互聯網交易網路保安檢視

證券及期貨事務監察委員會（「**證監會**」）已發佈報告及於2020年9月23日發出通函（「**該通函**」），詳細闡述2018年7月生效的《降低及紓減與互聯網交易相關的駭客入侵風險指引》中規定的監管要求。本注釋概述了上述關於互聯網經紀行應為流動交易應用程式採用的特定系統保安監控措施的事實調查結果及指引。

系統登入適用的雙重認證

不足之處	證監會提出的措施
• 容許客戶解除系統登入的雙重認證功能 • 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 • 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	• 不應容許客戶解除系統登入的雙重認證功能 • 不應經電郵傳送一次性密碼 • 應定期進行技術評估，以識別保安漏洞 • 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

偵測未經授權接達的監察及監督機制

不足之處	證監會提出的措施
• 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 • 自動化互聯網協定（internet protocol，簡稱IP）地址監察工具的設計有缺陷	• 應顧及互聯網交易業務的規模，並實施就業務需要而言屬適當及相稱的監察及監督機制 • 應至少每天進行監察及監督 • 應在實施自動化的IP位址監察工具前進行充分的技術測試及使用者測試

資料加密

不足之處	證監會提出的措施
某些公司沒有充分地加密及保護客戶登入資料、密碼及交易資料，因為它們所實施的加密程式並不符合國際保安標準	互聯網經紀行應持續檢視國際保安標準，查核其資料加密程式的狀況，及在適當時將其升級

網頁超時

不足之處	證監會提出的措施
• 網頁超時監控功能可被客戶關掉 • 網頁超時的時限可長達24小時	• 不應容許客戶關閉網頁超時監控功能 • 互聯網經紀行應限制閒置超時時限（例如在30分鐘以內），但須事先作出評估及持續進行監察 • 互聯網經紀行應進行充分的測試，以確保網頁超時監控措施妥為設定及運作

遙距連接的保安監控措施

不足之處	證監會提出的措施
某些供應商獲授予隨時適用的永久的遙距接達權，因而增加了網路保安風險。	互聯網經紀行應避免向外界人士授出永久的遙距接達權

網路保安管理及監督

不足之處	證監會提出的措施
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	互聯網經紀行應至少每年在其資訊科技稽核或網路保安評估中檢視其遵守基本規定的情況

流動交易應用程式

不足之處	證監會提出的措施
• 未能偵測並阻止被破解的裝置登入互聯網交易系統 • 沒有充分地保護原始碼，使駭客得以繞過內置的保安監控程序 • 流動交易應用程式中存在沒有使用的程式碼庫或模組，增加了駭客安裝惡意軟體的風險 • 容許客戶的敏感性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駭客存取的風險 • 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資料，及沒有在多次登入嘗試失敗後停用生物特徵認證	• 應偵測及阻止被破解的流動裝置登入互聯網交易系統 • 應模糊原始碼以加強保護，避免其遭惡意利用 • 應將沒有使用的程式碼庫或模組從原始碼中清除 • 應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，便將客戶敏感性資料從有關程式中清除 • 互聯網經紀行應收緊生物特徵認證的保安監控措施，例如：- o 規定客戶生物特徵資料的任何改變須接受核實檢查；及 o 限制認證失敗的次數

鑒於該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。

如有進一步諮詢，請聯絡本律師行楊元建律師（電話：(852) 2854 3070 或 電郵：lawrence.yeung@ycylawyers.com.hk）。

本注釋並非也不應被視為法律意見。如有任何疑問，請就具體個案諮詢法律顧問。

2021年2月24日