and law enforcement agencies who mark securities fraud as their territory, the SEC stands alone in its expertise, experience and wherewithal, so it is not surprising that the Second Circuit validated the SEC's outsider trading theory (albeit with a malware reverse-engineering glitch).

To deter this rising 21st century menace, the SEC proceeded methodically with the Lohmus Havel, Blue Bottle, Dorozhko and even Stummer enforcement actions. Next, with its two 2016 sprawling outsider trading ring busts (Turchynov and Zavodchiko) and its first law firm hacking case (Hong), the SEC reinforced its assertion of outsider trading jurisdiction.

The SEC's initial creativity and its use of an initially ambitious outsider trading legal theory is not surprising. SEC staffers probably found inspiration from the almost 50-year-old pivotal U.S. Supreme Court decision written by Justice (and former SEC Commissioner (1935) and Chairman (1936-37)) William O. Douglas and captioned Superintendent of Insurance v. Bankers Life and Casualty Co. In that decision, Justice Douglas opined:

> We believe that section 10(b) and Rule 10b-5 prohibit all fraudulent schemes in connection with the purchase or sale of securities, whether the artifices employed involve a garden type variety fraud, or present a unique form of deception. Novel or atypical methods should not provide immunity from the securities laws.

Would courts intervene and halt the SEC from expanding insider trading liability to hack-and-trade schemes perpetrated by Dorozhko and the litany of other outsider trading culprits? Probably not.

First, judicial expansion of insider trading law is a tradition, some might say even a jurisprudential national pastime. And until Congress opts to define insider trading (a debate that has been raging for decades), using judge-made law remains the only way prosecutors can address the deceitful and dishonest practice of trading securities based on material, nonpublic information.

Second, with respect to outsider trading, the specially trained SEC staff are the most capable law enforcement organization to scrutinize, appreciate, understand and bring to justice the complex trading violations involved.

Finally, the SEC's efforts targeting outsider trading, under any theory (even an aggressive one), is not only good for investors but also good for capital markets — two constituencies the SEC is sworn to protect. The public's reaction to the EDGAR data breach dramatically proves this point.

Reporters, politicians and pundits all sounded a similar alarm: If the EDGAR hackers were caught, insider trading would be the crime.

But whatever the vagaries of the SEC's Depression-era insider trading statute, when it comes to outsider trading, SEC Chairman Jay Clayton has little choice but to dig in. As the guardian of the U.S. capital markets and sworn protector of investors, the SEC cannot allow itself to become a securities fraud kingpin, inadvertently sourcing ironclad tips of nonpublic information to an online outsider trading ring.

Looking Ahead

The EDGAR data breach was more than just a run-of-the-mill cyberattack (if there is such a thing). By exploiting an SEC data security weakness and attempting to use the exfiltrated EDGAR data for trading on material, nonpublic information, the cyberattackers ironically ensnared the SEC in its own crosshairs.

But there was a silver lining to it all. Like a beat cop who is mugged and robbed, the SEC would never look at data breach victims the same way again — or so we hoped. Now that a year or so

has passed since the SEC's announcement of the EDGAR data breach, the SEC should take the opportunity for some reflection — and consider its apparent abandonment of outsider trading enforcement.

The flexibility of the SEC's statutory weaponry has always been its hallmark. As renowned SEC scholar and Georgetown Law School professor (and former SEC staffer) Donald Langevoort wrote way back in 1993, Rule 10b-5 is an adaptive organism — and it works. Along those same lines, in 1996, William McLucas, the SEC enforcement director at the time, co-authored an article titled, "Common Sense Flexibility and Enforcement of the Federal Securities Laws," explaining how enforcement programs such as insider trading, foreign payments, municipal bond fraud and so many others grew out of the intentionally flexible SEC anti-fraud provisions.

Later, in 1999, when Steve Cutler became SEC enforcement deputy director and I was named chief of the SEC's Office of Internet Enforcement, we co-authored an article, "The SEC's Statutory Weaponry to Combat Internet Fraud," reiterating McLucas' thesis in the context of the SEC's internet program. In our article, Cutler and I cited the same adaptive capacity extolled by Langevoort and championed by McLucas (and the legendary Stanley Sporkin before him).

The SEC should get with the virtual program and redouble its efforts at policing outsider trading, an alarming and futuristic category of wrongdoing. The SEC has experienced firsthand the humility and alarm of playing the dupe in some offshore outsider trading scheme, and is clearly the best-equipped to fight back. For more than 80 years, the SEC's dedicated and vigilant enforcement staff has stood as a proud sentinel for investors, and Clayton should cut the SEC enforcement staff loose and refuse to allow a preposterously strict reading of the '34 Act's broadly vested anti-fraud provisions to stand in its way.

That the SEC experienced a hack-and-trade cyberattack was unfortunate to say the least — and the SEC's cybersecurity failure caused a fair degree of pain for SEC staff and investors alike. But the EDGAR data breach also provided the SEC with a rare glimpse into the perilous dangers of outsider trading plots. And it would be even more unfortunate for the SEC to fail to learn from such an extraordinarily teachable moment.

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 in this series.