Regulatory Notice 20-30

Imposter Registered Representative Websites

Fraudsters Using Registered Representatives Names to Establish Imposter Websites

August 20, 2020

Notice Type
- Special Alert

Suggested Routing
- Legal
- Legal and Compliance
- Risk Management
- Senior Management

Key Topics
- Cybersecurity
- Fraud
- Imposter websites

Summary

Several firms have recently informed FINRA that malicious actors are using registered representatives' names and other information to establish websites ("imposter websites") that appear to be the representatives' personal sites and are also calling and directing potential customers to use these imposter websites. Imposters may be using these sites to collect personal information from the potential customers with the likely end goal of committing financial fraud.[1] This *Notice* describes certain common characteristics of these sites and actions firms and registered representatives can take to monitor for and address these sites.

Questions concerning this *Notice* should be directed to David Kelley, Director, Member Supervision Specialist Programs, at (816) 802-4729 or by email.

Background and Discussion

Recently, several member firms have notified FINRA that they are observing fraudsters using registered representatives' names and other legitimate information to establish imposter websites. (*See* Attachment A for sample screen shots of such sites.) In addition, FINRA has received reports that the fraudsters are calling and directing potential customers to the imposter websites.

Common features of these websites include the following:

- using the registered representative's name as the domain name for the website (*e.g.,* firstnamemiddlenamelastname.com);[2]
- including a picture purporting to be the registered representative;
- providing information about the registered representative's employment history, including prior employers' CRD numbers and examination history; and
- asking individuals to fill out a contact form with the individuals' names, email addresses, phone numbers, the subject of the inquiry and space for a message.

In addition, some of the sites contain poor grammar, misspellings, odd or awkward phrasings, or misuse financial services terminology.

In addition, it is possible malicious actors could leverage the domain to send fake emails purporting to be from the registered representative and which may include imbedded phishing links or attachments containing malware.

Member firms and registered representatives can take steps to identify these pages by conducting periodic web searches using registered representatives' names. In addition, some search engines allow users to create alerts that automatically search for defined terms (*e.g.,* a registered representative's name) and inform the user of new activity.

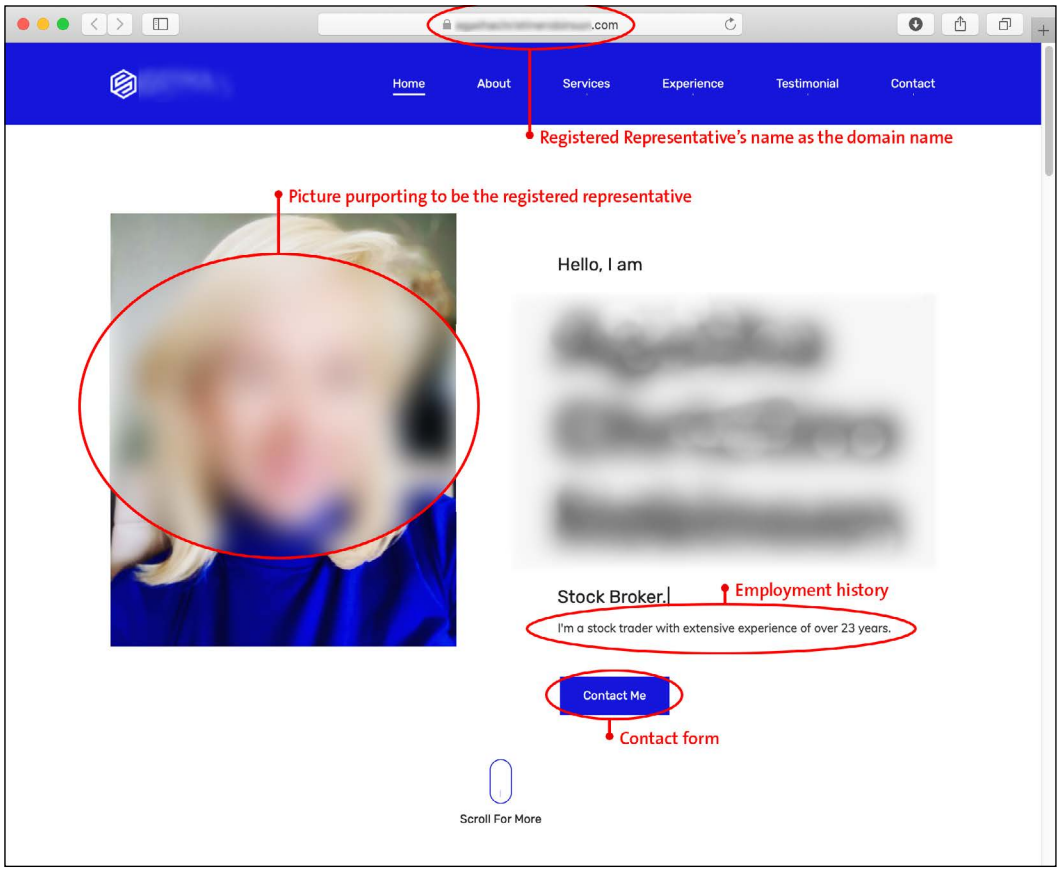
Firms may also consider the following steps similar to those FINRA noted last year in connection with risks relating to firm imposter websites:

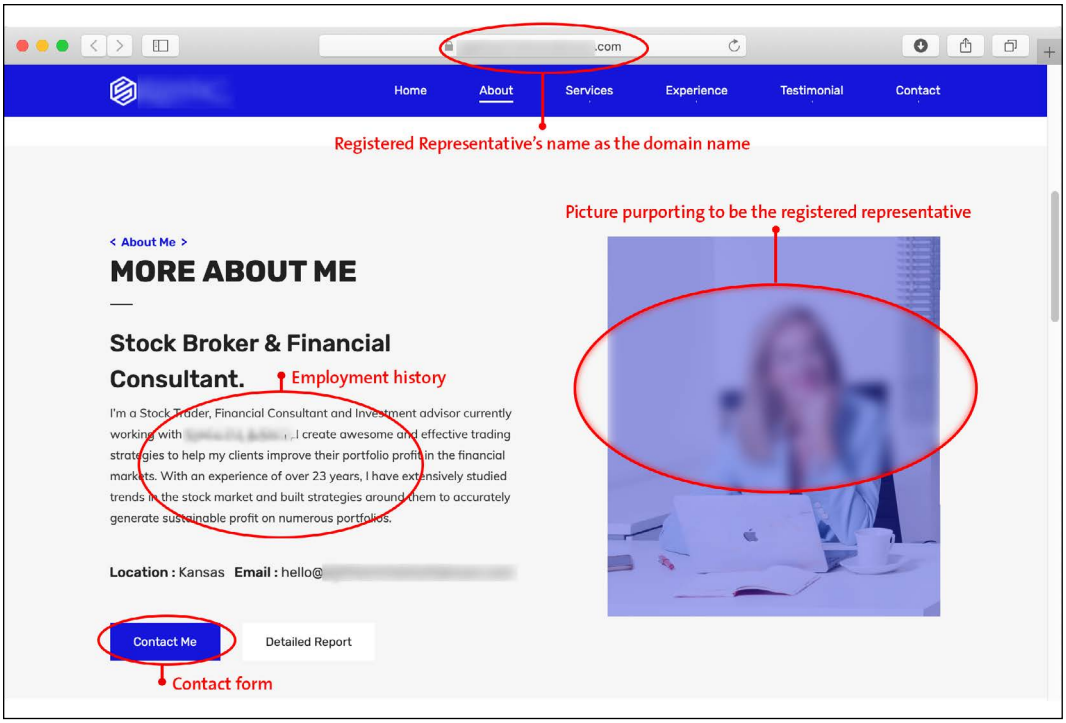
- Report the attack to the nearest Federal Bureau of Investigation (FBI) field office or the FBI's Internet Crime Complaint Center, and the relevant state's Attorney General via their websites or, if possible, a phone call.[3]
- Run a "WHOis" search (www.whois.net) on the site to determine the hosting 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. 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 your 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.

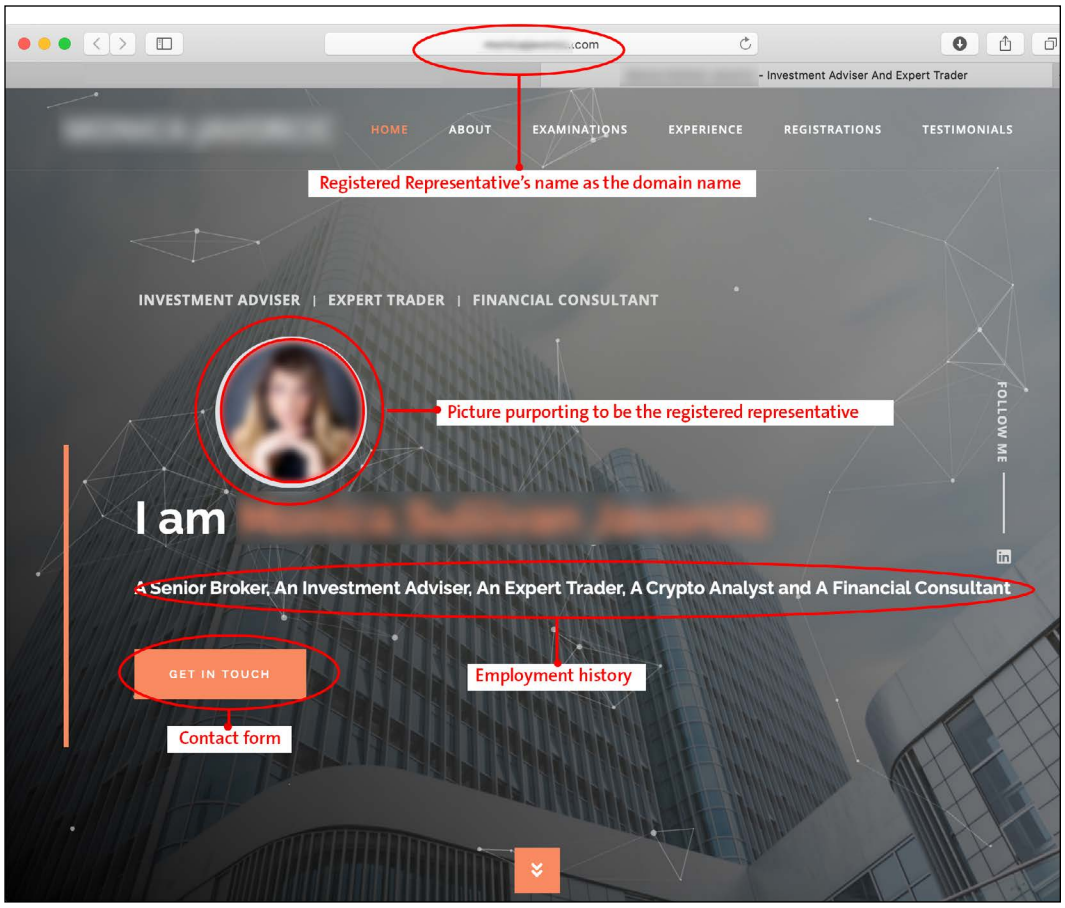
Endnotes

1. FINRA issued *Information Notice 4/29/19* last year to alert firms of imposter websites targeting firms.
2. The websites reported to FINRA to date use the correct spelling of the representative's name unlike some of the imposter firm websites FINRA observed last year that sometimes used common misspellings of a name or visually similar character substitutions.
3. 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.

Attachment A




.com
Home
About
Services
Experience
Testimonial
Contact
Registered Representative's name as the domain name
Picture purporting to be the registered representative
< About Me >
MORE ABOUT ME
Stock Broker & Financial Consultant.
Employment history
I'm a Stock Trader, Financial Consultant and Investment advisor currently working with , I create awesome and effective trading strategies to help my clients improve their portfolio profit in the financial markets. With an experience of over 23 years, I have extensively studied trends in the stock market and built strategies around them to accurately generate sustainable profit on numerous portfolios.
Location : Kansas Email : hello@
Contact Me
Detailed Report
Contact form


.com
- Investment Adviser And Expert Trader
HOME
ABOUT
EXAMINATIONS
EXPERIENCE
REGISTRATIONS
TESTIMONIALS
Registered Representative's name as the domain name
INVESTMENT ADVISER | EXPERT TRADER | FINANCIAL CONSULTANT
Picture purporting to be the registered representative
FOLLOW ME
I am
A Senior Broker, An Investment Adviser, An Expert Trader, A Crypto Analyst and A Financial Consultant
GET IN TOUCH
Employment history
Contact form