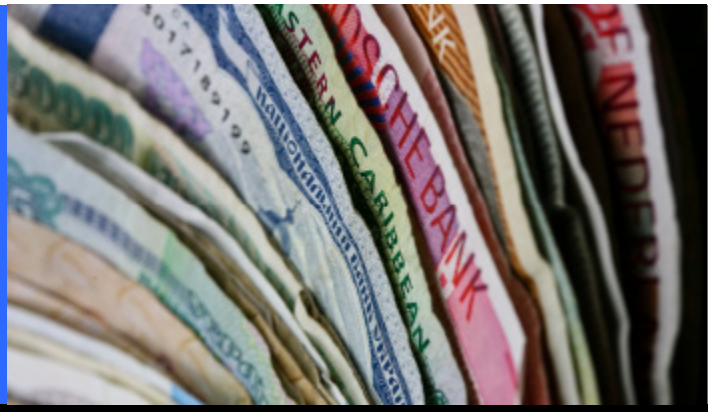
View on our website.

GIBSON DUNN



Financial Regulatory Update August 12, 2026

Hong Kong SFC Takes Enforcement Action Against Firm for Cybersecurity Deficiencies

This is, in our view, intended as a pointed reminder to the market that the SFC expects licensed corporations to maintain robust cybersecurity frameworks – and is willing to take action against firms whose frameworks fail to meet their expectations, even if clients are not directly affected.

On July 28, 2026, the Securities and Futures Commission (**SFC**) reprimanded and fined Luk Fook Securities (HK) Limited (**LFSHK**) HK$2.1 million for failing to implement adequate and effective cybersecurity control measures.[1] While the fine itself is not large, this matter is notable given that it is the first known example of the SFC taking disciplinary action against a licensed corporation because of a cyberattack against the firm's trading systems. Importantly, the SFC took action notwithstanding the absence of client asset misappropriation, unauthorized trading, client complaints or client financial loss – factors which the SFC treated as mitigating rather than exculpatory. This is, in our view, intended as a pointed reminder to the market that the SFC expects licensed corporations to maintain robust cybersecurity frameworks – and is willing to take action against firms whose frameworks fail to meet their expectations, even if clients are not directly affected.

I. SFC ENFORCEMENT ACTION

LFSHK is licensed to carry on Type 1 (dealing in securities), Type 4 (advising on securities) and Type 9 (asset management) regulated activities. During the COVID-19 pandemic, LFSHK enabled remote working through a VMware virtual environment, which allowed employees, third-party vendors, and IT staff to access office systems remotely.

On September 19, 2022, a hacker exploited the VMware environment to gain access to LFSHK's Active Directory (**AD**) server. The SFC described the resulting disruption to LFSHK's critical IT infrastructure as sweeping, extending to its file servers, domain controllers, email servers, trading application servers and accounting servers. Throughout the resulting disruption, LFSHK's clients lost access to both its internet and mobile trading channels, leaving orders placed through account executives as the only available route to market. Full restoration was achieved only on October 7, 2022, approximately three weeks after the attack, with systems brought back online in stages.

LFSHK reported the incident to the SFC on the day of the attack and engaged external experts, including an independent reviewer at the SFC's request, to investigate the incident and assess its internal controls. The SFC found no evidence of client asset misappropriation, unauthorized trading, financial loss, data leakage, or client complaints.

However, the SFC's investigation revealed various cybersecurity deficiencies across LFSHK's IT environment, as follows:

- ***Insufficient Network Security Controls:*** A number of LFSHK's network devices and equipment lacked firewall protection and were not monitored by a Security Information and Event Management tool. This left the network exposed to external threats and enabled the attacker to access an internal system directly from the Internet.
- ***Inadequate User Access and Privileged Account Management:*** LFSHK failed to establish effective controls over user access and privileged accounts, heightening the risk that a single compromised account could be used to move laterally across the network.
- ***Use of Unsupported Legacy Systems:*** The infected VMware environment was running outdated operating systems (Microsoft Windows 2008 and Windows 7) that did not receive security updates and were incompatible with modern endpoint protection. This left critical vulnerabilities unpatched and exposed to exploitation.
- ***Outdated Antivirus Protection:*** Antivirus signatures on LFSHK's AD server were approximately one year out of date, which directly undermined their ability to detect and prevent malware such as ransomware.
- ***Inadequate Controls over Remote Access:*** LFSHK did not implement sufficient controls for remote access, such as two-factor authentication, proper access restrictions, device security, and remote device management. These gaps increased the risk of unauthorized access.
- ***Poor Password Management Practices:*** LFSHK staff did not receive effective training regarding password management, nor did LFSHK have effective policies with regards to management of passwords by staff. Additionally, system account credentials were stored in an unencrypted Excel file on the AD server, which created a critical vulnerability that attackers likely exploited to further compromise the network.
- ***Lack of Controls over External Device Security:*** LFSHK did not restrict or monitor the use of USB devices, allowing users to connect external storage devices without oversight. This exposed the firm's network to the risk of malware introduction and propagation.
- ***Insufficient Cybersecurity Awareness Training:*** The last cybersecurity training session had been held in 2018 and focused solely on two-factor authentication for the trading

system. No further training or regular updates were provided, which left staff unprepared for evolving cyber threats.

The SFC further found that LFSHK's recovery was significantly delayed due to deficiencies in its business continuity and data backup arrangements. Daily data backups were stored on an external hard drive that was not consistently disconnected from the network, resulting in the compromise of backup files. LFSHK's business continuity plan was inadequate, having failed to address specific scenarios such as ransomware attacks. Moreover, LFSHK had not established policies for incident management, data security, or record retention.

The SFC found that LFSHK's cybersecurity failures breached requirements under the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (**Code of Conduct**)[2] and the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (**Cybersecurity Guidelines**).[3] In summary, the Code of Conduct requires licensed corporations to exercise due skill, care and diligence, maintain adequate resources and controls, comply with regulatory requirements, ensure the security and resilience of electronic trading systems, and implement appropriate cybersecurity, contingency, staffing and documentation measures. The Cybersecurity Guidelines additionally obligate licensed corporations to maintain secure network infrastructure, robust access and remote-access controls, timely patch management, effective endpoint protection, adequate backup and recovery arrangements, cybersecurity contingency plans, and ongoing staff cybersecurity training.

In determining the sanction, the SFC took into account a number of mitigating factors, including LFSHK's self-report, its co-operation in resolving the SFC's concerns, the reviews it conducted to identify the root causes and extent of its failings (including the appointment of the independent reviewer), the remedial steps taken to prevent recurrence, the absence of evidence of client loss, and its clean disciplinary record.

II. KEY TAKEAWAYS

The LFSHK enforcement action should be viewed against the SFC's broader focus on operational resilience and cyber risk management. The SFC's Cybersecurity Guidelines, supplemented by the Circular on Management of Cybersecurity Risks Associated with Remote Office Arrangements,[4] set out detailed expectations for licensed corporations in areas including network security, access management, patch management, endpoint protection, data backup, and staff training.

More recently, the SFC has intensified its supervisory focus on cybersecurity risk:

- In February 2025, the SFC published its report on the 2023/24 thematic cybersecurity review of licensed corporations, which identified control deficiencies relating to two-factor authentication for system login, security patch management, and the use of end-of-life software and unpatched VPN solutions. The report noted that phishing attacks remain the most common form of cyberattack, with large-scale SMS phishing campaigns targeting clients of internet brokers and VASPs.[5]
- On June 2, 2026, the SFC reminded licensed virtual asset service providers (**VASPs**) and their associated entities to review and strengthen their cybersecurity measures in light of heightened risks posed by artificial intelligence (**AI**)-enabled cyberattacks.[6]

- On July 9, 2026, the SFC issued a further circular to licensed corporations and VASPs to strengthen cybersecurity controls by implementing robust authentication measures and effective monitoring to detect suspicious activities. This includes undertaking phishing-resistant authentication (e.g., passkeys and bound devices), transaction and login monitoring, incident response and reporting procedures, as well as client education on phishing risks.[7]

Viewed in this context, the LFSHK enforcement action is not an isolated response to a ransomware incident, but part of an increasingly proactive strategy by the SFC to drive higher cybersecurity standards across the financial sector that addresses emerging threats, third-party dependencies and sector-wide cyber risk. Licensed corporations should therefore expect continued scrutiny by the SFC of their cybersecurity controls, outsourcing arrangements, incident response capabilities and senior management oversight.

Two further features of this case merit attention. First, the SFC's action came almost four years after the September 2022 attack – a reminder that cyber incidents carry a long enforcement tail, and that incident records, board and committee minutes and vendor correspondence need to be retained and retrievable well beyond ordinary retention periods. That point is sharpened by the SFC's criticism of LFSHK for having established no record retention policy at all. Second, the independent reviewer appointed at the SFC's request both supplied much of the evidential foundation for the SFC's findings. Firms asked to appoint a reviewer following an incident should therefore consider at the outset the reviewer's scope, the basis on which findings will be reported, and the management of privilege, since that output is likely to shape both the regulatory outcome and any follow-on exposure.

The SFC did not pursue any individuals in this case. Firms should not read that as a settled position. The SFC's June 2026 circular cited primary responsibility for cyber resilience with senior management and highlighted the role of the Manager-In-Charge of Information Technology, and we would expect questions of individual accountability to feature in future cases of this kind.

Given this, we recommend that licensed corporations proactively review their cybersecurity frameworks against the SFC's requirements and expectations to identify potential deficiencies which could be the subject of criticism or action by the SFC. In particular, we recommend that firms benchmark their frameworks against each of the eight areas of deficiency identified in the SFC's findings, together with the business continuity and data backup failings described above. Additionally, firms that have not already taken action to comply with the SFC's June 2026 circular on AI-enabled cyberattacks and July 2026 circular on authentication and monitoring should ensure that they take prompt action to do so. This is particularly important given that while the SFC observed that no client losses occurred as a result of the LFSHK cybersecurity attack, the July circular warned that firms may be held accountable for client losses resulting from inadequate measures to prevent, detect or stop large-scale unauthorized transactions following hacking incidents.

[1] *SFC reprimands and fines Luk Fook Securities (HK) Limited $2.1 million for inadequate cybersecurity control to fend off cyberattack*, published by the Securities and Futures Commission on July 28, 2026, accessible at: https://apps.sfc.hk/edistributionWeb/gateway/EN/news-and-

announcements/news/doc?refNo=26PR118.

[2] *Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission*, published by the Securities and Futures Commission in January 2026, accessible at: https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/codes/code-of-conduct-for-persons-licensed-by-or-registered-with-the-securities-and-futures-commission/Code_of_conduct-Dec-2025_Eng-Final-with-Bookmark_Jan-2026.pdf?rev=8768a10c17c44385ab1ad8c0a29d2844.

[3] *Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading*, published by the Securities and Futures Commission on October 27, 2017, accessible at: https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf?rev=eb44681c436548c1bb37092f2145f45c.

[4] *Circular on Management of Cybersecurity Risks Associated with Remote Office Arrangements*, published by the Securities and Futures Commission on April 29, 2020, accessible here.

[5] *Report on the 2023/24 thematic cybersecurity review of licensed corporations*, published by the Securities and Futures Commission in February 2025, accessible at: https://www.sfc.hk/-/media/EN/files/IS/publications/Cybersecurity-thematic-review-report-20250206ENG-Final--Clean.pdf?rev=fb76dfc008ab49c48d3a6d9a937160f2.

[6] *Circular to licensed corporations, SFC-licensed virtual asset service providers and associated entities: Enhanced cybersecurity measures to address evolving risks arising from artificial intelligence-enabled cyberattacks*, published by the Securities and Futures Commission on June 2, 2026, accessible here. See also *Hong Kong Regulators Call for Strengthened Cyber Resilience Against AI-Enabled Cyber Threats*, published by Gibson, Dunn & Crutcher dated June 10, 2026, accessible at: https://www.gibsondunn.com/hong-kong-regulators-call-for-strengthened-cyber-resilience-against-ai-enabled-cyber-threats/.

[7] *Circular to licensed corporations and SFC-licensed virtual asset service providers: Implementing (i) robust authentication methods to reduce and mitigate hacking risks from phishing attacks and (ii) adequate monitoring and surveillance measures to identify suspicious activities*, published by the Securities and Futures Commission on July 9, 2026, accessible here.

The following Gibson Dunn lawyers prepared this update: William Hallatt, Emily Rumble, and Jane Lu.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. If you wish to discuss any of the matters set out above, please contact any member of Gibson Dunn's Financial Regulatory team, including the following members in Hong Kong:

William R. Hallatt (+852 2214 3836, whallatt@gibsondunn.com)

Emily Rumble (+852 2214 3839, erumble@gibsondunn.com)

Arnold Pun (+852 2214 3838, apun@gibsondunn.com)

Becky Chung (+852 2214 3837, bchung@gibsondunn.com)

Jane Lu (+852 2214 3735, jlu@gibsondunn.com)

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm, please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists, please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit our website.