Enforcement Activity in the SEC's Newly-Created Cyber Unit: The First Six Months and What's Next

March 30, 2018

On September 25, 2017, the U.S. Securities and Exchange Commission ("SEC" or the "Commission") announced the creation of a Cyber Unit within the Enforcement Division in order to further the Division's "substantial expertise in the detection and pursuit of fraudulent conduct in an increasingly technological and data-driven landscape."[1] Commenting on the launch of the new unit, Enforcement Division Co-Director Stephanie Avakian described "[c]yber-related threats and misconduct" as "among the greatest risks facing investors and the securities industry."[2]

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

NEW YORK

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

WASHINGTON

Matthew C. Solomon
+1 202 974 1680
msolomon@cgsh.com

Anne Titus Hilby
+1 202 974 1635
ahilby@cgsh.com

In the six months since the Cyber Unit was launched, cybersecurity has remained at the forefront of the SEC's priorities, repeatedly highlighted as a focus of senior SEC officials' public comments[3] and a prominent component of the SEC's 2018 exam priorities.[4] In this memorandum, we begin by highlighting certain of the SEC's cyber enforcement actions since the Cyber Unit was formed, which unsurprisingly have focused on hacking as well as cryptocurrencies and initial coin offerings ("ICOs"). We then consider how these early actions, together with public statements and commentary from Enforcement Division leadership, are likely to translate into additional enforcement activity. In particular, we expect that the next wave of enforcement activity may involve cases against SEC registrants in connection with their failure to maintain adequate cybersecurity safeguards.

---

[1] Press Release, SEC, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017) ("Cyber Unit Press Release"), https://www.sec.gov/news/press-release/2017-176.

[2] *Id.*

[3] *See, e.g.*, Robert J. Jackson, Jr., Comm'r, SEC, Corporate Governance: On the Front Lines of America's Cyber War (Mar. 15, 2018), https://www.sec.gov/news/speech/speech-jackson-cybersecurity-2018-03-15; William Hinman, Dir. Div. Corp. Fin., SEC, Keynote Address at the PLI's Seventeenth Annual Institute on Securities Regulation in Europe (Feb. 1, 2018), https://www.sec.gov/news/speech/speech-hinman-020118; Jay Clayton, Chairman, SEC, Opening Remarks at the Securities Regulation Institute (Jan. 22, 2018), https://www.sec.gov/news/speech/speech-clayton-012218; Stephanie Avakian, Co-Dir. Div. Enf't, SEC, Securities Enforcement Forum Keynote Speech (Oct. 26, 2017) ("Avakian Cyber Unit Speech"), https://www.sec.gov/news/speech/speech-avakian-2017-10-26.

[4] *See* SEC Office of Compliance Inspections and Examinations, 2018 National Exam Program Examination Priorities 9 (Feb. 7, 2018) ("We will continue to prioritize cybersecurity in each of our examination programs. Our examinations have and will continue to focus on, among other things, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response."), https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf.

Early Enforcement Actions

The Cyber Unit was launched to focus principally on six areas of SEC enforcement: (1) "market manipulation schemes involving false information spread through electronic and social media," (2) "hacking to obtain material nonpublic information," (3) "violations involving distributed ledger technology and initial coin offerings," (4) "misconduct perpetrated using the dark web," (5) "intrusions into retail brokerage accounts," and (6) "cyber-related threats to trading platforms and other critical market infrastructure."[5]

While the Enforcement Division has taken action in a number of these areas in recent years, enforcement efforts made public since the Cyber Unit was launched have been concentrated in two areas: alleged improper trading involving hacking, and fraud and misrepresentations related to cryptocurrencies and ICOs.[6]

Improper Trading Cases. In one of the Cyber Unit's early enforcement actions, in October 2017, the SEC brought a fraud and market manipulation action against an individual for his role in an alleged scheme to gain unauthorized access to other individuals' online trading accounts, place unauthorized trades through those accounts in order to affect the prices of various publicly traded securities, and then trade in those securities through his own accounts at a profit.[7] The case is currently stayed pending the parallel criminal proceedings brought by the U.S. Department of Justice ("DOJ").[8] Both cases remain pending.

In another case brought by the Cyber Unit in parallel with the DOJ earlier this month, the Commission filed insider trading charges against the former Chief Information Officer ("CIO") of an Equifax business unit in connection with his trading in the company's stock prior to Equifax's public disclosure that it had been the victim of a massive data breach.[9] The indictment alleges that the CIO used material non-public information about the breach to sell his Equifax stock before the breach was made public thereby avoiding approximately $117,000 in losses. Some of the alleged evidence against the CIO includes inculpatory text messages and Internet searches, including searches for terms related to the drop in stock price of another credit reporting agency that had faced a breach, shortly before the CIO executed his trades in Equifax stock.[10] Both the SEC and DOJ cases remain pending.

Cryptocurrency and ICO Cases. Perhaps the clearest and most pronounced impact of the Cyber Unit to date is in the area of cryptocurrencies and ICOs. Here, the SEC has brought a number of actions against companies for allegedly operating unregistered exchanges,[11] engaging in the unregistered offering and sale of securities,[12] and misleading investors with claims of outsized returns and unsubstantiated product

[5] Cyber Unit Press Release.

[6] A list of cyber-related SEC enforcement actions is available at https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

[7] *See* Complaint ¶¶ 1-4, *SEC v. Willner*, No. 1:17-cv-06305 (E.D.N.Y. Oct. 30, 2017), ECF No. 1, https://www.sec.gov/litigation/complaints/2017/comp-pr2017-202.pdf.

[8] *See Willner*, ECF No. 9 (Nov. 29, 2017); *see also United States v. Willner*, No. 1:17-cr-00620 (E.D.N.Y. Jun. 8, 2017).

[9] *See* Complaint ¶¶ 1-2, *SEC v. Ying*, No. 1:10-cv-01069 (N.D. Ga. Mar. 14, 2018), https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf; *see also* Rahul Mukhi, Alexis Collins & Kal Blassberger, *DOJ and SEC Charge Former Equifax Executive With Insider Trading*, Cleary Cybersecurity and Privacy Watch Blog (Mar. 15, 2018), https://www.clearycyberwatch.com/2018/03/doj-sec-charge-former-equifax-executive-insider-trading/.

[10] *See Ying* ¶¶ 42-43.

[11] *See, e.g.*, Complaint ¶¶ 52-54, *SEC v. Montroll*, No. 1:18-cv-01582 (S.D.N.Y. Feb. 21, 2018), https://www.sec.gov/litigation/complaints/2018/comp-pr2018-23.pdf.

[12] *See, e.g.*, Complaint ¶¶ 47-49, *SEC v. AriseBank*, No. 3:18-cv-00186 (N.D. Tex. Jan. 25, 2018), https://www.sec.gov/litigation/complaints/2018/comp-pr2018-8.pdf; Munchee Inc., Securities Act Release No. 10445 (Dec. 11, 2017), https://www.sec.gov/litigation/admin/2017/33-10445.pdf.

offerings.[13] It has also suspended trading in the securities of a number of cryptocurrency-related enterprises following questions about the accuracy and adequacy of information about these companies, including their operations, compensation structures, and assets.[14] Among the issues being litigated by the SEC, and by the DOJ in parallel criminal actions, is whether and when a cryptocurrency qualifies as a form of a security called an "investment contract" under the test set forth by the Supreme Court in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).[15] As of the time of this memorandum, at least one SEC administrative order has found that ICO-based digital tokens to be issued on a distributed ledger constitute securities under *Howey* and its progeny,[16] and the issue is currently under consideration in a DOJ prosecution in the Eastern District of New York.[17]

Looking Ahead

As described above, the SEC's cyber enforcement has largely been concentrated in alleged improper trading involving hacking, and fraud and misrepresentation related to cryptocurrencies and ICOs since the launch of the Cyber Unit. The Unit's focus on alleged illicit trading and fraudulent offering of securities is not surprising as these cases are a traditional focus of the Commission's Enforcement Division. Looking ahead, the enforcement actions brought thus far by the Cyber Unit, as well as the Commission's guidance and public comments by SEC officials over the past six months, provide a potential roadmap for the Unit's priorities going forward, many of which may echo the SEC's actions to date:

— Continued enforcement relating to **misconduct involving cryptocurrencies** and **fraudulent and prohibited trading practices**. Avakian recently told an audience of investment advisers that the SEC has "dozens" of cryptocurrency investigations underway and that they should "expect to see more and more."[18] Separately, cybersecurity guidance the Commission released in February 2018 ("2018 Cybersecurity Guidance") reminded public companies that the prohibition on trading on material non-public information includes material non-public information regarding cybersecurity incidents and

[13] *See, e.g.*, Complaint ¶¶ 49-53, *SEC v. PlexCorps*, No. 1:17-cv-07007 (E.D.N.Y. Dec. 1, 2017), https://www.sec.gov/litigation/complaints/2017/comp-pr2017-219.pdf; Complaint ¶¶ 38-49, *SEC v. Recoin Grp. Found., LLC*, No. 1:17-cv-05725 (E.D.N.Y. Sept. 29, 2017), https://www.sec.gov/litigation/complaints/2017/comp-pr2017-185.pdf.

[14] *See, e.g.*, HD View 360 Inc., Exchange Act Release No. 82800 (Mar. 1, 2018), https://www.sec.gov/litigation/suspensions.shtml and https://www.sec.gov/litigation/suspensions/2018/34-82800-o.pdf; PDX Partners Inc., Exchange Act Release No. 82725 (Feb. 15, 2018), https://www.sec.gov/litigation/suspensions.shtml and https://www.sec.gov/litigation/suspensions/2018/34-82725-o.pdf; UBI Blockchain Internet, Ltd., Exchange Act Release No. 82452 (Jan. 5, 2018), https://www.sec.gov/litigation/suspensions.shtml and https://www.sec.gov/litigation/suspensions/2018/34-82452-o.pdf; The Crypto Co., Exchange Act Release No. 82347 (Dec. 18, 2017), https://www.sec.gov/litigation/suspensions/suspensionsarchive/susparch2017.shtml and https://www.sec.gov/litigation/suspensions/2017/34-82347-o.pdf.

[15] Under *Howey*, an investment contract is (1) an investment of money (2) in a common enterprise (3) with a reasonable expectation of profits (4) to be derived from the efforts of others. *See* 328 U.S. at 298-99; *see also SEC v. Edwards*, 540 U.S. 389, 393 (2004) (same).

[16] *See* Munchee, at 1-2.

[17] *See* Motion to Dismiss Indictment for Subject Matter Jurisdiction and Vagueness and Memorandum in Opposition to Motion to Dismiss the Indictment, *United States v. Zaslavskiy*, 1:17-cr-00647 (E.D.N.Y.), ECF Nos. 22 (Feb 27, 2018), 24 (Mar. 19, 2018). While it does not appear that this issue has been decided in the context of the cryptocurrency-related actions brought by the Cyber Unit, federal courts in Texas and New York have granted preliminary injunctions in at least three of these actions. *See AriseBank*, ECF Nos. 61 (Mar. 9, 2018), 69 (Mar. 19, 2018); *PlexCorps*, ECF No. 25 (Dec. 14, 2017); *Recoin Group*, ECF No. 11 (Nov. 13, 2017).

[18] Andrew Ramonas, *SEC Working on 'Dozens' of Cyptocurrency Probes, Official Says*, BLOOMBERG (Mar. 15, 2018), https://www.bna.com/sec-working-dozens-n57982089945/.

cyber risks.[19] SEC enforcement in these areas appears to be here to stay and will likely only increase.

— Enforcement surrounding **cyber-related disclosures, policies, and procedures**. Cyber-related public company disclosures has also been identified as an "enforcement interest" for the Cyber Unit. The 2018 Cybersecurity Guidance expanded upon 2011 guidance[20] that public company disclosure requirements may apply to cyber incidents and risks.[21] As we previously discussed, factors that may inform whether a cyber risk or incident is material requiring disclosure include the harm the incident could cause to a company's reputation, financial performance, or customer or vendor relationships, and an incident's potential to lead to adverse actions such as a regulatory investigation or litigation.[22] The 2018 Cybersecurity Guidance also recommended public companies implement and regularly assess corporate cybersecurity policies and procedures, including those related to disclosure of cyber incidents and risks as well as to the prevention of trading on material non-public information about such incidents and risks.[23] Some SEC Commissioners have gone even further to call for new SEC rulemaking requiring the filing of a current report on form 8-K upon a material cyber event.[24] Although the SEC has not yet brought a disclosure action related to cybersecurity risks or incidents, Yahoo! and Equifax have both publicly acknowledged receiving SEC inquiries following the disclosures of their respective data breaches.[25]

— Enforcement against **cyber-related misconduct to gain an unlawful market advantage**. In an October 2017 speech, Avakian described misconduct, such as hacking, to gain unlawful market advantages as an area of "enforcement interest" for the Cyber Unit.[26] This was echoed in cases highlighted in the Enforcement Division's most recent Annual Report[27]: In late 2016, the SEC brought charges against three Chinese traders

[19] *See* SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg 8166, 8171-72 (Feb. 26, 2018), https://www.federalregister.gov/documents/2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cybersecurity-disclosures. For a complete analysis of the 2018 Cybersecurity Guidance, see Cleary's alert memorandum, *SEC Issues Interpretive Release on Cybersecurity Disclosure*, Cleary Cybersecurity and Privacy Watch Blog (Feb. 28, 2018), https://www.clearycyberwatch.com/wp-content/uploads/sites/458/2018/02/2018_02_28-SEC-Issues-Interpretive-Release-on-Cybersecurity-Disclosure.pdf.

[20] *See generally* SEC Div. Corp. Fin., CF Disclosure Guidance Topic No. 2: Cybersecurity (Oct. 23, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[21] The 2018 Cybersecurity Guidance specifically noted disclosures related to regular periodic reports, registration statements, and keeping shelf registrations statements current. *See* 83 Fed. Reg. at 8168-69.

[22] *See SEC Issues Interpretive Release on Cybersecurity Disclosure*, at 2.

[23] *See* 2018 Cybersecurity Guidance, 83 Fed. Reg. at 8171-72.

[24] *See* Jackson, Corporate Governance: On the Front Lines of America's Cyber War; Kara M. Stein, Comm'r, SEC, Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/public-statement/statement-stein-2018-02-21.

[25] *See* Equifax Inc., Quarterly Report (Form 10-Q), at 41 (Nov. 9, 2017) (explaining Equifax was "cooperating with federal . . . agencies and officials investigating or otherwise seeking information and/or documents, including through Civil Investigative Demands, regarding the cybersecurity incident and related matters, including . . . the U.S. Securities and Exchange Commission"), https://otp.tools.investis.com/clients/us/equifax/SEC/sec-show.aspx?FilingId=12372346&Cik=0000033185&Type=PDF&hasPdf=1; Yahoo! Annual Report (Form 10-K), at 46 (Mar. 1, 2017) (explaining Yahoo! was "cooperating with federal, state, and foreign governmental officials and agencies seeking information and/or documents about the Security Incidents and related matters, including the U.S. Securities and Exchange Commission"), https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm#tx293630_29.

[26] *See* Avakian Cyber Unit Speech.

[27] *See* SEC Div. Enf't, Annual Report A Look Back at Fiscal Year 2017, at 13 (Nov. 15, 2017),

for allegedly trading on material non-public information obtained by hacking the computer systems of two large law firms.[28] And in early 2017, the SEC brought charges against an individual who allegedly used a false EDGAR filing to manipulate the price of Fitbit stock for personal profit.[29]

Failure to Maintain Cybersecurity Safeguards: The Next Wave?

While it is safe to assume that the Cyber Unit will pursue trading, cryptocurrency, and disclosure cases in the months ahead, there are also signs that the SEC may seek to bring enforcement actions in an area that has been somewhat less publicized—alleged failures to maintain **reasonable cybersecurity safeguards**. In the same October 2017 speech cited above, Avakian identified safeguarding information and ensuring system integrity as another area of "enforcement interest" for the Cyber Unit.[30] Specifically, she noted that SEC Regulations S-P, SCI, and S-ID require that covered entities "understand the risks they face and take reasonable steps to address those risks," including to put "reasonable safeguards in place to address cybersecurity threats."[31] While such cases have not been brought by the Cyber Unit to date, other Enforcement Division actions provide a roadmap of what some of these cases could look like.

Regulation S-P. Rule 30(a) of Regulation S-P, the so-called "Safeguards Rule," requires SEC-registered brokers, dealers, investment companies, and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."[32] These policies and procedures must be "reasonably designed" to (1) "[i]nsure the security and confidentiality of customer records and information," (2) "[p]rotect against any anticipated threats or hazards to the security or integrity" of such records and information, and (3) "[p]rotect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[33]

In 2016, the SEC brought an action against Morgan Stanley Smith Barney ("MSSB"), a registered broker-dealer and investment adviser, after an employee misappropriated personally identifiable customer information from 730,000 customer accounts, including names, phone numbers, addresses, account information, and securities holdings, and some of that data was later made available for sale online.[34] The SEC found that MSSB violated the Safeguards Rule by failing to adopt written policies and procedures reasonably designed to protect customer records and information, such as authorization mechanisms restricting employee access to confidential customer data, auditing and/or testing such authorizations over the 10 years they had been in effect, or monitoring employee access to relevant databases for unusual or suspicious patterns.[35] Under the terms of the settlement, MSSB paid a $1 million civil money penalty, agreed to cease and desist from violating the Safeguards Rule, and was censured.[36] Although this action preceded the new Cyber Unit, it provides a useful roadmap of how the new Unit might

https://www.sec.gov/files/enforcement-annual-report-2017.pdf.

[28] *See* Complaint ¶¶ 1-13, 18-20, *SEC v. Hong*, No. 1:16-cv-9947 (S.D.N.Y. Dec. 27, 2016), https://www.sec.gov/litigation/complaints/2016/comp-pr2016-280.pdf.

[29] *See* Complaint ¶¶ 1-4, *SEC v. Murray*, No. 1:17-cv-03788 (S.D.N.Y. May 19, 2017), https://www.sec.gov/litigation/complaints/2017/comp23836.pdf. Earlier this month, Murray was sentenced to two years imprisonment after pleading guilty to charges brought by the DOJ for the same conduct. *See* False EDGAR Filer Sentenced to Two Years in Prison for Fitbit Manipulation Scheme, Litigation Release No. 24075 (Mar. 22, 2018) (citing *United States v. Robert Murray*, No. 1:17-cr-00452 (S.D.N.Y. May 5, 2017)).

[30] *See* Avakian Cyber Unit Speech.

[31] *Id.*

[32] 17 C.F.R. § 248.30(a).

[33] *Id.*

[34] *See* Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, at 1 (June 8, 2016), https://www.sec.gov/litigation/admin/2016/34-78021.pdf.

[35] *See id.* ¶¶ 1-3, 8.

[36] *See id.* ¶ 19.

employ the Safeguards Rule as an enforcement tool in the wake of a data breach.

Regulation SCI. Rule 1001(a)(1) of Regulation SCI requires SCI entities, *i.e.*, SCI self-regulatory organizations, SCI alternative trading systems, plan processors, or exempt clearing agencies subject to the SEC's Automation Review Policies,[37] to have and enforce "written policies and procedures reasonably designed to ensure that its SCI systems . . . have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets."[38] Such policies and procedures must include, among other things, "[b]usiness continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption."[39]

Earlier this month, the Commission brought an action against the New York Stock Exchange and an affiliated exchange (together, "NYSE") for failing to have in place adequate policies and procedures reasonably designed to ensure operational capability.[40] In the event of a "wide-scale disruption" that left NYSE's trading systems unable to operate, the exchanges planned to rely on the backup system of a third affiliated exchange which would support NYSE trading but report those intraday trades on its own (rather than NYSE's) tapes and conduct those trades according to its own rules.[41] The Commission found this violated the requirement of Rules 1001(a)(1) and 1001(a)(2)(v) of Regulation SCI to have policies and procedures reasonably designed to ensure operational capability, including business continuity and disaster recovery plans "reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems."[42] SCI entities would do well to consider these requirements when planning for business continuity and operational capabilities following a wide-scale cyber-disruption.

Regulation S-ID. Regulation S-ID requires brokers, dealers, investment advisers, and investment companies, among others, to maintain a written program "designed to detect, prevent, and mitigate identity theft" in connection with certain covered accounts.[43] Requirements of the program include having policies and procedures reasonably designed to identify, detect, and respond to red flags; policies and procedures reasonably designed to ensure periodic updates to the program in light of changes in the risks identity theft poses to customers and to the safety and soundness of the institution; and calibrating the program to the "size and complexity" of the institution and "nature and scope of its activities."[44]

The MSSB and NYSE actions shed light on how the Cyber Unit might approach future actions for failure to maintain reasonable cybersecurity safeguards. Notably, both occurred following incidents that left individuals or systems vulnerable—in one case, a breach that

[37] *See* 17 C.F.R. § 242.1000; SEC, Regulation Systems Compliance and Integrity, 79 Fed. Reg. 72252, 72258-59 (Dec. 5, 2014).

[38] 17 C.F.R. § 242.1001(a)(1).

[39] *Id.* § 242.1001(a)(2)(v).

[40] *See* N.Y. Stock Exch. LLC, Exchange Act Release No. 82808 (March 6, 2018), https://www.sec.gov/litigation/admin/2018/33-10463.pdf.

[41] *See id.* ¶¶ 37-38.

[42] *Id.* ¶ 39.

[43] *See* 17 C.F.R. §§ 248.201(a) (listing regulated entities), (d)(1) (setting out requirements). A "covered account" is "[a]n account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties," and "[a]ny other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks." *Id.* § 248.201(b)(3).

[44] *See id.* § 248.201(d).

exposed customer personally identifiable information, and actual trading disruptions in the other. And, both were pursued despite an absence of findings that the policies, procedures, or processes at issue caused obvious economic harm to customers or investors, *i.e.*, that customers' were the victims of actual identity theft as a result of the breach of their personal data or that they suffered losses or the inability to trade as a result of the backup systems employed.[45]

Conclusion

The Cyber Unit's first six months have been marked by actions both in longstanding areas of SEC enforcement, such as prohibited trading practices, and emerging technologies and activities, such as cryptocurrencies and ICOs. Signals from the SEC and its senior leadership in speeches, reports, and guidelines, as well as cases and comments from other financial industry regulators, indicate that the SEC and other regulators are likely only to ramp up cyber-related enforcement going forward. One area that is worth watching is the SEC's interest in bringing investigations and cases based on the failure to maintain adequate cybersecurity safeguards. While the SEC might be constrained in the number of such cases it could bring, given the limited number of regulated entities that have obligations to maintain such safeguards, all regulated entities will want to monitor the Cyber Unit's actions in this area as a potential bellwether of the SEC's interest in using its enforcement powers to promote prophylactic measures against cyberattacks while at the same time continuing to bring traditional reactive cases.

…

CLEARY GOTTLIEB

[45] Of course, cybersecurity priorities and enforcement authorities do not end with the SEC. Similar to Regulation SCI, the Financial Industry Regulatory Authority requires members to establish and maintain business continuity plans that address, at minimum, data back-up and recovery; operational assessments; critical business, constituent, and counterparty impacts; and customer access to funds and securities in the event of a significant disruption. *See* FINRA Rule 4730. And the Regulation S-ID requirements are mirrored by CFTC rules instituting these requirements for certain CFTC-regulatees. *See* 17 C.F.R. §§ 162.30, 162.32; *see also* CFTC & SEC, Identity Theft Red Flags Rules, 78 Fed. Reg. 23638 (Apr. 19, 2013). In February 2018, the CFTC reached a settlement enforcing these parallel rules. *See* Jonathan S. Kolodner, Rahul Mukhi & Richard Cipolla, *Recent Enforcement Actions by Regulators Show Continued Focus on Cybersecurity and Data Protection Issues*, Cleary Cybersecurity and Privacy Watch Blog (Mar. 12, 2018), https://www.clearycyberwatch.com/2018/03/recent-enforcement-actions-regulators-show-continued-focus-cybersecurity-data-protection-issues/#more-2107.