SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

2020 年 9 月 23 日

致持牌法團的通函

互聯網交易網絡保安檢視

證券及期貨事務監察委員會（證監會）最近對透過桌面電腦、流動裝置及指定交易網站平台提供網上交易服務的選定互聯網經紀行[1]進行了一項主題檢視[2]，重點關注與流動交易應用程式有關的網絡保安問題及漏洞。證監會對 55 家互聯網經紀行進行調查，並對其中 10 家進行實地視察。是次檢視發現，大部分經紀行均遵守證監會的主要監管規定。

今天發表的主題檢視報告撮述了主要發現和觀察所得，及就本會的預期標準提供指引，並重點闡述在例如以下範疇的不足之處，及沒有遵守相關規定的情況：雙重認證、數據加密、網頁超時，及為識別可疑的未經授權交易而進行的監察和監督。該報告亦載有關於其他規定的提示及這些經紀行所採納的良好作業方式。

連同以上所述，本通函闡述了在 2018 年 7 月生效的《降低及紓減與互聯網交易相關的黑客入侵風險指引》[3]（《網絡保安指引》）所載的監管要求。此外，由於《網絡保安指引》沒有涵蓋流動交易應用程式所獨有的某些漏洞，故本通函亦就互聯網經紀行根據《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》）的規定，應為流動交易應用程式而採取的特定系統保安監控措施，提供指引。

A. 系統登入適用的雙重認證

根據《網絡保安指引》第 1.1 段，互聯網經紀行應就客戶的互聯網交易帳戶的登入程序實施雙重認證，而雙重認證意指使用以下任何兩項元素的認證機制：客戶所知的、客戶所有的及客戶是誰。

實際上，就“客戶所知的”而言，互聯網經紀行通常採用使用者名稱及密碼。就“客戶所有的”而言，互聯網經紀行一般透過不同方法向客戶提供一次性密碼，或在其互聯網交易系統內綁定或註冊客戶的裝置，以使有關裝置被辨識為屬該客戶所有。“客戶是誰”通常是利用生物特徵認證，這是將客戶的指紋或人臉識別數據與儲存在其流動裝置的資料進行比對的程序。

證監會的主題檢視識別出多個監控不足之處及沒有遵守有關規定的情況，例如：

[1] 在香港從事互聯網交易業務的持牌法團。

[2] 是次檢視主要涵蓋選定的互聯網經紀行的系統監控措施和相關管理監控措施，以評估這些持牌法團有否遵守《網絡保安指引》所載的 20 項基本規定及《操守準則》所載的其他相關的一般網絡保安規定。

[3] 《網絡保安指引》的規定以原則為本，互聯網經紀行可自由選擇實施哪些監控措施和舉措，前提是這些監控措施和舉措就其架構、業務運作及需要而言是足夠、有效及相稱的。

- 經電郵傳送一次性密碼作為第二認證元素的做法並不可靠[4]；
- 容許客戶解除系統登入的雙重認證功能；及
- 與綁定客戶裝置有關的問題，例如技術性保安漏洞，或容許客戶綁定過多裝置。

為處理上述不足之處，互聯網經紀行：

(i) 不應經電郵傳送一次性密碼；

(ii) 不應容許客戶解除系統登入的雙重認證功能；

(iii) 應定期進行技術評估，以識別保安漏洞；

(iv) 不應容許客戶就其互聯網交易帳戶綁定或註冊過多裝置，及應就並行登入（concurrent login）實施監控措施，例如：

- 了解個人客戶要求綁定或註冊超過三個裝置的原因，及評估有關要求是否合理；
- 若公司客戶要求綁定或註冊多個裝置，以便獲其授權的人士可操作這些裝置，則互聯網經紀行應提議該公司客戶開立子帳戶（各自具有獨立的雙重認證）；及
- 若子帳戶的安排並不可行，應將並行登入的數量限制在獲授權操作公司客戶的互聯網交易帳戶的人數之內。

B. 偵測未經授權的接達的監察及監督機制

根據《網絡保安指引》第1.2段，互聯網經紀行應實施有效的監察及監督機制，以偵測未經授權而接達客戶的互聯網交易帳戶的情況。

我們在主題檢視期間，注意到多個不足之處，可能因而導致未能及時偵測涉嫌未經授權的交易及延誤跟進。

這些不足之處包括：

- 某些大型互聯網經紀行只對客戶交易進行人手檢視；
- 只不定期、按周或按月進行監察及監督；及
- 自動化互聯網協定（internet protocol，簡稱 IP）位址監察工具的設計有缺陷，例如錯誤地將同一個通用的 IP 位址分配給來自不同的流動電話或網絡使用者的所有登入嘗試。

[4] 這是因為基於以下因素，使用經電郵傳送的一次性密碼來登入的人不一定是實際的客戶：經電郵傳送的一次性密碼： (a)可被發送至多部裝置，例如同時發送至流動電話及電腦，以及可被每個這些裝置上的多個應用程式取用或讀取；及(b)可能未必由客戶本人讀取，原因是客戶電郵帳戶的登入資料可由多人共用。 此外，電郵帳戶的安全保障不足，例如電郵的轉寄功能可導致不慎將一次性密碼與他人分享。

為處理上述不足之處，互聯網經紀行應：

(i) 顧及其互聯網交易業務的規模，並實施就其業務需要而言屬適當和相稱的監察及監督機制；

(ii) 至少每天進行監察及監督；及

(iii) 在實施自動化的 IP 位址監察工具前進行充分的技術測試和使用者測試。

C. 數據加密

根據《網絡保安指引》第1.4段，互聯網經紀行應就數據傳輸及儲存實施強效的加密程式。

我們在主題檢視期間，注意到某些公司沒有充分地加密和保護客戶登入資料、密碼和交易數據，因為它們所實施的加密程式並不符合國際保安標準（例如美國國家標準與技術研究所（National Institute of Standards and Technology）提供的加密標準）。

互聯網經紀行應持續檢視國際保安標準，查核其數據加密程式的狀況，及在適當時將其升級。

D. 網頁超時

根據《網絡保安指引》第1.6段，互聯網經紀行應設立嚴格的監控措施，以確保網頁在閒置一段時間後被設定為已超時。

我們在主題檢視期間，注意到網頁超時監控功能可被客戶關掉或網頁超時的時限過長，其閒置時限可長達24小時。

為處理上述不足之處，互聯網經紀行應：

(i) 不容許其客戶關閉網頁超時監控功能；

(ii) 限制閒置超時時限（例如在 30 分鐘以內），但須事先作出評估及持續進行監察。舉例來說，進行程式買賣的客戶可能需要交易帳戶處於備用狀態以便隨時執行交易。在此情況下，可容許較長的閒置超時時限，但互聯網經紀行必須更緊密地監察該客戶的登入和登出紀錄及交易活動；及

(iii) 進行充分的測試，以確保網頁超時監控措施妥為設定及運作。

E. 安全的網絡基礎設施

根據《網絡保安指引》第2.1段，互聯網經紀行應透過妥善的網絡隔離措施（即設有多重防火牆的隔離區）來配置安全的網絡基礎設施。

我們在主題檢視中注意到，有欠妥善的網絡隔離措施，令網絡基礎設施的安全受損，例如將互聯網交易應用程式和其他關鍵系統設置於隔離區內而非隔離區後。

為處理上述不足之處，互聯網經紀行應：

(i) 將互聯網交易應用程式和其他關鍵系統設置於隔離區後的可靠內部網絡內；及

(ii) 將儲存敏感度較低的數據的伺服器（例如寄存公司網頁的網絡伺服器）寄存於隔離區內。

F. 遙距連接的保安監控措施

根據《網絡保安指引》第2.3段，互聯網經紀行應只容許有需要的人士遙距接達其內部網絡，並對遙距接達實施保安監控措施。

我們在主題檢視期間，注意到某些供應商獲授予隨時適用的永久的遙距接達權，因而增加了網絡保安風險。

為處理上述不足之處，互聯網經紀行應避免向外界人士授出永久的遙距接達權。

G. 修補管理

根據《網絡保安指引》第2.4段，互聯網經紀行應及時監察和評估軟件提供者發布的保安修補程式或修正程式，並視乎評估結果，在切實可行的情況下盡快進行測試，並在測試完成後一個月內執行該等程式。

我們在主題檢視期間，注意到在監控方面存在不足之處，可能會令關鍵的保安修補及修正程式被延誤執行。這些不足之處包括：

- 花了超過六個月來執行保安修補程式及修正程式，即使是被列為關鍵或極度嚴重的保安修補程式及修正程式亦然；
- 只每隔六個月分批進行修補管理；及
- 採用使用期完結的軟件[5]。供應商不再為使用期完結的軟件提供保安修正程式服務，導致被暴露出來的網絡及系統漏洞可能遭到黑客利用。

為處理上述不足之處，互聯網經紀行應：

(i) 盡快識別及執行急需的保安修補程式或修正程式；

(ii) 只批量執行非關鍵的保安修補程式或修正程式，及至少每季批量執行一次這些程式，除非經評估後斷定該等程式可能與系統應用程式不相容，故無法執行；及

[5] 指的是使用期已告結束，並且供應商已停止就其提供支援的軟件（例如 Windows 伺服器 2008）。

(iii) 持續和及時監察現有軟件的有效性，並將使用期完結或接近完結的軟件予以替換或升級，藉以確保其使用的軟件獲供應商支援。

H. 網絡保安管理及監督

根據《網絡保安指引》第3.1段，負責互聯網交易的負責人員應設定網絡保安風險管理框架及列明主要責任，例如定期安排就有關框架進行自我評估。

我們在主題檢視中注意到，許多公司沒有在其資訊科技審計或自我評估中充分涵蓋有關的基本規定。

為處理上述不足之處，互聯網經紀行應至少每年在其資訊科技稽核或網絡保安評估中檢視其遵守基本規定的情況。

I. 流動交易應用程式

在十家提供流動交易應用程式的被視察公司中，許多都未能符合《操守準則》附表7第1.2.4段所載有關保安監控措施的規定。尤其是：

- 六家公司未能偵測並阻止被破解的裝置登入其互聯網交易系統；
- 五家公司沒有充分地保護其原始碼，使黑客得以繞過內置的保安監控程式；
- 三家公司的流動交易應用程式中存在沒有使用的程式碼庫或模組，增加了黑客安裝惡意軟件的風險；
- 六家公司容許客戶的敏感資料儲存在流動裝置內，及有關資料不會在登出後從系統進程記憶體中被刪除，從而增加了有關資料被黑客存取的風險；及
- 一家公司容許在沒有妥善驗證的情況下，修改儲存在客戶流動裝置內有關該客戶的生物特徵數據，及沒有在多次登入嘗試失敗後停用生物特徵認證。

為處理上述不足之處，互聯網經紀行應：

(i) 偵測及阻止被破解的流動裝置登入其互聯網交易系統；

(ii) 模糊其原始碼以加強保護，避免其遭惡意利用；

(iii) 將沒有使用的程式碼庫或模組從其原始碼中清除；

(iv) 在客戶一旦離開安裝於其流動裝置的互聯網交易應用程式或登出其互聯網交易帳戶後，便將客戶敏感資料從有關程式中清除；及

(v) 收緊生物特徵認證的保安監控措施，例如規定客戶生物特徵數據的任何改變須接受核實檢查，及限制認證失敗的次數。

雖然在基本規定於 2018 年 7 月生效後並無任何客戶帳戶遭黑客入侵的報告，互聯網經紀行仍需：

- 注意上述指引；
- 充分了解現行規定；及
- 嚴格檢視其理應與業務模式相稱的系統及監控措施，並按需要加以糾正或改善。

鑑於本通函主題事項的技術性質，互聯網經紀行應按需要向其供應商及其他顧問尋求專業協助。

如對本通函的內容有任何疑問，請聯絡你的個案主任。

證券及期貨事務監察委員會
中介機構部
中介機構監察科

連附件

完

SFO/IS/033/2020