

今期內容

Inside this issue:

可疑交易報告統計(上半年) 1

Suspicious Transaction Reports Statistics (Semi-Annually)

個案例子 2

Case Studies 4

國際趨勢 – 嶄新的付款方式 6

International Trend - New Payment Methods 7

國際趨勢 – 嶄新的付款方式 8

(續)

International Trend - New Payment Methods (Cont.)

金融情報辦公室資訊: 8

與其他機構舉辦的專題講座

GIF Information: Seminars Held with Different Organizations

可疑交易報告統計(上半年)

STR數量(份)	2011年 1至6月	2010年 1至6月
由金融及保險機構舉報	223 (30%)	131 (30%)
由幸運博彩經營者舉報	519 (69%)	280 (64%)
由其他機構舉報	4 (1%)	26 (6%)
總數	746	437

- 本辦公室於 2011 年 1 至 6 月所收到的 STR 數量，較 2010 年同期上升了 71%。
- 來自金融機構的 STR 佔總數量的 30%，而由博彩公司舉報的 STR 約佔 69%。
- 本辦公室向檢察院舉報的 STR 共 31 份。

Suspicious Transaction Reports Statistics (Semi-Annually)

Number of STRs	2011 Jan to Jun	2010 Jan to Jun
From Financial Institutions and Insurance Companies	223 (30%)	131 (30%)
From Games of Fortune Operators	519 (69%)	280 (64%)
From Other Institutions	4 (1%)	26 (6%)
Total	746	437

- The total number of STRs received by GIF from 2011 Jan to Jun increased by 71%, as compared with the same period in 2010.
- STRs received from financial institutions and gaming sectors constituted 30% and 69% of total respectively.
- A total of 31 STRs were sent to the Public Prosecutions Office for further investigation.



個案例子

個案一 於信用卡帳戶存入可疑資金

個案例子:

- 於信用卡帳戶存入可疑資金
- 通過預付卡進行洗黑錢活動
- 透過網上購物平台清洗不法資金
- 透過網上銀行清洗黑錢

F先生的信用卡帳戶收到一筆由X國銀行匯 **疑點：**

入的大額匯款，但發卡銀行發現F先生的帳戶並沒有任何尚未清還之款項。數天後，F

先生授權第三者代他以購買本票形式提取

上述匯款，聲稱用途為償還朋友借貸。其後

該等本票於同日被存入F先生在同一銀行之

帳戶，而全數款項於數天後以現金被提走。 **建議：**

由於銀行發現F先生的交易模式可疑，故向金融情報組織舉報。

根據金融情報組織收集到的情報，F先生為毒販，透過其信用卡帳戶以接收其海外同黨的販毒贓款。

● 信用卡帳戶存入不尋常資金，而且不作消費用途；

● 要求立即提取剛存入信用卡帳戶內之資金；

● 授權第三者進行交易。

● 金融機構應設有足夠之監察系統以偵測任何不正常或不合理之交易模式，例如以頻繁或大額現金存入信用卡帳戶，異常交易量與客戶之背景不符；

● 當交易由獲授權的第三者進行時，金融機構應向客戶查詢有關交易之目的；

● 若客戶未能就不尋常的交易模式提供合理解釋或理據，金融機構應向金融情報組織舉報及考慮終止有關交易或客戶關係。

個案二 通過預付卡進行洗黑錢活動

W先生利用一個免費的軟件程式，於互聯網 **疑點：**

上搜尋一些載有金融帳戶資料且較容易入侵之私人或商用電腦。他先利用虛假交易，

把資金由受害人的帳戶轉至其以空殼公司

名義開立的帳戶，再利用該等公司的不法資金充值預付卡以作購物。

從警方收集到的資料顯示，懷疑W先生利用盜取的資料，將他人的資金不法地轉入其控制之帳戶內。

● 大量不同來源之資金(例如:來自不同地區的銀行轉帳、信用卡或現金)存入同一帳戶內；

● 預付卡經常由不明來歷的第三者增值或注資。

建議：

● 金融機構應設立有效之監察系統，以偵測由不同來源的第三者注資的嶄新付款方式之帳戶；

● 金融機構應採取加強客戶盡職審查措施，以了解客戶之背景及交易目的。



個案例子

個案三 透過網上購物平台清洗不法資金

D小姐為家庭主婦，她於網上購物平台開設帳戶並 **疑點：**

於一個月內進行超過100宗交易，交易金額累積達港幣五十萬。銀行於帳戶結算時發現她的網上消費甚為頻繁。銀行因考慮到D小姐為家庭主婦，理應沒有固定收入而對以上交易存疑，故向金融情報組織作出舉報。

經金融情報組織分析後，發現D小姐的帳戶經常由第三者存入小量現金，因此懷疑她有可能被洗黑錢集團利用作為人頭戶，而且她亦會於短時間內不惜蝕讓貨物來套現。

建議：

- 金融機構應設有足夠的監察系統，以偵測出客戶之單一交易或累計產品消費/交易到達一定限額，並且在超過有關限額時加強客戶盡職審查措施；
- 當發現客戶有不合理交易模式或與客戶背景不符之交易時，金融機構應向客戶了解原因。

個案四 透過網上銀行清洗黑錢

銀行舉報 A 太太與 A 先生共同擁有一手提電話零 **疑點：**

售公司，A 太太之帳戶經常存入大額現金，並通過銀行提供的網上匯款服務將款項匯予 Y 國的 B 先生及 C 先生。雖然 A 太太聲稱其現金存款來自其手提電話公司的盈利，但觀其盈利與其業務並不相符。因此，銀行向金融情報組織舉報。

根據金融情報組織的情報，A 先生現正因涉及非法地下錢莊匯款而被調查，並且懷疑 A 先生通過網上匯款服務，利用其公司帳戶與 Y 國的同黨清算匯款交易。

建議：

- 當涉及網上或海外交易時，金融機構應設有足夠之監察系統，以偵測任何不正常或不合理之交易模式；
- 設置根據交易金額、於短時間內累積的交易金額、或交易次數而制定的檢測門檻或審批權限，有助偵測出洗錢者故意策劃之結構性洗錢罪行；
- 由於網上銀行屬非面對面交易，金融機構除應有適當的客戶接納程序外，於開戶時亦應加強客戶盡審查措施及對所進行之交易作持續監控。

常見疑點：

- 大額 / 經常性不明來歷之現金存款
- 交易模式與客戶背景 / 業務性質不符
- 帳戶經常由第三者增值或注資

Case Studies

Case 1 Suspicious Funds deposited into Credit Card Account

A large amount of remittance had been remitted to Mr. F's credit card account via a bank in country X. The card issuing bank found out that Mr. F did not have any outstanding balance for settlement. Few days later, Mr. F gave power of attorney to a third party to withdraw the remitted funds by draft on his behalf, claimed as repayment of loans from a friend. Within the same day, the requested draft was deposited into the account of Mr. F in the same bank and all funds were then withdrawn in full by cash in couple of days afterwards. The bank found the transaction pattern of Mr. F suspicious and the case was reported to the FIU.

According to the information gathered by the FIU, Mr. F was a drug dealer, receiving illicit proceeds of his drug sale business from his overseas gangsters via his credit card account.



Red flags:

- Abnormal funds deposited into credit card account but not for spending purpose;
- Immediate request for withdrawal of deposited funds from the credit card account ;
- Authorization to third party to carry out transaction.

Recommendations:

- Financial Institutions should have adequate monitoring system to trigger any irregular or unreasonable transaction patterns, such as frequent or large amount of cash deposits into credit card accounts, unreasonable quantity of transactions not in line with the customer profile;
- Financial Institutions should enquire the customers about the purpose of transactions especially when the transaction is authorized to a third party;
- Financial Institutions should report to FIU and consider terminating the transactions or the customer relationship if they cannot obtain reasonable ground or explanation from the customer to support the irregular pattern of transactions.

Cases:

- Suspicious Funds deposited into Credit Card Account
- Money Laundering through Prepaid Cards
- Laundering of Illicit Funds through Online Shopping Website
- Money Laundering through Internet Banking

Case 2 Money Laundering through Prepaid Cards

Mr. W used a freely available software program to scan the internet for vulnerable personal and commercial computers holding financial account information. Fraudulent transactions were initiated to transfer funds from the victims' accounts to accounts created in the names of front companies. The illicit proceeds in the front company accounts were then used to load prepaid cards which Mr. W used to make purchases.

From the information gathered by the police, Mr. W was suspected of using stolen information to transfer money illegally from bank accounts to accounts controlled by him.

Red flags:

- Large and diverse source of funds (e.g. bank transfers, credit card and cash funding from different locations) used to fund the same account;
- Frequent loading / funding of prepaid cards from different third parties.

Recommendations:

- Financial Institutions should have proper monitoring system to detect New Payment Method (NPM) account funding through third parties, especially from different sources;
- Financial Institutions should perform enhanced CDD measures to understand the client's background and nature of transactions.



Case Studies

Case 3 Laundering of Illicit Funds through Online Shopping Website

Ms. D, a housewife, opened an account in an online shopping website. Within a month, more than 100 transactions were made through her account in the shopping website and the transactions amounted to HKD 500,000. In settling her account, the bank found that her online spending was quite frequent. The transactions were treated as suspicious, considering that she was a housewife without regular income. As a result, the case was reported to the FIU.

After analysis by the FIU, it was observed that Ms. D's account was frequently loaded with small amount of cash deposits by third parties and she was suspected to be a straw man possibly used by the money laundering group. She would resell the products shortly afterwards at a loss in order to redeem cash.

Red flags:

- Frequent loading or funding of account by third parties;
- Frequency and amount of the transactions do not correspond to the customer's profile;
- Multiple third party funding activities of account, followed by the immediate transfer of funds for internet transactions.

Recommendations:

- Financial Institutions should have adequate IT triggering system to detect where a customer reaches a limit (on one product / transaction or cumulatively) beyond which full customer due diligence has to be applied;
- Financial Institutions should enquire the customers for any unreasonable transaction patterns or transactions that are inconsistent with their profile.

Case 4 Money Laundering through Internet Banking

A bank reported that Mrs. A, together with her husband, Mr. A, owned a mobile phone retail company, frequently deposited large amount of cash into her account and then remitted the funds through the internet remittance service provided by the bank to Mr. B and Mr. C in country Y. Although Mrs. A claimed that the source of the cash deposits was from her mobile phone retail business profit, the profit amount did not seem to be commensurate with the business nature. As a result, the case was reported to the FIU.

Based on the information of the FIU, it was revealed that Mr. A was being investigated for underground remittance services and suspected that he used his "company" bank account to settle the remittance amount with his foreign counterparts in country Y through the internet remittance service.

Red flags:

- Frequent and large amount of cash deposits;
- Transaction patterns and amount do not correspond to the business nature ;
- Frequent remittance of cash deposits to different third parties in other countries within a short period of time.

Recommendations:

- Financial Institutions should have proper monitoring system to detect any unusual or suspicious transaction patterns when transactions involve internet and overseas patterns;
- By setting triggering thresholds or approval limits based on amount, accumulated amount over short period of time or frequency of transactions is helpful to detect intentional structuring of money launders;
- As online banking is non face-to-face transactions, financial institutions should have proper customer acceptance policy in place and carry out enhanced CDD in account opening. Moreover, it should perform ongoing monitoring on the transactions.

Frequently Observed Indicators:

- Large-scale/ Frequent Cash Deposits with Non-verifiable Source of Funds
- Transaction Patterns do not Correspond to the Customer's Profile/ Business Nature
- Frequent Loading or Funding of Account by Third Parties

國際趨勢 - 嶄新的付款方式

NPMs減輕風險措施

恰如其他金融產品，在缺乏適當的預防措施下，與嶄新付款方式(NPMs)相關的反洗黑錢/反恐融資的風險亦較高。然而，有效的減輕風險措施能顯著地減低已知的風險。

下列的減輕風險措施適宜整體地而非獨立地考慮。最重要是對所有的風險因素及減輕風險措施作全面考慮，從而可有效地評估個別的 NPM 產品所帶來的風險。

減輕風險措施類別

1) 身份識別及核實措施

身份識別及核實措施讓商戶更了解其客戶及有關的實益擁有人，並且能夠讓商戶核實客戶的身份，如擁有多個帳戶或多張預付卡之客戶，及提供文件記錄予執法機關。

- 對於倚靠互聯網的產品及服務，客戶的IP地址應為服務提供者所收集的身份資料的一部分，並由服務提供者所保存。即使是匿名帳戶，IP地址也能有助減低客戶使用多個帳戶的可能性。
- 如核實程序須在非面對面的情況下進行，商戶應採用防假冒的檢查以識別客戶。防假冒的檢查包括但不限於：通過可核實的住宅地址與客戶聯絡；要求客戶本人於被監管的機構進行首次繳費交易；及要求由認可的人士認證文件的影印副本。

2) 監管

嶄新付款方式主要是利用電腦科技，因此亦對有效的監管及報告程序提供很好的必要條件。

- 監管系統可有效地減低利用嶄新付款方式產品進行商業犯罪風險，該系統最少能讓服務提供者識別下列各項：
 - 已註冊IP地址的差異
 - 不尋常或可疑交易
 - 個案涉及多人使用同一帳戶
 - 個案涉及同一用戶開立多個帳戶
 - 個案涉及數項產品以同一資金來源付款

3) 設定值限制

- 設置帳戶餘額、交易額上限及次數的限制均能預防罪犯不斷存取大量金錢作不法用途。
- 透過風險為本的方法，可為反映不同的市場及NPM產品所連帶的要求及風險而制定不同的限制值。
- 使用限制值的其中一項挑戰就是如何界定合適的低風險門檻。低交易金額或可阻止清洗黑錢者，但對於恐怖主義融資活動仍具有一定的吸引力，因其金額一般較清洗黑錢涉及的金額為低。
- 金額及交易次數的限制可作為非常有效的減輕風險措施，尤其配合能防止購買多張低面值的預付卡，或單一客戶擁有多個低餘額帳戶的有效監管系統及程序。

4) 注資方法

- 與匿名付款方式有關的清洗黑錢風險，可透過限制付款方法的資金來源而得以減低。服務提供者可依靠另一機構的客戶盡職審查措施，例如過往已被識別的銀行帳戶及信用卡或扣帳卡。
- 作出限制付款方法要求的一方應留心監察利用第三者注資付款的方法。透過限制付款的方法及可允許支付產品的人數，從而限制利用第三者注資付款的可能性，並可進一步減低清洗黑錢/恐怖融資的風險。



International Trend – New Payment Methods (NPMs)

Risk Mitigants on NPMs

Like any financial product, the AML/CFT risk associated with NPMs is high in the absence of appropriate safeguards. However, there are effective risk mitigants that can significantly reduce the identified risks.

The following risk mitigants should not be looked at separately but as a whole. It is important to look at the whole picture including all risk factors and all risk mitigants in order to effectively assess the risk associated with a particular NPM product.

Types of Risk Mitigants

1) Identification and Verification Measures

Identification and verification measures allow firms to understand who their customer and, where relevant, the beneficial owner is. It also allows firms to verify that the customer is who they claim to be, identify whether a customer is associated with multiple accounts or prepaid cards and create a paper trail for law enforcement.

- For products and services that rely on the internet, the internet protocol address (IP-address) should be part of the identification data collected and retained by the provider.



The IP-address can help minimize the potential for a customer to access multiple accounts, even if those are anonymous.

- Where verification takes place on a non-face to face basis, it is important that firms employ anti-impersonation checks to be satisfied that their customer is who they claim to be. Anti-impersonation checks include, but are not limited to: correspondence with the customer at their verified home address; requiring the first payment to be carried out through an account in the customer's name with a regulated credit institution; and requiring copy documents to be certified by an appropriate person.

2) Monitoring

NPMs are based on computer technology and therefore provide good prerequisites for effective monitoring and reporting procedures.

- Monitoring systems can be a very effective tool to mitigate an NPM product's financial crime risk, at a minimum, such systems can allow the provider to identify the followings:
 - Discrepancies on registered IP address
 - Unusual or suspicious transactions
 - Cases where the same account is used by multiple users
 - Cases where the same user opens multiple accounts
 - Cases where several products are funded by the same source

3) Value Limits

- Account balance and transaction limits as well as restrictions in the frequency of transactions may prevent criminals from having continuous access to large amounts of money for illicit purposes.
- Applying a risk-based approach, value limits can be tailored to reflect the needs and risks attached to market segment and NPM product.
- One of the challenges for applying value limits is to define an appropriate

threshold which can be considered low risk. Furthermore, low transaction amounts that may deter money launderers might still be attractive for the purpose of terrorist financing, which is generally thought to involve much smaller amounts than money laundering.

- Value and transaction limits can be a very powerful risk mitigant, especially when coupled with effective monitoring systems and procedures that prevent multiple purchases of low-value cards or multiple low-value accounts for a single customer.

4) Funding Methods

- The money laundering risk associated with anonymous funding methods can be mitigated by restricting funding methods to sources where providers can rely on another institution's customer due diligence (CDD) measures, such as previously identified bank accounts and credit or debit cards.
- Issuers with restricted funding methods should be in a position to detect indirect funding through third parties by attentive monitoring. They can further reduce money laundering/ terrorist financing risk by not only restricting the funding method, but also restricting the number of parties allowed to fund the product, thus limiting the possibility of third party funding.



國際趨勢 – 嶄新的付款方式(續)

International Trend – New Payment Methods (Cont.)

通過嶄新付款方式清洗黑錢的常見疑點

- 客戶提供的資料與監測系統檢測到的資料存在差異。
- 同一個嶄新付款方式的帳戶資金來自不同城市之銀行帳戶。
- 於相同帳戶存入不同資金，並於短時間內透過櫃員機提走資金。
- 持有同一供應商不尋常數量的嶄新付款方式帳戶。
- 異常地使用支付產品(包括非預期及頻繁的跨境使用或交易)。
- 於不同的櫃員機進行多次提取(有時提款地方位於不同國家，有異於資金來源所屬的司法管轄地區)。
- 嶄新付款方式的帳戶並非用作POS消費或網上購物，而只是用作提款用途。

Red Flag Indicators of Money Laundering through New Payment Methods

- Discrepancies between the information submitted by the customer and information detected by monitoring systems.
- Multiple reference bank accounts from banks located in various cities used to fund the same NPM account.
- Multiple loading or funding of the same accounts, followed by ATM withdrawals shortly afterwards, over a short period of time.
- Individuals who hold an unusual volume of NPM accounts with the same provider.
- Atypical use of the payment product (including unexpected and frequent cross-border access or transactions).
- Multiple withdrawals conducted at different ATMs (sometimes located in various countries different from jurisdiction where NPM account was funded).
- NPM account only used for withdrawals, and not for POS or online purchases.

2011年11月出版

出版：澳門特別行政區政府
金融情報辦公室
地址：澳門蘇亞里斯博士大馬路
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
網址：http://www.gif.gov.mo

如對本通訊有任何意見或查詢，或欲索取本通訊，請與辦公室聯絡。

Published in November 2011

Published by: Financial Intelligence
Office,
Macao Special
Administrative Region
Government

Address: Avenida Dr. Mário
Soares, Nos. 307-323,
Edifício "Banco da
China", 22º andar,
Macao

Tel: (853) 2852 3666
Fax: (853) 2852 3777
E-mail: info@gif.gov.mo
Website: http://www.gif.gov.mo

If you have any suggestions and enquiries on this newsletter, or like to have more copies, please feel free to contact GIF.

金融情報辦公室資訊：與其他機構舉辦的專題講座

本辦公室應財政局之邀請，於2011年5月27日在《核數師和會計師在執行“預防及遏止清洗黑錢及資助恐怖主義犯罪”工作的責任及風險》專題座談會作演講。

本辦公室於2011年8月13日應澳門金融學會的邀請，為兩間銀行提供反洗錢及反恐主義融資培訓講座。

澳門銀行公會、澳門保險公會及金融管理局於2011年9月7日舉辦“博彩業的運作與監管”培訓講座，並邀請本辦公室就有關博彩業之反洗錢/反恐融資領域作介紹。

GIF Information: Seminars held with Different Organizations

GIF was invited by DSF to present in a seminar titled “AML/CFT—responsibility and risk for Auditors and Accountants” on 27th May 2011.

On 13th August 2011, GIF was invited by the Macau Institute of Financial Services to present in the “AML/CFT Training Program” for two banks.

The Macau Association of Banks, the Macau Insurers' Association and AMCM organized the seminar “Operation and Supervision of the Gaming Industry” on 7th September 2011. GIF was invited as one of the presenters to give a presentation on AML/CFT issues in the seminar.