King & Spalding

Financial Services

Providing Strategic Legal Guidance to the Global Financial Services Industry

Data, Privacy and Security | Securities Enforcement and Regulation

MAY 15 2019

For more information, contact:

Natasha Moffitt
+1 404 572 2783
nmoffitt@kslaw.com

Russell Johnston
+1 212 827 4081
rjohnston@kslaw.com

Michael Hollander
+1 212 556 2377
mhollander@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

New York
1185 Avenue of the Americas
New York, New York 10036-4003
Tel: +1 212 556 2100

Imposter Websites Prompt Regulatory Warning to Financial Industry

On April 29, 2019, FINRA published an Information Notice alerting to a potential increase in member firms falling victim to imposter websites – websites designed to appear legitimate but that actually serve as a vehicle to compromise users' personally identifiable information (PII) or login credentials for the purpose of effecting financial fraud.[1] FINRA warns that member firms are increasingly being targeted regardless of whether they have an existing online presence.

As FINRA acknowledges in its Notice, attacks leveraging imposter websites are not new, but the prevalence of this attack strategy may be increasing. In September 2017, a Webroot study reported that, on average, approximately 1.4 million unique phishing websites are created each month.[2] And, the FTC recently announced in a February 28, 2019 press release that "[f]or the first time, imposter scams topped the list of consumer complaints submitted in 2018." [3] Unfortunately, with free website copying software available online, an attacker needs little experience to perpetrate such a fraud.

FINRA's Notice offers guidance on how member firms can protect themselves, for example by registering URL name variations, including misspellings and visually-similar character substitutions (e.g., www.realdomain.com vs. www.rea1domain.com), and by using imposter website monitoring services. FINRA offers further guidance on steps member firms may take upon learning of an imposter website.

In addition to these suggestions, a member firm should also consider:

- Taking an inventory of its assets and conducting a risk assessment to gain a complete understanding of which of the company's websites an attacker might be inclined to spoof. Some companies' websites comprise hundreds, if not thousands, of webpages, with only a subset being potential high-value targets for an attacker.

The first step to ensuring adequate protection is understanding which assets within an organization require added protection.

- Leveraging tools to trigger notifications whenever content is copied from a high-value webpage. Imposter websites frequently use copied content from the victim website, and such notifications might alert a company to potential attacker activity.
- Implementing multi-factor authentication (MFA) for all financial transactions. An exemplary implementation might include the member firm displaying an MFA token to the client on the website; the client prompting generation of a client-side MFA token by way of a pre-trusted mechanism and receiving the MFA token via SMS, email, etc. (or through integrated mobile applications); and the client proceeding with the transaction only if the MFA token the client received matches the token displayed on the member firm website.

Cybersecurity continues to be an area of increasing focus, especially for regulators like FINRA that oversee private sector financial institutions who maintain vast amounts of sensitive information. This Notice comes after a series of other recent messages from FINRA in this space. In December, FINRA issued a Report on Selected Cybersecurity Practices, and then earlier this year a reminder to the industry in their Priorities Letter that the regulator would further scrutinize the adequacy of cybersecurity programs at member firms.[4] As guardians of enormous amounts of data, financial institutions would be wise to heed these messages, and the warnings inherent within them, as they move forward in a world of increasing reliance on, and use of, cyber platforms by market participants and customers alike.

[1] FINRA Information Notices, *Imposter Websites Impacting Member Firms*, Apr. 29, 2019 (available at https://www.finra.org/sites/default/files/notice_doc_file_ref/Information-Notice-042919.pdf).
[2] Webroot, *Quarterly Threat Trends, Phishing Attacks Growing in Scale and Sophistication*, Sept. 2017 (available at https://www-cdn.webroot.com/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf).

[3] FTC Press Release, *Imposter Scams Top Complaints Made to FTC in 2018*, Feb. 28, 2019 (available at https://www.ftc.gov/news-events/press-releases/2019/02/imposter-scams-top-complaints-made-ftc-2018).
[4] FINRA, *Report on Selected Cybersecurity Practices - 2018*, Dec. 2018 (available at https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf); FINRA, *2019 Risk Monitoring and Examination Priorities Letter*, Jan. 2019 (available at https://www.finra.org/sites/default/files/2019_Risk_Monitoring_and_Examination_Priorities_Letter.pdf).