Financial Services Regulatory Authority
ADGM Authorities Building,
ADGM Square,
Al Maryah Island,
Abu Dhabi

30 March 2020

Notice No.: FSRA/FCPU/04/2020

Dear Authorised Persons (“APs")

RE: Heightened risk of cyber-attacks amidst the COVID-19 pandemic

The financial services industry worldwide is experiencing turbulent times in the midst of the global COVID-19 (Coronavirus) pandemic. Cyber risks has taken on greater prominence as reliance is placed on technology to assure operational continuity and the shift towards remote working models to restrict the spread of the virus.

This brings to the forefront the digital vulnerabilities such as phishing attacks, hacking, malware intrusions and fraud stemming from potential information breaches containing personally identifiable information.

The FSRA wishes to alert APs of various *modus operandi* employed where threat actors may be leveraging information on COVID-19 to spread malware infections through phishing emails. The subject lines of these emails are designed to contain seemingly valuable information about the current status of the outbreak to lure individuals into opening attachments or clicking on malicious links.

In addition, remote working models in a distributed work environment magnify the vulnerabilities of potential cyber-attacks. This is an important factor to address where documents containing confidential customer and/or financial information are shared between staff via a distributed work environment.

It is of utmost importance for APs to remain vigilant during these times. The FSRA emphasizes the importance of APs instituting incident response plans that are commensurate with the nature, scale and complexity of the AP’s business. This will increase AP’s preparedness in identifying and mitigating operational and cyber risks, thus enhancing the overall resilience profile to diminish the impact of possible cyber-attacks.

APs should also prepare for possible business disruption and proactively assess the cyber hygiene practices followed by their remote workforce, enterprise-wide. APs should consider the following **effective cyber hygiene practices,** which are not limited to:

- Ensure Virtual Private Network (VPNs) and other remote access systems are fully patched
- Enhance system monitoring to receive early detection and alerts of suspicious activity
- Implement multi-factor authentication (MFA)
- Ensure all devices have proper configured firewalls, as well as anti-malware and intrusion prevention software installed
- Avoid clicking on links in unsolicited emails and be wary of email attachments
- Double-check any links by hovering over them to ensure you will not be redirected to a fraudulent website
- Review URL domain names for typos and/or missing characters
- Restrict the sharing of personal or financial information in emails, and do not respond to email solicitations for such information
- Refer to trusted sources and legitimate, government websites for up-to-date, fact-based information about COVID-19

The FSRA wishes to thank all that have participated in the Cyber Resilience Stock-take Questionnaire. This has provided us with meaningful insights on existing cyber risk management practices amongst firms in developing risk-appropriate supervisory plans for the regulated activities of our firms.

Sincerely,

Richard Teng
Chief Executive
Financial Services Regulatory Authority