ISSUE 31

警察總局
金融情報辦公室通訊

本期內容

金融情報辦公室併入警察總局

為配合澳門特區政府“精兵簡政”的施政方針，推動行政改革，以及進一步加強金融情報辦公室與警方的合作，以期在預防及打擊相關犯罪取得更大成效，澳門特區政府透過修改法律及行政法規，將（項目組）金融情報辦公室併入警察總局。

於2024年2月1日，經第23/2023號法律修改之第1/2001號法律《澳門特別行政區警察總局》正式生效，警察總局獲賦予參與預防及打擊清洗黑錢、資助恐怖主義及資助大規模毀滅性武器擴散等犯罪活動的職責及職權。同日，經第3/2024號行政法規修改之第5/2009號行政法規《警察總局的組織及運作》亦告生效，金融情報辦公室正式併入警察總局的組織架構，作為具有技術及獨立運作的從屬機構，以確保澳門特區在國際組織上的成員資格不受影響，繼續履行法定職責。

於2024年2月1日，警察總局舉行金融情報辦公室主任及副主任就職儀式，由警察總局梁文昌局長主持及監誓，並在三位局長助理、局長辦公室協調員及各部門主管見證下，金融情報辦公室朱婉儀主任及馮婉琪副主任正式宣誓就任。

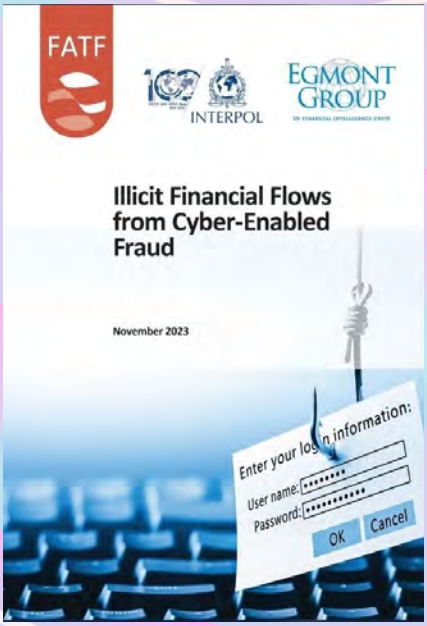
可疑交易報告統計（2023 年）

可疑交易報告（STR）數量	2023年	2022年
由金融及保險機構舉報	887 （19.2%）	765 （34.8%）
由幸運博彩經營者舉報	3,431 （74.4%）	1,177 （53.5%）
由其他機構舉報	296 （6.4%）	257 （11.7%）
總數（份）	4,614	2,199

- 警察總局金融情報辦公室（金情辦）於 2023 年共收到 4,614 份 STR，較 2022 年增加 109.8%。
- 來自金融業的 STR 佔總數量的 19.2%，而由博彩業舉報的 STR 佔 74.4%。
- 金情辦於 2023 年向檢察院舉報的 STR 共 116 份。

國際趨勢 — 網路詐騙所產生的非法資金流動

前言

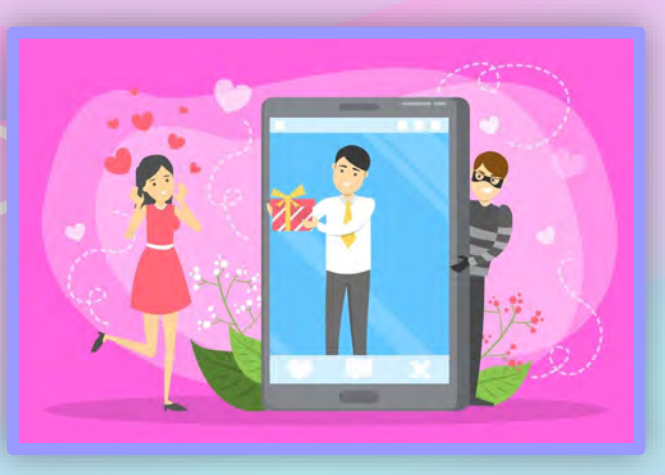


（圖片來源：金融行動特別工作組）

網絡詐騙是指通過互聯網或電子郵件等方式進行的網絡犯罪活動，並以全球化的趨勢在世界各地紛紛冒起，對現今的數碼世界構成重大威脅。這種形式的犯罪組織往往是結構嚴密，分有不同的小團伙，並在特定範疇上具有專門知識的犯罪專家，包括清洗黑錢。由於這些犯罪組織通常遍佈在不同的司法管轄區，故調查網絡詐騙活動的執法工作變得更為複雜。

與網絡詐騙有關的威脅

網絡詐騙是一種跨國性的威脅，其借助了數碼化的金融服務實施詐騙活動，包括商業電子郵件入侵詐騙、網絡釣魚詐騙、社交媒體和電信冒充詐騙、網上交易／交易平台詐騙、網戀詐騙和求職詐騙。例如：非洲的網上銀行詐騙活動急劇增加，美洲報告了大量與虛擬資產有關的投資詐騙，亞太地區的非法投資詐騙也激增。這些犯罪活動不僅造成巨大的經濟損失，還帶來了嚴重的清洗黑錢風險，因為犯罪分子便是利用數碼和金融技術在跨國清洗其非法所得。



與網絡詐騙有關的挑戰

打擊網絡詐騙充滿多項挑戰：

- ❖ 為掩飾犯罪分子真正的身份和活動，其等會透過高端技術在不同司法管轄區開展相關犯罪活動，使犯罪網絡變得複雜化；

- ❖ 網絡詐騙的收益可透過遍佈多個司法管轄區和金融機構的“錢騾”帳戶群迅速洗白；
- ❖ 這類跨國性的犯罪活動使司法部門及法院在檢控和判罪的工作上變得更複雜；

- 日新月異的科技發展，以及數碼和金融技術的使用也進一步對偵查和執法工作帶來挑戰；
- 在清洗犯罪所得方面，匿名技術和加密貨幣之使用存有具挑剔的問題；
- 網絡“犯罪服務”是指利用專業人士如律師、會計師、稅務顧問、公司服務提供者和銀行家等提供專業的清洗黑錢服務，使網絡詐騙活動更專業化，從而使執法工作面臨更大的挑戰。

相關風險緩解措施

為打擊網絡詐騙及相關的清洗黑錢風險，各個司法管轄區應加強當地監管部門和私營機構之間的協調性，同時加強國際同行之間的合作和情報交流。這些措施能提升偵測可疑交易的分析能力，增強公眾的防騙意識，並強化法制來促進快速回應和資產追回。公私營間的合作夥伴關係也可通過策略性的情報交流去識別隱藏的清洗黑錢網絡，從而共建更好的偵測手段，並藉此加強追回資產的能力。私營機構的實時交易監控可以較容易地識別多個帳戶或交易中的可疑交易模式。此外，高效的監管、適當的發牌或註冊登記、客戶盡職調查之執行，並採用新技術進行實時交易監控、調查和公私營間的合作是同樣重要。

相關風險指標

以下與網絡詐騙相關的風險指標是適用於金融機構、指定非金融行業和職業及其他須偵測和監控與網絡詐騙有關的可疑交易的實體。這些指標涵蓋客戶多方面的資訊，有關指標列舉如下：

交易模式

- 開戶後隨即進行大額交易；
- 收到大額資金後快速提取現金或轉帳；
- 交易量與客戶背景不一致；
- 涉及高風險司法管轄區的交易；
- 新成立公司的大額及頻繁交易與其業務性質不一致。

客戶交易指示和備註

- 標有緊急或機密請求的交易；
- 文字表述方式或交易金額與客戶過往的交易模式不一致；
- 受益人資訊與過往交易不匹配；
- 客戶提交的證明文件存有文法或拼寫錯誤 。

對帳戶持有人資料的懷疑

- 未能順利進行客戶盡職審查；
- 缺乏對資金來源的瞭解；
- 對交易的性質 / 金額 / 目的或與交易對手的商戶關係瞭解不足。

對帳戶持有人或用戶身份的懷疑

- 試圖隱瞞真實身份；
- 關於帳戶持有人的負面資訊（如司法管轄區內的業務並不活躍）；
- 與負面新聞或詐騙報告有關；
- 線上行為可疑，例如：輸入交易時猶豫不決、按鍵延遲、自動化交易跡象和多次登錄嘗試失敗等；
- IP 地址來自高風險司法管轄區；
- 一個帳戶關聯多個 IP 地址或多個帳戶關聯一個 IP 地址。

其他指標

- 帳戶資訊不匹配：帳戶號碼與帳戶持有人姓名不符，或通過閉路電視觀察到交易在指導下進行，反映存有詐騙交易的可能。

澳門特區關於網絡詐騙的現況

隨著網絡詐騙具全球化的趨勢日益嚴重，澳門特區也難以獨善其身，有關網絡詐騙的活動近年在本澳也有持續上升及具複雜化的現象。根據保安司司長辦公室的統計數據顯示，2023 年本澳共發生 2,496 宗詐騙案，較 2022 年的 1,315 宗增加了 1,181 宗，當中利用電腦或互聯網詐騙的案件有 894 宗，較 2022 年的 622 宗增加了 272 宗。澳門特區一直積極參與全球打擊這類詐騙犯罪的工作。例如，澳門特區的執法部門曾參與國際刑警組織的行動名為“HAECHI-II 行動”，該行動旨在打擊各種形式的線上詐騙，包括戀愛詐騙、投資詐騙以及與非法線上賭博有關的清洗黑錢活動。是次行動逮捕了 1,000 多人，攔截近 2,700 萬美元的非法資金。由於網絡金融犯罪持續發生，澳門特區必須開展國際合作並完善法律框架，才能有效地應對這些挑戰。

此外，根據司法管轄區的經驗和案例，偵測和調查與清洗黑錢有關的網絡詐騙的兩個主要資訊來源是受害人舉報和可疑交易報告，因此，澳門特區的相關權限部門已採取不同的教育推廣活動，包括於不同媒體渠道推廣反詐宣傳活動和廣告，目的為教育公眾和提高其等之防範意識，從而防止網絡詐騙。最近，司法警察局於 2024 年 4 月正式啟動“反詐程式”，協助公眾防範詐騙活動，其功能包括詐騙搜尋器、詐騙線索上報、詐騙知多 D 及騙案識別。

（圖片來源：司法警察局）

結論

總括而言，網絡詐騙是一種複雜的全球性犯罪，故必須採取全面、策略性和多方合作的方法，包括監管、採用能提高偵測能力的高端技術以識別風險指標、加強公私營夥伴關係的情報交流、完善法制以及促進本地和國際合作，以便有效降低這類詐騙活動所造成的風險。

內容參考金融行動特別工作組於 2023 年 11 月發佈的《Illicit Financial Flows from Cyber-Enabled Fraud》：
https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

首屆“優秀可疑交易舉報個案嘉許活動”

為進一步推動本澳的預防清洗黑錢及恐怖活動融資工作，切實提升本澳反清洗黑錢工作水平及履職效能，強化可疑交易舉報個案的質量水平，有效應對反清洗黑錢工作面臨的新挑戰，金情辦為本澳的銀行業界舉辦首屆“優秀可疑交易舉報個案嘉許活動”，冀持續提高金融業界對潛在金融犯罪的風險防範意識，深化對反清洗黑錢及反恐怖融資的整體認知，並藉以透過優秀個案對有關銀行作出嘉許及鼓勵。是次活動的評審委員會由金情辦領導及代表、澳門金融管理局及司法警察局各一名主管組成，評選採用不記名的評分方式，從舉報機構對可疑交易的識別工作及分析過程、在案例中採取的防範或預防清洗黑錢及恐怖融資的各項措施、案例涉及之案件特徵及借鑑意義等各方面進行評分，評選出最佳可疑交易案例。

金情辦於 2023 年 12 月 1 日在澳門金融管理局舉辦的“反洗黑錢及反恐融資研討會”上頒發嘉許活動獎項，並邀請獲獎機構代表在研討會上介紹獲獎之舉報案例，冀銀行同業能借鑑獲獎案例，進一步了解有效的可疑交易識別工作，同時藉此加強內部風險防控的力度，深化防範及打擊潛在金融犯罪風險的各項措施，使更好地預防及阻截金融犯罪。

金情辦期望持續透過嘉許活動推廣本澳預防清洗黑錢及恐怖活動融資工作，以激勵各舉報機構及相關從業人員持續提高舉報工作的水平，同時亦鼓勵更多合理舉報個案，進一步深化各行業對反清洗黑錢及反恐怖融資的預防性措施的認知，提高社會公眾對清洗黑錢及恐怖活動融資的關注度。

最佳可疑交易案例

得獎機構：中國銀行股份有限公司澳門分行

個案例子

A 君於深夜收到銀行短訊通知，手機銀行的快捷支付密碼被更改，且帳戶轉出金額 MOP 1,000 予 B 君。 A 君並無作出上述操作，懷疑其手機銀行被盜用。銀行根據 A 君提供的線索，發現收款方 B 君帳戶當月收到約 20 筆等額轉入帳且涉及不同存入方，銀行根據 B 君存入方的登錄手機銀行設備及 IP 地址進行檢查，發現 1 部可疑手機設備在一個月內曾先後嘗試登錄 38 名客戶的手機銀行，交易 IP 地址多位於美國及英國兩地，期間多名客戶手機銀行出現被登錄、加好友後發送紅包的情況，當中大部分客戶聲稱交易並非本人操作，亦不認識紅包收款方，懷疑客戶手機銀行被盜用並進行有關操作。案件中發現 5 名非本地居民客戶和 1 間本地獨資公司客戶懷疑為騙徒所操控的收款帳戶，累計涉及金額約 MOP 57 萬及 HKD 2.9 萬。

可疑特徵分析

- 可疑交易通過同一手機設備進行，先後登錄多名受害人手機銀行，添加指定收款人為好友，再向其發送等額紅包，資金最終歸集至同一帳戶後流出；
- 資金通過小額紅包形式流轉，呈現快進快出特徵，資金過渡性質明顯；

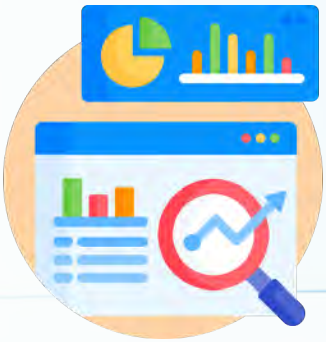
- 可疑交易顯示交易發生地在境外，而實際相關人士大部分在澳門，帳戶疑似被他人操縱，接收不法資金。

傑出可疑交易案例

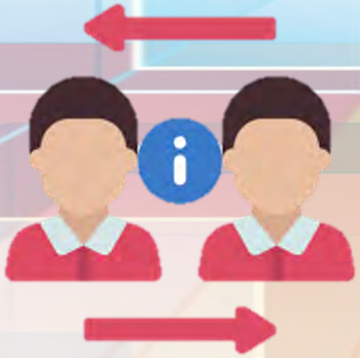
得獎機構：大豐銀行股份有限公司

個案例子

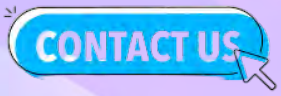
銀行發現客戶 A 在開立股票投資帳戶後，於短時間內持續購入香港上市公司 D 的股票（細價股），所涉金額約 900 萬港元，佔該上市公司已發行股本的 4.995%，非常接近香港上市公司的權益披露水平（持 5%或以上的股份權益），之後再無發生其他交易。客戶 A 持有香港證件，但銀行懷疑其故意隱瞞境外人士身份，而上述投資股票的行為與一般投資者不同，因此銀行隨即對客戶展開調查，透過內、外部信息收集，及採用關聯網絡分析方法，發現客戶 A 於上市公司的附屬公司任職高級管理層，且其親屬 K 及其多名僱員曾經購買同一上市公司 D 之股票，因透過代理人異常買賣上市公司股票被銀行舉報。



可疑特徵分析



- 客戶交易行為符合可疑交易特徵：只購買單一特定股票、細價股大額交易、只買入不賣出、持股量接近 5%的法定披露水平；
- 客戶有意隱瞞其境外人士身份；
- 客戶及其親屬與該上市公司存在密切關係，及使用代理人進行交易；
- 有跡象顯示客戶存在規避香港《證券及期貨條例》之披露權益制度、進行內幕交易或操縱市場的可能性，可能涉及破壞金融管理秩序相關犯罪，屬清洗黑錢罪之上游犯罪。



2024年5月出版

出版：澳門特別行政區政府
警察總局金融情報辦公室

地址：澳門蘇亞利斯博士大馬路
307至323號
中國銀行大廈22樓

電話：(853) 2852 3666
傳真：(853) 2852 3777
電郵：info@gif.gov.mo

如對本通訊有任何意見或查詢，
請與警察總局金融情報辦公室聯絡。