



CYBER DAILY ANALYTICAL UPDATE

The Cyber Risk Register

6 January 2022



KEY DEVELOPMENTS – 6 January 2022

US: DOJ conviction underscores growing threat that fraud will pose to US investors in 2022

The US Department of Justice (DOJ) disclosed on 5 January that a US citizen pleaded guilty to charges of running a large-scale internet-based fraud scheme that stole an estimated USD 50 million from 70 investors between 2012 and October 2020. This individual and his co-conspirators reportedly impersonated Financial Industry Regulatory Authority (FINRA) brokers and used 150 fraudulent websites to advertise "investment opportunities" that promised "higher than average rates of return on certificates of deposit". This conviction confirms the Federal Bureau of Investigation's (FBI) July 2021 warning that threat actors are increasingly impersonating registered investment professionals, such as brokers, to conduct investment fraud. Furthermore, this scheme is indicative of the FBI's March 2021 findings that business email compromise (BEC) operations, romance and confidence scams, and investment fraud accounted for roughly half of the USD 4.2 billion in cyber crime-related losses that organisations recorded in 2020. Further such scams are highly likely to be launched in the coming six months due to their low technical requirements and high pay-out rates. High-profile investors, C-Suite executives, or finance sector employees will constitute some of the most at-risk for this activity.

End of Report

The Cyber Risk Register

Cyber Daily Analytical Updates form part of Sibylline's **Cyber Risk Register**, a ground-breaking analytical service designed to help organisations of all sizes navigate an uncertain world.

Please **contact us** if you would like more information on how our strategic risk information could work for your organisation.

Email: info@sibylline.co.uk

Tel: +44 203 411 0697

