THE FUTURE OF FINANCIAL CRIME AND ENFORCEMENT IS CYBER-BASED

Date: 3 January 2018

Investigations, Enforcement and White Collar Alert

By: Christopher L. Nasson, Neil T. Smith

I. *U.S. V. WILLNER:* THE FIRST "CYBER BOILER ROOM"

On November 8, 2017, federal prosecutors in the Eastern District of New York indicted Joseph P. Willner—a securities trader from Pennsylvania—for securities fraud, money laundering, and associated conspiracy charges related to his alleged operation of a fraudulent cyber trading scheme. [1] The scheme, described by the FBI as "a 21st century cyber boiler room," cost the targeted brokerage firms more than $2 million, according to the indictment. [2] Prosecutors alleged that between September 2014 and May 2017, Willner offered stock of publicly traded companies at artificially high, above-market prices while his co-conspirators concurrently hacked into the online securities brokerage accounts of targeted brokerage firms and used the accounts of unsuspecting victims to purchase the overpriced stock. [3] By then repurchasing the stocks from the hacked accounts at a lower price, Willner was able to quickly capitalize on the margin, resulting in more than $700,000 in profits. [4] Willner now faces up to twenty years in prison. [5]

II. *WILLNER* IS ONE PIECE OF A LARGER PUZZLE

A. Predecessor Cases to *Willner*

This cyber-enabled financial fraud prosecution should not be viewed in a vacuum. Indeed, this particular prosecution emerges from a backdrop of increasingly concentrated efforts by federal authorities to combat rapidly evolving and innovative cyber fraud schemes. To fully understand the context of DOJ's and the SEC's heightened focus, we should look to the *U.S. v. Korchevsky et al., U.S. v. Turchynov et al.,* and *SEC v. Dubovoy, et al.*, a series of cyber-enabled financial crimes cases involving high profile prosecutions and enforcement actions that underscored federal authorities' pivot toward this emerging area of complex financial crimes. [6] *Korchevsky, Turchynov,* and *Dubovoy* involved a hacking and insider trading scheme that Andrew Ceresney, the then-Director of the SEC's Division of Enforcement, called "one of the most intricate and sophisticated trading rings that we have ever seen." [7] The scheme spanned more than five years, during which conspirators allegedly hacked into newswire services to steal hundreds of corporate earnings announcements prior to public release. [8] The hackers allegedly transmitted the stolen data to traders across the globe, who then used the information to place illicit trades before the information was released to the public. [9] Authorities allege that this scheme generated approximately $100 million in illicit profits. [10]

©2005-2026 K&L Gates LLP. All Rights Reserved.

Since *Korchevsky* and its related cases, federal authorities have prosecuted a number of cyber-enabled financial crimes across the country. In October 2016, federal prosecutors in the Southern District of New York charged three Chinese traders with insider trading, conspiracy, wire fraud, and computer intrusion for their fraudulent cyber trading scheme, which involved hacking two large U.S. law firms and trading on information stolen from them. [11] In August 2017, Daniel Rivas—a technology consultant working in a global investment bank's Research and Capital Markets Technology Group—was charged with conspiracy, wire fraud, and multiple counts of securities fraud for his alleged involvement in a scheme in which Rivas accessed and transmitted sensitive information to financial advisers and friends in Miami, New Jersey, and California so that they could trade on this confidential information ahead of the market. [12]

B. Hack of the SEC and Creation of SEC Cyber Unit

This line of cyber-enabled financial crimes is not limited to private institutions and their databases. On September 20, 2017, the SEC announced that its computer system, EDGAR—which receives 1.7 million corporate and securities filings a year—had been hacked, potentially providing "the basis for illicit gain through trading." [13] Following this cyber intrusion, the SEC announced the creation of a Cyber Unit on September 25, 2017. The SEC's Cyber Unit has been tasked with "targeting cyber-related misconduct" including market manipulation schemes, hacking to obtain material nonpublic information, intrusions into retail brokerage accounts, and other cyber-related threats. [14] Its resources include staff from across the SEC Enforcement Division with "substantial expertise in the detection and pursuit of fraudulent conduct in an increasingly technological and data-driven landscape." [15] Its sole mission will be to investigate and bring cases involving cyber-enabled financial fraud.

III. ON THE HORIZON: A WAVE OF CYBER-ENABLED FINANCIAL FRAUD CASES

In the past two years, public interest surrounding cyber-enabled financial crimes has steadily increased. The public curiosity surrounding these alluring, intricate schemes runs parallel to federal authorities' heightened interest. The SEC's formation of a unit dedicated entirely to fighting cyber-enabled financial crimes illustrates the agency's intent to pursue this new breed of financial fraud. Because the SEC has dedicated additional resources, personnel, and funding to this initiative, we believe that the SEC is expecting a fruitful return on its investment. In fact, on December 4, 2017, the SEC announced the Cyber Unit's first filing of charges against Dominic Lacroix, an alleged recidivist Quebec securities law violator who operated a fast-moving initial coin offering fraud scheme that generated at least $15 million in sales of securities over the internet since August 2017. [16] This type of action is a sign of what is to come as federal authorities continue to focus their resources on cyber-enabled financial crime. But, because of the complex nature of these cases, it may take several years for the pursuit of some of these sophisticated schemes to unfold publicly. Any lull in media coverage of these cases should not be misinterpreted as calm on the war front. Cyber criminals continue to grow bolder, smarter, and more creative in perpetrating their illegal schemes.

As federal authorities aggressively tackle the threat of cyber-enabled financial crimes with full force, securities firms, broker-dealers, financial advisory firms, and public companies—and their regulatory and compliance personnel—must take note and revisit their internal controls, for the threat is not posed solely by cybercriminals. Victims of these crimes also may find themselves the targets of cyber-related enforcement actions. For example, the SEC can employ the "Safeguards Rule" against regulated financial institutions for failing to adopt policies and

©2005-2026 K&L Gates LLP. All Rights Reserved.

procedures reasonably designed to protect customer data. [17] For public companies, the SEC may bring action against companies for failing to timely disclose information about a material cybersecurity failure. Going forward, firms must stay up to date on cybersecurity rules and threats and implement policies and controls in response to these growing risks.

---

[1] *U.S. v. Willner*, Case No. 17-cr-00620 (E.D.N.Y. filed Nov. 8, 2017). Willner was indicted on four counts: (1) conspiracy to commit wire fraud, (2) conspiracy to commit securities fraud and computer intrusions, (3) securities fraud and (4) conspiracy to commit money laundering. The indictment is available at https://www.justice.gov/opa/press-release/file/1009531/download. The SEC filed a parallel action, *SEC v. Willner*, Case No. 17-cv-06305 (E.D.N.Y. filed Oct. 30, 2017). The SEC Complaint is available at https://www.sec.gov/litigation/complaints/2017/comp-pr2017-202.pdf.
[2] Press Release, DOJ, "Day Trader Indicted in Computer Hacking and Securities Fraud Scheme Targeting Online Brokerage Accounts" (Nov. 8, 2017), https://www.justice.gov/usao-edny/pr/day-trader-indicted-computer-hacking-and-securities-fraud-scheme-targeting-online.
[3] *See* Indictment, *supra* note 1.
[4] *Id.*
[5] *See Day trader accused of online brokerage hacking is indicted in Brooklyn*, Reuters, Nov. 8, 2017, https://www.reuters.com/article/us-usa-crime-cyber/day-trader-accused-of-online-brokerage-hacking-is-indicted-in-brooklyn-idUSKBN1D830R?mid=1.
[6] *U.S. v Korchevsky, et al*., Case No. 15-cr-00381 (E.D.N.Y. filed Aug. 5, 2015); *U.S. v. Turchynov et al*., Case No. 2:15-cr-00390 (D.N.J. filed Aug. 6, 2015); *Securities and Exchange Commission v. Dubovoy, et al.,* Civil Action No. 2:15-cv-06076 (D.N.J. filed Aug. 10, 2015) (amended Aug. 23, 2015).
[7] Press Release 2015-163, "SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases" (Aug. 11, 2015), https://www.sec.gov/news/pressrelease/2015-163.html.
[8] *Id.*
[9] *Id.*
[10] Press Release, DOJ, "Nine People Charged In Largest Known Computer Hacking and Securities Fraud Scheme" (Aug. 11, 2015), https://www.justice.gov/usao-edny/pr/nine-people-charged-largest-known-computer-hacking-and-securities-fraud-scheme.
[11] *U.S. v. Hong et al,* Case No. 16-cr-00360 (S.D.N.Y. filed May 26, 2016). The indictment, filed October 13, 2016, is available at https://www.justice.gov/usao-sdny/press-release/file/921006/download. *See also* Press Release 2016-280, "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.
[12] Press Release, DOJ, "Five Individuals Charged With Participating in Three Insider Trading Schemes Generating More Than $5 Million In Profits On Inside Information Misappropriated From An Investment Bank" (Aug. 16, 2017), https://www.justice.gov/usao-sdny/pr/five-individuals-charged-participating-three-insider-trading-schemes-generating-more-5. The indictment is available at https://www.justice.gov/usao-sdny/press-release/file/990256/download.
[13] Press Release 2017-170, "SEC Chairman Clayton Issues Statement on Cybersecurity" (Sept. 20, 2017), https://www.sec.gov/news/press-release/2017-170; *see also* Public Statement, SEC, "Statement on Cybersecurity" by Chairman Jay Clayton (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-

©2005-2026 K&L Gates LLP. All Rights Reserved.

clayton-2017-09-20; *see also* Press Release 2017-186, "Chairman Clayton Provides Update on Review of 2016 Cyber Intrusion Involving EDGAR System" (Oct. 2, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.
[14] Press Release 2017-176, "SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors" (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176.
[15] *Id.*
[16] Press Release 2017-219, "SEC Emergency Action Halts ICO Scam" (Dec. 4, 2017), https://www.sec.gov/news/press-release/2017-219. You can read the full SEC Complaint at https://www.sec.gov/litigation/complaints/2017/comp-pr2017-219.pdf.
[17] SEC Regulation S-P, 17 C.F.R. § 248.30.

KEY CONTACTS



CHRISTOPHER L. NASSON
MANAGING PARTNER, BOSTON OFFICE

BOSTON, NEW YORK
+1.617.261.3135
CHRISTOPHER.NASSON@KLGATES.COM



NEIL T. SMITH
PARTNER

BOSTON
+1.617.261.3180
NEIL.SMITH@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.