Information Notice

Imposter Websites Impacting Member Firms

April 29, 2019

Suggested Routing

- Compliance
- Information Technology
- Legal
- Operations
- Registered Representatives
- Risk
- Senior Management

Key Topics

- Cybersecurity
- Fraud
- Imposter Websites

Summary

Several member firms have recently notified FINRA that they have been victims of imposter websites—which are sites designed to mimic a firm's actual website with the end goal of committing financial fraud. This *Notice* outlines steps firms can take to monitor for imposter websites and what to do if an imposter website is found.

Questions concerning this *Notice* should be directed to:

- David Kelley, Surveillance Director, at (816) 802-4729 or *David.Kelley@finra.org.*

Background and Discussion

Recently, several member firms have informed FINRA that they have experienced challenges related to imposter websites developed by various malicious parties. An imposter website typically is designed to mimic a member firm's actual website to obtain existing or potential clients' personally identifiable information (PII) or login credentials, which the website sponsors subsequently use to engage in financial fraud. Malicious parties have been targeting member firms regardless of whether those firms have an existing online presence. In some cases, they have also created email domains and accounts to correspond to the imposter websites. While this is not a new attack strategy, FINRA has observed that the frequency of such attacks on broker-dealers may be increasing.

Member firms can take proactive steps to monitor for imposter websites. For example, firms may consider registering website URL name variations, such as common misspellings or visually similar character substitutions, and using social media or website monitoring services to watch for imposter websites.

FINRA
Financial Industry Regulatory Authority

If a member firm becomes aware of an imposter website (through its own monitoring, the services of a vendor, notification from a customer or other source), the firm may consider the following actions to address the issue and deactivate the website:

- Report the attack to local law enforcement, the nearest Federal Bureau of Investigation (FBI) field office or the Bureau's Internet Crime Complaint Center, and the relevant state's Attorney General via their websites or, if possible, a phone call.[1]
- Run a "WHOis" search (*www.whois.net*) on the site to determine the hosting provider and domain name registrar associated with the imposter website (which may be the same organization in some instances). In some cases, this site also provides relevant contact information.
- Submit an abuse report to the hosting provider or the domain registrar asking them to take down the imposter website. Keep the pressure on these providers with repeated calls or emails, or, if necessary, seek the assistance of an attorney, cybersecurity specialist or consultant.
- Seek the assistance of a cybersecurity specialist attorney or consultant who deals with this type of fraud as they may have some law enforcement or hosting provider contacts or potential legal or other steps not outlined above.
- Notify the U.S. Securities and Exchange Commission (SEC), FINRA or other securities or financial regulators.
- Consider posting an alert on your website and sending email notifications to warn clients of the imposter website(s) and the associated URL(s).

If you are a member of Financial Services-Information Sharing and Analysis Center (FS-ISAC) or other information security or cybersecurity controls organizations, please contact them to share information about your attack so they may be able to provide additional mitigation advice.

Endnote

1. Member firms should consider proactively reaching out to these authorities to establish a relationship. A pre-established relationship can help facilitate the reporting and resolution process when a member firm experiences an attack.