Schulte Roth&Zabel

Alert

FinCEN Issues Suspicious Activity Report Guidance Concerning Cybersecurity

November 1, 2016

On Oct. 25, 2016, in the wake of other recent regulatory action on the subject of cybersecurity, the Financial Crimes Enforcement Network ("FinCEN") released new guidance and FAQs addressing financial institutions' suspicious activity reporting obligations related to cybercrime.[1,2] FinCEN has stated that the guidance "does not change existing [Bank Secrecy Act ("BSA")] requirements or other regulatory obligations for financial institutions."[3] Nevertheless, the guidance sets forth regulatory expectations regarding when financial institutions are required to file suspicious activity reports ("SARs") involving "cyber-enabled crime" or a "cyber-event."[4] The guidance also specifies what "cyber-related information" FinCEN expects to be reported in the SAR itself.[5]

"Cyber-Enabled Crime" is defined as "illegal activities (i.e., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers."[6] A "Cyber-Event" is defined as "an attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information."[7] And "Cyber-Related Information" is defined as "information that describes technical details of electronic activity and behavior, such as IP addresses, timestamps, and Indicators of Compromise (IOCs) ... [and] data regarding the digital footprint of individuals and their behavior."[8]

According to the guidance, a financial institution must file a SAR when it "knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or series of transactions."[9] In determining whether such cyber-events require the filing of a SAR, financial institutions must take into account the nature of the event and the information or systems

---

[1] FIN-2016-A005, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (Oct. 25, 2016) (hereinafter, "Advisory").

[2] Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs) (Oct. 25, 2016) (hereinafter, "Cyber-Event FAQs").

[3] Advisory at 3.

[4] *Id.* at 1.

[5] *Id.* at 2.

[6] *Id.* at 1.

[7] *Id.*

[8] *Id.* at 2.

[9] *Id.* at 4.

it targeted. Specifically, financial institutions must determine if the cyber-event compromised, or attempted to compromise, systems which contained information such as account numbers, credit card numbers, balances, online-banking credentials, or passwords which could be used to conduct or facilitate transactions.

The guidance emphasizes that, in the event of a cyber-attack, "no actual transaction [need] have occurred" in order to trigger a financial institution's SAR obligations.[10] Rather, if "the circumstances of the cyber-events and the systems and information targeted could reasonably lead [a] financial institution[] to suspect [that] the events were intended to be part of an attempt to conduct, facilitate, or affect an authorized transaction or series of unauthorized transactions aggregating or involving at least $5,000 in funds or assets," a SAR should be filed.[11] As such, even unsuccessful cyber-events that target such information or systems could require the filing of a SAR.[12]

Although the usual threshold for filing a SAR is $5,000,[13] it is likely that the monetary threshold prompting a SAR filing requirement will be satisfied when an attacker gains access to "sensitive customer information such as account numbers, credit card numbers, balances, limits, scores, histories, online-banking credentials, passwords/PINs, challenge questions and answers, or other similar information useful or necessary to conduct, affect, or facilitate transactions." This is so because the guidance counsels that, in determining the monetary amounts involved in a cyber-event, financial institutions should "consider in aggregate the funds and assets involved in or put at risk by the cyber-event," and even if an attack did not otherwise involve assets worth $5,000, access to sensitive customer information would often "put at risk" that amount. [14] In many cases "a financial institution could reasonably suspect the cybercriminals intended to steal and sell the exposed sensitive customer information to other criminals for financial exploitation to include unauthorized transactions at the institution."[15]

If a cyber-event SAR is required, the SAR should include all relevant and available cyber-related information and identifiers associated with the event. Relevant cyber-related information includes items like IP (internet protocol) addresses, URL (uniform resource locator) addresses, suspected malware filenames, email addresses, indicators of compromise (IOCs), as well as more traditional information associated with any affected accounts. The FAQs include a list of additional, though still non-exhaustive, examples.

Beyond the requirements, FinCEN raises the possibility of voluntary reporting. That is, "FinCEN encourages, but does not require, financial institutions to report egregious, significant, or damaging

[10] Advisory at 5; 31 C.F.R. § 1010.100(bbb) (defining "transaction").

[11] Advisory at 5.

[12] Cyber-Event FAQs at 3, FAQ No. 6 ("An otherwise reportable cyber-event should be reported regardless of whether it is considered unsuccessful.").

[13] See 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above $2,000. 31 C.F.R. § 1022.320(a)(2).

[14] Advisory at 4.

[15] *Id.* at 5.

cyber-events and cyber-enabled crime when such events and crime do not otherwise require the filing of a SAR."[16]

This guidance comes as part of a wider government focus on preventing cybercrime. Earlier this month, the federal banking regulators issued a joint advance notice of proposed rule-making concerning cybersecurity regulations and efforts to improve the safety and soundness of the U.S. financial system.[17] State-level regulatory bodies are also displaying an increased interest in cybercrime and proposing new and aggressive requirements on the entities that they regulate.[18] The FinCEN guidance itself formalizes the comments of former FinCEN Director Jennifer Shasky Calvery in which she encouraged financial institutions to file SARs on cyber-attacks and include cyber-derived information (particularly IP addresses) on SARs in an effort to combat cybercrime.[19]

In light of the increased focus by regulators in enhancing cybersecurity, and to best implement this guidance, financial institutions should increase collaboration and communication between their anti-money laundering ("AML") compliance personnel and cybersecurity or information technology personnel. In addition, financial institutions should update their AML training to reflect the new guidance and train AML compliance personnel in order to understand both when to file a cyber-related SAR, and what information should be included on a cyber-related SAR. Further, cybersecurity and information technology personnel must also be trained in order to understand when a cyber-event should be escalated to the attention of AML compliance personnel and what information AML compliance personnel will need in order to effectively file SARs.

Authored by Betty Santangelo, Gary Stein, Michael L. Yaeger, Jennifer M. Opheim, Melissa G.R. Goldstein and Nicholas Dingeldein.

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

Schulte Roth&Zabel
New York | Washington DC | London
www.srz.com

[16] *Id.* at 6.

[17] *SRZ Client Alert*, Federal Banking Agencies Propose New Cybersecurity Regulations (Oct. 24, 2016).

[18] *SRZ Client Alert*, NYDFS Proposes Detailed and Sweeping Cybersecurity Regulation for Financial Services Companies (Sept. 15, 2016).

[19] Former FinCEN Director Jennifer Shasky Calvery, Prepared Remarks at the FSSCC-FBIIC Joint Meeting (Dec. 9, 2015).