

Strategic Analysis Report on Stored Value Facilities

策略分析報告 — 儲值支付工具



Joint Financial Intelligence Unit
聯合財富情報組






TABLE OF CONTENTS

目錄

01

P.1

概覽
Overview

02

P.3

主要結果
Key Findings

03

P.6

引言
Introduction

04

P.7

儲值支付工具的背景資料
Background Information on SVF

- 一般資料
General Information
- 香港的儲值支付工具帳戶概況
SVF Account Situation in Hong Kong

05

P.15

儲值支付工具特點的分析
Analyses on SVF Features

- 身份辨認和資料核證的特點
Identification and Verification Features
- 存入資金特點
Fund-in Features
- 轉出資金特點
Fund-out Features

06

P.23

類型學分析
Typologies Analyses

1 概覽 Overview

近年，科技突飛猛進，一般稱為儲值支付工具¹的非傳統支付及結算系統發展一日千里。儲值支付工具冒起，解除了以往現金交易在交易量、速度和覆蓋地點等方面早已存在的限制。然而，根據觀察，洗錢及恐怖分子資金籌集活動很可能會利用儲值支付工具的部分特點，以避過現有打擊洗錢及恐怖分子資金籌集活動措施的偵查。

根據《販毒（追討得益）條例》（第405章）、《有組織及嚴重罪行條例》（第455章）及《聯合國（反恐怖主義措施）條例》（第575章），舉報可疑交易的法例規定適用於任何人士（包括儲值支付工具持牌人）。此外，《支付系統及儲值支付工具條例》（第584章）自2016年11月生效開始，香港已全面實施儲值支付工具的監管架構。法例規定持牌儲值支付工具營運商須採用充足和合適的監管系統，以制止或打擊洗錢及恐怖分子資金籌集。

Over recent years, the advent of technology resulted in rapid growth of non-traditional payment and settlement systems, generally referred as Stored Value Facilities (“SVFs”)¹. The emergence of SVFs has overcome some of the pre-existing limitations of cash-based transactions, such as volume, speed and geographical coverage. However, it is observed that some features of SVFs could possibly be exploited for ML/TF activities that detection by existing AML/CFT measures might be circumvented.

Apart from the legal requirement of suspicious transaction reporting applicable to any persons (including SVF licensees) under DTRDP, OSCO and UNATMO, a regulatory framework for SVFs has been fully implemented in Hong Kong when the Payment Systems and Stored Value Facilities Ordinance (Cap. 584, “PSSVFO”) was effective since November 2016. Among other things, the legislation requires licensed SVF operators to adopt adequate and appropriate systems of control for preventing or combating ML/TF.

¹ 根據《支付系統及儲值支付工具條例》（第584章）第2A條，某工具即屬儲值支付工具，如（a）該工具可用作儲存款額的價值，而該款額是不時存入該工具的；及是可根據該工具的規則儲存於該工具的；及（b）該工具可作以下兩項或其中一項用途—（i）用作就貨品或服務付款的方法；（ii）用作向另一人付款（個人對個人支付）的方法。

¹ Referring to Section 2A of the Payment Systems and Stored Value Facilities Ordinance, Cap 584 (“PSSVFO”), a facility is an SVF if (a) it may be used for storing the value of an amount of money that is paid into the facility from time to time; and may be stored on the facility under the rules of the facility; and (b) it may be used for either or both of the following purposes - (i) as a means of making payments for goods or services; (ii) as a means of making payments to another person (“P2P”, person-to-person).

本組定期檢視新發現的洗錢及恐怖分子資金籌集風險，進行持續的策略分析，目的旨在進一步改善各單位報告的資料質素、促進情報交流、促成執法行動及/ 或為整個打擊洗錢及恐怖分子資金籌集就制訂規例/ 政策提供意見。

本儲值支付工具策略分析報告（本報告）的檢討期為2016年11月至2018年3月，並就本組的情報及有關儲值支付工具的其他資料，重點介紹有關的類型學分析及所得觀察。另外，鑑於儲值支付工具業不斷推行改革，相關內容亦已參考業界的最新發展（截至2019年3月底）。

The JFIU of Hong Kong, taking into account the emerging ML/TF risks, conducts ongoing strategic analysis with a view to further improving quality of information reported by entities, promoting intelligence exchanges, triggering law enforcement actions and/ or providing insights into formulation of regulations/ policy for AML/CFT community as a whole.

This Strategic Analysis Report on SVFs (the "Report") highlights the key typologies and observations based on the JFIU's intelligence and other information related to SVFs during the review period (i.e. between November 2016 and March 2018), also with reference to the latest development in this sector (as of end of March 2019) in view of the dynamic changes the SVF sector has undergone.

2 主要結果 Key Findings

儲值支付工具的背景資料

根據《支付系統及儲值支付工具條例》第2A條，儲值支付工具指可不時存入儲存款額價值的工具，而且該工具可用作就貨品及服務付款及/或付款給另一人。

自《支付系統及儲值支付工具條例》實施以來，所有儲值支付工具均受金管局的發牌制度規管。截至2018年3月31日（即檢討期末），有16名儲值支付工具持牌人²提供不同範圍的服務，例如，銷售點消費支付、網上消費支付、個人對個人轉帳、海外匯款、帳單繳費、信用卡繳費及乘搭交通工具之用等。

根據金管局2016年第4季至2018年第4季期間的統計數字，儲值支付工具之帳戶總數，以及銷售點消費支付、網上消費支付及個人對個人轉帳的總額分別上升+38.6%及+58.9%。當中，銷售點消費支付是最為普遍。

² 包括13間儲值支付工具公司和根據《支付系統及儲值支付工具條例》第8G條規定的3間銀行，它們分別為三金服務有限公司、Alipay Financial Services (HK) Limited、快易通有限公司、全球付技術有限公司、HKT Payment Limited、僑達國際有限公司、八達通卡有限公司、Optal Asia Limited、PayPal Hong Kong Limited、TNG (Asia) Limited、滙滙(香港)投資諮詢有限公司、UniCard Solution Limited、WeChat Pay Hong Kong Limited、交通銀行(香港)有限公司、大新銀行有限公司及香港上海滙豐銀行有限公司。

自2019年5月，再有2間公司獲批給牌照，分別是銀傳集團有限公司及匯元通卡服務有限公司。

儲值支付工具持牌人紀錄冊可於 <https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/regulatory-regime-for-svf-and-rps/regulation-of-svf/register-of-svf-licensees.shtml> 查閱。

Background Information on SVF

According to Section 2A of the PSSVFO, SVF is a facility for storing the value of an amount of money that is paid into the facility from time to time and may be stored on the facility under the rules of the facility, and may be used as a means of making payments for goods or services and/or to another person.

Since the commencement of PSSVFO, all SVFs have fallen under the licensing regime and supervision of HKMA. As of 31 March 2018 (i.e. end of the review period), there were 16 SVF licensees² in Hong Kong with different scopes of services such as payments at point-of-sales (“POS”), online shopping, person-to-person (“P2P”) funds transfers, overseas remittances, bill payments, credit card repayments, transportation fee, etc.

According to the statistics from the HKMA between Q4 2016 and Q4 2018, the total number of SVF accounts and the total amount of POS, online payment and P2P funds transfer have shown increases by 38.6% and 58.9% respectively. Amongst which, POS is the most prevalent.

² Including 13 SVF companies and three licensed banks, which are regarded as SVF licensees as stipulated in Section 8G of the PSSVFO where a licensed bank is regarded as being granted a licence. They are 33 Financial Services Limited, Alipay Financial Services (HK) Limited, Autotoll Limited, ePaylinks Technology Co., Limited, HKT Payment Limited, K & R International Limited, Octopus Cards Limited, Optal Asia Limited, PayPal Hong Kong Limited, TNG (Asia) Limited, Transforex (Hong Kong) Investment Consulting Co., Limited, UniCard Solution Limited, WeChat Pay Hong Kong Limited, Bank of Communications (Hong Kong) Limited, Dah Sing Bank Limited and The Hongkong and Shanghai Banking Corporation Limited.

Two other SVF companies Yintran Group Holdings Limited and Geoswift Cards Services Limited have been licensed since May 2019.

A list of licensed SVF operators could be found at <https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/regulatory-regime-for-svf-and-rps/regulation-of-svf/register-of-svf-licensees.shtml>.

儲值支付工具特點的分析

辨認身份和核證資料

帳戶限額(包括最高儲值額及年度交易額)及服務範圍會因應不同儲值支付工具產品而有所不同，以減低各類客戶帶來的洗錢及恐怖分子資金籌集風險。客戶盡職審查的級別亦按不同的儲值支付工具產品作出相應調整。

部分儲值支付工具帳戶乃屬不具名性質，而部分則需個人資料作登記以辨認帳戶持有人身份。

一般來說，不具名儲值支付工具帳戶比可辨認身份的儲值支付工具帳戶在服務範圍及金額限額的相關限制上較嚴格。然而，不具名帳戶仍會因為其難以被追查及稽核其蹤迹而產生洗錢風險。

儲值支付工具帳戶使用者以非親身方式遞交的身份證明文件，其真偽或不容易被確定。

罪犯或會利用非法取得的身份證明文件/ 銀行帳戶資料/ 信用卡資料，假冒他人設立偽冒儲值支付工具帳戶以作非法用途。

Analyses on SVF Features

Identification and Verification

Account limit (including limits of maximum stored value and annual transaction amount) and scope of services vary across for different SVF products to mitigate possible ML/TF risk presented by various customers. Thus, the level of customer due diligence (“CDD”) for different SVF products vary accordingly.

Some SVF accounts are observed to be anonymous in nature whilst some are registered with particulars that make the account holder identifiable.

In general, the scope of services and the amount limit of anonymous SVF accounts have a more stringent restriction than those of identifiable SVF accounts. However, the anonymous accounts may still create some ML risks as the audit trail could not be traced.

The authenticity of the identity documents submitted by SVF account users may not be easily ascertained in the course of non-face-to-face submission.

Culprits may impersonate others by using illegally obtained identity document/ bank account information/ credit card information to set up bogus SVF accounts for illicit purposes.

存入資金和轉出資金

不同的儲值支付工具產品的存入和轉出資金特點有別，或會因而構成一些潛在的洗錢及恐怖分子資金籌集風險。

罪犯一旦發現某儲值支付工具之特點有相對脆弱的地方，或會濫用該些特點，以輸送非法資金。

類型學分析

此分析歸納了五種不同個案類型，概述部分儲值支付工具特性或會被用作洗錢的情況。

1. 使用數據機池登記大量不具名儲值支付工具帳戶作非法用途
2. 偽冒身份/ 未經授權使用個人資料作欺詐交易/ 付款
3. 使用儲值支付工具帳戶在網上平台購買非法物品
4. 詐騙案—入侵社交媒體帳戶，透過儲值支付工具帳戶收受資金
5. 使用預付卡形式的儲值支付工具，在海外自動櫃員機提取現金作洗錢

Fund-In and Fund-Out

Different SVF products allow different methods of fund-in and fund-out from which some potential ML/TF risks could be anticipated.

Culprits may abuse some relatively vulnerable fund-in or fund-out features and misuse SVF as a vehicle in channeling illicit funds.

Typologies Analyses

The analyses include five typologies summarizing some vulnerabilities of SVF features in ML.

1. Use of Modem Pool to Register Anonymous SVF Accounts in Bulk for Illicit Purposes
2. Impersonation/ Unauthorized Use of Personal Data for Fraudulent Transactions/ Payments
3. Use of SVF Accounts for Purchase of Illegal Goods on Online Platform
4. Deception – Hacking Social Media Accounts and Receiving Funds via SVF Accounts
5. Use of SVF Prepaid Cards to Withdraw Cash at Overseas ATMs for ML

3 引言 Introduction

此報告介紹本組就儲值支付工具進行的策略分析，包括儲值支付工具的背景資料、其特點之分析，以及類型學分析。

本報告的資料主要來自金管局發表的統計數字、本組收集的財富情報，以及其他公開的資訊。

本報告的檢討期為2016年11月（當《支付系統及儲值支付工具條例》（第584章）全面生效時）至2018年3月。本報告也適度涵蓋了直至2019年3月底有關儲值支付工具的最新發展。

本報告之目的是讓讀者加深了解本地儲值支付工具系統所涉的洗錢及恐怖分子資金籌集趨勢及風險。除展示統計數字外，本報告亦會闡述使用儲值支付工具之不同特點/功能及其所涉及及打擊洗錢及恐怖分子資金籌集之風險，並舉列處境個案作分析。

本報告針對在檢討期內所收集的情報作分析。在本報告發布時，有些在本報告中所提及的漏洞已被儲值支付工具業界堵塞。

The Report provides highlights of strategic analysis on SVFs, conducted by the JFIU, including a summary of background information on SVF, analysis on SVF features and relevant typologies.

The information in this Report has been drawn primarily from statistics published by the HKMA, financial intelligence received by the JFIU and other information from open source.

The data covering period of this Report is between November 2016 (when the PSSVFO came into full operation) and March 2018. Remarks on the latest update of relevant SVF developments till end of March 2019 are also included as appropriate.

The objective of this Report is to provide readers with a better understanding of the prevailing ML/TF trends and risks involving SVF system operated locally. Apart from presentation of statistics, different features/ functions observed in the usage of SVF that are identified to have AML/CTF implication will be elaborated, supported with sanitized scenarios.

The analyses of the Report are based on the intelligence received during the review period. It is understood that some of the risks illustrated in the Report have been identified and certain loopholes have been plugged by the SVF sector at the time of publishing this Report.

4 儲值支付工具的背景資料

Background Information on SVF

根據《支付系統及儲值支付工具條例》第2A條，儲值支付工具指可不時存入儲存款額價值的工具，而且該工具可用作就貨品及服務付款及/或付款給另一人。自《支付系統及儲值支付工具條例》實施以來，所有儲值支付工具均受金管局的發牌制度規管。截至2018年3月31日（即檢討期末），儲值支付工具持牌人有16名。另外兩家儲值支付工具公司於2019年5月獲發牌，使儲值支付工具持牌人增至18名。由於《支付系統及儲值支付工具條例》已就儲值支付工具訂立更廣闊的定義，儲值支付工具持牌人可將完全不同的經營模式或科技應用於不同的服務範圍，例如銷售點消費支付、網上消費支付、個人對個人轉帳、海外匯款、帳單繳費、信用卡繳費及乘搭交通工具之用等。

一般資料

儲值支付工具可分為實體的儲值支付工具或網絡形式運作的儲值支付工具兩種。實體的儲值支付工具是發行人以實物裝置形式向使用者提供，而有關儲值儲存在該裝置上。至於以網絡形式運作的儲值支付工具（即儲值支付工具帳戶），其儲值則透過通訊網絡或系統儲存在該工具。

According to Section 2A of the PSSVFO, SVF is a facility for storing the value of an amount of money that is paid into the facility from time to time and may be stored on the facility under the rules of the facility, and may be used as a means of making payments for goods or services and/or to another person. Since the commencement of PSSVFO, all SVFs have fallen under the licensing regime and supervision of HKMA. As of 31 March 2018 (i.e. end of the review period), there were 16 SVF licensees. Two additional SVF companies were licensed in May 2019, making the total number of SVF licensees 18. As the PSSVFO has adopted a broader definition on SVF, SVF licensees could have a distinctively different business model or technology for different scopes of services such as payments at POS, online shopping, P2P funds transfers, overseas remittances, bill payments, credit card repayments, transportation fee, etc.

General Information

SVFs could be classified as device-based or network-based. Device-based SVF is in the form of a physical device provided by the issuer to the user and the value is stored on the device. For network-based SVF (“SVF account”), the value is stored on the facility by using a communication network or system.

香港的儲值支付工具 帳戶概況

根據金管局在2016年第4季至2018年第4季期間發表的儲值支付工具業界統計數字³：

使用中的儲值支付工具帳戶的季度數目⁴介乎4,050萬個至5,610萬個。

銷售點消費支付、網上消費支付及個人對個人轉帳之總交易量為131億，涉及總額為3,381億港元。

銷售點消費支付之總交易量為125億，涉及總額為1,827億港元。

SVF Account Situation in Hong Kong

According to the statistics³ of SVF sector published by the HKMA during the period from Q4/2016 to Q4/2018:

The quarterly number of SVF accounts in use⁴ ranged from 40.5 million to 56.1 million.

The total number of POS, online payment and P2P funds transfer during the same period was 13.1 billion with total transaction value at HKD 338.1 billion.

The total number of transactions as well as the total transaction amount of POS reached as high as 12.5 billion and HKD 182.7 billion respectively.



圖1：2016年第4季至2018年第4季的儲值支付工具總交易量及總額
Figure 1: Total Number and Amount of SVF Transactions between Q4/2016 and Q4/2018

(資料來源：金管局) (Source: The HKMA)

³ 參考金管局在2017年及2018年發布的新聞稿。

⁴ 指截至檢討期季度完結前可使用的儲值支付工具帳戶總數。由於進位關係，個別數字總和未必與總數相等。數字可能會在日後被修訂。

³ Referring to the press releases published by the HKMA in 2017 and 2018.

⁴ Referring to the total number of SVF accounts that can be used as at the end of the quarters under review. Individual figures may not add up to the total due to rounding. Figures may be subject to subsequent adjustment.

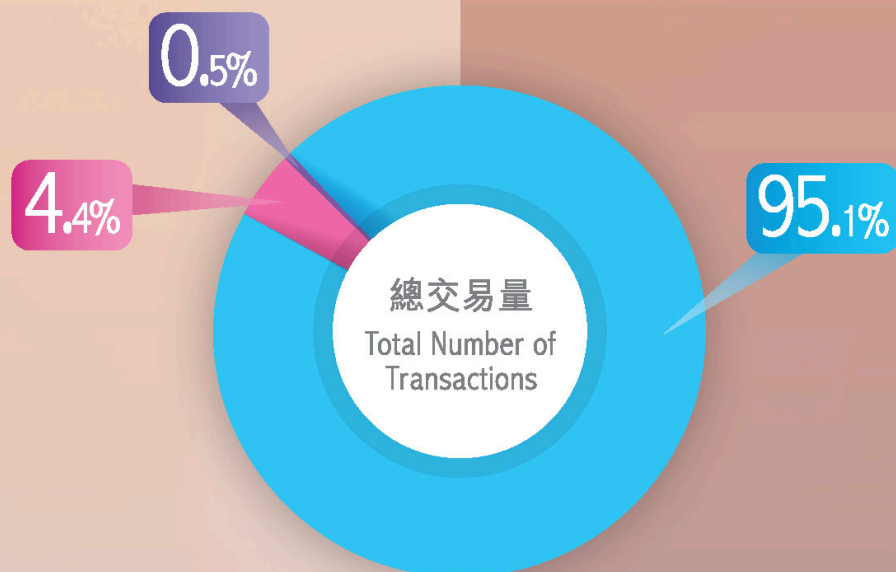


圖2：2016年第4季至2018年第4季的儲值支付工具總交易量
Figure 2: Total Number of Transactions between Q4/2016 and Q4/2018

(資料來源：金管局) (Source: The HKMA)

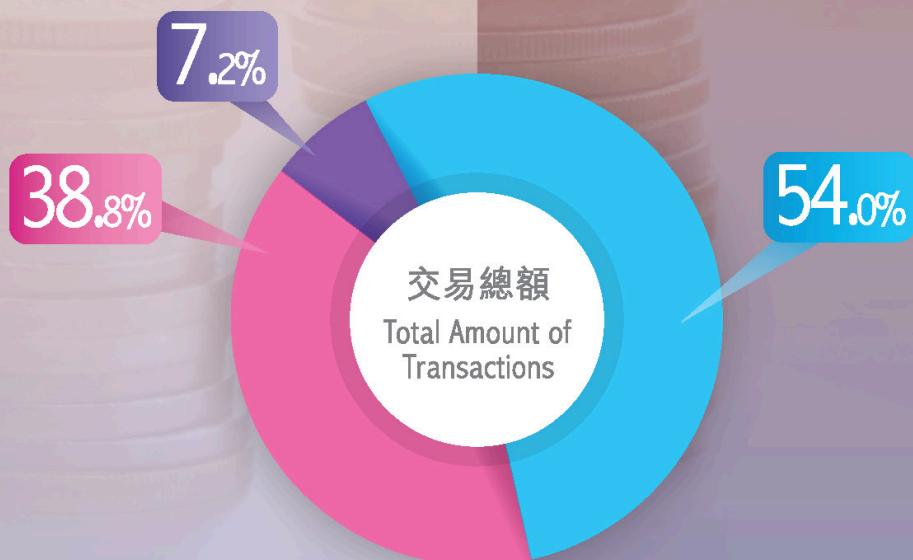
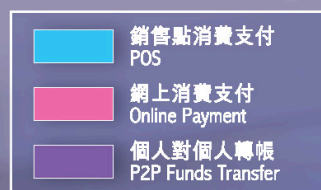


圖3：2016年第4季至2018年第4季的儲值支付工具總額
Figure 3: Total Amount of Transactions between Q4/2016 and Q4/2018

(資料來源：金管局) (Source: The HKMA)



2016年第4季至2018年 第4季的儲值支付工具 交易趨勢

2016年第4季至2018年第4季期間，儲值支付工具帳戶總數，以及銷售點消費支付、網上消費支付和個人對個人轉帳的總額穩步上升，帳戶數目由40,491,000個增加至56,102,000個（+38.6%），而涉及總額則由302.62億港元上升至480.99億港元（+58.9%）。

Trend of SVF Transactions from Q4 2016 to Q4 2018

Between Q4 2016 and Q4 2018, it is noted that the total number of SVF accounts and the total amount of POS, online shopping and P2P funds transfer were on the rise gradually from 40,491,000 to 56,102,000 (+38.6%) and from HKD 302,622 million to HKD 480,992 million (+58.9%) respectively.

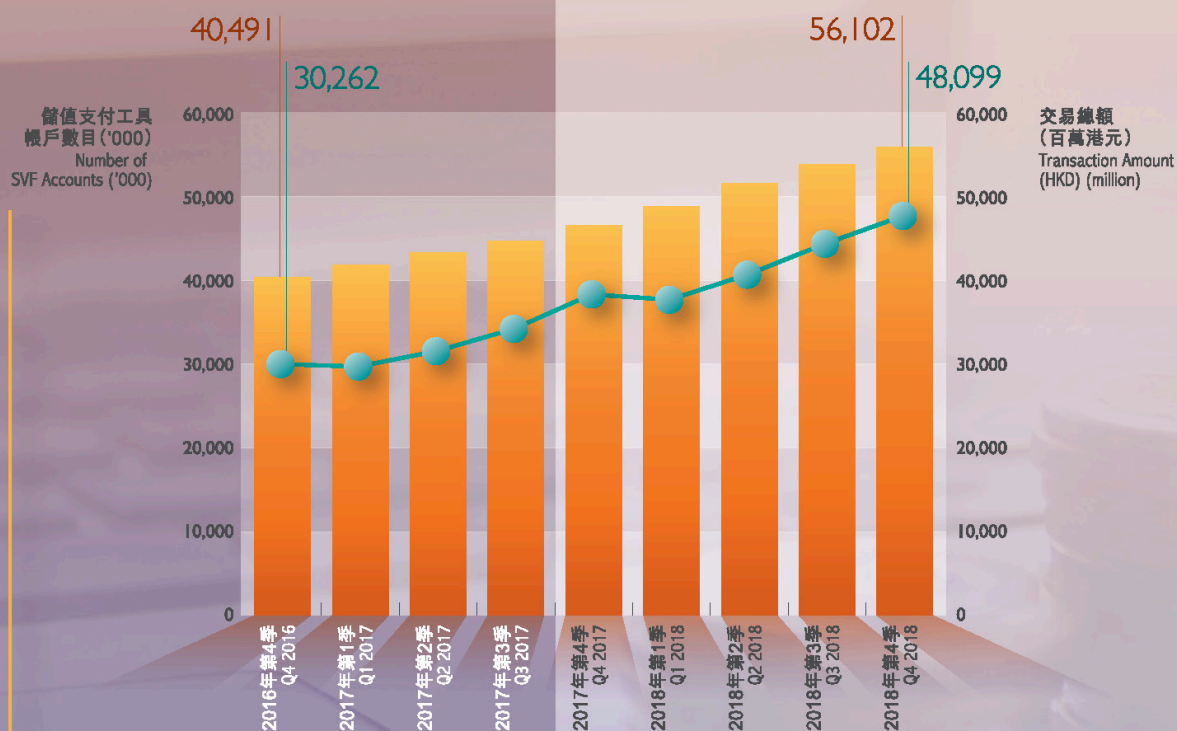


圖4：2016年第4季至2018年第4季的儲值支付工具帳戶總數，以及銷售點消費支付、網上消費支付和個人對個人轉帳之交易總額
Figure 4: Total Number of SVF Accounts and Total Amount of POS, Online Shopping and P2P Funds Transfer between Q4/2016 and Q4/2018

(資料來源：金管局) (Source: The HKMA)

儲值支付工具帳戶數目 ('000)
Total Number of SVF Accounts ('000)
交易總額 (百萬港元)
Total Amount of Transactions (HKD) (million)

下圖5至8闡釋銷售點消費支付、網上消費支付及個人對個人轉帳的交易量、交易額及其平均交易額。

The charts of the number of POS, online shopping and P2P funds transfer as well as their average transaction amounts are illustrated in figures 5-8 below.



銷售點消費支付是主要的交易方式，其交易總數由2016年第四季約14億，升至2018年第四季近15億。其2016年第四季至2018年第四季的平均交易額維持少於20港元。

The majority of transactions was POS, at about 1.4 billion in Q4 2016 and nearly 1.5 billion in Q4 2018 respectively. The average transaction amount remained less than HKD20 between Q4 2016 and Q4 2018.

網上消費支付 Online Payment

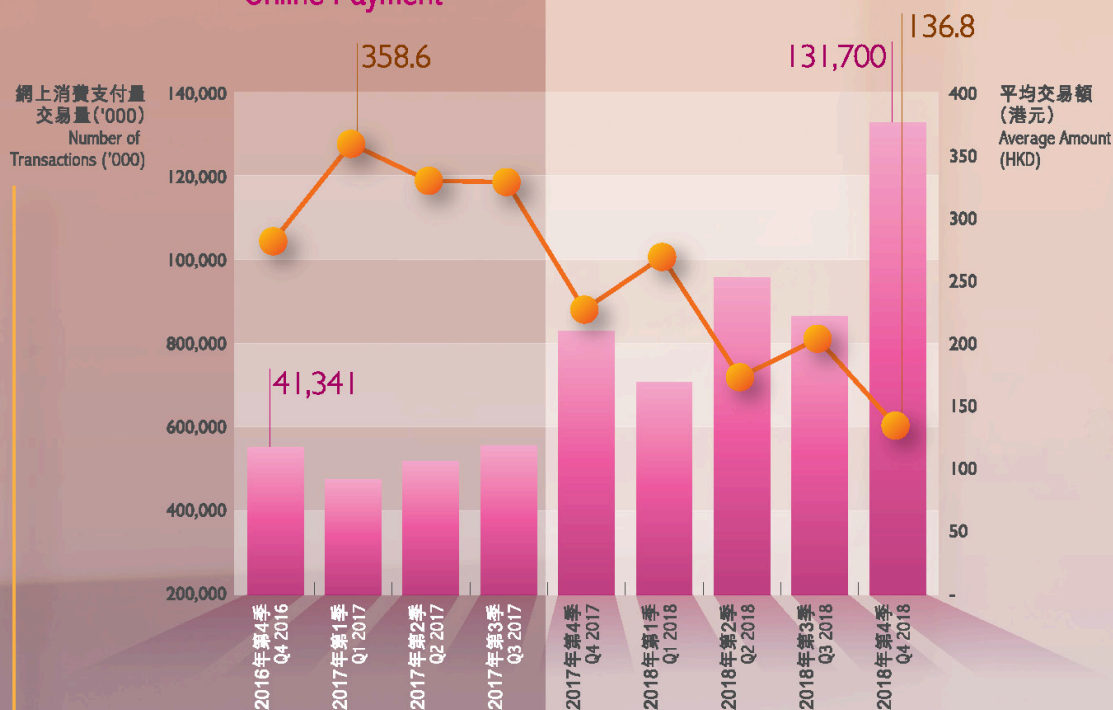


圖6：2016年第四季至2018年第四季網上消費支付量及其平均交易額

Figure 6: Number of Online Payment and its Average Amount between Q4/2016 and Q4/2018

(資料來源：金管局) (Source: The HKMA)

■ 網上消費支付交易量 ('000)
 Number of Online Payment Transactions ('000)
● 平均交易額 (港元)
 Average Amount (HKD)

網上消費支付的交易量由2016年第四季4,130萬增加至2018年第四季1億3,170萬 (+218.6%)。平均交易額出現緩步下降趨勢，在2018年第四季跌至約136.8港元。

The number of online payments increased from approximately 41.3 million in Q4 2016 to roughly 131.7 million in Q4 2018 (+218.6%). The average transaction amount showed gentle declining trend and reached about HKD 136.8 in Q4 2018.

個人對個人轉帳 P2P Funds Transfer

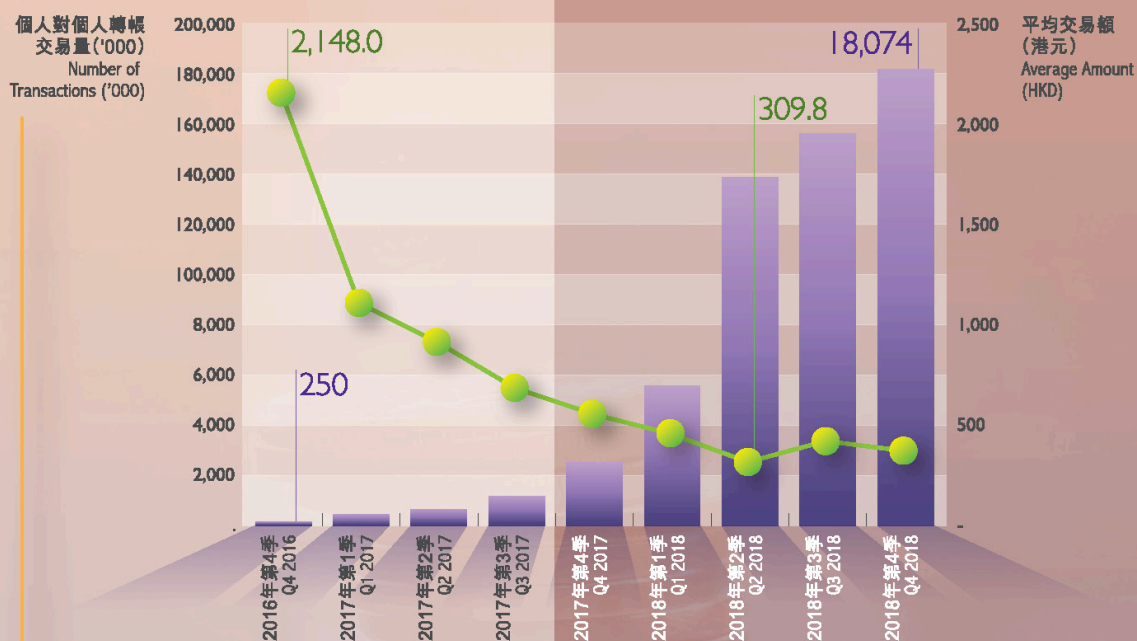


圖7：2016年第四季至2018年第四季的个人對个人轉帳交易量及其平均交易額

Figure 7: Number of P2P Funds Transfer and its Average Amount between Q4/2016 and Q4/2018

(資料來源：金管局) (Source: The HKMA)

個人對個人轉帳交易量 ('000)
Number of Online Payment Transactions ('000)

平均交易額 (港元)
Average Amount (HKD)

個人對個人轉帳的交易量由2016年第四季約25萬大幅增加至2018年第一季接近560萬(+2,126.4%)，並進一步急升至2018年第四季約1,810萬(比2016年第四季+7,129.6%)。相反，個人對個人轉帳的平均金額由2016年第四季的2,148港元下降至2018年少於500港元。

The number of P2P funds transfer increased drastically from about 250,000 in Q4 2016 to nearly 5.6 million in Q1 2018 (+2,126.4%). It further rocketed to around 18.1 million in Q4 2018 (+7,129.6% when compared with that of Q4 2016). On the contrary, the average P2P funds transfers amount dropped from HKD 2,148 in Q4 2016 to less than HKD 500 in 2018.

比較銷售點消費支付、網上消費支付和個人對個人轉帳在同期的平均交易金額，個人對個人轉帳的平均交易金額出現較大波幅，而金額比其他兩項亦較大。

When comparing the average transaction amount of POS, online payment and P2P funds transfer over time, it is observed that the average transaction amount of P2P funds transfer had a larger fluctuation and a higher value than that of others.

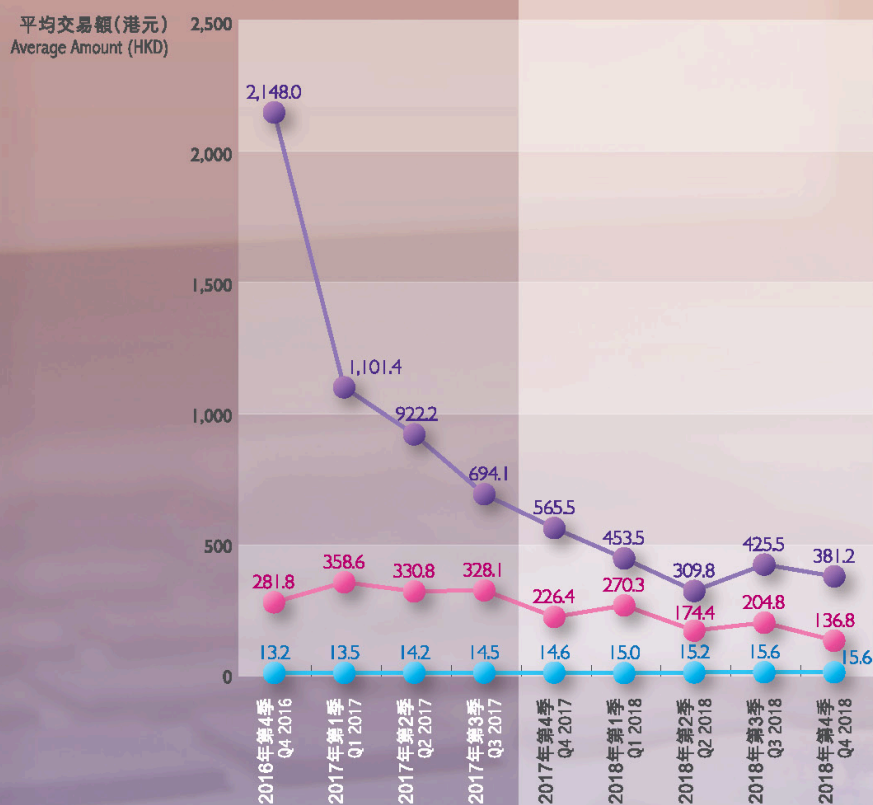


圖8：2016年第四季至2018年第四季的销售點消費支付、網上消費支付及個人對個人轉帳的交易平均金額

Figure 8: Average Amount of POS, Online Shopping and P2P Funds Transfer between Q4/2016 and Q4/2018

(資料來源：金管局) (Source: The HKMA)



5 儲值支付工具特點的分析

Analyses on SVF Features

不同的儲值支付工具持牌人推出不同特點的產品，以顧及各自的市場需要。本報告辨識數項特點，以及對其可能遭洗錢及恐怖分子資金籌集利用的脆弱性加以闡釋。

由於儲值支付工具產品之特點各具不同，本組並不建議以劃一方法去檢視其風險。以下列表只歸納重點，以供監管機構及儲值支付工具持牌人作參考。

As different SVF licensees have different features for their products to cater the needs of their own market segment, the Report has identified several features as well as their possible vulnerabilities of being exploited for ML/TF.

Taking into account the different features of SVF products, the JFIU does not suggest a “one-size-fits-all” solution. Instead, the summary only provides some pointers that may be useful to regulators and SVF licensees.

身份辨認和 資料核證的特點

一般而言，不同的儲值支付工具產品都設有不同的最高儲值額、年度交易限額和服務範圍，其客戶盡職審查級別亦會根據相關洗錢及恐怖分子資金籌集威脅的所需措施而相應調整。部分儲值支付工具產品不需進行客戶盡職審查（即「不具名」的儲值支付工具產品），而部分則需個人資料作登記以辨認帳戶的持有人（即「可辨認身份」的儲值支付工具產品⁵）。

Identification and Verification Features

Generally, maximum stored value, annual transaction amount and scope of services are different for SVF products. The level of CDD for different SVF products also varies according to the ML/TF mitigating measures required. Some SVF products require no CDD (i.e. “anonymous” SVF products) whilst some are registered with particulars that make the account holder identifiable (i.e. “identifiable” SVF products⁵).

⁵ 本報告中可辨認身份的儲值支付工具產品是指需要身份證明文件註冊登記之產品。

⁵ Identifiable SVF products in this Report refers to SVF products that registered with identity document.

表 1：身份辨認和資料核證的特點和已識別的風險
Table 1: Identification and Verification Features and Risks Identified

「不具名」 的儲值支付 工具產品 Anonymous SVF Products	所觀察的特點 Features Observed	已識別的風險 Risks Identified
	<ul style="list-style-type: none"> 沒有客戶盡職審查的要求。 CDD is not required. 	<ul style="list-style-type: none"> 雖然部分儲值支付工具產品不需客戶盡職審查，但其不具名性質可能會潛在洗錢及恐怖分子資金籌集的風險或阻礙罪案偵查。 Although by default some SVF products are not required to conduct CDD, the anonymity of those products may still pose some ML/TF risk or hinder crime detection.
	<ul style="list-style-type: none"> 部分只需流動電話號碼作登記。 Only mobile phone number suffices to register an SVF account. 	<ul style="list-style-type: none"> 至於以預付智能卡(即沒有以個人資料在電訊供應商登記的流動電話號碼)透過流動電話應用程式登記的儲值支付工具產品，或會用作隱藏帳戶持有人的身份。 SVF accounts that allow using prepaid SIM cards in registration, i.e. no personal information being registered with telecommunications provider, may be used to hide the account holder's identity. 雖然使用不具名儲值支付工具產品互相進行的交易金額偏低，並已受限制，但其交易不能被追蹤。 Transactions amongst anonymous SVF products, despite minimal or restricted amount on some occasions, could not be traced.
	<ul style="list-style-type: none"> 服務範圍和帳戶限額均受限制。 The scope of services and the account limit are restricted. 	<ul style="list-style-type: none"> 雖然儲值支付工具之帳戶已設限額，以減低洗錢及恐怖分子資金籌集風險，罪犯仍可將大額可疑資金分拆為多項小額交易或經多個不具名儲值支付工具產品進行交易。 Given that account limits are set for SVF products to mitigate ML/TF risk, culprits may still split a large amount of suspicious fund into lesser quantities for multiple transactions or make use of a large number of anonymous SVF products for transactions. 不具名帳戶的特性或會遭利用進行非法活動。 The anonymous nature of the account may be misused in illicit activities.

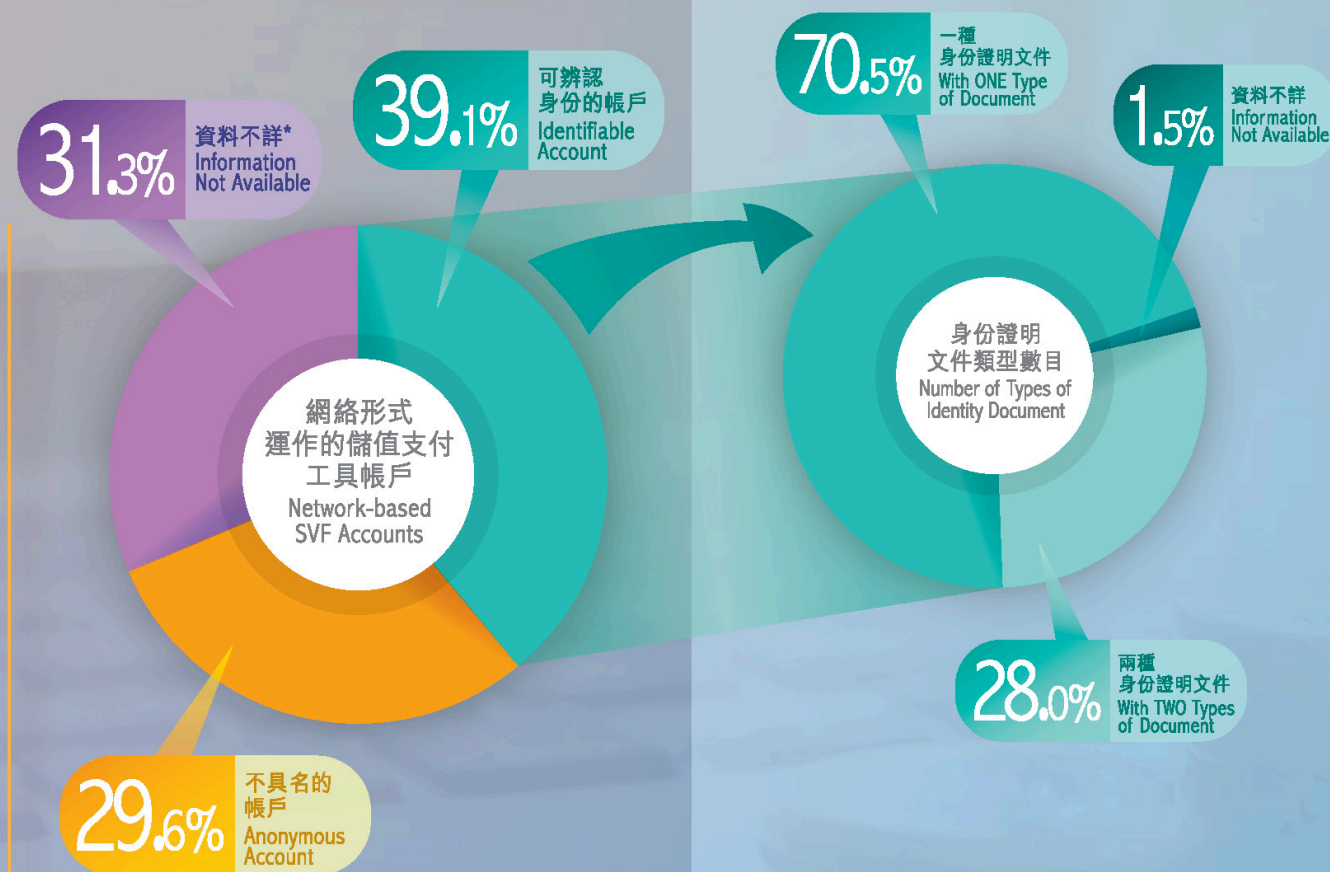
	<p>所觀察的特點 Features Observed</p>	<p>已識別的風險 Risks Identified</p>
<p>可辨認身份的儲值支付工具產品 Identifiable SVF Products</p>	<ul style="list-style-type: none"> • 所需身份資料取決於有關儲值支付工具產品的洗錢及恐怖分子資金籌集風險評估，從而按情況決定不同級別的客户盡職審查。 The identification information required depends on the ML/TF risk assessed on SVF products, and thus different level of CDD information is required accordingly. • 儲值支付工具持牌人在與客戶建立業務關係的過程中會辨認自然人客户的個人資料，並參考來源可靠和獨立的文件⁶、數據和資料，以核實客户身份。 SVF licensees may identify the customer (that is a natural person) by obtaining the personal particulars and verifying customer’s identity by reference to documents, data or information provided by a reliable and independent sources⁶ during on-boarding process. • 部分服務或需要客户綁定其銀行帳戶或信用卡，或獲取客户身份證明文件的副本作辨認和核證用途。 Some services may need to identify and verify the customer’s identity by binding the customer’s bank account or credit card, or by obtaining a copy of the customer’s identification document. • 身份證明文件可能經非親身方法(例如以傳真、電郵、流動應用程式等方式)遞交。 The identification document may be produced by non-face-to-face means (e.g. by fax, email, mobile applications, etc.). 	<ul style="list-style-type: none"> • 在開戶過程中以非親身方式遞交的身份證明文件、數據或資料或難以被核實其真偽。部分遞交作身份辨認和核證的文件可能是偽造、被報遭盜用或遺失的。罪犯或會以此假冒他人開設偽冒的儲值支付工具帳戶作非法用途。 The authenticity of the identification documents, data or information may not be easily ascertained through non-face-to-face means. Some documents submitted for identification and verification may be forged, reported stolen or lost. Culprits may then be able to set up bogus SVF account for illicit purposes.

⁶ 參考《打擊洗錢及恐怖分子資金籌集指引》(儲值支付工具持牌人適用) (2018年10月修訂版)，(a)政府機構；(b)金管局或任何其他有關當局；(c)在香港以外地方執行與金管局或任何其他有關當局職能相若的主管當局；或(d)金管局認可的任何其他可靠及獨立來源。

⁶ Referring to (a) a government body; (b) the HKMA or any other relevant authority (“RA”); (c) an authority in a place outside Hong Kong that performs functions similar to those of the HKMA or any other RA; or (d) any other reliable and independent source that is recognized by the HKMA, in the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Stored Valued Facility Licensees) revised in October 2018.

根據本組的情報⁷，所有在檢討期內的實體的儲值支付工具帳戶都是不具名的，即沒有客戶盡職審查的要求。至於以網絡形式運作的儲值支付工具帳戶，39.1%是可辨認身份的帳戶，而近29.6%的帳戶則是不具名的。在上述可識別帳戶中，70.5%的帳戶以一種的身份證明文件⁸進行身份驗證，而28.0%的帳戶以兩種身份證明文件作驗證。

Amongst JFIU's intelligence⁷, all device-based SVFs under review were anonymous, i.e. no CDD requirement imposed. For network-based SVF accounts, 39.1% were identifiable accounts whereas nearly 29.6% of such SVF accounts were anonymous. Amongst the aforesaid identifiable accounts, 70.5% of those accounts were registered with one type of document for identity verification⁸ whilst 28.0% were registered with two types of document.



* 沒有提供身份證明文件（例如只提供姓名）
* Particulars provided are not supported with ID document (eg. Only names are provided)

圖9：網絡形式運作的儲值支付工具帳戶
Figure 9: Network-based SVF Accounts

圖10：用於驗證可識別帳戶的身份證明文件類型數目
Figure 10: Number of Types of Identity Document Used for Verification for Identifiable Accounts

⁷ 在檢討期內本組共接收到943宗儲值支付工具產品有關的情報（其中119宗為實體形式的儲值支付工具及824宗網絡形式的儲值支付工具）

⁷ The JFIU's intelligence under the review period covered 943 SVF products (119 device-based and 824 network-based).

⁸ 文件類型包括香港身份證、旅行證件、香港及澳門居民的內地旅行證件，以及地址、職業、資金來源、商業登記等證明文件。

⁸ Types of document include Hong Kong identity card, travel document, Mainland travel permit for Hong Kong and Macau Residents, proof of address, occupation, source of fund, business registration, etc.

存入資金特點

各種儲值支付工具的存入資金特點有所不同。儲值支付工具可以單一或結合現金存款、銀行帳戶轉帳、綁定信用卡、個人對個人轉帳等方式進行增值。部分增值方法或會遭罪犯利用作非法活動。

Fund-In Features

The fund-in features of different SVF products vary. An SVF product may be topped-up in a single or a composite of cash deposits, bank account transfers, credit card binding, P2P funds transfers, etc. Some fund-in methods generate features that might be exploited by culprits for illicit activities.

表2：存入資金特點和已識別的風險

Table 2: Fund-In Features and Risks Identified

	所觀察的特點 Features Observed	已識別的風險 Risks Identified
現金存款 Cash Deposits	<ul style="list-style-type: none"> 在指定商戶/便利店/收銀車以現金增值。 Cash deposit at designated merchants stores/ convenience stores/ coin carts. 向指定商戶/ 便利店員工出示收款人的儲值支付工具二維碼⁹以存入現金。 Cash deposit by showing recipients' SVF Quick Response (“QR”) code⁹ to keepers of designated merchants stores/ convenience stores. 二維碼也可以用於個人對個人轉帳。 The QR code can also be used to facilitate P2P funds transfers. 	<ul style="list-style-type: none"> 如使用儲值支付工具的二維碼存入資金，存款者不需擁有儲值支付工具。罪犯或會利用其便利作收受犯罪得益。 The senders do not need to keep an SVF product for making payments if an SVF QR code is used, providing a convenient way for culprits to receive crime proceeds.

⁹ 一些儲值支付工具允許在進行交易時使用二維碼作為用戶標識，即透過掃描接收者的儲值支付工具二維碼以用於現金增值/個人對個人轉帳。

⁹ Some SVFs allow the use of QR code as user identification in making transactions, i.e. by scanning the recipient's SVF QR code to facilitate top-up with cash deposits/ P2P funds transfers.

	所觀察的特點 Features Observed	已識別的風險 Risks Identified
銀行帳戶 轉帳 Bank Account Transfers	<ul style="list-style-type: none"> 儲值支付工具用戶可設立直接扣帳授權服務綁定銀行帳戶以便使用。 (註：金管局於2018年10月已完成檢視和公布經优化的直接扣帳授權服務申請流程，並要求儲值支付工具營運商和銀行採納優化流程以提升用戶保障¹⁰。) By setting-up Direct Debit Authorization (“DDA”), SVF users are able to link their bank accounts with SVF products for subsequent usage. (Note: The HKMA has reviewed and published the refined process of electronic wallets users setting up direct debit authorisation (“eDDA”) in October 2018 and requested SVF operators and banks to adopt refined process to enhance user protection¹⁰.) 部分儲值支付工具持牌人利用自己的銀行帳戶接收資金為儲值支付工具帳戶增值。第三者可透過向儲值支付工具持牌人提供銀行收據（通過電子郵件/郵件/傳真等），為指定的儲值支付工具帳戶增值。 Some SVF licensees use their own bank accounts to receive funds for SVF account top-up. By producing bank receipts to the SVF licensees (by email/ mail/ fax, etc.), designated SVF accounts can be topped-up by third parties. 	<ul style="list-style-type: none"> 罪犯或會利用非法獲取的銀行帳戶資料/身份證明文件，以非親身方式申請直接扣帳授權服務。 Culprits may set up DDA by non face-to-face means using illegally obtained bank account information and identity document. 容許第三者通過儲值支付工具持牌人的銀行帳戶向儲值支付工具增值，可能會便利罪犯清洗犯罪得益。 Allowance of topping-up by third parties via depositing funds to SVF licensees’ bank accounts may facilitate culprits in laundering illicit funds.
綁定信用卡 Credit Card Bindings	<ul style="list-style-type: none"> 容許對儲值支付工具帳戶進行增值/ 個人對個人轉帳。 Top-up/ P2P funds transfers are allowed. 	<ul style="list-style-type: none"> 罪犯或會利用盜取得來的信用卡/ 卡資料綁定儲值支付工具帳戶，令真正的信用卡卡主蒙受損失。 Culprits may use stolen credit card/ its information for binding to SVF accounts and cause loss to the genuine credit card holder.
個人對個人 轉帳 P2P Funds Transfers	<ul style="list-style-type: none"> 接收來自儲值支付工具用戶的款項。 Receiving funds from SVF users. 	<ul style="list-style-type: none"> 如交易雙方涉及不具名儲值支付工具帳戶，追蹤個人對個人轉帳的款項將相當困難。 It is difficult to trace funds in P2P funds transfers amongst anonymous SVF accounts. 儲值支付工具帳戶或會利用作收受犯罪得益以進行非法活動。 SVF accounts may be misused to receive crime proceeds for illicit activities.

¹⁰ <https://www.hkma.gov.hk/eng/key-information/press-releases/2018/20181026-6.shtml>

轉出資金特點

與存入資金特點相若，部分儲值支付工具產品支援資金轉出功能，例如網上消費支付、銷售點消費支付，個人對個人轉帳等。雖然在日常消費中轉出資金的方法十分便利，但該些方法亦存有一定之脆弱度，可能使儲值支付工具成為轉移非法資金的洗錢途徑。

Fund-Out Features

Similar to fund-in features, some SVF products support fund-out features such as online payments, POS and P2P funds transfers, etc. Whilst the ways of fund-out are user-friendly in daily spending, those payment methods may be also vulnerable to make SVF as a vehicle in dissipating illicit funds in ML.

表3：轉出資金特點和已識別的風險

Table 3: Fund-Out Features and Risks Identified

	所觀察的特點 Features Observed	已識別的風險 Risks Identified
網上 消費支付 Online Payments	<ul style="list-style-type: none"> 用戶可利用已綁定之銀行帳戶/ 信用卡或儲存於儲值支付工具之資金經網上購物平台進行網上消費支付。 <p>Credit cards/ bank accounts bound or funds stored in SVF products can be used to settle online payments.</p>	<ul style="list-style-type: none"> 使用被盜用的儲值支付工具帳戶作網上購買高端產品或其他物品以作日後變賣。 Using compromised SVF accounts to settle online purchases of high-end products and realize them afterwards. 罪犯或會利用網上虛假商店把犯罪得益偽裝成正當的交易。 Culprits may make use of an online front shop to disguise proceeds of crime by making false trades using SVF accounts.
銷售點 消費支付 POS	<ul style="list-style-type: none"> 商戶店內消費支付（本地/ 海外）。 <p>In-store merchant payments (local/ overseas).</p>	<ul style="list-style-type: none"> 使用被盜用的儲值支付工具帳戶在商戶店內購買高端產品作日後變賣。 Using compromised SVF accounts to settle purchases of high-end products at in-store merchants and realize them afterwards.
個人對個人 轉帳 P2P Funds Transfers	<ul style="list-style-type: none"> 向儲值支付工具用戶傳送款項。 <p>Sending funds to other SVF users.</p>	<ul style="list-style-type: none"> 如交易雙方涉及不具名儲值支付工具帳戶，追蹤有關個人對個人的轉帳款項是相當困難。 It is difficult to trace funds in P2P funds transfers amongst anonymous SVF accounts. 儲值支付工具帳戶或會被用作傳送犯罪得益以進行非法活動。 SVF accounts may be misused to send crime proceeds for illicit activities.

	所觀察的特點 Features Observed	已識別的風險 Risks Identified
儲值支付工具帳戶和預付卡形式的儲值支付工具(屬同一持牌人)之間的轉帳 Funds Transfers between SVF Accounts and SVF Prepaid Cards (Under the Same Licensee)	<ul style="list-style-type: none"> 一些預付卡形式的儲值支付工具可經流動電話應用程式以儲值支付工具帳戶增值，反之亦然。 <p>Some SVF prepaid cards are reloadable by SVF accounts and vice versa via mobile application.</p>	<ul style="list-style-type: none"> 儲存在儲值支付工具帳戶的資金可輕易轉移至不具名的預付卡形式的儲值支付工具，反之亦然。 <p>Funds stored in SVF accounts could easily be transferred to anonymous SVF prepaid cards, and vice versa.</p>
海外匯款 Overseas Remittances	<ul style="list-style-type: none"> 由香港的儲值支付工具帳戶匯款至海外代理(例如：金融機構及現金提取點)，其後由海外收款人提取資金。 <p>Sending funds from SVF accounts in Hong Kong to designated overseas agents (e.g. financial institutions and cash pick-up points), for subsequent collection of funds by overseas recipients.</p>	<ul style="list-style-type: none"> 資金或會流向洗錢及恐怖分子資金籌集風險較高的司法管轄區。 執法機關進行海外調查時，資金難以追查。 <p>Funds may be channeled to other jurisdictions with higher ML/TF risk.</p> <p>It is difficult to trace funds during law enforcement agencies' investigation if an overseas jurisdiction is involved.</p>
銀行帳戶轉帳 Bank Account Transfers	<ul style="list-style-type: none"> 由儲值支付工具帳戶傳送款項至銀行帳戶。 <p>Sending funds from SVF accounts to bank accounts.</p>	<p>/</p>
提取現金 Cash Withdrawals	<ul style="list-style-type: none"> 在本地/ 海外自動櫃員機或指定商戶提取現金。 <p>Cash withdrawn at local/ overseas ATMs or designated merchants stores.</p>	<ul style="list-style-type: none"> 在海外自動櫃員機提取現金或會助長跨境洗錢，並使追蹤資金變得更困難。 預付卡形式的儲值支付工具所具備的可增值、可攜帶及不具名之特點或會被罪犯利用成現金的替代品作非法用途。 <p>Cash withdrawals at overseas ATM may facilitate cross-border ML and increase the difficulty in funds tracing.</p> <p>The reloadable, portable and anonymous features of SVF prepaid cards may be misused by culprits as an alternative to cash in illegal activities.</p>
預付卡形式的儲值支付工具或儲值支付工具帳戶後的退款 Refunds upon Termination of SVF Prepaid Cards or SVF Accounts	<ul style="list-style-type: none"> 在終止預付卡形式的儲值支付工具或儲值支付工具帳戶後退還現金。 <p>Refunds of cash upon termination of SVF prepaid cards or SVF accounts.</p>	<ul style="list-style-type: none"> 如不具名的預付卡形式的儲值支付工具被盜，其持有人未必是真正的用戶。 <p>Anonymous SVF prepaid card holders may not be the genuine users if the SVF prepaid cards are stolen.</p>

6 類型學分析 Typologies Analyses

根據本組對不同儲值支付工具特點的研究和財富情報的檢視，現整理出一系列涉及儲值支付工具服務之案例，讓儲值支付工具業界可偵查及防止洗錢或其他不合法活動，旨在協助監管機構制訂相關政策及指引，以及提升執法人員之整體能力及作情報分享之用。

From the JFIU's studies on the features of various SVF services and review on its financial intelligence, an assortment of scenarios involving SVF services are collated for SVF sector to detect/ prevent of ML or other illicit activities. The observations and remarks from the JFIU are intended to assist in the formulation of relevant policy/ guidelines by regulators and for capacity building/ intelligence sharing amongst law enforcement officers.

1 使用數據機池登記大量不具名儲值支付工具帳戶作非法用途 Use of Modem Pool to Register Anonymous SVF Accounts in Bulk for Illicit Purposes

案例
Scenario

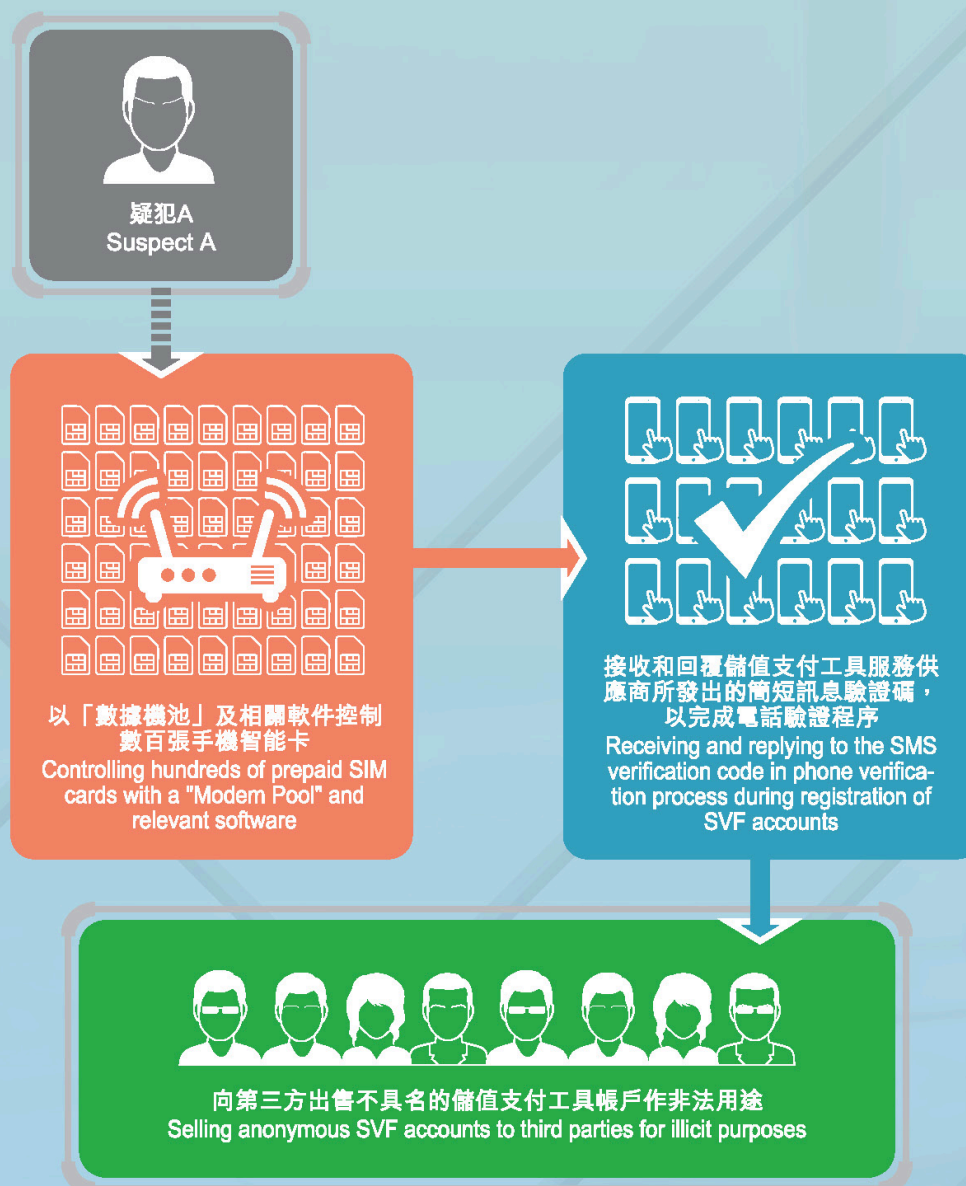
「數據機池」是一組模擬數據機及軟件，允許連接大量智能卡，並控制這些智能卡的數據活動，例如：傳統的語音通話服務、短訊服務、互聯網數據服務。數據機池近期常誤用作登記儲值支付帳戶的工具。

疑犯A購買數百張手機智能卡，並把卡插入數據機池，用來在登記儲值支付工具帳戶時接收和回覆短訊驗證碼，以完成大量帳戶的電話驗證程序。然而，這種登記並不需提供個人資料。該些以手機智能卡登記的不具名儲值支付工具帳戶其後被轉售予第三方作非法用途。

“Modem Pool”, a group of analog modems and software allowing multiple connection of SIM cards and controlling data flow such as traditional voice call service, SMS service, internet data service of those SIM cards, has recently been misused for SVF account registration.

Suspect A purchased several hundreds of prepaid SIM cards and inserted them into the Modem Pool to receive and reply to the SMS verification code in phone verification process during registration of SVF accounts that are without CDD requirement. Those anonymous SVF accounts were then resold to third parties for illicit purposes.

案例1 使用數據機池登記大量不具名儲值支付工具帳戶作非法用途 Scenario 1 Use of Modem Pool to Register Anonymous SVF Accounts in Bulk for Illicit Purposes



本組的觀察

- 雖然利用數據機池和相關的軟件連接多張手機智能卡並非違法。然而，在短時間內登記大量不具名儲值支付工具帳戶的用途值得關注。
- 登記這些帳戶的其中一個目的，可能是利用新登記儲值支付工具帳戶的不具名特性進行非法活動。

JFIU's Observations

- While the application of Modem Pool and relevant software for multi-SIM card connection is not illegal, the purpose of using such in registration of a large number of anonymous SVF accounts is worthy of attention.
- The possibility that anonymity of the newly registered SVF accounts is being used in illicit activities cannot be ruled out.

案例
Scenario

2

偽冒身份/ 未經授權使用個人資料作欺詐交易/ 付款 Impersonation/ Unauthorized Use of Personal Data for Fraudulent Transactions/ Payments

儲值支付工具帳戶持有人綁定其信用卡和/ 或銀行帳戶以支付消費乃屬平常，但罪犯或會濫用該服務而利用盜取得來的信用卡或銀行帳戶的資料進行未獲授權的交易。

受害人並不察覺遺失了信用卡，直至她收到發卡銀行的月結單上有多項未經授權的交易。疑犯B以非法途徑盜用受害人的信用卡，假冒受害人，並以她的名義開設儲值支付工具帳戶。疑犯B進一步把受害人的信用卡綁定至該儲值支付工具帳戶。（在某些情況，罪犯會先入侵受害人用作登記儲值支付工具的電郵帳戶，取得受害人的儲值支付工具帳戶控制權後，再以預先綁定的信用卡作非法用途。）

Whilst it is common for SVF account holders to link own credit cards and/ or bank accounts for making payments, culprits may impersonate the account users to conduct unauthorized transactions by using information of stolen credit cards or bank accounts.

A victim did not realize she had lost her credit card until she received monthly statement from the issuing bank and noted some unauthorized transactions. Suspect B, who inappropriately obtained the victim's credit card, impersonated the victim to open an SVF account and further linked her credit card to the SVF account. (In some cases, victim's email account, which was used for SVF account registration, was found hacked by culprits in the first place in order to gain control of victim's SVF account and use the pre-linked credit card for illicit use.)

疑犯B繼而購買高端產品/ 現金禮券/ 遊戲點數，並以已綁定的受害人的信用卡作支付，所買貨品及後運往在司法管轄區W的疑犯C（疑犯B的同黨）。疑犯B亦會從受害人的信用卡提取資金作個人對個人轉帳、增值及銀行提款方法（如使用預付卡形式的儲值支付工具，則會透過取消卡進行退款）。

除以上案例外，罪犯或會利用非法得來的受害人信用卡資料綁定儲值支付工具帳戶作非法用途。同時，部分金融機構接受自動增值服務的申請（利用申請人之信用卡資料為預付形式的儲值支付工具增值）。罪犯或會利用卡主的個人及信用卡資料申請該服務令卡主蒙受損失。

除信用卡外，部分罪犯或會在受害人不知情的情況下，不當地利用受害人的銀行帳戶資料，申請直接扣帳授權服務。

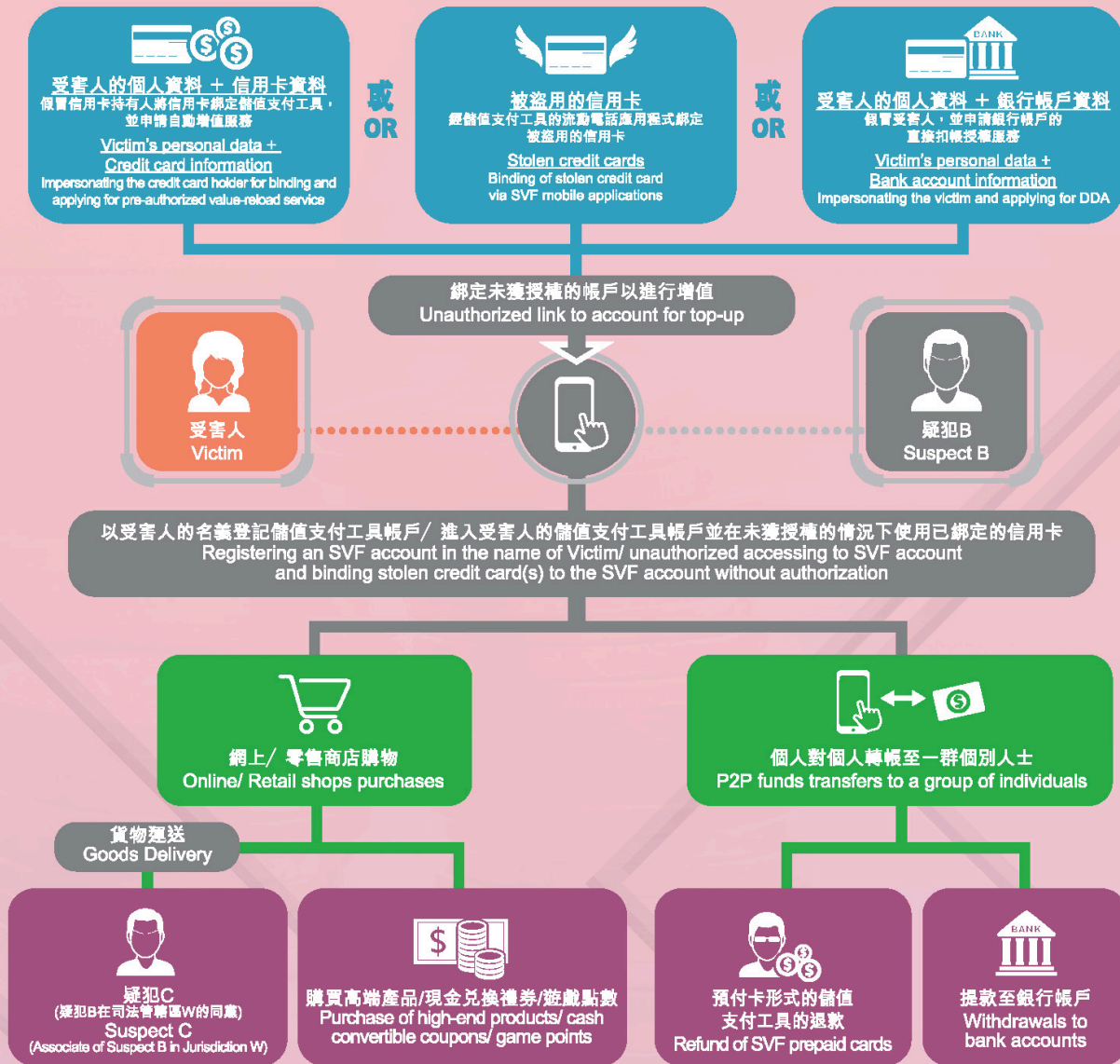
Suspect B then made purchases of high-end products/ cash coupons/ game points and settled payments through victim's linked credit card. The goods purchased were delivered to Suspect C (the associate of Suspect B) in Jurisdiction W. It is also noted that Suspect B would transfer funds that were withdrawn from victim's credit card to his associates via P2P funds transfers or top up the SVF account with victim's credit card for further bank withdrawals (or card refund if funds were transferred to a SVF prepaid card).

Apart from the above scenario, it is observed that culprits may use illegally obtained credit card information to bind an SVF account for illegitimate purpose. It is also noted that some financial institutions accept the application of pre-authorized value-reload service (i.e. reloading credit to SVF prepaid cards by using applicant's credit card information). Culprits may apply for such service by providing illegally obtained credit card information with card holder's personal particulars, causing loss to the genuine credit card holder.

Other than credit card, some culprits may inappropriately use bank account information in the name of victim without his/ her knowledge and set up DDA in SVF accounts.

案例2 偽冒身份/ 未經授權使用個人資料作欺詐交易/ 付款

Scenario 2 Impersonation/ Unauthorized Use of Personal Data for Fraudulent Transactions/ Payments



本組的觀察

- 以銀行帳戶及/ 或信用卡綁定儲值支付工具帳戶是辨認儲值支付工具用戶身份的其中一種方法。然而，如用作綁定的資料有誤，而未有穩健的核證方法，綁定帳戶之舉或會造成一定風險，讓罪犯有機可乘。
- 罪犯一旦成功把盜用的信用卡/ 被盜信用卡的資料綁定至儲值支付工具帳戶，便可濫用作支付交易。
- 同時，罪犯或會入侵受害人的電子郵件帳戶，以取得受害人的儲值支付工具帳戶的控制權。
- 當受害人的信用卡/ 銀行帳戶被罪犯綁定了儲值支付工具帳戶，資金可經以下途徑轉移：(i) 個人對個人轉帳、(ii) 購買貨物作變賣或運送到海外、(iii) 退款及/ 或 (iv) 提款至銀行帳戶。

(註：於2018年10月，金管局已加強電子直接扣帳授權服務的認證要求。)

JFIU's Observations

- Binding of bank account and/ or credit card to SVF account is a way of identification of SVF users. However, if the information used for binding is tainted and there is no verification for such, the binding itself may provide possible risks for culprits to commit crime.
- Stolen credit card/ information of stolen credit card, once successfully linked to an SVF account by culprits, could be misused in making payment transactions.
- It is also noted that culprits may hack the email account of victims before gaining control of their SVF accounts.
- Once victim's credit card/ bank account is linked to an SVF account (under culprits' control), funds could be dissipated via (i) P2P funds transfers, (ii) purchase of goods for subsequent realization or shipping overseas, (iii) top-up followed by refund and/ or (iv) bank withdrawals.

[Note: In October 2018, the HKMA has strengthened the verification requirements for eDDA.]

案例
Scenario

3

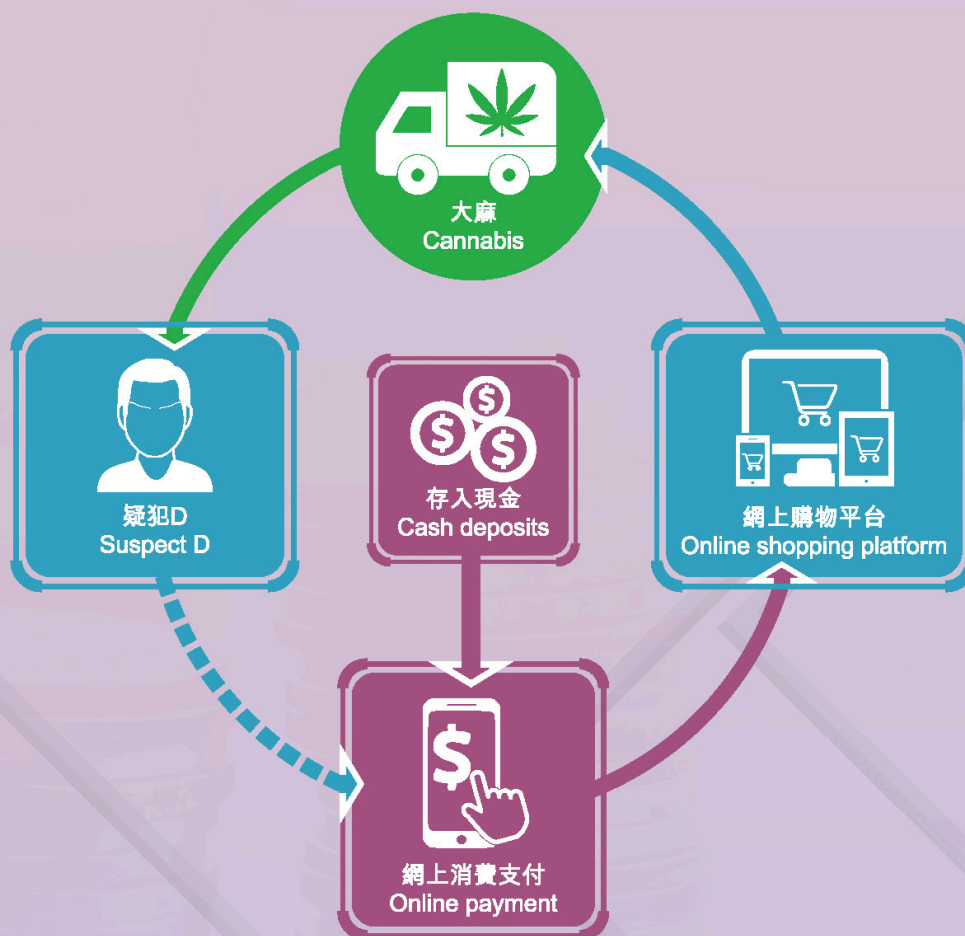
使用儲值支付工具帳戶在網上平台購買非法物品 Use of SVF Accounts for Purchase of Illegal Goods on Online Platform

疑犯D居於香港，是一個不具名儲值支付工具帳戶的持有人。疑犯D將現金存入儲值支付工具帳戶後，到訪海外網上商店購買大麻。疑犯D雖知悉大麻在香港並非合法，但他仍使用其儲值支付工具帳戶進行訂購和付款。大麻其後送付香港的疑犯D。

Suspect D is an anonymous SVF account holder living in Hong Kong. Having deposited cash into his SVF account, Suspect D visited an overseas online shop for cannabis. Knowing that cannabis was illegal in Hong Kong, Suspect D placed orders and made payments through his SVF account. The cannabis was then delivered to Suspect D in Hong Kong.

案例3 使用儲值支付工具帳戶在網上平台購買非法物品

Scenario 3 Use of SVF Accounts for Purchase of Illegal Goods on Online Platform



本組的觀察

- 同一運作模式亦見於購買製造危險藥物的原材料、電子煙、冒牌物品或兒童色情物品。
- 使用不具名儲值支付工具帳戶在海外網上平台支付非法物品，有礙執法機關的偵查工作。

JFIU's Observations

- The same modus operandi (“MO”) is also observed in the purchase of ingredients for manufacturing dangerous drugs, e-cigarettes, counterfeit goods or child pornographic materials.
- The use of anonymous SVF accounts for online payments of illegal goods on overseas online platforms could hinder detection by law enforcement agencies.

案例
Scenario

4

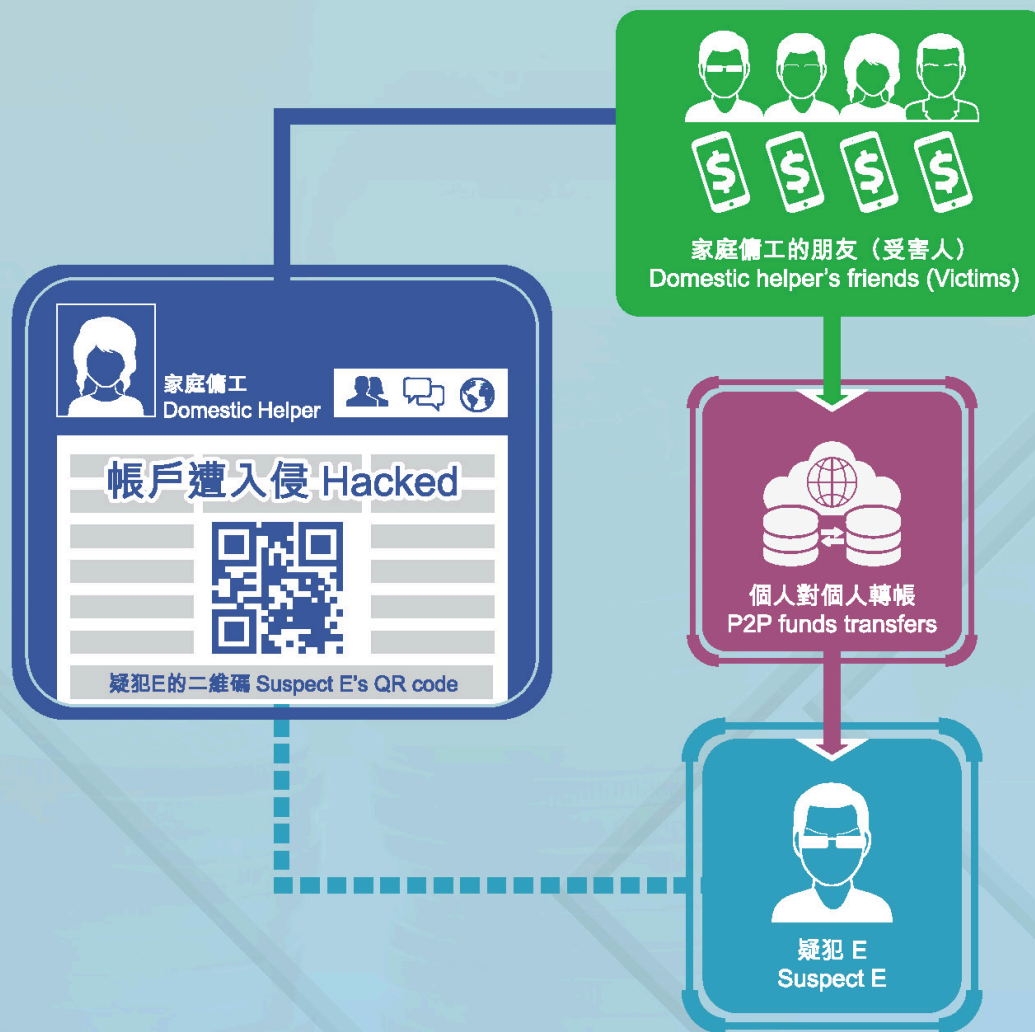
詐騙案—入侵社交媒體帳戶，透過儲值支付工具帳戶收受資金 Hacking Social Media Accounts and Receiving Funds via SVF Accounts

司法管轄區Y的一名家庭傭工是社交媒體平台的用戶。該家庭傭工的社交媒體帳戶遭疑犯E入侵並上載疑犯E之儲值支付工具帳戶的二維碼。疑犯E假冒為該家庭傭工並訛稱因急事需要經濟援助，要求該家庭傭工的朋友提供財政支援。該家庭傭工的友人不虞有詐，掃描疑犯E的二維碼（聲稱是該家庭傭工的），並進行個人對個人轉帳。

A domestic helper of Jurisdiction Y is a user of a social media platform whose account was hacked by Suspect E. A QR code of Suspect E's SVF account was uploaded to the compromised social media account, falsely claiming that the domestic helper was in financial need for urgent matter and requesting financial assistance from friends of that domestic helper. Her friends complied and scanned Suspect E's QR code (purported to be domestic helper's) for P2P funds transfers.

案例4 詐騙案—入侵社交媒體帳戶，透過儲值支付工具帳戶收受資金

Scenario 4 Hacking Social Media Accounts and Receiving Funds via SVF Accounts



本組的觀察

- 當個人社交媒體帳戶用戶所設定的保安措施不足時，其帳戶便容易遭入侵。
- 家庭傭工常以社交媒體平台與朋友和家人溝通。罪犯或會利用該等平台的流通及普遍性，入侵家庭傭工的帳戶，並向該家庭傭工之相識人士（潛在的受害人）索取金錢。
- 部分家庭傭工因忙於處理家務，或未能即時被聯絡上，其友人或會在未能核實情況下直接傳送資金。
- 罪犯以儲值支付工具二維碼索取金錢的訊息，一旦上載至社交媒體平台，便可在帳戶持有人的朋友間廣傳。此舉可同時令多名受害人被騙。

JFIU's Observations

- Hacking of personal social media accounts is not uncommon when users' security measure setting is not adequate.
- Social media platforms are common amongst domestic helpers for communication between friends and families. Culprits may make use of the broad usage of such platforms and hack the accounts of domestic helpers in order to solicit funds from acquaintances (potential victims).
- Some domestic helpers could not be contacted immediately if they are engaging in household duties. Their friends may simply send funds without further clarification.
- The message for soliciting funds with culprit's SVF QR code could spread widely amongst account holder's friends once being uploaded onto the social media platform. It could attract multiple victims at the same time.

案例
Scenario

5

使用預付卡形式的儲值支付工具，在海外自動櫃員機提取現金作洗錢

Use of SVF Prepaid Cards to Withdraw Cash at Overseas ATMs for ML

部分預付卡形式的儲值支付工具因可透過現金存款和銀行轉帳而預先儲值，以及世界各地的商戶和自動櫃員機的認受性，而愈趨普遍。

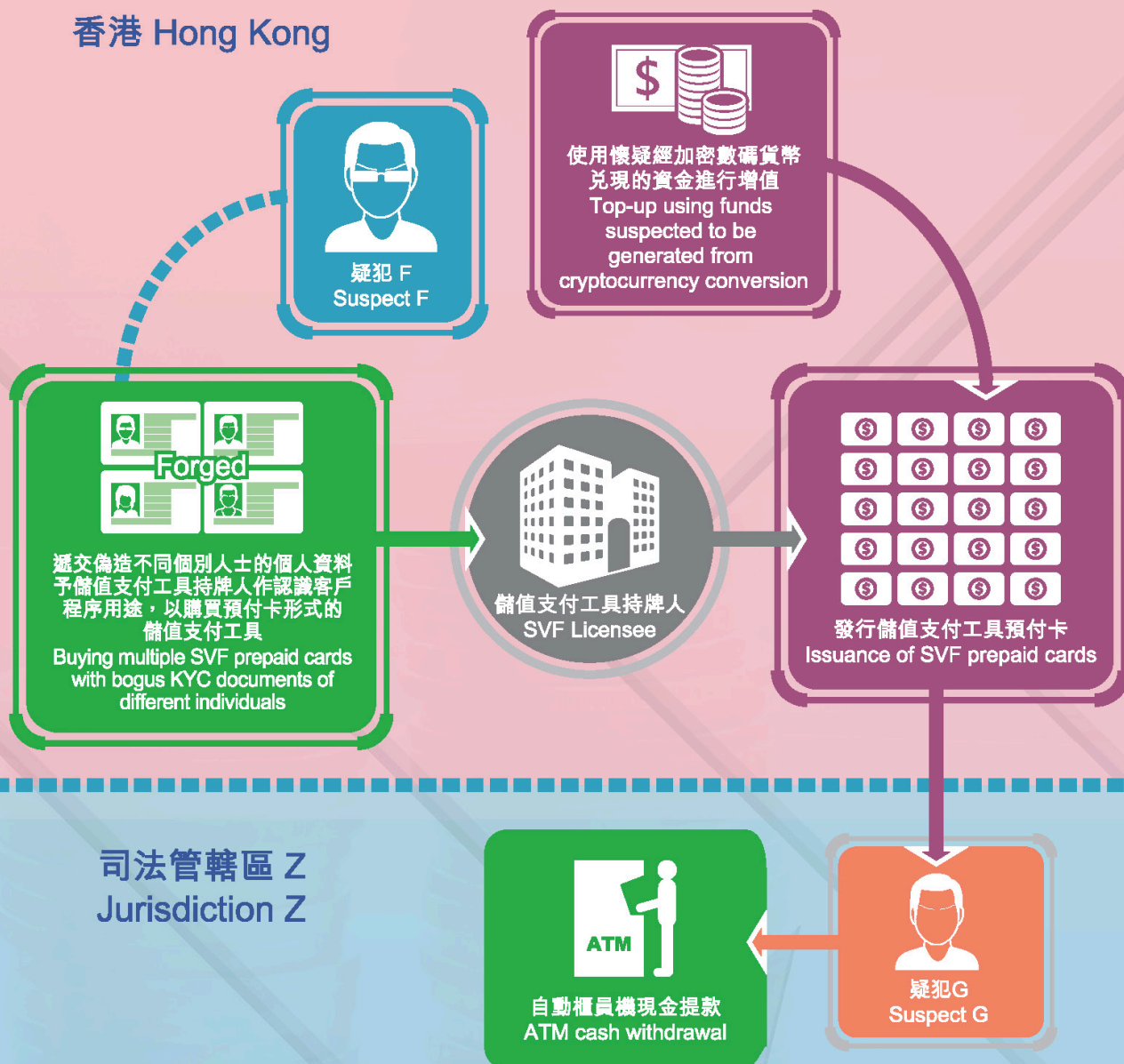
疑犯F使用大量預付卡形式的儲值支付工具作洗錢。他偽造不同個別人士的身份證明文件及住址證明，申請大量預付卡形式的儲值支付工具，以供相關儲值支付工具的持牌人作核實客戶程序用途。當申請獲批後，該些預付卡形式的儲值支付工具獲加密數碼貨幣相關行業的公司增值大額資金，並送付疑犯F在司法管轄區Z的同黨疑犯G。在政治不穩而貪污率高的司法管轄區（例如司法管轄區Z），這些預付卡形式的儲值支付工具被多次從自動櫃員機內提取現金。

Some SVF prepaid cards are gaining popularity for its versatility of being able to preload funds via cash deposits and bank transfers as well as wide acceptance of merchants stores and ATMs worldwide.

Suspect F was suspected of using large quantity of SVF prepaid cards as a vehicle of ML by submitting bogus know-your-customer (“KYC”) documents such as identity documents and address proofs of different individuals to the issuing SVF licensee for SVF prepaid cards application. Once approved, those SVF prepaid cards would be topped-up with large amount of funds sent from a company in cryptocurrency-related business. Those SVF prepaid cards were then sent to Suspect F’s associate, Suspect G, in Jurisdiction Z. Multiple ATM cash withdrawals were observed from locations often associated with politically unstable jurisdictions with high corruption rate (e.g. Jurisdiction Z).

案例5 使用預付卡形式的儲值支付工具，在海外自動櫃員機提取現金作洗錢

Scenario 5 Use of SVF Prepaid Cards to Withdraw Cash at Overseas ATMs for ML



本組的觀察

- 因加密數碼貨幣的資金來源及目的地不容易被追蹤，屬高風險的洗錢及恐怖分子資金籌集的工具。
- 偽造的身份證明文件及住址證明用作申請預付卡形式的儲值支付工具，以隱藏罪犯身份。
- 部分預付卡形式的儲值支付工具易於攜帶，全球通用。當它們預先儲值（非法資金），便可於其他具較高洗錢及恐怖分子資金籌集風險的司法管轄區，經自動櫃員機提取現金。

IFIU's Observations

- Cryptocurrency is considered high risk in ML/TF where the source and the destination of fund could not be easily traced.
- Forged identity documents and address proofs could be used in applying SVF prepaid cards with a view to hiding the culprit's identity.
- Some SVF prepaid cards are portable and usable worldwide. Once those SVF prepaid cards are preloaded with illicit funds, they can be used in other jurisdictions with serious AML/CFT deficiencies, for subsequent funds withdrawals at ATMs thereat.

聯合財富情報組出版
Published by the Joint Financial Intelligence Unit

聯合財富情報組 Joint Financial Intelligence Unit
電話 Tel : (852) 2866 3366
傳真 Fax : (852) 2529 4013
電郵 E-mail : jfiu@police.gov.hk
郵遞 Mail : 香港郵政總局信箱 6555 號
GPO Box 6555 Hong Kong

© 版權屬香港特別行政區政府所有
© Copyright reserved