Cyber-SARs

Anti-money laundering and cybersecurity rules

MICHAEL L. YAEGER, MELISSA G. R. GOLDSTEIN, JENNIFER M. OPHEIM AND NICHOLAS DINGELDEIN, SCHULTE ROTH & ZABEL LLP

Investment advisers may soon have a new cybersecurity reporting requirement from a federal regulator. Anti-money laundering ("AML") requirements have recently been interpreted to include cybersecurity suspicious activity reporting ("SAR") requirements, so if AML obligations are extended to investment advisers, then these newly articulated cybersecurity reporting obligations will follow.

And AML obligations are on the horizon: On August 25, 2015, the US Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") proposed a regulation to add investment advisers who are registered with the SEC or required to be registered with the SEC under Section 203 of the Investment Advisers Act of 1940 ("Investment Advisers") to the definition of "financial institution" in the Bank Secrecy Act ("BSA") implementing regulations, and to require Investment Advisers to maintain AML programs and file suspicious activity reports ("SARs") ("Proposed Rule").[1] If the Proposed Rule becomes effective, Investment Advisers will be required to abide by FinCEN's rules and regulations and follow its guidance relating to AML. AML may also become a focus of SEC exams.

As for cybersecurity, FinCEN has recently released guidance, consisting of an advisory and FAQs, setting forth its views about when financial institutions must file SARs involving "cyber-enabled crime" or a "cyber-event" (collectively, "Cyber-SAR Guidance" or "Guidance").[2,3] Thus, Investment Advisers would be covered by the Cyber-SAR Guidance as soon as the FinCEN's Investment Adviser rule becomes final and takes effect.[4] This article is designed to provide background about that Cyber-SAR Guidance, as well as considerations Investment Advisers may want to start taking into account now in light of that Guidance.

Defining Suspicious Cyber Activity

According to the Cyber-SAR Guidance, a financial institution must file a SAR when it "knows, suspects, or has reason to suspect that a [C]yber-[E]vent was intended, in whole or in part, to conduct, facilitate, or affect a transaction or series of transactions."[5] A "Cyber-Event" is, in turn, defined as "an attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information."[6]

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 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.

> "Of particular note for Investment Advisers, the Cyber-SAR Guidance emphasizes that in the event of a cyber-attack, 'no actual transaction [need] have occurred'."

Of particular note for Investment Advisers, the Cyber-SAR 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.[7] Rather, if "the circumstances of the [C]yber-[E]vents 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.[8] As such, even unsuccessful Cyber-Events may require the filing of a SAR.[9]

Although the Proposed Rule includes a SAR-filing threshold of $5,000 that would be applicable to Investment Advisers,[10] the Cyber-SAR 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 [C]yber-[E]vent."[11] 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."[12] "Sensitive customer information" includes "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."[13]

Beyond the requirements, the Cyber-SAR Guidance raises the possibility of voluntary reporting. That is, "FinCEN encourages, but does not require, financial institutions to report egregious, significant, or damaging Cyber-Events and cyber-enabled crime when such events and crime do not otherwise require the filing of a SAR."[14]

Writing a Cyber-SAR

According to the Cyber-SAR Guidance, if an Investment Adviser files a cyber-SAR, the SAR should include all relevant and available Cyber-Related Information and identifiers associated with the event. "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,"[15] and includes such information as suspected malware filenames, and email addresses. The Cyber-Event FAQs include a list of additional, though still non-exhaustive, examples of information that should be contained in the filing.

Developing a Cyber-SAR Program

There are several steps that Investment Advisers should take to prepare for the possibility that they will be defined as "financial institutions" under FinCEN regulations and thus required to file SARs, including cyber-SARs, in light of the Cyber-SAR Guidance.

First, when developing and/or updating their AML programs (to the extent an Investment Adviser has already voluntarily adopted an AML program), Investment Advisers should take the Guidance into account. Accordingly, Investment Advisers ought to take steps to ensure that their policies and procedures clearly require that suspicious Cyber-Events and cyber-enabled crime be escalated and reported in SARs, consistent with the Guidance. Likewise, audit teams should be advised to test systems, controls and SAR reporting in this context.

Second, AML personnel and cyber/information technology personnel should start coordinating with each other. Cybersecurity and IT personnel ought to be made aware of when Cyber-Events need to be escalated to the Investment Adviser's AML personnel, and what information AML personnel will require. And AML personnel, on the other hand, ought to become sufficiently conversant with the cybersecurity risks their firm encounters in order to, among other things, provide accurate and specific guidance to the firm's employees regarding escalation of suspicious Cyber-Events.

Moreover, Investment Advisers ought to implement procedures to coordinate their reporting of cyber-related events. Information that might be included in a SAR pursuant to the new Cyber-SAR Guidance could also be included on any incident response report that an Investment Adviser prepares pursuant to its cybersecurity incident response plan (a document that the SEC's Investment Management Division has encouraged investment advisers to adopt).[16] Such reports may ultimately be viewed by regulators during annual exams, including regulators who may also be able to view the Investment Adviser's SARs.

Accordingly, Investment Advisers should ensure that the information contained in the SAR does not contradict the information in any incident response report, and vice versa, as contradictions could cause the regulator to find an exam deficiency. In addition, Investment Advisers should consider if any other disclosure documentation (such as offering memoranda or subscription documents) will need to be revised in light of Investment Adviser's potential SAR filing requirements, generally, and Cyber-Event reporting, specifically. **THFJ**

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

FOOTNOTES

1. Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers, 80 Fed. Reg. 52680 (proposed Aug. 25, 2015) (hereinafter "Proposed Rule") at 52683 ("FinCEN is proposing ... [i]ncluding investment advisers within the general definition of 'financial institution' in the regulations implementing the [Bank Secrecy Act].").
2. FIN-2016-A005, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime (Oct. 25, 2016) (hereinafter, "Advisory").
3. 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").
4. See Proposed Rule at 52690.
5. Advisory at 4.
6. Id at 1.
7. Advisory at 5; 31 C.F.R. § 1010.100(bbb) (defining "transaction").
8. Advisory at 5.
9. Cyber-Event FAQs at 3, FAQ No. 6 ("An otherwise reportable [C]yber-[E]vent should be reported regardless of whether it is considered unsuccessful.").
10. Proposed Rule at 56290 ("Proposed § 1031.320(a) sets forth the obligation of investment advisers to report suspicious transactions that are conducted or attempted by, at or through an investment adviser and involve or aggregate at least $5,000 in funds or other assets.").
11. Advisory at 4.
12. Id. at 5.
13. Id.
14. Id. at 6.
15. Id. at 2.