

從舉報的挪用資產個案中發現的預警跡象及監控缺失

本附錄列舉一些由持牌法團匯報或投訴人舉報的挪用資產個案的例子，當中的涉事持牌法團忽視了多項預警跡象及監控缺失。持牌法團務必以這些個案為鑑，提高防範意識，避免客戶帳戶遭受欺詐及內部失當行為的威脅。

1. 某些騙徒使用偽冒或盜取的電郵地址來冒充持牌法團的客戶發出指示。
 - (a) 一名騙徒利用與客戶的電郵地址（contact@domain.com）甚為相似的偽冒電郵地址（contact@domainn.com）向一家持牌法團發電郵指示，要求將自己添加為獲授權人以管理該客戶帳戶。該持牌法團沒有識別出該欺詐電郵地址，遂批准了有關要求。騙徒其後使用偽冒電郵地址向該持牌法團發送電郵，指示該持牌法團向由騙徒安排的第三者支付巨款。
 - (b) 一名騙徒在入侵客戶的電郵帳戶後，向一家持牌法團發送電郵要求提取資金。騙徒要求該持牌法團，將該客戶的大量資金轉移至聲稱以該客戶名義開立但由騙徒控制的非指定海外銀行帳戶。該持牌法團沒有按其內部政策的規定，直接向客戶確認及取得客戶更改指定銀行帳戶的書面指示，便執行了有關提款要求。
2. 某些騙徒偽冒客戶的簽名並透過郵寄、電郵或傳真方式向持牌法團發出偽冒的書面指示。
 - (a) 一家持牌法團接獲偽冒的書面指示，要求更改一名客戶用以收取戶口結單的電郵地址，並以實物股票形式提取該客戶價值不菲的證券，再由騙徒安排的第三者領取有關證券。該持牌法團沒有致電客戶核實指示，便批准了有關要求。
 - (b) 一家持牌法團接獲偽冒的書面指示，要求更改一名客戶的所有聯絡資料，包括其流動電話號碼、電郵地址及住址。這些改動使該客戶無法收取戶口結單。騙徒其後要求該持牌法團，將該客戶的全部資金轉移至聲稱以該客戶名義開立但由騙徒操控的非指定銀行帳戶。該銀行所處的國家，並非該客戶的居住或工作地點。
 - (c) 一家持牌法團接獲偽冒的書面指示，要求更改一名客戶的流動電話號碼及電郵地址。該持牌法團的政策規定，其交收部職員須在作出改動前致電客戶以確認有關更改資料的要求，但有關交收部職員卻致電了由騙徒提供的新流動電話號碼進行確認。騙徒在更改這些客戶資料後，得以重設及獲取新一組登入密碼，以登入該客戶的網上交易帳戶進行未經授權的交易。
3. 持牌法團在銀行帳戶的操作方面出現監控缺失，以致被不誠實的職員加以利用。
 - (a) 一家持牌法團的會計職員在該持牌法團的網上銀行平台，獲指配“輸入”及“批准”職能，以致他能夠獨自執行付款操作，並在其他人員不知情的情況下，將該持牌法團的公司資金轉移至其銀行帳戶。

- (b) 一家持牌法團的兩名負責人員獲授權共同為該持牌法團的公司及客戶銀行帳戶執行網上銀行付款。然而，他們沒有妥善保管相關登入資料（即登入名稱和密碼）及保安編碼器。一名職員盜取了這些登入資料及編碼器，並將大量資金從該持牌法團的公司及客戶銀行帳戶轉移至其銀行帳戶，隨後不知所終。

總結教訓

4. 持牌法團在處理客戶指示時，應勤勉盡責地核實指示，以確保指示由真正的客戶發出。持牌法團亦應保持警惕，留意是否有任何偏離客戶慣常做法的指示，例如一名客戶通常在網上發出指示，卻突然選擇以郵遞的方式發出書面指示。
5. 持牌法團應提高職員在處理客戶指示時對上述預警跡象及監控缺失的警覺性。持牌法團亦應加強其內部政策及程序，並規定職員在處理有關更改客戶資料、提取或轉移客戶資產，以及涉及第三者或並非由客戶指定的銀行帳戶的交易的要求時，須嚴格遵守有關政策及程序。負責的職員如有疑問，應直接向客戶核實指示。
6. 為防範內部欺詐行為，持牌法團應就包括網上銀行在內的主要操作，實施妥善的輸入與核對的分工監控措施。用戶的登入資料及保安編碼器亦應妥善地保管，以確保可就已進行的交易問責及偵測未經授權的交易。
7. 有關持牌法團就上述範疇應達到的監管標準的詳情，請參閱附錄2。