Dubai Financial Services Authority

BY EMAIL

23 March 2020

To the Senior Executive Officers of DFSA Authorised Firms; Managing Partners of Registered Auditors; Money Laundering Reporting Officers of DNFBPs; and Principal Representatives of Representative Offices (collectively referred to as "Firms").

RE: Cyber Risk Monitoring and Reporting

Dear SEO, Managing Partner, Principal Representative, and Money Laundering Reporting Officer:

We are sure you have seen recent media attention that the current extraordinary circumstances can increase a Firm's vulnerability to cyberattacks. For example, there has been an increase in the volume of email phishing campaigns used by cybercriminals attempting to exploit concerns about COVID-19, and higher numbers of staff working remotely may increase the risk of unauthorised access to a Firm's network and IT systems.

Firms should continue staff cybersecurity awareness programmes to ensure staff are equipped to identify security threats and know how to avoid, report, and/or remove them. Firms must ensure they maintain appropriate controls to limit the risk of unauthorised access and maintain ongoing and effective network and perimeter monitoring. They must remain diligent in keeping up to date with hardware and software patches to prevent cybercriminals from leveraging vulnerabilities in VPN gateways. Finally, Firms should review their remote access controls and implement enhancements were necessary. For example, where a Firm has not already done so, it should implement two-factor authentication.

Threat intelligence is an invaluable tool in preventing cybercrime, especially in an environment of increased threat activity. Therefore, we encourage Firms to register to use the DFSA Threat Intelligence Platform (TIP) and make use of the cyber threat information available on TIP to enhance their cybersecurity. Firms can register via the DFSA ePortal.

We also remind Authorised Firms and Registered Auditors to report material cyber incidents to the DFSA using the Cyber Incident Notification Form on the DFSA ePortal. To assist in completing the form, we have prepared a guidance document called "Cyber Incident Notification Form – Guidance." Firms should familiarise themselves with the Cyber Incident Notification Form and the guidance document before they experience a reportable incident. For ease of reference, and sharing among relevant stakeholders, we include with this letter links to a copy of the Cyber Incident Notification Form and a copy of the guidance document.

Level 13, The Gate, PO Box 75850, Dubai, UAE
Telephone: +971 (0)4 362 1500
Fax: +971 (0)4 362 0801

Finally, in addition to reporting cyber incidents, we remind Authorised Firms and Registered Auditors of the notification requirements of GEN 4.2.10; GEN 11.10 and in particular, GEN 11.10.7(b), GEN 11.10.7(g) and 11.10.13; as well as AUD 2.6.6.

If you have any questions in relation to this letter, please contact us using the DFSA Supervised Firm Contact Form found on the DFSA Website.

Yours sincerely,

Bryan Stirewalt
Chief Executive

Level 13, The Gate, PO Box 75850, Dubai, UAE
Telephone: +971 (0)4 362 1500
Fax: +971 (0)4 362 0801