By email

14 July 2023

To: Senior Executive Officers

Subject: Recent systemic supply chain cyber-attack

Dear SEO,

This letter is in response to recent events involving the MOVEit cyber-attack.

MOVEit Transfer is a file transfer application used throughout the financial sector to securely transfer large volumes of sensitive data between systems. Various international press and cyber monitoring bodies have reported concerns about threat actors actively exploiting vulnerabilities in the MOVEit software in order to steal sensitive data, deploy ransomware and disrupt business operations. Progress Software (the vendor of the MOVEit Transfer software) has recently released remediation measures and patches to address these vulnerabilities.

DFSA encourages Authorised Firms to:

- check if you or any firms in your supply chain have exposure to MOVEit and understand the extent of any vulnerabilities and/or impacts;
- apply remediation measures and patches published on Progress Software's official webpage, in the event that your Firm has exposure to MOVEit; and
- report to the DFSA without delay, via the Cyber Incident Notification form, any impacts or signs of malicious activity. The notification form can be located on the DFSA ePortal.

Promptly patching software vulnerabilities is crucial due to the increasing prevalence of cyberattacks targeting such vulnerabilities. Attacks like the MOVEit, exploit vulnerabilities in supply chains and third-party software, posing a significant threat to organisations. Therefore, the DFSA reminds Authorised Firms of the importance of implementing effective vulnerability and third-party risk management programs to:

- identify critical third-party service providers and their security levels;
- prioritise vulnerabilities based on their severity, impact, and exploitability;
- implement a robust patch management process to promptly apply security patches and updates to all systems and software;
- understand the security risks posed by third-party suppliers;
- set and communicate minimum security requirements for their suppliers; and

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

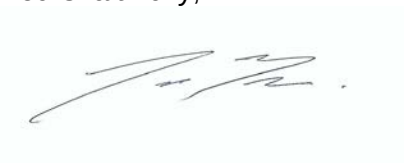
- build assurance activities (e.g., setting key performance indicators, periodically assessing performance, and including the 'right to audit' into agreements) into third-party risk management agreements.

If you have not already done so, we encourage you to register for the DFSA Cyber Threat Intelligence Platform (TIP) in order to receive timely cyber threat information.

You may also refer to our cyber related Dear SEO letters on the DFSA's website for further information concerning the DFSA's Cyber Risk Management Guidelines, Cyber Incident Notification Form – Guidance, and cyber risk focus areas.

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

Yours faithfully,



Justin Baldacchino
Managing Director, Supervision

Cc: Compliance Officers of Authorised Firms