Information Notice

FINRA Warns of Fraudulent Phishing Emails Targeting Member Firms

February 13, 2019

Suggested Routing

- Compliance
- Legal
- Risk
- Senior Management
- Training

Key Topics

- Fraud
- Phishing Scams

Summary

FINRA warns member firms to be on the lookout for a fraudulent phishing email that is currently circulating. Brokerage firms reported to FINRA that they have received suspicious emails targeting their compliance personnel. The email appears to be from a legitimate credit union attempting to notify the firm about potential money laundering involving a purported client of the firm. The email directs the recipient to open an attached document—which likely contains a malicious virus or malware designed to obtain unauthorized access to the recipient's computer network.

As a reminder, phishing scams are ever-changing and are designed to infiltrate the computer network of the recipient. Use caution when opening emails from unknown senders and do not open attachments until you verify the sender and information that might be included in the document.

Questions regarding this *Notice* may be directed to Joseph Ozag, Jr., Vice President, Office of the Whistleblower—Office of Fraud Detection and Market Intelligence, at (240) 386-6668.

Discussion

Phishing scams typically involve emails that falsely claim to be from financial institutions, credit card companies, internet auction sites, electronic payment services or some other service. These scams take steps to appear legitimate but are typically an attempt to lure you into providing sensitive personal or financial information by requesting that you provide it in a reply email, by clicking on a link to a website that mimics a legitimate website or by opening an attachment.

Member firms recently reported receiving suspicious emails from a purported BSA-AML compliance officer working at what appears to be a legitimate Indiana-based credit union. The email references a transfer of money made by a firm client to the credit union, a transaction that according to the email was placed on hold due to concerns about potential money laundering. The email contains an attachment that, if opened, could pose security risks to the firm. The sender attempted to give some legitimacy to the email by including a reference to a provision of the USA Patriot Act that relates to the ability of financial institutions to share information with each other. FINRA reminds member firms that attachments from unknown sources should not be opened unless cleared by your network security provider.

The email contains red flags of potential fraud, including:

- an email address that appears to be from Europe, rather than the U.S.-based credit union;
- numerous instances of poor grammar and sentence structure; and
- a request that the recipient open the email attachment for more details.

FINRA advises firms that receive suspicious emails from an unknown source to use caution before replying to the sender or opening any links or attachments. If your firm has received suspicious emails, here are some ways to report the incident to FINRA:

- contact your Regulatory Coordinator;
- file an online regulatory tip at *www.finra.org*;
- send an email to *whistleblower@finra.org*; or
- call FINRA's Whistleblower Line at (866) 963-4672.