

MEMO# 30225

September 8, 2016

FinCEN Advisory on E-mail Compromise Fraud Schemes

[30225]

September 8, 2016

TO: COMPLIANCE MEMBERS No. 27-16

INVESTMENT ADVISER MEMBERS No. 17-16

OPERATIONS MEMBERS No. 26-16

SMALL FUNDS MEMBERS No. 40-16

TRANSFER AGENT ADVISORY COMMITTEE No. 44-16 RE: FINCEN ADVISORY ON E-MAIL COMPROMISE FRAUD SCHEMES

Earlier this week, the Financial Crimes Enforcement Network (“FinCEN”) of the U.S. Department of the Treasury published an Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes. [\[1\]](#) According to FinCEN, the Advisory was issued “to help financial institutions guard against a growing number of e-mail fraud schemes, in which criminals misappropriate funds by deceiving financial institutions and their customers into conducting wire transfers.” [\[2\]](#) The Advisory defines “e-mail compromise fraud,” “business e-mail compromise,” and “e-mail account compromise” and describes, in very basic terms, how each of these fraudulent schemes work. Generally speaking, they involve fraudsters either impersonating victims to submit seemingly legitimate transaction instructions for a financial institution to execute or accessing victims’ accounts to directly execute transactions without submitting transaction instructions. In other words, they involve compromised e-mail accounts being used to mislead financial institutions and their customers into conducting unauthorized wire transfers.

According to the Advisory, success in stopping these attacks “requires careful review and verification of customers’ transaction instructions and consideration of the circumstances surrounding such instructions.” [\[3\]](#) The Advisory lists eleven “fraud red flags” that might be indicative of a fraudulent scheme occurring. It also reminds institutions of their obligation to file a Suspicious Activity Report (SAR) if the institution “knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from: illegal activity; attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the Bank Secrecy Act (BSA); lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.” [\[4\]](#) It provides tips on how to reference the Advisory in any SAR filed by the institution concerning e-mail fraud compromise schemes.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] See Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes, which is available at: https://www.fincen.gov/statutes_regs/guidance/html/FIN-2016-A003.html

[2] Advisory at p. 1.

[3] Advisory at p. 4.

[4] Advisory at p. 6. [Emphasis in original.]

Copyright © by the Investment Company Institute. All rights reserved. Information may be abridged and therefore incomplete. Communications from the Institute do not constitute, and should not be considered a substitute for, legal advice.