UK P&I CLUB

L P Bulletin

2016 年 9 月 28 日 星期三

防損公告 1112 號——09/16 ——網路詐騙——全球

2014年12月，協會調查部門Signum Services針對“發票造假”發佈了防損意見（2014年12月16日防損公告1014號）。鑒於此類犯罪屢禁不止，有必要提醒會員應格外謹慎。建議會員要求其會計部門謹防詐騙。

上述詐騙或稱“授權詐騙”或“釣魚付款詐騙”。雖然所稱不同，但手法基本一致。

通常，詐騙犯會攻入進受害者的電郵網路，這些電郵在近期曾發出付款要求。原始郵件發出後不久，詐騙犯會回復郵件，冒充原始郵件的寄件者。詐騙方完全複製受害者郵件的格式，僅對信頭稍作改動，經常是只修改一個字母。

這封新郵件聲稱原來的付款帳號有問題，要求受害者向該帳號的子帳戶付款，該帳戶其實是詐騙犯事先開立的帳戶。在個別案件中，詐騙犯甚至運用Photoshop軟體對郵件隨附發票的銀行資訊進行改動。

之後，受害者付款，但幾天後才發現交易有詐。不幸的是，屆時詐騙犯已經通過一系列銀行轉帳轉走詐騙款，無法追回。

讓受害者迷惘的是，在這個號稱安全有保障的現代銀行業務的時代，詐騙犯竟然可以在另一個國家開立銀行帳戶，而且會有資金轉入。

詐騙犯可利用幾種方式開立帳戶，“地下網路”相關資訊應有盡有，詐騙犯可從中得到協助。有組織的犯罪集團時常會收買銀行職員，以便利用虛假身份開設銀行帳戶。即使有些銀行行員盡忠職守，因為無從著手，他們也無法核查外國戶主的身份。舉例來說，一名英國銀行職員可以識別虛假的英國護照，卻可能無法辨別羅馬利亞護照的真偽。

此類詐騙一般容易得手，因為詐騙犯無需辦理開設銀行帳戶的手續。詐騙犯可輕易取得或偽造帳單等單據，攔截郵件單據等。一旦獲得足夠受害者的個人身份和財務資訊，詐騙犯便能接管受害者的銀行帳戶或冒充受害人。詐騙犯會通過銀行分行或呼叫中心破解受害者的網上安全資訊，登陸其銀行帳戶，或通過團夥作案或安插人員進入受害者的所在銀行，控制其帳戶。

通過“國際銀行帳戶號碼”（IBAN）進行的交易是自動交易。由於銀行每天需要處理大量付款業務，將匯款轉入指定帳戶前，銀行無法核查每項交易中匯款人指定的收款人的名稱是否與該收款人帳號持有人的姓名一致。只要匯款人提供的收款人銀行代碼正確，匯款將自動記入收款人賬上，除非收款人帳戶被凍結。如果收款人帳戶凍結，匯款將自動退回。

詐騙犯通常跨越多個司法管轄區跨國作案，以致國家執法機關打擊此類詐騙屢屢受阻，受害人想要追回被騙款項極其困難。

鑒於以上，建議會員提高防範意識，避免受騙。協會建議，無論在何種情況下，一旦收到可疑的付款要求，應重複核查該請求的真實性，最好是親自向對方經手人核實情況，但前提是應確保該經手人的真實身份不是詐騙犯。

隨附 TT Club 近期發佈的相關文章，有興趣的會員可點擊閱讀：
http://www.ttclub.com/loss-prevention/tt-talk/article/tt-talk-mandate-fraud-133885/

資訊來源

David J. Thompson
Signum Services
Thomas Miller P&I (Europe) Ltd. Department
電話：+44 20 7283 5616