Hogan Lovells

Anti-Money Laundering and Cybersecurity Among the 2017 SEC Examination Priorities

January 30, 2017

On January 12, 2017, the Securities and Exchange Commission (SEC) announced its Office of Compliance Inspections and Examinations' (OCIE) 2017 Examination Priorities.[1] The priorities identify certain practices, products, and services that OCIE believes to present potentially heightened risk to investors and/or the integrity of U.S. markets. One of OCIE's goals in publishing the priorities is to encourage registrants to "evaluate their own compliance programs in these important areas and make necessary changes and enhancements." While the priorities cover a wide range of issues, two priorities on the list that SEC-regulated firms may want to pay particularly close attention to are anti-money laundering (AML) and cybersecurity. Both AML and cybersecurity were on the SEC's 2016 Examination Priorities list[2] and they are also both included in FINRA's 2017 Annual Regulatory and Examination Priorities Letter.[3] This client alert will provide a brief overview of these two important issues.

Anti-Money Laundering

The 2017 priority list entry for anti-money laundering states that "[m]oney laundering and terrorist financing continue to be risk areas" and that OCIE "will continue to examine broker-dealers to assess whether AML programs are tailored to the specific risks that a firm faces, including whether broker-dealers consider and adapt their programs, as appropriate, to current money laundering and terrorist financing risks." Note that at the present time registered investment advisers are not yet subject to the AML requirements to which broker dealers are subject.[4] OCIE also plans to "review how broker-dealers are monitoring for suspicious activity at the firm, in light of the risks presented," "the effectiveness of independent testing," as well as "compliance with suspicious activity report (SAR) requirements and the timeliness and completeness of SARs filed." As a reminder, the primary AML regulations promulgated by FinCEN and the SEC require broker-dealers to:

> (1) establish and implement risk-based anti-money laundering program which must include, at a minimum; (a) policies and internal controls to ensure compliance with the BSA; (b) independent testing for compliance; (c) designation of a chief compliance officer to ensure day-to-day compliance; (d) ongoing training for personnel; and (e) appropriate risk-based procedures for ongoing customer due diligence;[5]

---

1 https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf.

2 https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf.

3 http://www.finra.org/sites/default/files/2017-regulatory-and-examination-priorities-letter.pdf.

4 At this time, mutual funds and registered broker-dealers are the only SEC-regulated entities subject to BSA/AML obligations. However, in 2015, the Financial Crimes Enforcement Network (FinCEN) proposed a rule that would also require registered investment advisers to comply with AML program requirements. 80 Fed. Reg. 52680 (Sept. 1, 2015). This proposed rule is still pending.

5 31 C.F.R. § 1023.210.

(2) establish and implement a Customer Identification Program;[6]

(3) file required reports, including Currency Transaction Reports[7] (for transactions in currency greater than $10,000) and Suspicious Activity Reports;[8] and

(4) maintain records relating to certain funds transfers.[9]

For those looking to review broker-dealer AML obligations, the SEC's "Anti-Money Laundering Source Tool for Broker Dealers"[10] provides a detailed summary of the various authorities and obligations.

While the AML requirements are complicated and wide-ranging, it is important to note that the SEC's and FINRA's increased focus on them has led to several enforcement actions against firms that have failed to satisfy their AML obligations:

- In February 2016, the SEC fined a Miami-based brokerage firm, E.S. Financial, US$1 million to settle charges that it violated AML rules by allowing foreign entities to buy and sell securities without verifying the identities of non-U.S. citizen beneficial owners.[11]

- In May 2016, FINRA fined Raymond James & Associates US$17 million for a series of AML program deficiencies related to AML compliance procedures and personnel, due diligence and correspondent accounts of foreign financial institutions, and the absence of an effective customer information program. FINRA also fined its compliance officer, Linda Busby, US$25,000 and suspended her from the industry for three months.[12]

- In June 2016, the SEC charged a New York brokerage, Albert Fried & Company, with failing to sufficiently evaluate or monitor customers' trading for suspicious activity. The SEC found that the firm had failed to file SARs with bank regulators for over five years despite red flags tied to customer transactions. The firm ultimately agreed to pay a US$300,000 penalty to settle the charges.[13]

- In December 2016, FINRA penalized Credit Suisse Group AG for AML deficiencies and other violations. Imposing various remedial measures and a fine of US$16.5 million, FINRA found that Credit Suisse had primarily relied on its registered representatives to identify and escalate potentially suspicious trading, and that high-risk activity was not always escalated and investigated as required. Additionally, the firm's automated surveillance system to monitor potentially suspicious money movements was not properly implemented.[14]

Cybersecurity

Given cybersecurity's high profile in 2016, it should come as no surprise that cybersecurity is one of the SEC's 2017 Examination Priorities for both broker-dealers and registered investment advisers. The Commission plans to "continue [its] initiative to examine for cybersecurity compliance procedures and controls, including the implementation of those procedures and controls." A key cybersecurity obligation is Regulation S-P,[15] known as the "Safeguards Rule," which requires registered broker-dealers, investment companies, and

---

6 31 C.F.R. § 1023.220.
7 31 C.F.R. §§ 1010.311, 1010.306, 1010.312.
8 31 C.F.R. § 1023.320.
9 31 C.F.R. § 1010.410(e).
10 https://www.sec.gov/about/offices/ocie/amlsourcetool.htm#3.
11 https://www.sec.gov/news/pressrelease/2016-23.html.
12 http://www.finra.org/newsroom/2016/finra-fines-raymond-james-17-million-systemic-anti-money-laundering-compliance.
13 https://www.sec.gov/news/pressrelease/2016-102.html.
14 https://www.finra.org/newsroom/2016/finra-fines-credit-suisse-165-million-significant-deficiencies-its-aml-program.
15 17 C.F.R. § 248.30.

investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." For these purposes, customers are persons that have consumer relationships with the regulated organization.

The SEC and FINRA have gone after both investment advisers and broker-dealers in recent years for failing to implement adequate cybersecurity protections.

- In 2015, the SEC charged R.T. Jones Capital Equities Management, an investment adviser, with "fail[ing] to establish the required cybersecurity policies and procedures in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients."[16] The case was ultimately settled when R.T. Jones agreed to cease and desist from committing or causing any future violations of Regulation S-P, be censured, and pay a US$75,000 fine.

- The cost of inadequate cybersecurity was significantly higher for Morgan Stanley Smith Barney LLC which agreed to pay a US$1 million fine to the SEC in 2016 for "fail[ing] to adopt written policies and procedures reasonably designed to protect customer data."[17] These failures ultimately allowed a then-employee to impermissibly access and transfer data regarding approximately 730,000 accounts to his personal server, which was subsequently hacked by third parties.

- In 2015, FINRA brought an action against an Alabama firm, Sterne, Agee & Leach, Inc., for violating Regulation S-P, NASD Conduct Rule 3010, and FINRA Rule 2010 by failing to establish and maintain a supervisory system reasonably designed to safeguard confidential customer data.[18] These policy failures were compounded by the fact that confidential customer data was placed at risk when an unencrypted company laptop containing sensitive customer information was lost. The firm ultimately settled the action by agreeing to be censured, conduct an internal review, and pay a US$225,000 fine.

Both the SEC and FINRA have indicated their continued interest in both anti-money laundering and cybersecurity in their 2017 examination priorities. And – as prior years have shown – they are not reluctant to use their enforcement authorities to remedy noncompliance. Broker-dealers and registered investment advisers, like other financial institutions, should continue to ensure that their programs, internal controls, and personnel are ready for this continued scrutiny.

***

Please let us know if you have any questions or if we can be of assistance on these matters.

16 https://www.sec.gov/news/pressrelease/2015-202.html.
17 https://www.sec.gov/news/pressrelease/2016-112.html.
18 http://disciplinaryactions.finra.org/Search/ViewDocument/51064.

Contacts

Gregory Lisa
Partner, Washington, D.C.
Tel +1 202 637 3647
gregory.lisa@hoganlovells.com

Aleksandar Dukic
Partner, Washington, D.C.
Tel +1 202 637 5466
aleksandar.dukic@hoganlovells.com

Henry Kahn
Partner, Baltimore, and
Washington, D.C.
Tel +1 410 659 2780
henry.kahn@hoganlovells.com

Deen Kaplan
Partner, Washington, D.C.
Tel +1 202 637 5799
deen.kaplan@hoganlovells.com

Harriet Pearson
Partner, Washington, D.C.
Tel +1 202 637 5477
harriet.pearson@hoganlovells.com

Beth Peters
Partner, Washington, D.C.
Tel +1 202 637 5837
beth.peters@hoganlovells.com

Special thanks to Ryan Woo for his contribution to this update.