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

2022 年 3 月 24 日

致持牌法團的通函

管理商業電郵騙案的風險

證券及期貨事務監察委員會（證監會）最近接獲持牌法團有關商業電郵騙案的匯報。商業電郵騙案屬網絡欺詐，騙徒會冒充持牌法團所認識的業務聯繫人，欺騙不虞有詐的員工向他們發送金錢或敏感資料。這些事件導致客戶資料外洩，不但損害了客戶的利益，在某些情況下更令持牌法團蒙受重大的財政損失。

商業電郵騙案

商業電郵騙案的計劃通常涉及騙徒採取以下的一種或多種手法[1]：

- 偽造一個與真正客戶聯繫人相似的電郵地址以便與目標持牌法團溝通[2]；
- 冒充客戶聯繫人並提出看似合理的要求，例如索取帳戶結單的副本、增加或更改授權簽署人、申請開設用戶帳戶或發出交易指令；及
- 發出資金轉移的指示，通常是轉帳至騙徒在多家收款銀行（有些位於海外）所操控的銀行帳戶，以盡量提高他們收到款項的機會。

在騙徒成功得手的大多個案中，電郵發件人的身分不是未經核實，就是未獲適切檢查。舉例來說，持牌法團的員工只是致電騙徒所提供的電話號碼，從而獲得確認並處理其資金轉移的指示。

此外，持牌法團忽略了很多預警跡象。在一宗事件中，某些銀行拒絕或不受理多筆資金轉移。該持牌法團沒有立即調查有關不合常規的情況，反而繼續按照騙徒指示將資金轉移至其他銀行。最終，銀行執行了多筆資金轉移，令該持牌法團蒙受財政損失。

持牌法團應注意附件中有關商業電郵騙案的例子。

證監會的期望

證監會期望持牌法團應設有妥善的內部監控程序、財務資源及操作能力，而按照合理的預期，這些程序及能力足以保障其運作及客戶，以免受偷竊、欺詐及不誠實的行為、專業上的失當行為或不作為而招致財政損失[3]。持牌法團應嚴密地監控及有效地管理商業電郵騙案的風險，尤其是在遙距工作安排已成為常態的情況下[4]。

---

[1] 除了冒充客戶外，騙徒亦可能會冒充賣方或供應商等其他業務聯繫人，以要求付款。

[2] 偽造的電郵地址可能具有相似的域名（例如，xyzz.com 而非 xyz.com），或具有相同的域名，但用戶名稱略有不同（例如，abcc@xyz.com 而非 abc@xyz.com）。

[3] 《證券及期貨事務監察委員會持牌人或註冊人操守準則》第 4.3 段。

[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》。

監控機制

持牌法團應制訂有效的政策和程序，就管理商業電郵騙案的風險向員工提供指引。此外，持牌法團應在以下方面加強內部監控措施：

客戶聯絡資料

- 在開戶過程中確定客戶及其授權代表的真實身分。
- 定期審查和更新正式的紀錄，確保客戶的聯絡資料是準確及最新的。

更改客戶資料

- 當客戶要求更改其資料（包括更新授權代表資料）時，應要求客戶以書面方式發出指示[5]，並核實要求者的身分及簽名式樣。
- 使用持牌法團的正式紀錄內的聯絡資料來核實電郵要求，而不是透過該電郵地址或使用其提供的電話號碼來核實。在有需要的情況下，考慮安排與客戶進行視像會議或直接會面。
- 在接獲更改的要求時及在作出有關更改後，將確認通知發送到客戶的登記地址、電子郵箱或流動電話。

就交易指令及資金轉移發出的電郵要求

- 就金額超過合理門檻的要求實施有效的確認程序。
- 使用其他途徑及持牌法團原有紀錄來聯絡客戶及核實其要求，而不是直接回覆電郵要求。
- 考慮使用監測工具，以過濾偽造的電郵地址，及偵測未經授權而接達內部網絡和系統的情況。

預警跡象

- 若電郵要求有別於客戶的慣常做法，應保持警惕，並格外小心處理。如有不合常規的情況（例如，向海外銀行帳戶支付大筆款項，即時付款的要求及銀行多次拒絕轉帳），應立即跟進。
- 建立良好的風險文化，鼓勵員工匯報及跟進預警跡象。適時地讓主管、資訊科技管理人員及合規人員參與制訂適當的對策，以處理可疑的電郵指示。

[5] 《提高商號遵守〈證券及期貨（客戶證券）規則〉及〈證券及期貨（客戶款項）規則〉的能力的建議監控措施及程序》第 3(b)段。

高級管理層的責任

請注意，上述的監控措施及技術，並非鉅細無遺。證監會建議各持牌法團應檢視本身的情況，確保設立適當且有效的內部監控程序，以及有效地付諸實行。高級管理層有責任監察持牌法團實施內部監控政策和程序的情況，以有效地管理商業電郵騙案的風險，以及確保為有關監控職能分配足夠資源及實施適當的制衡措施。

持牌法團應定期向員工提供培訓，以提高他們對提防電郵騙案的警覺性，並確保他們了解適當的處理程序。持牌法團的員工應根據內部規程仔細地檢查電郵地址，審慎地查核有關要求的真實性，勤勉盡責地對預警跡象進行調查，並及時上報有關問題。

持牌法團亦應參考證監會就管理網絡安全風險[6]及防範電郵騙案[7]的監控措施及技術而發出的指引。

如對本通函內容有任何疑問，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

完

SFO/IS/019/2022

[6] 於 2017 年 10 月 27 日發出的《降低及紓減與互聯網交易相關的黑客入侵風險指引》。
[7] 於 2012 年 9 月 7 日發出的《致全體中介人的通函—小心“電郵騙案”》。