Ballard Spahr LLP

Business Crimes Bulletin

The Growing Convergence of Cyber-Related Crime and Suspicious Activity Reporting

May 2017
By Marjorie J. Peerce and Kevin Leitão

Regulators and law enforcement are taking proactive steps to further leverage anti–money-laundering monitoring and reporting tools in their battle with cyber attacks and cyber crimes. In-house legal and compliance teams need to be fully versed in the latest FinCEN and bank regulatory guidance on cyber-related crimes and have the right professionals available to assist them with these matters.

Cyber-related crimes increasingly are making headlines across the globe as cyber attacks and other cyber incidents grow in intensity, volume and sophistication against government, political and business targets. The motives of attackers are as varied as their methods, but there is clearly an increasing number of attacks and other illegal activity motivated by financial gain against businesses, including financial institutions. Recent regulatory developments reveal that that illegal cyber activity has become more relevant to the fight against money laundering and terrorist financing as well.

Regulators and law enforcement are taking proactive steps to further leverage anti-money laundering monitoring and reporting tools in their battle with cyber attacks and cyber crimes. Supporting these regulatory and law enforcement initiatives will require financial institutions to increase collaboration between in-house anti–money-laundering compliance and cyber security teams. In-house legal and compliance teams need to be fully versed in the latest FinCEN and bank regulatory guidance on cyber-related crimes and have the right professionals available to assist them with these matters.

EXCEPTIONAL TEAMWORK

Financial services regulators in the United States have issued, and continue to issue, regulations and guidance relating to cyber-related crime and cyber attacks. For example, the Federal Financial Institutions Examination Council (FFIEC), the interagency group that coordinates federal supervision of depository institutions, released a cyber security assessment tool in June 2015. In 2014 and 2015, the FFIEC also issued several joint statements on various types of cyber attacks, ranging from distributed denial of service attacks to malware and cyber extortion.

At the state level, the New York Department of Financial Services (NYDFS) recently issued high-profile cyber security regulations covering all supervised entities that became effective on March 1 of this year. A year earlier, the NYDFS issued regulations with specific standards for suspicious activity monitoring and watch list screening by certain entities under its jurisdiction.

FinCEN GUIDANCES

The Financial Crimes Enforcement Network (FinCEN), the bureau of the U.S. Department of Treasury responsible for combating money laundering, terrorist financing and other financial crimes, has been providing guidance on cyber crimes for many years. Most of this guidance has focused on the suspicious activity monitoring and suspicious activity report (SAR) filing requirements applicable to certain types of financial institutions, including banks, broker-dealers, insurance companies, mutual funds, residential mortgage lenders and originators, money services businesses and casinos (SAR Filers). In 2016, FinCEN issued two advisories for financial institutions relating to suspicious activity reporting and cyber-related crime and cyber attacks.

FinCEN issued a targeted advisory notice on email compromise fraud schemes on Sept. 6, 2016 (E-mail Advisory). The E-mail Advisory discussed schemes targeting financial institutions' commercial customers (Business E-mail Compromise) and targeting individuals' email accounts (E-mail Account Compromise). In the E-mail Advisory, FinCEN cited FBI statistics that there have been 22,000 reported cases since 2013 of Business E-mail Compromise and E-Mail Account Compromise involving $3.1 billion. These schemes focus on impersonating victims in order to submit seemingly legitimate transaction instructions for a financial institution to execute, rather than taking over the victim's actual account. FinCEN provided 11 examples of suspicious activity red flags involving email correspondence and fraudulent transaction instructions for which financial institutions should be monitoring. SAR Filers should consider incorporating these red flags in their employee training and in their suspicious activity monitoring processes and technology.

On Oct. 26, 2016, FinCEN issued a more far-reaching advisory to financial institutions regarding cyber events and cyber-enabled crime (Cyber Advisory) and related frequently asked questions (Cyber FAQs). Although FinCEN stated that the Cyber Advisory "does not change existing [Bank Secrecy Act] requirements or other regulatory obligations," the guidance will lead SAR filers to dedicate more resources to monitoring suspicious cyber activity and SAR reporting. The Cyber Advisory covers four areas with the primary objective of enhancing suspicious activity monitoring and SAR filings. The focus on SAR filing in the Cyber Advisory, according to FinCEN, is based on the demonstrated value of SARs in assisting law enforcement's ability "to track criminals, identify victims and trace illicit funds."

The first area covered by the Cyber Advisory is SAR filings for cyber events. FinCEN defines a "cyberevent" as "an attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources or information." FinCEN views cyber events as potentially suspicious activities that are reportable through a SAR filing if they meet the standard monetary or other thresholds for SAR filing by that financial institution. In determining the monetary amount involved in a cyber event, FinCEN advises that the financial institution should consider "in aggregate the funds and assets involved in or put at risk by the cyber-event." To FinCEN, a cyber event occurs merely based on an "attempt" — there is no requirement that there be an actual compromise or financial loss. It seems likely that the application of the "attempt" and "put at risk" standards will lead to many cyber events exceeding the $5,000 and $25,000 monetary thresholds. Indeed, one of the examples provided by FinCEN involves cybercriminals gaining access to sensitive customer information, such as account numbers, credit card numbers and authentication information. Applying FinCEN's standards, criminal access to such information would almost always meet the monetary threshold for a SAR filing.

The second area discussed in the Cyber Advisory is the requirement to "include available cyber-related information when reporting any suspicious activity" whether or not the underlying suspicious activity involves a cyber event. The Cyber FAQs provide a non-exhaustive list of cyber-related information that should be included in a SAR filing. With respect to information to include in SAR filings for cyber events, FinCEN provides additional guidance on details to be provided while indicating again that the Cyber Advisory is not creating new obligations or expectations.

The third area covered by the Cyber Advisory is greater collaboration within financial institutions between anti–money-laundering compliance teams, cyber security teams and other units involved in identifying and mitigating cyber-related risks. These other units may include risk management, fraud prevention, network administration and other IT functions. FinCEN would like to see cyber-event related information provided by in-house cyber security teams to anti–money-laundering compliance teams and to have the anti–money-laundering compliance teams add such cyber-event related information to suspicious activity monitoring systems. In addition, FinCEN believes that cyber security teams can better mitigate their companies' cyber risks by leveraging suspicious activity information that can be provided to them by anti–money-laundering teams.

Greater collaboration between in-house groups will certainly be beneficial. Unfortunately, in-house teams in these areas already have substantial workloads and are challenged to meet current threats and expanding regulatory requirements. In the Cyber FAQs, FinCEN helpfully states that anti –money-laundering personnel will not be required to become knowledgeable on cyber security and cyber events. While it is good news that this will not be required by FinCEN at this time, as a practical matter, some anti–money-laundering professionals will need to become conversant in cyber security topics in order for meaningful collaboration to take place. Cyber-related information added to monitoring tools will need to go through rigorous model governance processes as well. In addition, anti–money-laundering officers will need to educate cyber security professionals on the suspicious activity monitoring and reporting process, including the strict rules on SAR confidentiality.

The fourth area covered by the Cyber Advisory is the sharing of information among financial institutions pursuant to Section 314(b) of the USA PATRIOT Act. Financial institutions that voluntarily participate in the Section 314(b) program are able to exchange information regarding individuals, entities, organizations and countries for the purposes of identifying and reporting money laundering and terrorist activities. Section 314(b) provides a safe harbor from liability for information sharing regarding money-laundering and terrorist activities. FinCEN would like to see more information sharing regarding cyber events between financial institutions pursuant to the Section 314(b) regulatory framework.

The scope of the 314(b) safe harbor, however, is limited. As former FinCEN Director Jennifer Shasky Calvery noted in testimony before Congress in May 2016:

> One issue that we frequently hear about from industry regarding information sharing is the scope of their safe harbor for information sharing under section 314(b). The statute currently only provides a safe harbor from liability for disclosing information under section 314(b) for activities that may involve terrorist actions or money laundering activities. Activities that are the predicates for money laundering, like fraud, drug trafficking, cybercrimes, and others, are not explicitly included in the safe harbor. Giving institutions an explicit safe harbor to share information on other potential serious criminal activity that may lead to money laundering or that may be related to terrorism (like suspicious purchases of explosives) can allow institutions to work together to detect criminal activity that is spread across a number of different financial institutions.
>
> *Testimony of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network, Department of Treasury, U.S. House of Representatives Committee on Financial Services Task Force to Investigate Terrorism Financing, May 24, 2016.*

The Cyber Advisory did not directly address this liability challenge. Accordingly, companies should be careful in deciding whether to join the 314(b) program and in assessing what cyber-related information is appropriate to share pursuant to Section 314(b) in order to ensure that any sharing complies with safe harbor requirements.

CONCLUSION

Cyber attacks and cyber crimes will continue to grow. The nexus between this activity and money laundering and terrorist financing also is likely to increase. As usual, FinCEN is looking for ways to expand the resources available for the battle against financial crime. The Cyber Advisory is another sensible initiative by them, but it is not without operational and legal challenges for financial institutions in attempting to follow it. Given the high level of interest by FinCEN and financial services regulators in cyber attacks and cyber crimes, institutions should understand the implications of this guidance and should seek assistance from outside counsel, where appropriate, in applying the guidance to cyber-related SAR filings and information sharing.

Marjorie J. Peerce, a member of Business Crimes Bulletin's Board of Editors, is a partner at Ballard Spahr LLP and focuses on White Collar Criminal Defense, Securities and Commercial Litigation. Kevin Leitão, Of Counsel at the firm, advises clients on AML compliance and data security.

The views expressed in the article are those of the authors and not necessarily the views of their clients or other attorneys in their firm.

Ballard Spahr LLP

Reprinted with permission from the May 2017 issue of *Business Crimes Bulletin*.
© 2017 ALM Media Properties, LLC. Further duplication without permission is prohibited. All rights reserved.

Atlanta | Baltimore | Bethesda | Boulder | Delaware | Denver | Las Vegas | Los Angeles | New Jersey | New York | Philadelphia | Phoenix | Salt Lake City
San Diego | Washington, DC | www.ballardspahr.com