Blogs
September 01, 2020
Asset Management ADVocate

FINRA Repeats Warnings of Imposter Websites

The Financial Industry Regulatory Authority ("FINRA") issued two regulatory notices in August 2020 with warnings of imposter websites (Regulatory Notice 20-30 and Regulatory Notice 20-27). In Regulatory Notice 20-30, FINRA warned that it has received notifications from several member firms that malicious actors are using registered representatives' names and other information to create imposter websites that appear to be the representatives' personal sites. FINRA also reported that the malicious actors were calling and directing potential customers to use the imposter websites and, in turn, may be responding through imposter-based email addresses that could contain malware or imbedded phishing links. Regulatory Notice 20-30, raises concerns that imposters may be using these sites to collect personal information from the potential customers to commit financial fraud.

Too Many "Ns"

This warning came on the heels of Regulatory Notice 20-27 in which FINRA warned of a new imposter website: www.finnra.org (please note the extra "n" in the domain name). According to FINRA, the imposter site contains a link to a registration site that is illegitimate. FINRA also warned that it is possible for the actors behind the imposter website to leverage the domain to send fake emails including those with imbedded phishing links or attachments containing malware. These warnings follow FINRA's similar previous warnings regarding imposter websites. In a similar warning to Regulatory Notice 20-30, FINRA explained that FINRA member firms reported challenges related to imposter websites developed by various malicious parties. According to the Information Notice, malicious parties were targeting firms regardless of whether those firms had an existing online presence. Similar to the circumstances with registered representatives, the malicious actors also created email domains and accounts to correspond to the imposter websites to potentially aid in their efforts to obtain existing or potential clients' personally identifiable information or login credentials.

Guidance

In its guidance on imposter websites, FINRA provides the following steps that firms and their registered representatives may wish to take to potentially mitigate the risks of imposter websites:

- Conduct periodic web searches or set up search filters for the names of the firm's registered representatives.
- Report the attack to the nearest Federal Bureau of Investigation ("FBI") field office or the FBI's Internet Crime Complaint Center, and the relevant state's Attorney General via their websites or, if possible, a phone call.
- 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). Sometimes, this site also provides contact information.
- Submit an abuse report to the hosting provider or the domain registrar asking them to take down the imposter website. Continue to engage with the providers by phone or email until the matter is resolved.
- Seek the assistance of a cybersecurity specialist, attorney, or consultant who has experience with this type of fraud.

- Notify the U.S. Securities and Exchange Commission ("SEC"), FINRA, or other securities or financial regulators.
- Consider posting an alert about the imposter website and the associated URL on the firm's website, notifying registered representatives and alerting clients—especially those of the registered representative whose name is being misused—to the imposter website and also warning them not to open emails from that domain name.

Conclusion

FINRA member firms should be aware of cyber-attacks, as they are likely to increase and not decrease, and have a process for responding to and remediating the risks.

Explore more in

Investment Management
Blog series

Asset Management ADVocate

The Asset Management ADVocate provides unique analysis and insight into legal developments affecting asset managers in the United States. Subscribe ?

View the blog