紀律行動聲明

紀律行動

1. 證券及期貨事務監察委員會（**證監會**）依據《證券及期貨條例》（**該條例**）第194條，公開譴責六福證券（香港）有限公司（**六福證券**）[1]並處以罰款210萬港元。

2. 本會採取上述紀律行動，是因為六福證券沒有實施足夠及有效的網絡保安監控措施，從而可能導致六福證券無法抵禦2022年9月19日的勒索軟件攻擊，並令其系統從該攻擊中恢復的時間延誤約三星期，違反了：

   (a) 《證券及期貨事務監察委員會持牌人或註冊人操守準則》（**《操守準則》**）第2項一般原則（勤勉盡責）、第3項一般原則（能力）、第7項一般原則（遵守法規）、第12.1段（合規事宜：概論）、第18.5段（系統的充足性）和附表7（對就進行電子交易的持牌人或註冊人的額外規定）第1.1.4、1.2.4(a)、1.2.4(b)、1.2.4(c)、1.2.4(d)、1.2.6(b)、1.2.7及1.2.8(a)段；及

   (b) 《降低及紓減與互聯網交易相關的黑客入侵風險指引》（**《網絡保安指引》**）第2.1段（配置安全的網絡基礎設施）、第2.2段（使用者接達管理）、第2.3段（遙距連接的保安監控措施）、第2.4段（修補管理）、第2.5段（端點保護）、第2.6段（在未經授權的情況下安裝硬件及軟件）、第2.8段（系統及數據備份）、第2.9段（網絡保安情境的應變計劃）及第3.3段（網絡保安意識培訓）。

3. 該等條文整體上要求持牌法團維持穩健的網絡保安框架，包括安全的網絡基礎設施，有效的接達監控措施，定期的系統更新和修補管理，端點保護，全面的業務延續和應變計劃，及時的事故報告，持續的職員培訓，以及安全的資料管理。

4. 於2020年4月29日發出的《致持牌法團的通函：與遙距工作安排相關的網絡保安風險管理》，亦已闡明部分與遙距接達及工作安排相關的風險，並載有關於用以紓減該等風險的監控措施及程序的建議。

事實摘要

5. 2022年9月19日，六福證券向證監會主動報告其系統於同日遭勒索軟件攻擊（**該事故**）。作出報告後，六福證券委聘了外部顧問就該事故提供意見及進行調查。此外，六福證券應證監會的要求委任了獨立檢討機構，對該事故進行獨立評估，並就其本身與網絡保安相關的內部監控措施及補救行動進行監管檢討，而在檢討完成後，證監會就六福證券的行為展開進一步調查（統稱**該等調查**）。

6. 該等調查發現：

   (a) 在2019冠狀病毒病疫情期間，六福證券為僱員實施遙距工作安排。為配合此安排，該公司建立了一個運行Windows 7的VMware[2]虛擬化環境，作為職員遙距接達其

[1] 六福證券根據該條例獲發牌進行第 1 類（證券交易）、第 4 類（就證券提供意見）及第 9 類（提供資產管理）受規管活動。

辦公室工作站的跳板機。第三方供應商及資訊科技部門亦會接達此環境，以提供遙距系統支援。

(b) 2022年9月19日，一名黑客相當可能透過暫存的遙距桌面捷徑，利用對VMware環境的遙距接達進入Active Directory（**AD**）伺服器。該攻擊干擾了六福證券的關鍵資訊科技基礎設施，包括檔案伺服器、網域控制器、電郵伺服器、交易應用程式伺服器及會計伺服器。六福證券分階段恢復其系統，而有關過程直至2022年10月7日，即約三星期後才完成。

(c) 在此期間，六福證券的客戶無法透過流動交易應用程式或互聯網平台進行交易，只可透過客戶主任發出交易指示。六福證券於2022年9月19日透過短訊及其網站將該事故通知客戶。

(d) 並無證據顯示該事故導致客戶資產被挪用、未經授權交易、客戶財務損失，或客戶資料外洩。六福證券沒有收到任何客戶投訴。

7. 該等調查進一步發現，該事故可能歸因於六福證券網絡保安系統的多項缺失，概述如下：

(a) **網絡保安監控措施不足**：六福證券的多個網絡裝置及設備均缺乏防火牆保護，亦未受安全性資訊與事件管理（Security Information and Event Management，簡稱SIEM）工具監控。這使網絡面臨外部威脅，並讓攻擊者能夠直接從互聯網接達內部系統。

(b) **使用者接達及特權帳戶的管理不足**：六福證券沒有就使用者接達及特權帳戶制訂有效的監控措施。第三方供應商及職員的憑證被暫存於遙距支援系統中，增加了網絡遭入侵和在網絡內橫向移動的風險。

(c) **使用不受支援的舊有系統**：受感染的VMware環境運行過時的作業系統（微軟Windows 2008及Windows 7），該等系統已不再接收保安更新，且與現代端點保護不相容。這導致重大漏洞未獲修補，並面臨遭利用的風險。

(d) **過時的防毒保護**：AD伺服器上的防毒特徵碼已過時約一年，削弱了偵測和預防勒索軟件等惡意軟件的能力。

(e) **對遙距接達的監控措施不足**：六福證券沒有就遙距接達實施足夠的監控措施，包括強認證（例如雙重認證）、適當的接達限制、裝置保安及遙距裝置管理。這些不足之處增加了未經授權接達、數據外洩及延遲偵測事故的風險。

(f) **密碼管理手法欠佳**：六福證券並無有效的密碼管理政策或培訓。系統帳戶憑證儲存於AD伺服器上未加密的Excel檔案中，造成了重大漏洞，攻擊者相當可能曾利用該漏洞進一步入侵網絡。

(g) **欠缺對外置裝置保安的監控措施**：六福證券沒有限制或監控USB裝置的使用，令使用者可在缺乏監察下連接外置儲存裝置。這使網絡面臨惡意軟件植入及傳播的

[2] VMware 是一個較舊的系統環境，主要供外部系統供應商在進行維護時使用，以及用來讓少數內部使用者接達交易系統。 雖然兩組使用者均在同一個 VMware 環境內運作，但其接達權僅限於獨立的區域。系統供應商可接達控制面板，而內部使用者則只能接達交易系統。

風險。

(h) **網絡保安意識培訓不足**：上一次網絡保安培訓課程於2018年舉行，且只聚焦於交易系統的雙重認證。其後並無提供進一步培訓或定期更新，令職員未能為不斷演變的網絡威脅作好準備。

8. 此外，六福證券的網絡保安安排存在其他缺失，導致該公司從該攻擊中恢復的時間大幅延誤，歷時約三星期：

(a) 在該事故發生時，每日數據備份乃儲存於外置硬碟中，而該硬碟並非一直與網絡斷開連接。結果，備份檔案在該攻擊期間遭受破壞，令數據恢復受阻。

(b) 六福證券的業務延續計劃不足，因為它未能應對勒索軟件攻擊及數據遺失等特定情境，且沒有定期檢討或更新。

(c) 在該事故發生後及整個恢復期間，六福證券仍未制訂應對主要網絡保安風險範疇（例如事故管理、數據保安和紀錄保存）的政策及程序。

9. 這些系統性缺失顯示六福證券未能符合多個監管框架所規定的基本網絡保安要求，亦是導致該公司無法抵禦該事故及其影響如此嚴重的主因。

結論

10. 基於上述事項，證監會發現六福證券沒有：

(a) 全面遵守上文第 2 段所提述《操守準則》及《網絡保安指引》下的網絡保安規定，原因是它沒有實施足夠及有效的網絡保安監控措施。這些缺失可能是促致六福證券無法抵禦勒索軟件攻擊的成因，並令其恢復出現延誤；及

(b) 以適當的技能和小心審慎的態度行事，亦沒有實施足夠及有效的系統及監控措施，以確保遵守上述網絡保安規定，違反了《操守準則》第 2 項一般原則[3]、第 3 項一般原則[4]、第 7 項一般原則及第 12.1 段[5]。

11. 證監會認為六福證券犯有失當行為。

12. 證監會在決定採取上文第 1 段所述的紀律處分時，已考慮到所有相關情況，包括：

(a) 六福證券已進行檢討，以識別其缺失的根本原因及範圍，包括應證監會的要求委任獨立檢討機構，對該事故及其與網絡保安相關的內部監控措施進行獨立評估；

(b) 六福證券已採取措施改善其系統及監控措施，以防止日後發生違規行為；

(c) 並無證據顯示六福證券的客戶因該公司的缺失而蒙受任何損失；

---

[3] 《操守準則》第 2 項一般原則規定，持牌人在經營業務時，應以適當的技能、小心審慎和勤勉盡責的態度行事，以維護客戶的最佳利益及確保市場廉潔穩健。

[4] 《操守準則》第 3 項一般原則規定，持牌人應具備及有效地運用其所需的資源和程序，以便適當地進行其業務活動。

[5] 《操守準則》第 7 項一般原則及第 12.1 段規定，持牌人應遵守、實施及維持適當的措施，以確保相關監管規定獲得遵守。

(d) 六福證券在解決證監會提出的關注事項時表現合作；及

(e) 六福證券過往並無遭受紀律處分的紀錄。