聯合財富情報組年報 2018

Joint Financial Intelligence Unit Annual Report 2018

Joint Financial Intelligence Unit
聯合財富情報組

抱負及使命

抱負

保持聯合財富情報組在亞太區內其中一個主要的財富情報單位的領先地位

使命

聯合財富情報組致力協助政府保護香港免受清洗黑錢及恐怖分子資金籌集等非法活動的影響，方法包括：

致使聯合財富情報組的專業標準與相關的國際標準接軌

在交換財富情報方面與本地及國際機構加強合作

對接收的可疑交易報告進行精細分析並且適時發布

加強相關業界對清洗黑錢及恐怖分子資金籌集問題的意識及了解

VISION AND MISSION

Vision

That the Joint Financial Intelligence Unit (JFIU) remains one of the leading Financial Intelligence Units (FIUs) in the Asia/Pacific Region

Mission

That the JFIU continues to assist the Government in its efforts to protect Hong Kong from illicit activities of money laundering (ML) and terrorist financing (TF) by:

Juxtaposing the JFIU's professional standards with relevant international standards

Fostering and strengthening cooperation with local and international agencies in the exchange of financial intelligence

Intelligently analyzing suspicious transaction report (STR) received by the JFIU and making disseminations as appropriate

Upgrading relevant sectors' awareness and understanding of ML and TF issues

TABLE OF CONTENTS
目錄

1

聯合財富情報組
主管序言

MESSAGE FROM THE HEAD OF JFIU

2018年是聯合財富情報組，以及打擊洗錢及反恐籌資在本港發展的重要里程碑。打擊清洗黑錢財務行動特別組織（特別組織）順利完成對香港進行的第四輪相互評核，使香港的制度符合特別組織制訂的最新國際標準，藉以加強香港打擊洗錢及恐怖分子資金籌集活動的監管制度。此外，《打擊洗錢及恐怖分子資金籌集條例》（第615章）亦引入信託或公司服務提供者新發牌制度，規定有關服務提供者須向公司註冊處處長申請牌照。同時，所有香港公司（上市公司除外）須確定並保存實益擁有權的最新資料，以備存「重要控制人登記冊」。我深信各項嶄新措施都能提升香港作為可靠國際金融中心的公信力。

洗錢、恐怖分子資金籌集以至大規模毀滅武器擴散資金籌集皆日趨複雜，調查工作相當艱巨，而我們亦在這場硬仗遇上重重挑戰。年內，我樂見聯合財富情報組擴展人手編制及架構，以迎戰未來。2018年，國際財富情報交換的數字再刷下新記錄，高達2,646次，而全年的可疑交易報告數量則於十年內首次下跌（由2017年的92,115宗減至2018年的73,889宗）。數字下降反映舉報單位、監管機構，以及聯合財富情報組共同努力，積極採取審慎措施填報可疑交易報告，以改善報告質素。我希望藉此機會衷心向監管機構、專業團體、執法機關、金融機構，以及指定非金融企業及行業表達謝意，感謝各單位支持，充分利用可疑交易舉報的現行機制。

The year of 2018 could be seen as a landmark for both the JFIU and the Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) developments in Hong Kong. Apart from the 4th round of Financial Action Task Force (FATF) Mutual Evaluation (ME) on Hong Kong to align with the latest international standards set by the FATF and to enhance Hong Kong's regulatory regime for combating ML and TF, a new licensing regime for trust or company service providers (TCSPs) has been introduced under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) to require TCSPs to apply for a license from the Registrar of Companies. In addition, all Hong Kong companies (except listed companies) are required to ascertain and maintain up-to-date beneficial ownership information by way of keeping a Significant Controllers Register. I am confident that all these new measures will further enhance Hong Kong's credibility as a trusted international financial centre.

In face of the multi-faceted challenges along the uphill battle against increasingly complex ML, TF and proliferation financing, I am also delighted to see the expansion of JFIU's manpower and structure in 2018 to rise up those challenges. On the other hand, despite the number of international financial intelligence exchanges continued reaching another record high of 2,646 in 2018, the annual figures of STRs experienced the first drop (from 92,115 in 2017 to 73,889 in 2018) over the past decade. This is a reflection of concerted effort paid by reporting entities, regulatory authorities and the JFIU to take prudence measures in filing of STR and to improve its quality. I would like to take this opportunity to express my gratitude towards the continuous support from regulatory authorities , professional bodies, law enforcement agencies (LEAs.), financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) in capitalizing the existing suspicious transaction reporting framework.

洗錢及恐怖分子資金籌集活動屬跨國性質，極需國際合作抗衡該等威脅。香港向來不遺餘力與世界各地的財富情報單位交換財富情報及保持國際合作關係，為展示本港的決心，我在2018年繼續擔任埃格蒙特金融情報組織（埃格蒙特組織）亞太區代表和埃格蒙特委員會會員。聯合財富情報組依舊積極參與國際打擊洗錢及反恐籌資社區的活動，並珍視與各地同業交換的財富情報，這使我們的調查工作更見成效，以助截獲非法資金和偵查刑事罪行。

儘管我們有最優良的法律打擊清洗黑錢，亦有最完善的制度檢控違例人士，但若果欠缺人才施行有關法律和制度，我們所付出的努力也只徒然。正因如此，財富調查訓練和打擊洗錢及反恐籌資的外展計劃非常重要，可加強公私營機構執法人員和打擊洗錢及反恐籌資執業者的專門知識。培訓人才是聯合財富情報組的主要職責之一，我們會繼續與打擊洗錢及反恐籌資的本地持份者，以及全球合作伙伴共同提升能力。

正所謂「水往低處流」，罪犯亦往往取易捨難，尋找最簡單的途徑清洗他們的犯罪得益。現今科技發展迅速，罪犯洗錢的方法愈趨複雜，而由於全球金融業的科技進步，犯罪得益可在不同司法管轄區迅速轉移，過程便捷。香港的打擊洗錢及反恐籌資制度穩健，有賴公私營機構緊密合作，確保香港是個安全廉潔的營商地點。2019年，聯合財富情報組會保持強大的發展動力，致力提升香港打擊洗錢及反恐籌資制度的成效。

香港聯合財富情報組主管
周志鈞警司

ML and TF activities are by nature transnational and countering those threats call for international cooperation. With a view to exhibiting Hong Kong's persistent effort and commitment in financial intelligence exchange and international cooperation with FIUs worldwide, my role as the representative of the Asia and Pacific region of the Egmont Group of Financial Intelligence Units (Egmont Group) and the Egmont Committee member continues in 2018. The JFIU remains actively involved in the activities of international AML/CFT community and treasures the exchange of financial intelligence with our worldwide counterparts, which greatly facilitate investigations, resulting in the interception of illicit funds and detection of crimes.

We can have the best laws to combat ML, the best system to prosecute the offenders but if we lack the human capacity to implement them, then our efforts will be in vain. Hence, financial investigation training and AML/CFT outreach programmes are of great importance in strengthening specialized knowledge of law enforcement officers and AML/CFT practitioners in public and private sectors. This is one of the key activities of JFIU and we will continue to contribute to the capacity building with all AML/CFT stakeholders in Hong Kong as well as with worldwide partners.

Like water which will find its way to the lowest possible level, criminals always find the easiest spot through which to launder their criminal proceeds. In this time of technological advances, criminals are more sophisticated in ML and moving crime proceeds across different jurisdictions become more rapid and convenient, particularly with the technology advancement in the global financial sector. The robustness of AML/CFT regime in Hong Kong requires both public and private sectors to work in close partnership to ensure that Hong Kong is a safe and clean place for doing business. In 2019, the JFIU will keep up the strong momentum of development and dedicate to strengthening the effectiveness of the Hong Kong AML/CFT regime.

Edwin CHOW
Superintendent of Police
Head of JFIU, Hong Kong

2

ABOUT THE JFIU

聯合財富情報組

本組角色

聯合財富情報組由香港警務處及香港海關人員組成。本組屬執法型財富情報單位，而非調查單位。本組是負責管理本港可疑交易舉報機制的唯一機構，並與世界各地的財富情報單位及執法機關交換財富情報。

本組與不同機構通力合作，憑藉其情報分析能力和觀點，為本港的打擊洗錢及恐怖分子資金籌集制度出一分力。我們的合作伙伴，包括政府決策局及部門、金融監管機構及其他專業團體、執法機關及財富情報單位、洗錢及恐怖分子資金籌集風險評估小組，以及金融機構及指定非金融企業及行業。

Our Role

The JFIU is co-staffed by officers of the Hong Kong Police Force (HKPF) and the Hong Kong Customs and Excise Department (C&ED). It is a law-enforcement-type of FIU but not an investigative unit. Apart from being the sole agency to manage the suspicious transaction reporting regime for Hong Kong, it also engages in financial intelligence exchange with FIUs and Law Enforcement Agencies (LEAs) worldwide.

Distinctive in its intelligence analysis capabilities and perspectives, the JFIU contributes to the AML/CFT regime through close inter-agency collaboration with policy bureaux and government departments, financial regulators and other professional bodies, LEAs and FIUs, ML and TF Risk Assessment Unit (RAU), FIs and DNFBPs.

本組職責

本組因應對內和對外持續進行的風險評估，履行廣泛職務，銳意打擊和防範洗錢、相關的上游罪行及恐怖分子資金籌集。有關職務列舉如下：

- 就可疑交易報告進行行動分析
- 與世界各地交換財富情報及資訊
- 就財富情報及其他資訊進行策略分析
- 就洗錢及恐怖分子資金籌集活動趨勢和類型學進行研究
- 運作可疑交易報告管理系統(STREAMS)
- 為防止繼續處理可疑財產的臨時措施提供支援
- 參謀本地及國際打擊洗錢及恐怖分子資金籌集的政策事宜
- 籌辦打擊洗錢及恐怖分子資金籌集資培訓及外展活動

Our Charter

The JFIU performs diverse responsibilities to combat and deter ML, associated predicate offences and TF in view of the ongoing internal and external risk assessment. Its duties include:

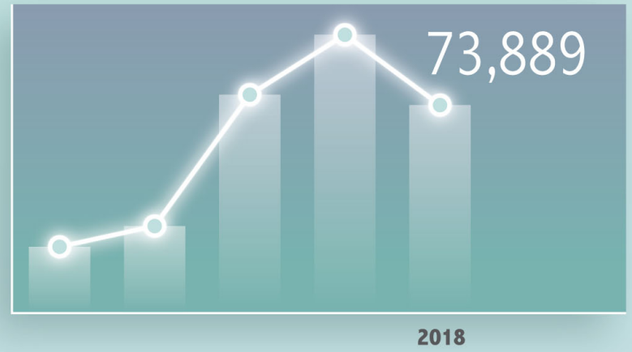
- operational analysis of STRs
- global exchange of financial intelligence and information
- strategic analysis of financial intelligence and other information
- research on ML/ TF trends and typologies
- operation of the Suspicious Transaction Report and management System (STREAMS)
- support on provisional measures to prevent further dealing of suspicious property
- staffing of local and international AML/CFT policy matters
- coordination of AML/CFT training and outreach

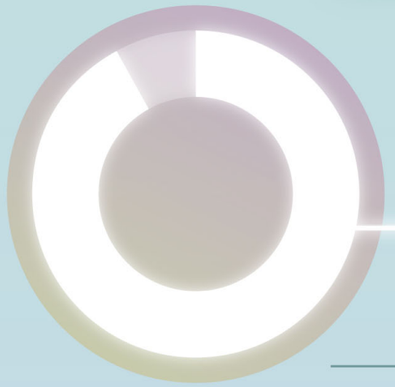
3

2018年聯合財富情報組的工作成果概覽

JFIU ACHIEVEMENT HIGHLIGHTS IN 2018

1 Total Number of STRs Received
接獲可疑交易報告總數





2 92.22%
of STRs were filed by banking sectors
92.2%的可疑交易報告由銀行業提交

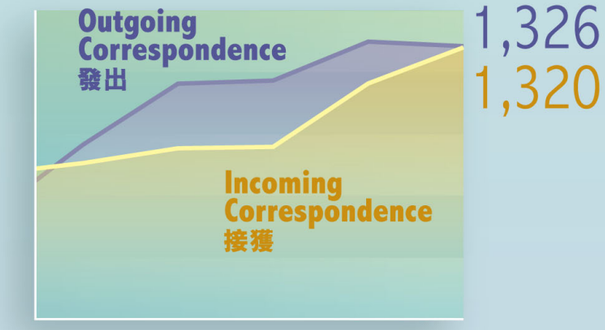
3 Total Number of STRs Disseminated
發布的可疑交易報告總數

4 81.11%
of the disseminated STRs were referred to the HKPF
發布的可疑交易報告中，81.1%發布至香港警務處

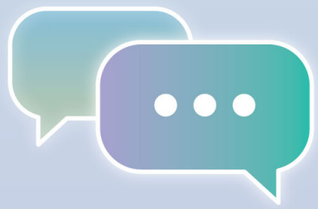
5 91.44% of STRs were filed via e-submission
91.4%的可疑交易報告經電子方式提交

6 14 MOUs or agreements were signed over the decade
10年間簽訂14份諒解備忘錄或協議

7 2,646 correspondence were recorded in Financial Intelligence Exchange between the JFIU & FIUs Worldwide
聯合財富情報組與世界各地財富情報單位交換財富情報的書信往來共錄得2,646次



8 23 AML/CFT seminars were delivered to convey key messages of suspicious transaction reporting to different sectors
舉辦23個打擊洗錢及恐怖分子資金籌集講座以向不同業界傳達舉報可疑交易的資訊



9 432 attended 2018 In-house Financial Investigation Courses
432人次出席內部財富調查課程

4

可疑交易報告
SUSPICIOUS TRANSACTION REPORT

舉報可疑交易的法律基礎

根據《販毒（追討得益）條例》（第405章）及《有組織及嚴重罪行條例》（第455章）第25A(1)條，以及《聯合國（反恐怖主義措施）條例》（第575章）第12(1)條，凡任何人知道或懷疑任何財產是(a)全部或部分、直接或間接代表任何人從販毒或可公訴罪行的得益；(b)曾在與販毒或可公訴罪行有關的情況下使用；或(c)擬在與販毒或可公訴罪行有關的情況下使用；或凡任何人知悉或懷疑任何財產是恐怖分子財產，該人須在合理/ 切實可行範圍內盡快（以舉報可疑交易的方式），將該知悉或懷疑向獲授權人（即聯合財富情報組人員）披露。

Legal Basis for Suspicious Transaction Report

Pursuant to sections 25A(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP, Cap. 405) and the Organized and Serious Crimes Ordinance (OSCO, Cap. 455), as well as section 12(1) of the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO, Cap. 575), where a person knows or suspects that any property (a) in whole or in part directly or indirectly represents any person's proceeds of; or (b) was used in connection with; or (c) is intended to be used in connection with drug trafficking or an indictable offence; or where a person knows or suspects that any property is terrorist property, the person shall as soon as it is reasonable/ practicable for him/ her to do so disclose that knowledge or suspicion (i.e. by way of STR) to an authorized officer (i.e. JFIU officer).

《打擊洗錢及恐怖分子資金籌集條例》（第615章）

修訂《打擊洗錢及恐怖分子資金籌集條例》，把當中就客戶作盡職審查及備存紀錄的規定延展至指定非金融企業及行業人士，包括法律專業人士、會計專業人士、地產代理及信託或公司服務提供者；並引入信託或公司服務提供者發牌制度，規定該等服務提供者須向公司註冊處處長申請牌照，並符合適當人選準則，方可在香港經營提供信託或公司服務的業務。經修訂的《打擊洗錢及恐怖分子資金籌集條例》已於2018年3月1日實施。

《公司條例》（第622章）

修訂《公司條例》，要求在香港成立為法團的公司須備存重要控制人登記冊，以提升法團實益擁有權的透明度。經修訂的《公司條例》已於2018年3月1日實施。

Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap.615 (AMLO)

Amend the AMLO to extend the customer due diligence and record-keeping requirements therein to designated non-financial business or professions including legal professionals, accounting professionals, estate agents and TCSPs; and to introduce a licensing regime for TCSPs requiring them to apply for a license from the Registrar of Companies and satisfy a "fit-and-proper" test before they can provide trust or company services as a business in Hong Kong. The amended AMLO commenced operation on 1 March 2018.

Companies Ordinance, Cap.622 (CO)

Amend the CO to require the keeping of significant controllers registers by companies incorporated in Hong Kong to enhance transparency of corporate beneficial ownership. The amended CO commenced operation on 1 March 2018.

《聯合國（反恐怖主義措施）條例》（第575章）

修訂《聯合國（反恐怖主義措施）條例》，加強凍結恐怖分子財產的機制，並禁止資助外國恐怖主義戰鬥人員的旅程。修訂《聯合國（反恐怖主義措施）條例》的法案於2018年3月獲立法會制定成為法例，並於2018年5月31日實施。

《實體貨幣及不記名可轉讓票據跨境流動條例》（第629章）《R32條例》

實施《R32條例》，以落實貨幣及不記名可轉讓票據（現金類物品）跨境流動的申報／披露制度。《R32條例》於2017年6月獲立法會制定成為法例，並於2018年7月16日實施。

United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 (UNATMO)

Amend the UNATMO to enhance the freezing mechanism of terrorist property and to prohibit the financing of travel of foreign terrorist fighter. The bill to amend UNATMO was enacted by the Legislative Council in March 2018 and operation was commenced on 31 May 2018.

Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance, Cap.629 (R32 Ordinance)

Introduce the R32 Ordinance to implement a declaration / disclosure system for cross-boundary movement of currency and bearer negotiable instruments. The R32 Ordinance was enacted by the Legislative Council in June 2017 and operation commenced on 16 July 2018.

接收可疑交易報告

可疑交易報告的年度總數自2013年開始持續上升，更在2017年創下新高，達92,115宗。2018年，聯合財富情報組共接獲73,889宗可疑交易報告，與2017年比較，下跌19.79%，即減少18,226宗報告。2018年的可疑交易報告數目顯著下降，主要是銀行業提交的報告數目減少。銀行業在提交可疑交易報告時更為謹慎，將重點放在提升可疑交易報告的質素。修訂的《打擊洗錢及恐怖分子資金籌集條例》(第615章）已於2018年3月1日生效，但未見其成效於指定非金融企業及行業。

Receipt of STR

The annual total of STRs has been on a rising trend since 2013 and peaked at 92,115 STRs in 2017. In 2018, the number of STRs received by the JFIU was 73,889, representing a decrease of 19.79% (or 18,226 STRs) when compared with that in 2017. The significant decrease in STR submissions in 2018 was mainly attributed to the banking sector. It is believed that the decrease was due to the adoption of a more prudent approach to submitting STRs by the banking sector, which put much emphasis on the quality of individual STR. DNFBPs have yet to see the impact associated with the commencement of operation of the amended AMLO (Cap. 615) on 1 March 2018.

下表載列本組在2014至2018年接獲的可疑交易報告宗數，並按呈報行業劃分。

The yearly breakdown of STRs received by category of reporting sectors between 2014 and 2018 is tabulated below:

Sectors 行業	2014	2015	2016	2017	2018
FIs 金融機構					
Banks 銀行	**31,095** (83.61%)	**34,959** (82.15%)	**68,745** (89.76%)	**86,029** (93.39%)	**68,146** (93.99%)
Securities Firms 證券公司	**1,574** (4.23%)	**1,095** (2.57%)	**1,423** (1.86%)	**2,090** (2.27%)	**1,337** (1.84%)
Insurance Companies 保險公司	**446** (1.20%)	**495** (1.16%)	**928** (1.21%)	**1,094** (1.19%)	**1,236** (1.70%)
Money Service Operators 金錢服務經營者	**2,772** (7.45%)	**3,566** (8.38%)	**2,554** (3.33%)	**908** (0.99%)	**1,219** (1.68%)
Money Lenders 放債人	**32** (0.09%)	**33** (0.08%)	**24** (0.03%)	**28** (0.03%)	**39** (0.05%)
SVF Licensees* 儲值支付工具持牌人* **(*New category since November 2016)** (*2016年11月起新設的界別)	/	/	**67** (0.09%)	**590** (0.64%)	**529** (0.73%)
Total Number of STRs Filed by All FIs 金融機構提交的報告總數 **(% of all STRs Received)** (佔可疑交易報告總數比率)	**35,919** (96.58%)	**40,148** (94.34%)	**73,741** (96.28%)	**90,739** (98.51%)	**72,506** (98.13%)
DNFBPs 指定非金融企業及行業					
Legal Professionals 法律專業人士	**222** (0.60%)	**894** (2.10%)	**969** (1.26%)	**555** (0.60%)	**416** (65.41%)
Estate Agencies 地產代理	**29** (0.08%)	**31** (0.07%)	**58** (0.08%)	**71** (0.08%)	**47** (7.39%)
Dealers in Precious Metals & Stones 貴重金屬及寶石交易商	**18** (0.05%)	**6** (0.02%)	**59** (0.08%)	**60** (0.07%)	**70** (11.01%)
TCSPs 信託或公司服務提供者	**46** (0.12%)	**22** (0.05%)	**27** (0.03%)	**31** (0.03%)	**81** (12.74%)
Accounting Professionals 會計專業人士	**3** (0.01%)	**6** (0.02%)	**3** (<0.01%)	**19** (0.02%)	**22** (3.46%)
Number of STRs Filed by All DNFBPs 指定非金融企業及行業提交的可疑交易報告總數 **(% of all STRs Received)** (佔可疑交易報告總數比率)	**318** (0.86%)	**959** (2.26%)	**1,116** (1.46%)	**736** (0.80%)	**636** (0.86%)
Number of STRs Filed by Others 其他行業提交的可疑交易報告宗數	**951** (2.56%)	**1,448** (3.40%)	**1,733** (2.26%)	**640** (0.69%)	**747** (1.01%)
Total Number of STRs Received 接獲可疑交易報告總數	**37,188**	**42,555**	**76,590**	**92,115**	**73,889**

分析可疑交易報告

本組日常行動分析和策略分析的獨有資料，主要來自可疑交易報告。本組接獲可疑交易報告後，會採取風險為本的方法，審視和評估每個報告，並定期參考洗錢及恐怖分子資金籌集的最新發展和趨勢。本組亦會根據可疑交易報告所涉的潛在洗錢及恐怖分子資金籌集風險、情報價值，以及促成往後調查或採取其他跟進行動的可行性，作出篩選，從而集中分撥資源，全面深入分析經選定具潛質的報告，冀能拓展優質的財富情報成果。

發布可疑交易報告

本組訂立可疑交易報告質素標準，以進行篩選和分析工作，從而甄別當中具充足資料的報告，從中摘錄有用，並可採取進一步行動的情報，向執法機關/ 財富情報單位發布，作情報用途或其他合適行動之用。儘管2018年的可疑交易報告宗數減少，本組仍致力為執法機關/ 財富情報單位辨識具情報價值的資料，最終共發布13,925宗可疑交易報告，比2017年的發布宗數更多。

Analysis of STR

STR is the major and unique source of information for JFIU to conduct operational and strategic analyses. Upon the receipt of STR, the JFIU adopts a risk-based approach to examining and assessing each of them, with regular reference to the latest ML/TF landscape and trends. Reviewing the level of inherent ML/TF risks, the value of intelligence, and the prospect for further investigation or other follow-up actions, the JFIU may allocate more resources to conduct a more holistic and in-depth analysis of selected STRs with the potential to develop quality financial intelligence products.

Dissemination of STRs

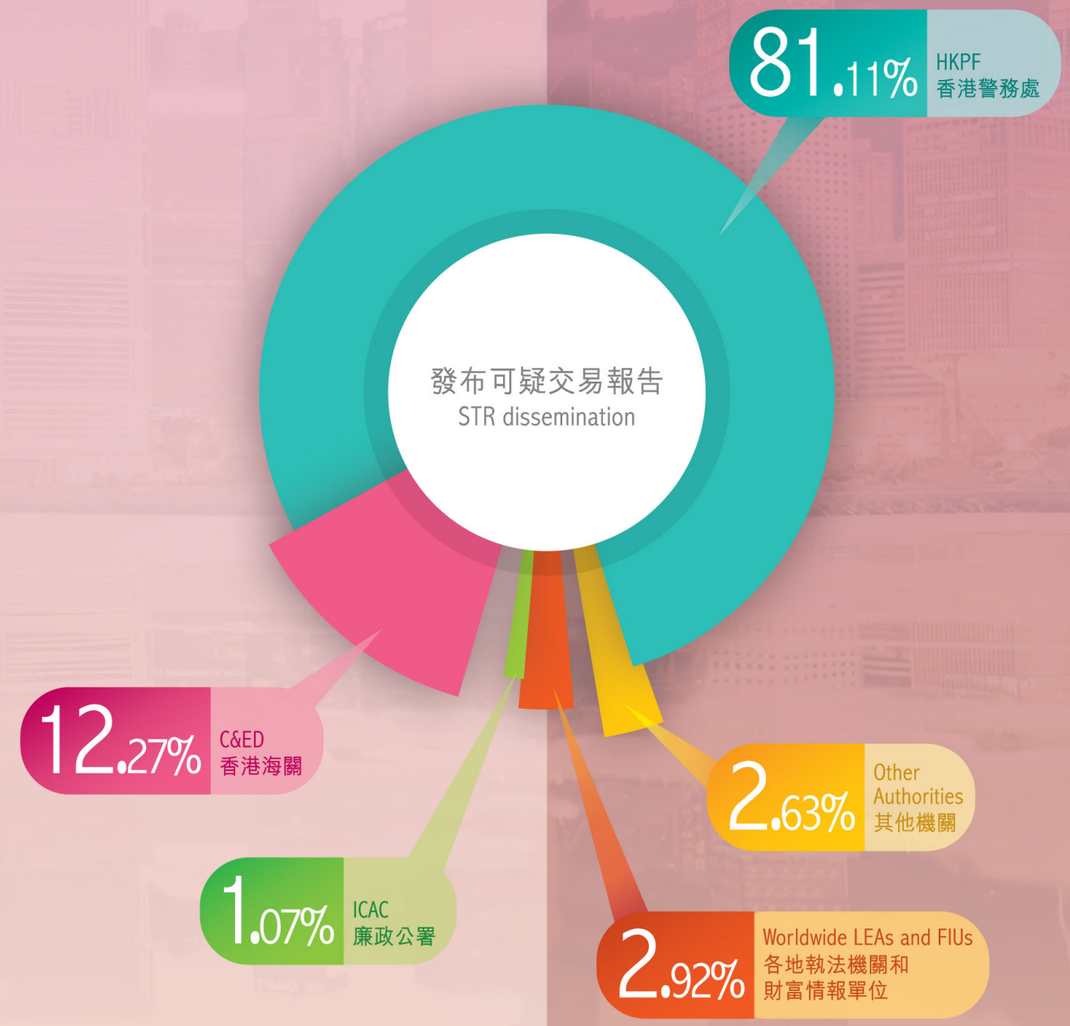
The JFIU sets quality standards, screens and analyses on STRs with a view to ascertaining if there is sufficient information for further extracting useful and/or actionable intelligence for dissemination to LEAs/ FIUs for intelligence purposes or any actions deemed appropriate. Despite a drop in the number of STRs in 2018, the JFIU endeavored to identify information of intelligence value to LEAs/FIUs in 2018, resulting in a total of 13,925 STRs disseminated in 2018, even higher than that in 2017.

本組在2014至2018年發布的可疑交易報告宗數，表列如下：
The yearly figures on STR dissemination between 2014 and 2018 are tabulated below:

	2014	2015	2016	2017	2018
Total Number of STRs Disseminated 發布的可疑交易報告總數	7,662	10,454	12,631	13,566	13,925

2018年，獲發布可疑交易報告的對象主要是香港警務處(81.11%)、香港海關(12.27%)、廉政公署(1.07%)、世界各地的執法機關和財富情報單位(2.92%)，以及其他機關(2.63%)。

In 2018, the major recipients of STRs were the HKPF (81.11%), C&ED (12.27%), the Independent Commission Against Corruption (ICAC) (1.07%), worldwide LEAs and FIUs (2.92%) and other authorities (2.63%).



取閱可疑交易報告資料

本組將大量可疑交易報告資料備存在可疑交易報告管理系統(STREAMS)的網絡平台。因應法定要求和資料保安措施，本港執法機關可向本組提出正式申請，要求索取在可疑交易報告管理系統的備存資料（有關資料可能涵蓋疑犯、可疑公司、可疑帳戶、交易及資金流向）。本港獲授權用戶（包括香港警務處、香港海關及聯合財富情報組人員）亦可直接在可疑交易報告管理系統搜尋資料，以便適當運用財富情報進行日常調查或情報拓展工作，並適時支援其他工作需要。

2014至2018年，每年要求在可疑交易報告管理系統進行資料索取的次數由2,362次上升至4,796次，錄得103.05%的升幅，而直接在可疑交易報告管理系統進行搜尋的次數，則累計有710,981次。兩項數字均反映各界對財富情報的需求急增，皆因有關情報有助對清洗黑錢、恐怖分子資金籌集及相關上游罪行採取執法行動。

Access to STR Information

The JFIU has a wealth of STR information available on its web-based STREAMS. In line with the statutory confines and information security safeguards, the JFIU welcomes local LEAs to make formal requests for STREAMS record checks for information (possibly covering suspects, suspected companies, suspicious accounts, transactions and fund flow); it also allows local authorized users (including the HKPF, C&ED and JFIU officers) to conduct direct searches on STREAMS to facilitate the appropriate use of financial information in daily investigations/ intelligence cultivation, and support various operational needs in a timely manner.

Between 2014 and 2018, the annual number of request for STREAMS record checks made to the JFIU mounted by 103.05% from 2,362 to 4,796 whilst a total of 710,981 direct searches were made on STREAMS. Both sets of figures reflect the escalating demand for Financial intelligence, which is considered conducive to enforcement actions against ML, TF and associated predicates.

2014至2018年，每年要求在可疑交易報告管理系統進行資料索取及直接搜尋的次數，表列如下：
Below are the annual totals of both requests for STREAMS record checks and direct searches on STREAMS between 2014 and 2018:

	2014	2015	2016	2017	2018
Total Number of Requests for STREAMS Record Checks 要求在可疑交易報告管理系統進行資料索取的次數	**2,362**	**2,166**	**3,113**	**3,301**	**4,796**
Total Number of Direct Searches on STREAMS 在可疑交易報告管理系統進行直接搜尋的次數	**101,803**	**166,592**	**135,421**	**135,863**	**171,302**

管理和提升可疑交易報告管理系統

可疑交易報告管理系統於2006年建立，便利用家以電子方式提交、處理、分析和發布可疑交易報告。可疑交易報告電子舉報系統於2018年8月啟用，用家可使用經修訂的可疑交易報告電子表格提交報告。

2018年，本組仍集中優化可疑交易報告管理系統，而所需款項已在2017年年底獲批。整個優化計劃旨在提升本組處理、分析和發布財富情報的能力，以及借助系統功能互用，應付將來數量龐大的可疑交易報告。展望未來，本組會就運用新科技，包括大數據及人工智能等方面進行可行性研究，以不斷提升我們進行行動及策略分析的效率和能力。

STREAMS Management and Enhancement

Launched in 2006, the STREAMS facilitates the e-submission, processing, analysis and dissemination of STRs. In order to enhance the efficiency and accuracy in STR submission and processing, "e-STR Submission" using a revised STR proforma has been rolled out in August 2018.

In 2018, JFIU also focused on the STREAMS enhancement project of which the funding was obtained in late 2017. The project aimed at improving the JFIU's capability in processing, analyzing and disseminating financial intelligence as well as leveraging its functional interoperability to better cope with the tremendous volume of STR in the long run. Looking forward, JFIU will conduct feasibility studies on the deployment of new technologies, including big data and artificial intelligence to further enhance its efficiency and capability in conducting operational and strategic analysis.

2014至2018年，以電子方式和人手處理的可疑交易報告宗數比率，以及電子呈報的宗數，表列如下：
The respective proportion of electronically and manually processed STRs, as well as the number of e-STRs, between 2014 and 2018 are shown below:

	2014	2015	2016	2017	2018
% of Electronic Processing of STRs 以電子方式處理的可疑交易報告比率 **(Total Number of STRs Involved)** (涉及的可疑交易報告總數)	**82%** (30,464)	**81%** (34,500)	**89%** (67,991)	**93%** (85,582)	**91.44%** (67,565)
% of Manual Processing of STRs 以人手方式處理的可疑交易報告比率	**18%**	**19%**	**11%**	**7%**	**8.56%**

可疑交易報告質素意見回饋

可疑交易舉報機制能否發揮效用，取決於不同呈報界別所提交可疑交易報告的整體質素。因此，本組會視乎需要，就可疑交易報告的質素及質量兩方面向監管機構、專業團體和呈報機構提供意見回饋。本組就可疑交易報告出版《可疑交易報告季度分析》(可於聯合財富情報組網頁限制區閱覽)，藉以加強與私營界別的雙向溝通，同時提升私營界別對打擊洗錢及恐怖分子資金籌集的意識。金融機構和指定非金融企業及行業可從中獲取最新資訊，例如撰寫優質可疑交易報告的指引和建議格式，顯示呈報趨勢的統計數字，有關洗錢及恐怖分子資金籌集的案例和類型學研究，以及他們日常遵從打擊洗錢及恐怖分子資金籌集的規定和管制措施而採取的良好行事方法。

本組不時為金融機構和指定非金融企業及行業舉辦研討會。本組深信公私營機構的合作相當重要，良好的夥伴關係能有效打擊洗錢及恐怖分子資金籌集活動。定期向金融機構和指定非金融企業及行業舉行講座，不但有助維護業界遵從打擊洗錢及恐怖分子資金籌集資規定的文化，亦可提高他們的警覺，以應對洗錢及恐怖分子資金籌集在相關業界的風險及弱點，從而加強他們偵查非法活動的能力，以及確保舉報可疑交易的質素。

Feedback on STR Quality

The overall quality of STR input from various reporting sectors is of paramount importance to the effectiveness of the suspicious transaction reporting regime. Thus the JFIU provides quantitative and qualitative feedback on STRs to regulatory agencies, professional bodies and reporting entities as appropriate. The JFIU publishes STR Quarterly Analysis (made available through the secure area of JFIU's website) to enhance mutual communication and raise AML/CFT awareness of the private sector. FIs and DNFBPs are kept up-to-date with useful guidelines and the preferred framework for making quality STRs, STR statistics that indicate their filing trends, case examples on the latest ML/TF-related typologies and other good practices observed in their daily AML/CFT compliance and control.

The JFIU conducts regular seminars of FIs and DNFBPs. The JFIU recognizes the growing importance of public-private partnership to combat ML/TF more effectively. Regular delivery of seminars to FIs and DNFBPs helps uphold the culture of AML/CFT compliance and increases their vigilance to ML/TF risks and vulnerabilities within their respective sectors, which are crucial to enhancing their abilities in detecting illicit activities and ensuring the quality of reporting suspicious transactions. At the same time, it provides direct opportunities for the JFIU to understand from practitioners' point of view their top concerns or mitigation measures in the AML/CFT dynamics faced by different industries.

與本港持份者合作

對打擊洗錢及恐怖分子資金籌集的社區而言，跨機構合作非常重要，本組亦不遺餘力，務求各方可合作無間。在策略層面，政府決策局、監管機構及專業團體就修訂有關可疑交易舉報機制的政策、法例和指引會向本組人員徵詢意見。本組亦協助整理有關打擊洗錢及恐怖分子資金籌集的統計數字，供政府高層會議討論。在行動層面，本組與不同執法機關和財富情報單位的財富情報交流頻密而迅速，在情報、調查和追討資產方面提供支援。

與舉報可疑交易的機構定期聯繫

香港的金融服務方便快捷，或惹罪犯或恐怖分子（及其聯繫者）覬覦，藉以清洗黑錢或進行恐怖分子資金籌集。因此，本組視私營機構為打擊清洗黑錢及恐怖分子資金籌集制度的第一道防線。

本組委派指定的聯絡人員與舉報可疑交易的主要機構協調和溝通，以達致更佳成果。

本組主持舉報可疑交易工作小組（成員包括香港警務處、香港海關、金融監管機構及私營界別代表），每年會面一次，但偶爾會按行動需要召開特別會議，就舉報可疑交易涉及共同關注的議題討論並提出意見。小組又就多項事宜進行交流，範疇涵蓋政策與優先處理的項目、行事方法和程序，以及在打擊洗錢及恐怖分子資金籌集方面加強合作等。2018年9月，本組與各代表參與舉報可疑交易工作小組會議。

一如既往，本組會繼續與反詐騙協調中心攜手合作，打擊金融罪案，以及減少受害人的損失。

Local Cooperation with Stakeholders

The JFIU treasures and seeks to enhance interagency collaboration within the AML/CFT community. At the strategic level, government bureau, regulatory authorities and professional bodies consult with the JFIU on changes of policies, legislation and/or guidelines that touch on the suspicious transaction reporting regime. The JFIU also assists in collating STRs or other AML/CFT-related statistics for the deliberation in high-level governmental meetings. At the operational level, the JFIU provides intelligence, investigative and asset-recovery support through frequent and responsive financial intelligence exchange with various LEAs and FIUs.

Regular Liaison with STR Reporting Entities

The JFIU recognizes the private sectors as the first line of defence in the AML/CFT regime as criminals or terrorists (and their associates) are inclined to make use of the easily accessible financial services in Hong Kong to launder proceeds of crime or perform TF.

The JFIU has assigned designated liaison officers to better coordinate and communicate with major STR reporting entities.

The JFIU chairs the Suspicious Transaction Reporting Working Group (attended by the HKPF, C&ED, financial regulator(s), and representatives from the private sector) annually and sometimes on ad-hoc basis depending on the operational needs to discuss and advise on matters of common interest in suspicious transaction reporting and share views on policy and operational priorities, practices and procedures, and strengthen other AML/CFT cooperation. The JFIU held the Suspicious Transaction Reporting Working Group Meeting with various representatives in September 2018.

As always, the JFIU will continue to join hands with Anti-Deception Coordination Centre (ADCC) in the fight against financial crime and mitigating the loss of victims.

5

國際財富情報交流

WORLDWIDE FINANCIAL INTELLIGENCE EXCHANGE

科技進步，連繫世界各地已非難事，國際間有效而緊密的合作，可算是成功打擊跨國洗錢和恐怖分子資金籌集的關鍵。本組向來珍視與全球各地財富情報單位所交換的情報。

2018年，接獲外地的交換情報書信數目大幅增加，顯示各地財富情報單位的合作愈趨頻繁，互相提供更多支援。

With the ease of international connectivity, there is no doubt that effective and enhanced international cooperation is the key to success in combating transnational ML and TF. The JFIU treasures and values the information exchanged with FIUs worldwide.

In 2018, there has been a significant increase in the incoming correspondence from other FIUs, marking the more frequent cooperation and mutual support among the FIUs.

本組與世界各地財富情報單位交換財富情報的統計數字
Financial Intelligence Exchange between the JFIU and FIUs Worldwide

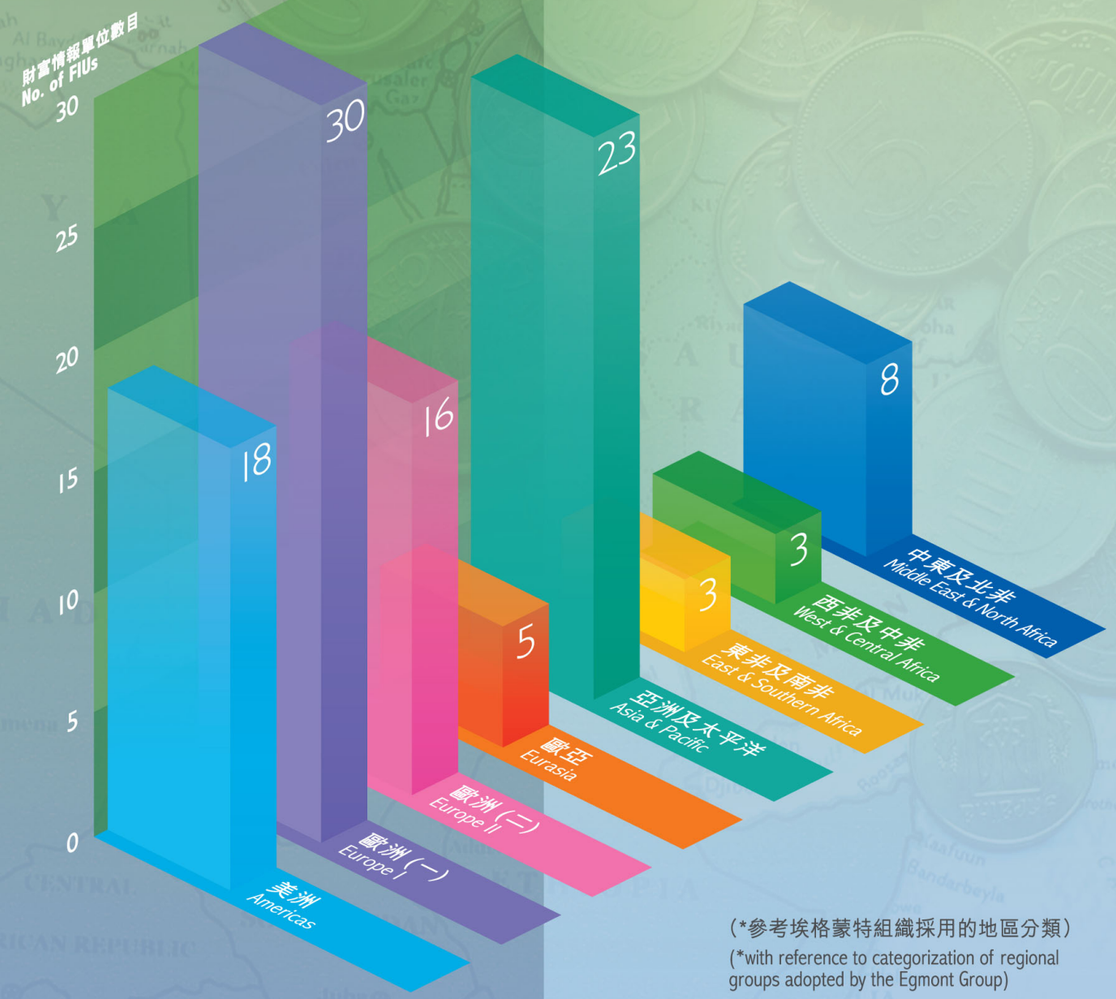
Year 年份		2014	2015	2016	2017	2018
Total No. of Incoming Correspondence 接獲外地的交換情報書信往來次數	(Egmont Group) (埃格蒙特組織)	744	824	794	991	1,197
	(Non-Egmont Group*) (非埃格蒙特組織)	14	6	43	154	123
Incoming Total 接獲總數		758	830	837	1,145	1,320
Total No. of Outgoing Correspondence 對外發出的交換情報書信往來次數	(Egmont Group) (埃格蒙特組織)	824	944	866	990	1,036
	(Non-Egmont Group*) (非埃格蒙特組織)	23	200	293	358	290
Outgoing Total 發出總數		847	1,144	1,159	1,348	1,326

(*非埃格蒙特組織成員主要包括非埃格蒙特組織的財富情報單位及偶爾是其他海外執法機關)
(*Non-Egmont Group members include mainly non-Egmont FIU(s) and occasionally other overseas LEAs)

2018年，本組與全球106個埃格蒙特組織成員及3個非埃格蒙特組織成員交換財富情報。各大洲所涉的財富情報單位數目如下：

In 2018, the JFIU exchanged financial intelligence with 106 Egmont Group members and three non-Egmont Group members across continents. The number of FIUs from each continent being engaged is shown as follows:

2018年與本組交換財富情報的全球財富情報單位數目（按地區劃分*）
Number of Worldwide FIUs Exchanged Financial Intelligence with the JFIU (by Regions*) in 2018

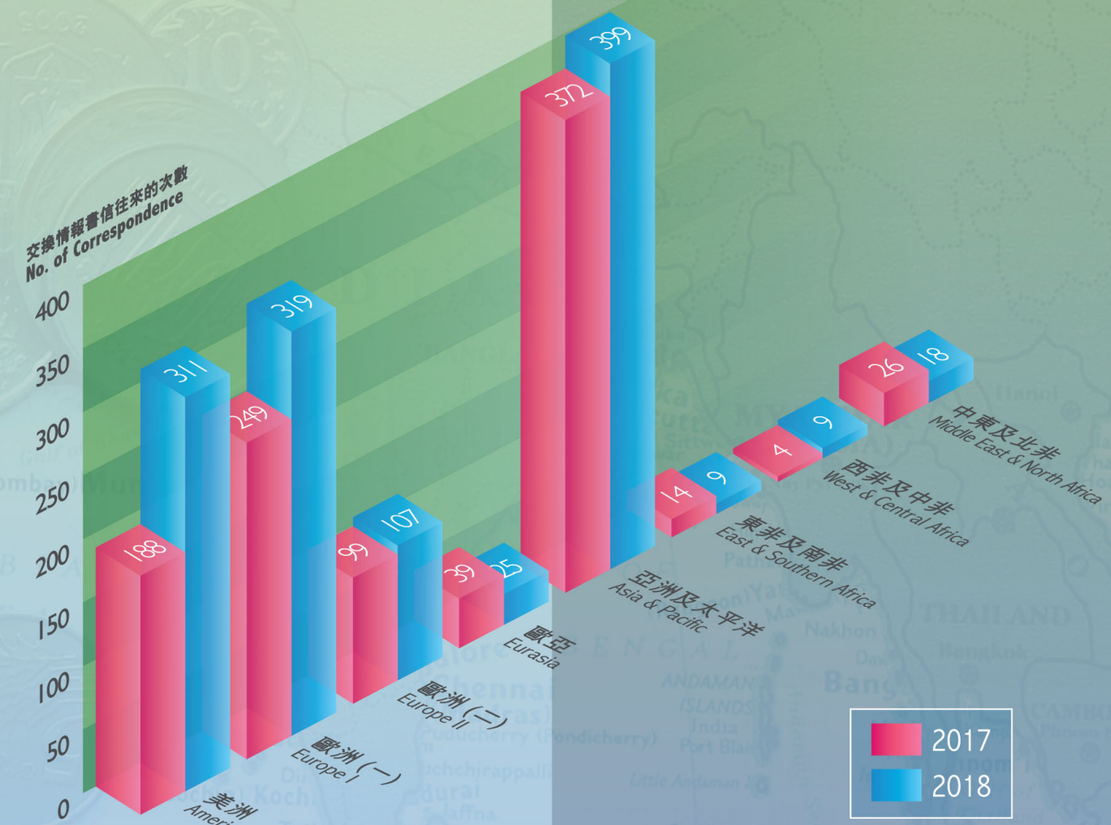


（*參考埃格蒙特組織採用的地區分類）
(*with reference to categorization of regional groups adopted by the Egmont Group)

如下圖所示，本組與亞洲及太平洋地區的成員交換情報的次數較頻繁。全年在各地區接獲的交換情報書信往來次數共錄得1,197次，而亞洲及太平洋地區的相關書信往來總數達399次，高踞各區首位。綜觀2018年所接獲的交換情報書信往來次數，其他地區，例如美洲及歐洲等地的相關書信往來數目，與2017年相比，均錄得顯著升幅。

As shown from the graph below, JFIU has more frequent exchange of intelligence with members from Asia & Pacific Region of which 399 out of 1,197 incoming correspondence were received from the Region. The year of 2018 also recorded a significant increase in incoming correspondence with other Regions, such as Americas and Europe I, as compared to 2017.

2017年及2018年接獲埃格蒙特組織成員的交換情報書信往來次數
Number of Incoming Correspondence with Egmont Group Members in 2017 and 2018



	1st 第一位	2nd 第二位	3rd 第三位	4th 第四位	5th 第五位
Incoming Request 接獲索取情報的要求	**Korea** 韓國	**USA** 美國	**Macao** 澳門	**Singapore** 新加坡	**France/Japan** 法國/日本
(671)	**(63)**	**(52)**	**(49)**	**(46)**	**(34)**
Nature of Incoming Request 接獲要求索取情報的性質	**Suspicious Transactions** 可疑交易	**Fraud** 訛騙	**Email Scam** 電郵騙案	**Tax Evasion** 逃稅	**Corruption** 貪污
	(142)	**(130)**	**(62)**	**(44)**	**(35)**
Incoming Spon. Sharing 接獲自發分享的情報	**USA** 美國	**Germany/ Luxembourg** 德國/盧森堡	**Jersey** 澤西島	**Singapore** 新加坡	**Czech** 捷克
(398)	**(207)**	**(21)**	**(18)**	**(16)**	**(14)**
Nature of Incoming Spon. Sharing 接獲自發分享情報的性質	**Email Scam** 電郵騙案	**Fraud** 訛騙	**Suspicious Transactions** 可疑交易	**Tax Evasion** 逃稅	**Corruption** 貪污
	(149)	**(109)**	**(31)**	**(13)**	**(12)**

*( ) 交易報告宗數交易報告宗數
*( ) denotes number of requests/ sharing

	1st 第一位	2nd 第二位	3rd 第三位	4th 第四位	5th 第五位
Outgoing Request 發出索取情報的要求	**BVI** 英屬維爾京群島	**Turkey/ Singapore/UK** 土耳其/新加坡/英國	**Cayman Islands/ USA** 開曼群島/美國	**Italy/ Macao/ Malaysia** 意大利/澳門/馬來西亞	**Indonesia/ Korea/ Philippines/ Samoa/UAE** 印度尼西亞/韓國/菲律賓/薩摩亞/阿聯酋
(65)	**(7)**	**(5)**	**(4)**	**(3)**	**(2)**
Nature of Outgoing Request 接獲要求索取情報的性質	**Fraud** 訛騙	**Crime Proceeds** 犯罪得益	**Email Scam** 電郵騙案	**Suspicious Transactions/ TF** 可疑交易/恐怖分子籌資	**Investment Fraud** 投資騙案
	(19)	**(10)**	**(8)**	**(5)**	**(3)**
Outgoing Spon. Sharing 接獲自發分享的情報	**Taiwan** 台灣	**USA** 美國	**Indonesia** 印度尼西亞	**UK** 英國	**India** 印度
(149)	**(43)**	**(25)**	**(12)**	**(9)**	**(8)**
Nature of Outgoing Request 接獲自發分享情報的性質	**Fraud** 訛騙	**Tax Evasion** 逃稅	**Insider Trading** 內幕交易	**Corruption** 貪污	**Investment Fraud** 投資騙案
	(27)	**(22)**	**(11)**	**(10)**	**(9)**

*( ) 交易報告宗數交易報告宗數
*( ) denotes number of requests/ sharing

與其他司法管轄區簽訂諒解備忘錄或協議
Memorandum of Understanding (MOU) or Agreements with Other Jurisdictions

根據香港法例，本組無需就情報交流簽訂任何法律文書或諒解備忘錄，便可交換情報，以支援有關洗錢、恐怖分子資金籌集和相關犯罪活動的調查。儘管如此，為了設定基礎架構以加強各方的合作和了解，本組可與個別司法管轄區就交換情報簽訂雙邊協議，務求符合相關地區的法例要求。

2018年，本組與柬埔寨的財富情報單位和南非共和國的財富情報中心就關乎洗錢及恐怖分子資金籌集的財富情報交流，簽訂2份諒解備忘錄。此後，本組共與13個司法管轄區，簽訂14份諒解備忘錄或合作協議。

Hong Kong's legislation does not require any exchange instruments or MOU to be in place for the exchange of information in supporting of investigations related to ML and TF and related criminal activities. However, in order to provide a structural framework for enhanced cooperation and understanding, JFIU would enter into MOU with jurisdictions where bilateral agreements are required under their domestic legislation for information exchange.

During 2018, JFIU signed two MOUs for the exchange of financial intelligence related to ML and TF with the Cambodia Financial Intelligence Unit (CAFIU) and the Financial Intelligence Centre (FIC) of the Republic of South Africa. This brings to a total number of 14 MOUs or Agreements that JFIU has signed on cooperation with 13 jurisdictions.

本組主管（左）於2018年9月在澳洲悉尼出席第25屆埃格蒙特集團全體會議，並與財富情報單位簽訂諒解備忘錄。
The head of JFIU (left) attended the 25th Egmont Group Plenary Meeting in Sydney, Australia and signed an MOU with the FIC in September 2018.

6

案件分析
及類型學

CASE STUDIES AND TYPOLOGIES

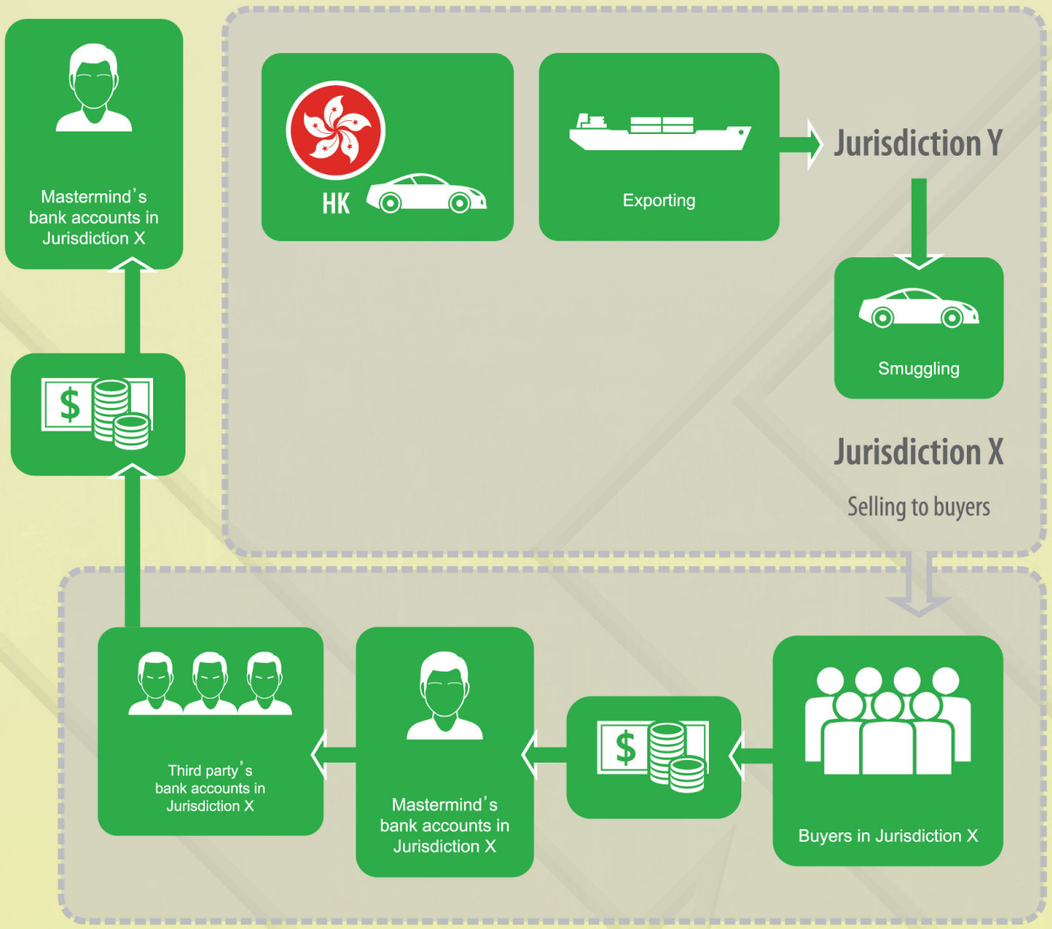
香港海關的案件分析
Case Examples from C&ED

案例 Case 1 與走私得益有關的洗錢案
Money Laundering in relation to Proceeds of Smuggling

2013年初，香港海關與X司法管轄區的執法機關就一個集團進行聯合行動，有關集團涉及由香港出口名貴左軚汽車至Y司法管轄區，繼而走私至X司法管轄區，並以轉折方法在香港清洗在X司法管轄區所獲的犯罪得益。買家把購買走私汽車的款項存入集體首腦在X司法管轄區所持有的銀行帳戶。首腦隨後安排該等金錢轉至第三者在X司法管轄區的銀行帳戶，並在香港集取匯款，而本組接獲的相關情報已協助本港就案件展開細緻的財富調查。2013年9月，集團首腦被香港海關拘捕，其後並控以清洗總值5,900萬港元黑錢。2016年1月，透過法庭命令限制價值1,700萬港元的可變現資產。該首腦於2018年3月被裁定洗錢罪名成立，並於2018年4月被判處5年監禁。

In early 2013, the C&ED conducted a joint investigation with the LEA of jurisdiction X against a syndicate involved in exporting luxury left-hand-drive vehicles from Hong Kong to jurisdiction Y and then smuggling them into Jurisdiction X, as well as laundering the crime proceeds from jurisdiction X into Hong Kong in circuitous ways. The buyers made the payments for the smuggled vehicles into the bank accounts in jurisdiction X held by the mastermind, who then arranged transfer of such monies into the bank accounts of third parties in jurisdiction X. The mastermind subsequently collected the monies in Hong Kong, where a nuanced financial investigation was conducted with the intelligence support from the JFIU. In September 2013, the C&ED arrested the mastermind and subsequently charged him for money laundering, with a laundered amount of HKD 59 million. In January 2016, HKD 17 million worth of realisable properties were restrained by means of a court order. In March 2018, the mastermind was convicted of money laundering and sentenced to five years' imprisonment in April 2018.

案例1 與走私得益有關的洗錢案
Case 1 Money Laundering in relation to Proceeds of Smuggling

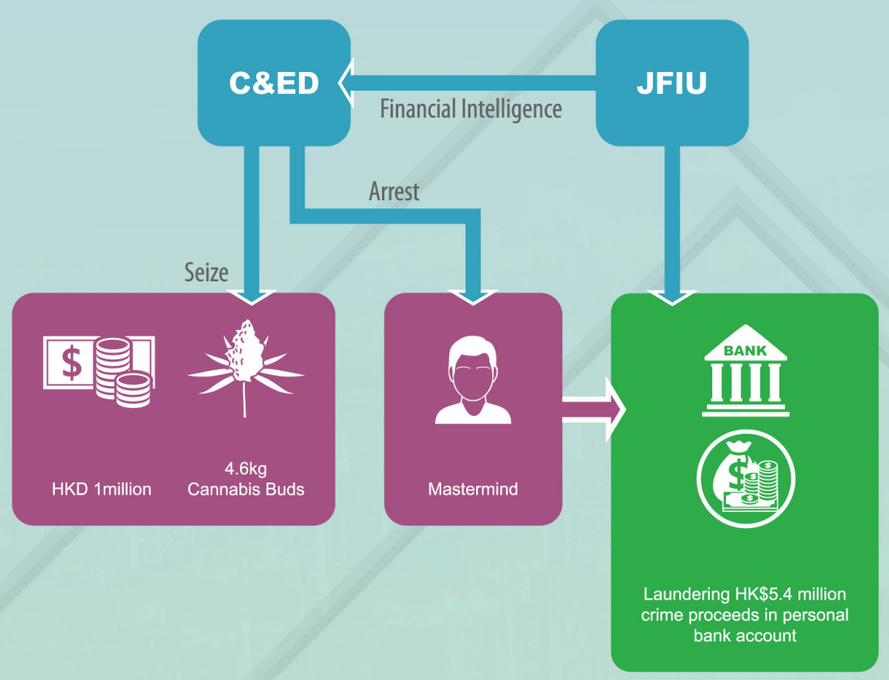


案例 Case 2 與販毒得益有關的洗錢案
Money Laundering in relation to Proceeds of Drug Trafficking

2017年3月，香港海關展開緝毒行動，最終拘捕一對情侶，並檢獲4.6公斤懷疑大麻花，以及100萬港元的懷疑販毒得益。在二人因販毒被捕後，香港海關隨即透過本組檢索被捕人的財富情報。相關銀行資料及可疑銀行記錄證明被捕男子於2016年8月及9月期間曾使用其個人銀行帳戶清洗懷疑犯罪得益。經進行全面的財富調查後，證據顯示該男子共清洗540萬港元犯罪得益。2018年3月，透過法庭命令限制價值370萬港元的可變現資產。男子於2018年11月被裁定販運危險藥物及清洗黑錢罪名成立，並判監4年2個月。

In March 2017, the C&ED mounted an anti-narcotics operation. As a result, a couple was arrested and 4.6 kg of suspected cannabis buds and HKD 1 million of suspected drug proceeds were seized. Financial intelligence on the arrestees were retrieved via the JFIU soon after the arrest for drug trafficking had been made. The relevant banking information and suspicious bank records supported that the male arrestee had made use of his personal bank account to launder suspected crime proceeds between August and September 2016. After extensive financial investigation, evidence showed that the man laundered HKD 5.4 million of crime proceeds. In March 2018, HKD 3.7 million worth of realisable properties were restrained by means of a court order. In November 2018, the man was convicted of Trafficking in Dangerous Drugs and Money Laundering charges and he was sentenced to four years and two months' imprisonment.

案例2 與販毒得益有關的洗錢案
Case 2 Money Laundering in relation to Proceeds of Drug Trafficking



毒品調查科財富調查組的
Case Examples from FID NB

案例 Case 1

針對本地三合會集團展開的財富調查
Financial Investigation against Local Triad Syndicate

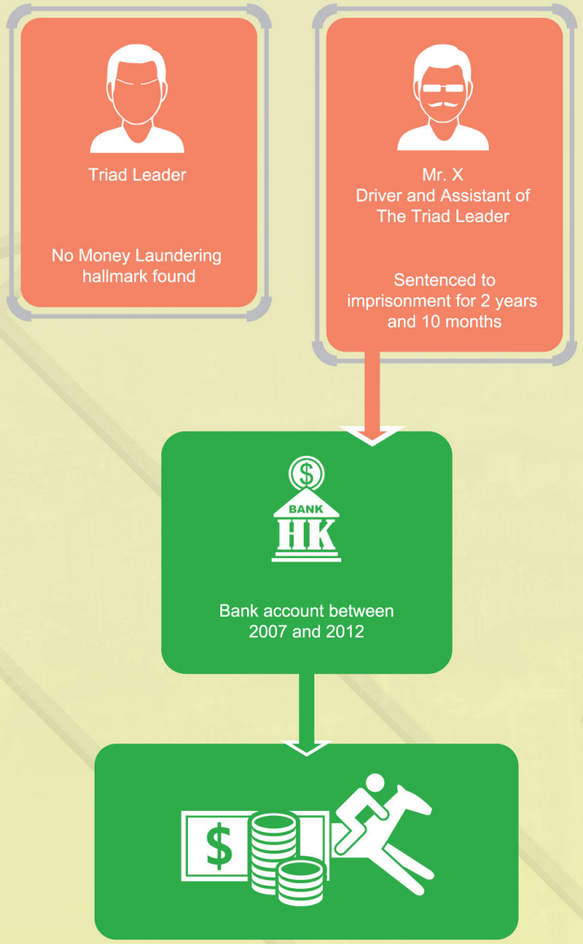
2012年，有組織罪案及三合會調查科與毒品調查科財富調查組展開聯合調查及行動，目標是一個本地三合會集團及其成員。情報顯示部分三合會成員利用他們的銀行帳戶協助高調的集團元老級執事清洗犯罪得益。毒品調查科財富調查組以本組的情報支援，發現罪犯均為集團的骨幹成員，並負責清洗犯罪得益。

X先生是集團高調元老級執事的助理，因清洗黑錢被捕。經過多年的全面財富調查，發現X先生於2007年至2012年間清洗300萬港元的犯罪得益。X先生於2018年1月經審訊後被裁定罪名成立，判監2年10個月。

In 2012, OCTB initiated a joint investigation and operation with FID NB targeting a local triad syndicate and its members. Intelligence indicated that some triad members had been using their bank accounts for laundering crime proceeds of their high-profile senior bearers. With the intelligence support of the JFIU, FID NB identified the criminals who were believed to be the core members and responsible for laundering the crime proceeds.

Mr. X, the key assistant of a high-profile senior bearer, was arrested for money laundering. After years of holistic financial investigation, Mr. X was found to have laundered HKD 3 million crime proceeds between 2007 and 2012. In January 2018, Mr. X was convicted after trial and sentenced to imprisonment for 2 years and 10 months.

案例1 針對本地三合會集團展開的財富調查
Case 1 Financial Investigation against Local Triad Syndicate



In 2012, OCTB initiated a joint investigation targeting a local triad syndicate and its core members.

Investigation expands to the leaders' assistants. It was found D1's personal bank account was used as a temporary repository of fund receiving cash of HKD 1.8 million without reasons

A total sum of HKD 3.5 million was deposited between 2007 and 2012

During trial, the defendant alleged the cash was used for horseracing gambling for X but it was rebutted upon comparing the HKJC records

案例 Case 2 針對跨境外圍賭博集團展開的財富調查
Financial Investigation against Cross-boundary Bookmaking Syndicate

毒品調查科財富調查組根據情報，調查一個跨境外圍賭博集團，並於2013年6月與有組織罪案及三合會調查科，以及N司法管轄區的執法機關展開聯合行動，同步進行突擊搜查。最終在香港拘捕33人，而23人則在X司法管轄區被捕。搜查期間檢獲共值200億港元的投注記錄及160萬港元現金。

財富調查顯示集團首腦（A先生）及骨幹成員（B先生、C先生及D女士）曾於2005年至2013年間使用他們的個人銀行帳戶清洗1億7,460萬港元。在該等銀行帳戶均發現清洗黑錢特徵，包括存入大量現金、結構性匯款，以及星期一／星期四的交易模式，而涉案帳戶的龐大資金流量亦與集團成員報稱的收入不成比例。

Acting on intelligence, FID NB conducted investigation against a cross-boundary bookmaking syndicate. Joint operation was mounted with OCTB and LEA of Jurisdiction X in June 2013 with synchronized raids conducted. 33 persons were arrested in Hong Kong, while 23 persons were arrested in Jurisdiction X. Betting records valued at HKD 20 billion and cash HKD 1.6 million were seized.

Financial investigation revealed that the mastermind (Mr. A), and core syndicate members (Mr. B, Mr. C and Ms. D) had made use of their personal bank accounts to launder HKD 174.6 million between 2005 and 2013. Money laundered hallmarks, which included substantial cash deposits, structuring funds, and Monday - Thursday Pattern, were identified in the bank accounts. The large turnover in the accounts concerned were also incommensurate with the reported earnings of the syndicate members.

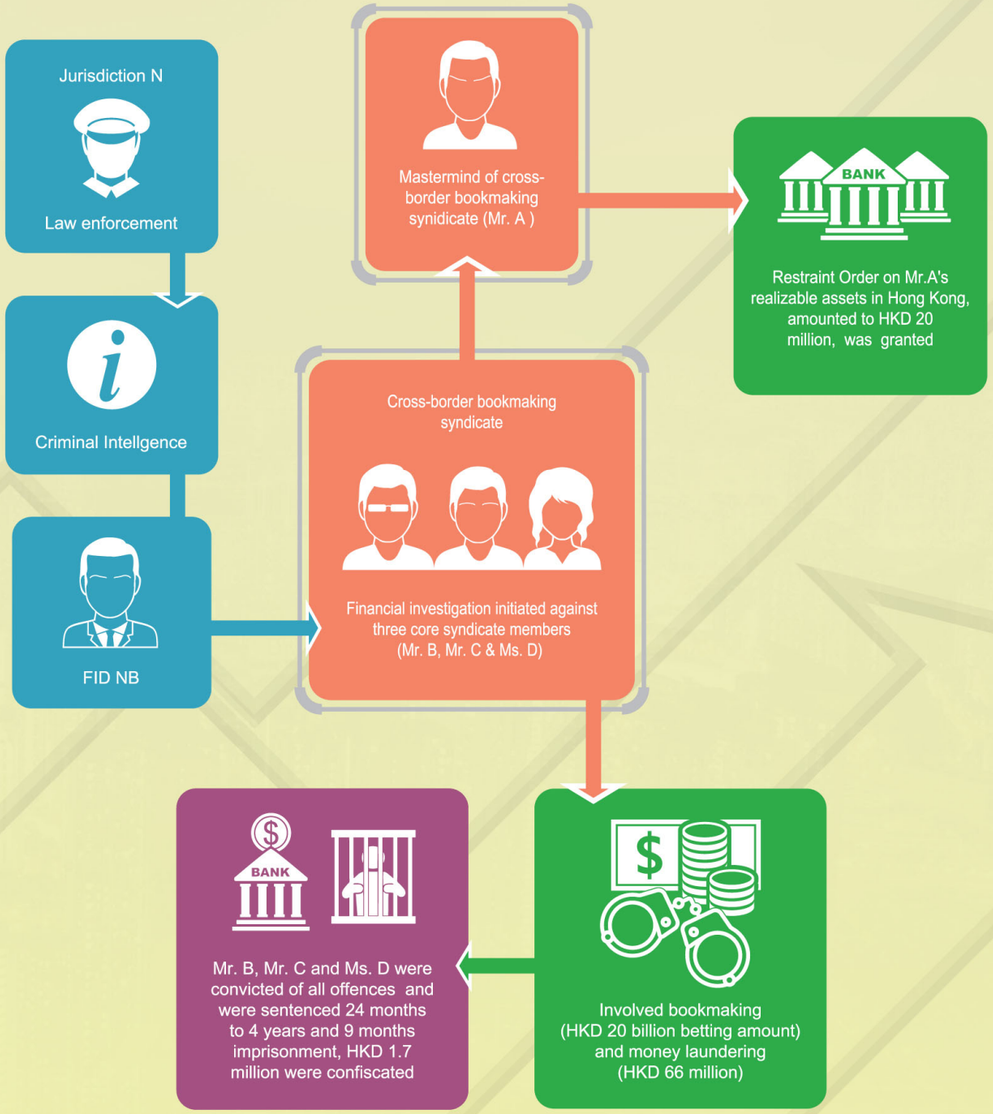
A先生在N司法管轄區被捕，裁定非法賭博罪名成立，並於2013年判處監禁4年。法庭亦就A先生可變換現金的資產總值2,000萬港元發出限制令，並正根據潛逃者法律程序沒收有關被限制的資產。

B先生、C先生及D女士亦同因清洗黑錢及/ 或收受外圍投注罪行被捕和檢控。B先生於2019年2月被裁定洗錢罪名成立。C先生及D女士於2018年6月同被裁定清洗黑錢罪名成立，並分別判監24及42個月。各人帳戶共174萬港元的餘額亦被沒收。

Mr. A was arrested and convicted of illegal gambling in Jurisdiction N. He was sentenced to 4-year imprisonment in 2013. A Restraint Order on Mr. A's realizable assets amounting to HKD 20 million was obtained. Absconder proceedings are on-going to confiscate his restrained assets.

Mr. B, Mr. C and Ms. D were also arrested and charged for Money Laundering and/or Bookmaking offences. Mr. B was convicted of Money Laundering in February 2019. Mr. C and Ms. D were convicted of Money Laundering and sentenced to 24 months and 42 months' imprisonment in June 2018 respectively. The residual balance of HKD 1.74 million in their respective accounts were confiscated.

案例2 針對跨境外圍賭博集團展開的財富調查
Case 2 Financial Investigation against Cross-boundary Bookmaking Syndicate



案例 Case 3

財富情報引發而達致限制資產的洗錢案
ML case originated from financial intelligence resulting in restraint

2011年9月，財富調查組根據情報，就A先生及其前妻（B女士）展開財富調查，揭發12個由二人操控的銀行帳戶。在2004年至2011年的7年間，發現他們的帳戶合共曾存入7億6,730萬港元。交易記錄發現清洗黑錢的特徵，例如「星期一/ 星期四交易模式」，以及暫時保管資金等。其間，帳戶的資金被迅速轉移至其他不明人士。二人於2013年5月被捕。

A先生及B女士於2016年12月被控合共12項清洗黑錢罪行，涉及7億6,730萬港元。A先生自2017年11月潛逃至Y司法管轄區，並未有如期出席審訊。其後，審訊於2017年11至12月期間在區域法院展開，而A先生則缺席相關審訊。

法官於2018年3月作出判決，被告二人被裁定12項洗錢罪名全部成立。A先生及B女士分別判監4年及5.5年。

法庭就A先生及B女士在銀行帳戶總值1,400萬港元的可變換現金資產，以及17萬港元保釋金發出限制令。

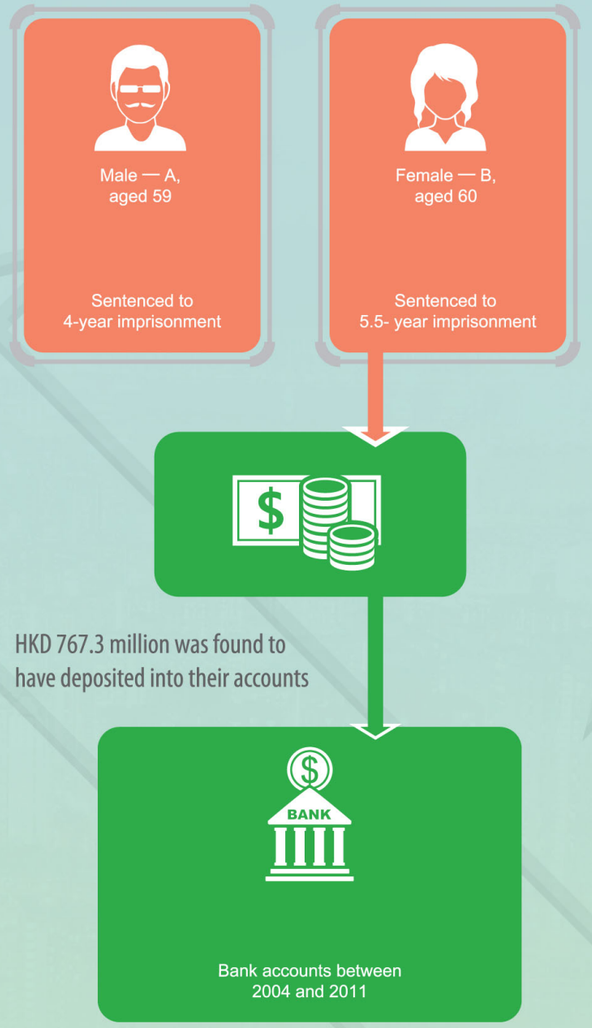
In September 2011, acting on intelligence, a financial investigation was initiated against Mr. A and his ex-wife (Ms. B), which unveiled 12 bank accounts under their effective control. During a 7-year period between 2004 and 2011, a total of HKD 767.3 million was found to have deposited into their accounts. Money laundering hallmarks such as 'Monday-Thursday Pattern' and temporary repository of funds were identified in the transaction records. The money were swiftly dissipated to other unknown counterparties. In May 2013, they were arrested.

In December 2016, both Mr. A and Ms. B were charged with a total of 12 counts of Money Laundering involving HKD 767.3 million. Mr. A has absconded to Jurisdiction Y since November 2017 and he did not attend the trial as scheduled. The trial was then commenced in the absence of Mr. A between November and December 2017 in the District Court.

In March 2018, the Judge handed down the verdict and both defendants were found guilty of all the 12 charges. Mr. A and Ms. B were sentenced to 4 years and 5.5 years' imprisonment respectively.

A Restraint Order has been issued against Mr. A and Ms. B's realizable assets amounting to a total of HKD 14 million in their bank accounts, together with HKD 170,000 bail money.

案例3 財富情報引發而達致限制資產的洗錢案
Case 3 ML case originated from financial intelligence resulting in restraint



In 2011, Mr. A declared in the divorce hearing that he was convicted of 'Operating a Gambling Establishment' in Mainland in 2009 and his source of income was 'Gambling'. The Judge in the Family Court opined that D1 might be involved in Money Laundering and thus referred the case to police.

Financial investigation was initiated against Mr. A and Ms. B, which unveiled they had 12 bank accounts whereas a total of HKD 767.3 million was found to have deposited into their accounts during a 7-year period. Money laundering hallmarks such as 'Monday-Thursday Pattern' and temporary repository of funds were identified in the transaction records. The money had swiftly dissipated to other unknown counterparties .

In pursuant to legal advice, Mr. A and Ms. B were charged with 12 counts of 'Money Laundering' concerning the deposits of HKD 767.3 million.

案例 Case 4

財富情報引發的洗錢案
ML case originated from financial intelligence

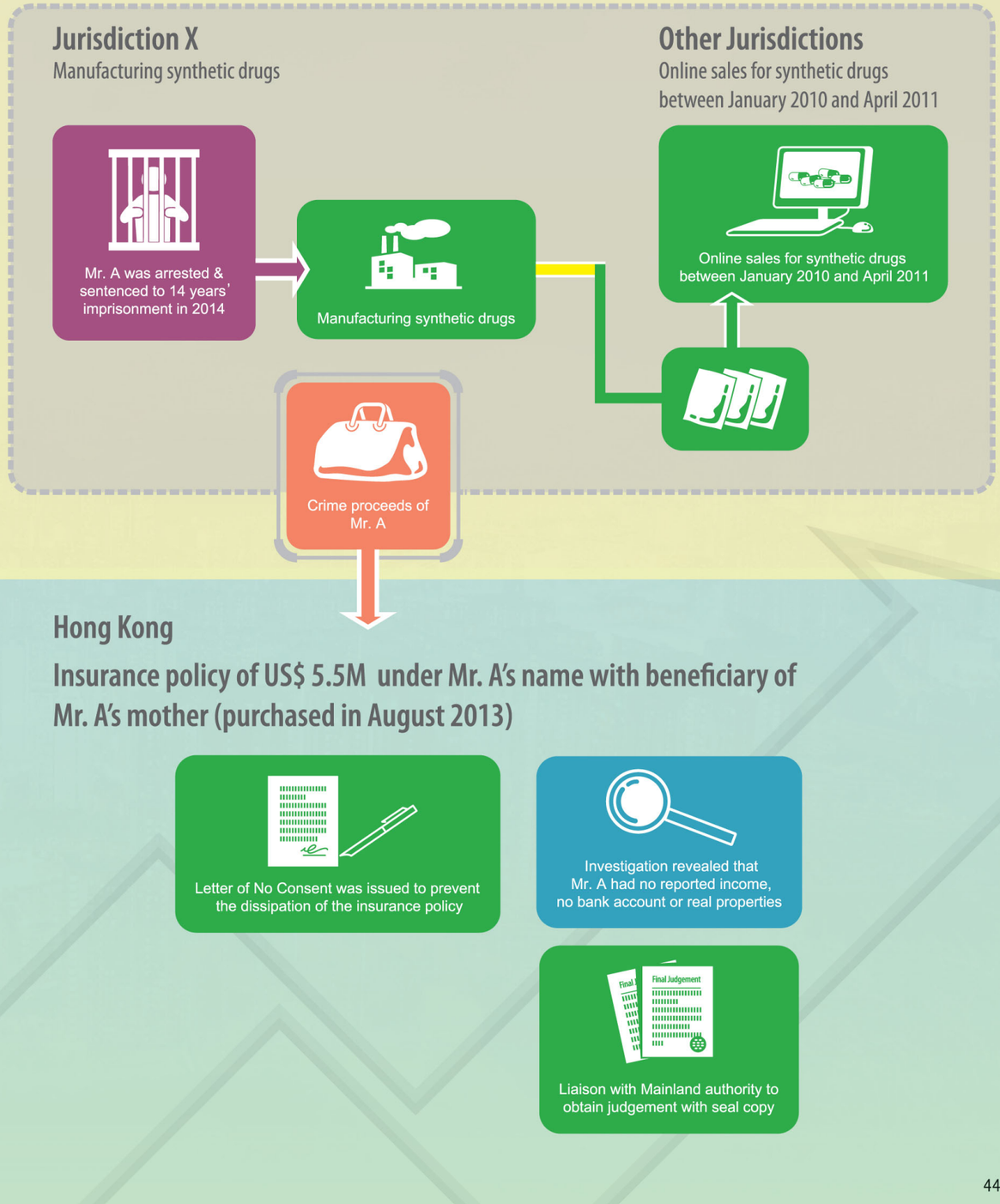
2018年8月，本組的財富情報顯示A先生在香港持有一份約值550萬美元的保單，但他是X司法管轄區的國民，並因製造合成毒品，以及透過網上渠道向其他司法管轄區售賣有關毒品而判處長期監禁，而現正服刑。

背景調查顯示A先生在香港並沒有申報的入息，亦沒有銀行帳戶或物業。毒品調查科財富調查組發現A先生在香港購買保單的資金來自X司法管轄區，並可能是他的販毒得益。該份保單價值550萬美元。

In August 2018, a piece of financial intelligence provided by the JFIU unveiled that Mr. A, who had maintained an insurance policy of about USD 5.5 million in Hong Kong, is a national of Jurisdiction X and is serving a long custodial sentence in the jurisdiction for manufacturing and selling of synthetic drugs to other jurisdictions via online channels.

Background investigation revealed that Mr. A had no reported income, no bank account or properties in Hong Kong. FID NB revealed that the fund used to purchase the insurance policy in Hong Kong originated from Jurisdiction X, which might be derived from his drug proceeds. The insurance policy valued USD 5.5 million.

案例4 財富情報引發的洗錢案
Case 4 ML case originated from financial intelligence



案例 Case 5 針對跨境販運毒品及清洗黑錢的行動
Operation against Cross-boundary DD trafficking & ML

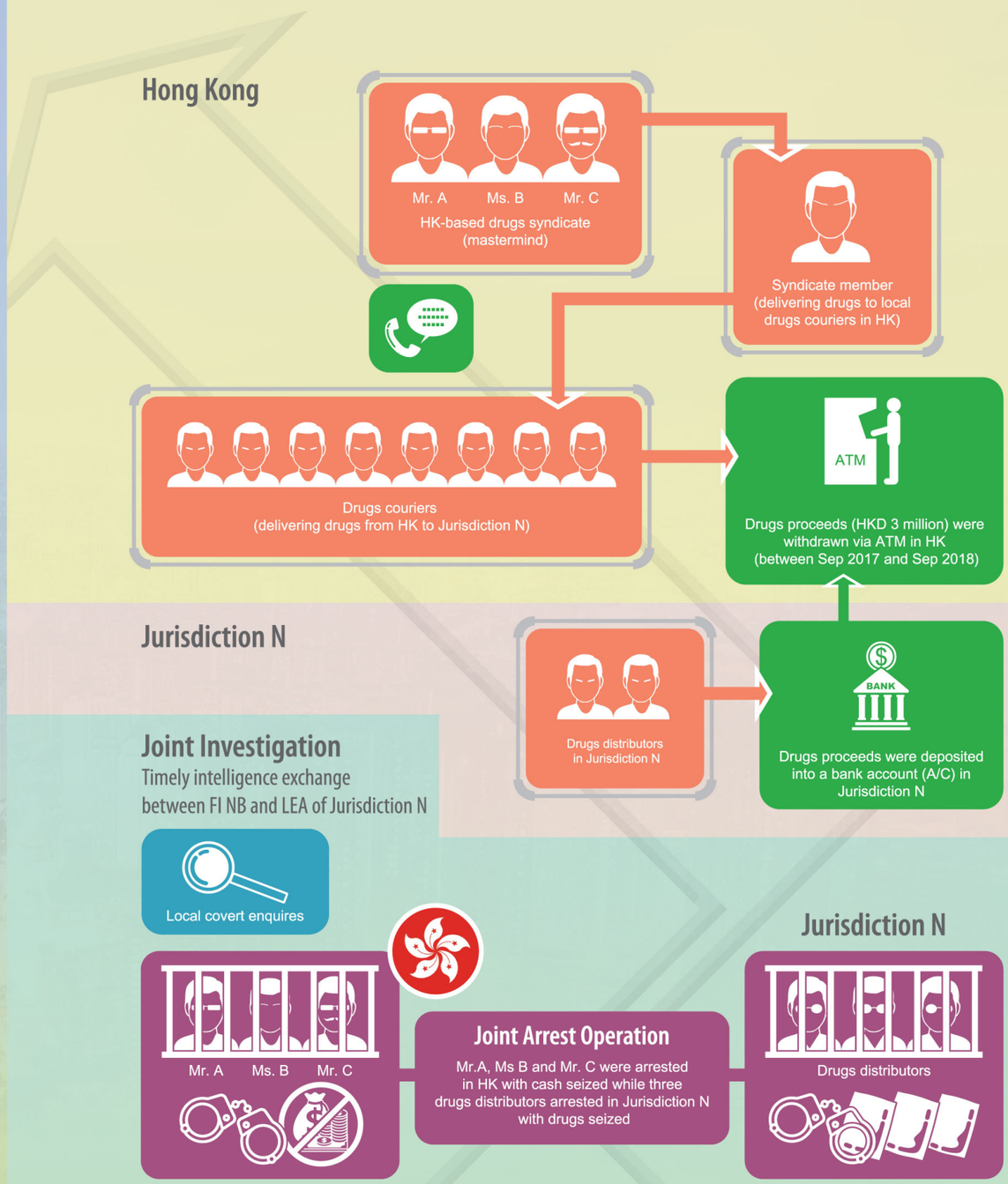
自2017年10月起，毒品調查科財富調查組與N司法管轄區的執法機關就一個跨境販毒集團展開聯合調查。N司法管轄區的情報顯示涉及三名香港疑犯的販毒集團安排兩名毒販在N司法管轄區販賣毒品。在接獲犯罪得益後，該兩名毒販會將現金存入N司法管轄區的銀行帳戶，並通知管有該銀行戶口提款卡的集團成員迅速在香港提取現金。

拘捕行動於2018年9月進行，三名香港集團成員在本港因清洗黑錢被捕，而其他成員則因販運危險藥物被N司法管轄區的執法機關拘捕。銀行帳戶合共27萬港元的懷疑犯罪得益已被扣押，以防非法資金被進一步轉移。

Since October 2017, FID NB and an LEA in Jurisdiction N initiated a joint investigation targeting a cross-boundary DD trafficking syndicate. Intelligence from Jurisdiction N indicated that a drug syndicate involving three Hong Kong suspects, who had arranged two traffickers to sell drugs in Jurisdiction N. Upon receiving the crime proceeds, the two traffickers deposited the cash in the bank accounts in Jurisdiction N and informed the syndicate members who were in control of the ATM card of the bank accounts and then swiftly withdrew the cash in Hong Kong.

An arrest operation was conducted in September 2018 and the three Hong Kong syndicate members were arrested in Hong Kong for money laundering, whereas the others were arrested by the LEA in Jurisdiction N for DD trafficking. A total of HKD 0.27 million of suspected crime proceeds in the bank accounts were withheld with a view to preventing further dissipation of the illicit funds.

案例5 針對跨境販運毒品及清洗黑錢的行動
Case 5 Operation against Cross-boundary DD trafficking & ML



案例 Case 6

針對跨境外圍賭博集團的行動
Operation against Cross-boundary Bookmaking Syndicate

毒品調查科財富調查組於2017年9月接獲有關四名外圍賭博集團骨幹成員的情報，四名疑犯在香港參與網上賭場、賽馬，以及足球外圍博彩活動。情報亦顯示該集團擴展非法外圍投注網絡至X司法管轄區，藉二名經常往返X司法管轄區的香港市民接收賭注。

經進行財富調查後，A先生（懷疑是該集團的司庫）的銀行帳戶錄得與其報稱收入不成比例的大額交易。他在18個月內共收逾900萬港元，而他申報的年薪只有90萬港元。

2018年7月，兩間投注中心被突擊搜查，超過40人（包括A先生）因外圍賭博、清洗黑錢及相關罪行被捕，並在現場檢獲面值逾7,770萬港元的投注記錄，以及超過250萬港元現金，懷疑是外圍賭博的得益。各人銀行帳戶共約168萬港元被扣押。

In September 2017, FID NB received intelligence relating to four suspects who were the core members of a bookmaking syndicate engaging in online casino, horse-racing and soccer bookmaking activities in Hong Kong. Intelligence also revealed that the syndicate expanded its illegal bookmaking network to Jurisdiction X through two Hong Kong citizens who traveled frequently to Jurisdiction X for receiving bets.

Upon conducting financial investigation, the bank account of Mr. A (suspected to be the Treasurer of the syndicate) recorded a large amount of transactions which were incommensurate with his reported income as he had received over HKD 9 million in 18 months while his reported annual income was only HKD 900,000.

In July 2018, two betting centres were raided with over 40 people arrested (including Mr. A) for bookmaking, money laundering and related offences. Betting records with a face amount of over HKD 77.7 million and cash over HKD 2.5 million which were suspected to be the proceeds of bookmaking were seized at the scene. About HKD 1.68 million was withheld in their bank accounts.

案例6 針對跨境外圍賭博集團的行動
Case 6 Operation against Cross-boundary Bookmaking Syndicate

案例 Case 7

財富情報引發而達致沒收資產的洗錢案
ML case originated from financial intelligence resulting in confiscation

本組的財富情報揭示X司法管轄區的受害人，誤墮電郵騙案，被騙將9,800萬美元匯至Y司法管轄區的銀行帳戶，而部分金錢，總值20萬美元再由Y司法管轄區轉至Z公司在香港持有的銀行帳戶。

以本組情報支援的財富調查顯示Z公司的董事及銀行帳戶簽署人同為A先生。A先生及Z公司均沒有在香港提交報稅表。資金流向分析發現銀行帳戶在2014年至2015年間的20個月內曾用作接收8,600萬港元，而帳戶亦出現清洗黑錢特徵，例如保管資金，以及大額可疑交易。

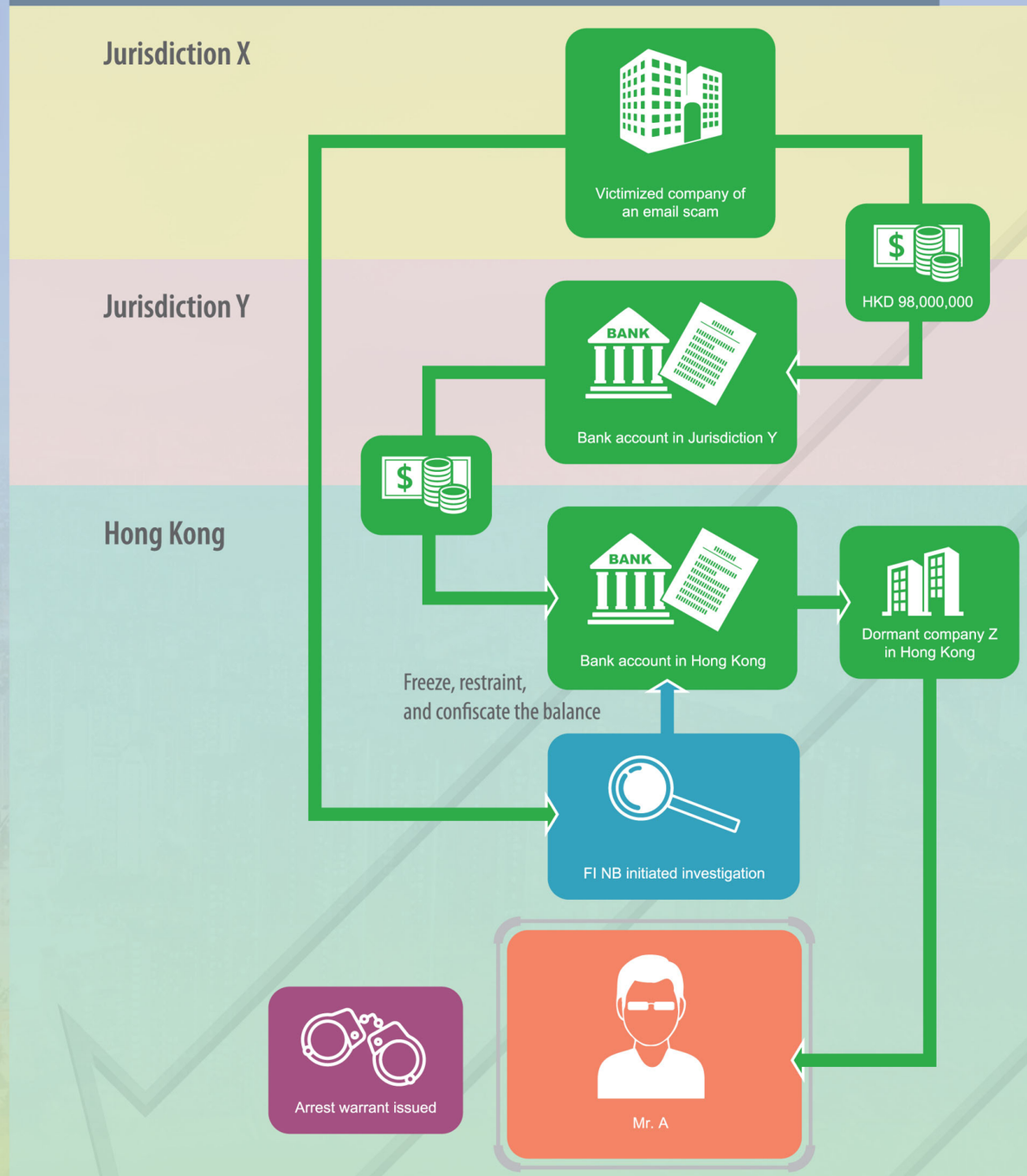
儘管A先生仍逍遙法外，但法庭於2018年1月已就A先生總值200萬港元的資產發出限制令，其後沒收令亦於2018年12月發出。

Financial intelligence from JFIU disclosed that a victim in Jurisdiction X had fallen prey to an email scam and was deceived into remitting USD 98 million into a bank account in Jurisdiction Y and part of the money totaling USD 200,000 was further transferred from Jurisdiction Y to a bank account in Hong Kong held under Company Z.

Financial investigation with the intelligence support of JFIU revealed that the director and the bank account signatory of Company Z is Mr. A. Both Mr. A and Company Z had not filed any tax returns in Hong Kong. Fund flow analysis revealed that the bank account was used for receiving HKD 86 million in 20 months between 2014 and 2015, with patterns of ML such as repository of funds and large amounts of suspicious transactions noted.

Despite the fact that Mr. A was at large, a Restraint Order against Mr. A's assets amounting to HKD 2 million was obtained in January 2018. A Confiscation Order was subsequently granted in December 2018.

案例7 財富情報引發而達致沒收資產的洗錢案
Case 7 ML case originated from financial intelligence resulting in confiscation



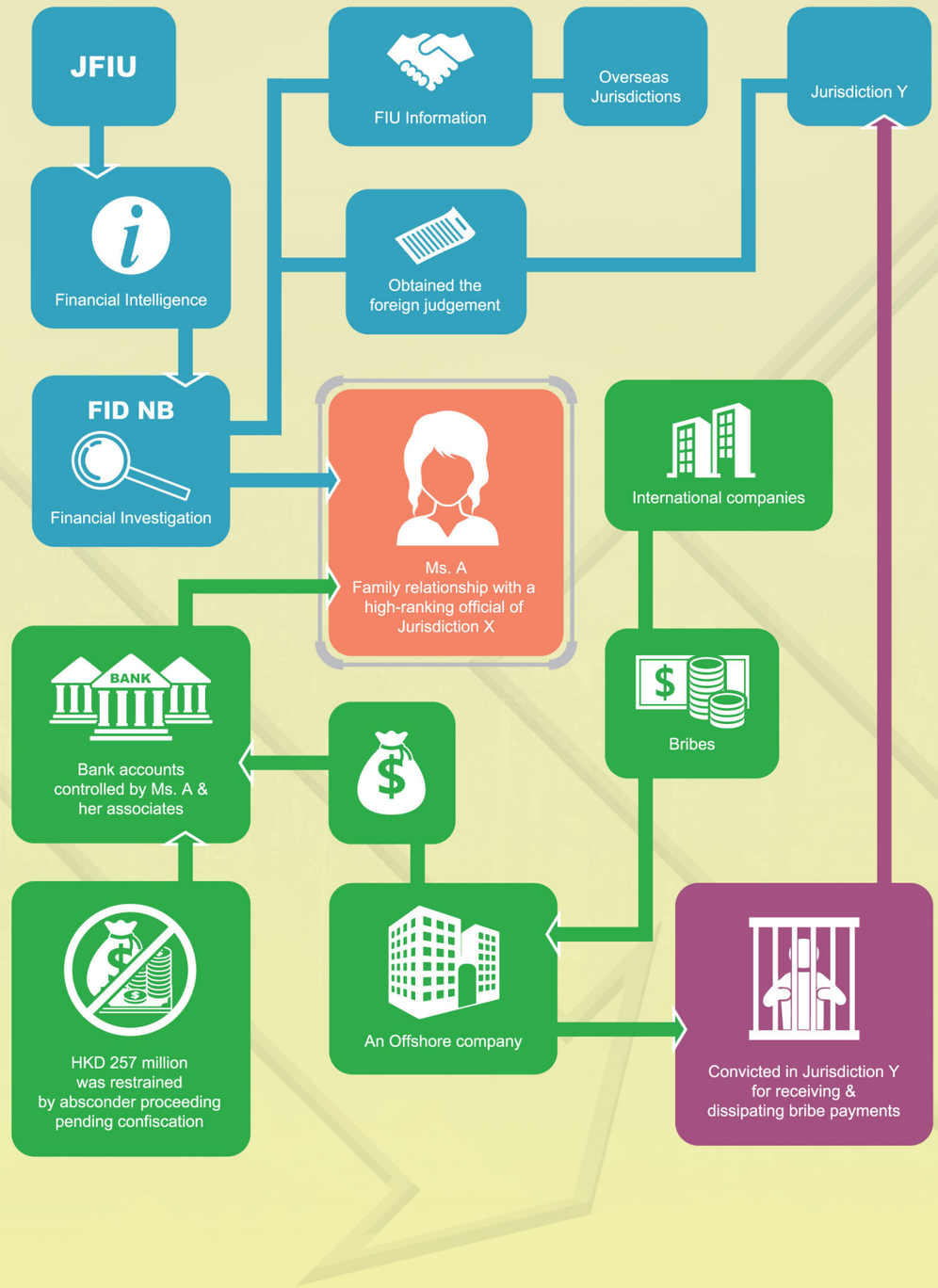
案例 Case 8

成功限制從貪污所得的收益
Successful Restraint of Proceeds of Corrupted Payments

本組於2013年接獲財富情報後，隨即對A女士展開財富調查。情報顯示A女士向X司法管轄區的高級官員提供賄款，以助國際公司獲准在X司法管轄區營商。調查發現A女士及其生意伙伴在香港操控的銀行帳戶存有大量存款，而資金大部分來自離岸公司。本組的情報亦顯示一筆匯至香港銀行帳戶的款項是來自A女士所操控的離岸公司。該離岸公司在Y司法管轄區因以中介人身分收受和轉移有利於A女士的賄款而被定罪。毒品調查科財富調查組聯絡Y司法管轄區的海外執法機關，並成功取得外地判決以確定判罪。限制令於2018年6月發出，成功扣押A女士及其生意伙伴總值2億5,700萬港元的銀行存款。

The financial investigation against Ms. A was initiated after receiving the financial intelligence from JFIU in 2013. The intelligence indicated that Ms. A had solicited and offered bribes to a high-ranking official in Jurisdiction X for allowing some international companies to do business in Jurisdiction X. The investigation revealed that the bank accounts controlled by Ms. A and her associates in Hong Kong has maintained substantial balances, in which the source of funds were mostly from offshore companies. With the intelligence provided by JFIU, it was unveiled that a remittance paid into the bank account of Hong Kong originated from an offshore company controlled by Ms. A. The said offshore company was convicted in Jurisdiction Y for being an intermediary for receiving and dissipating bribe payments in favour of Ms. A. FID NB approached the overseas LEA of Jurisdiction Y and successfully obtained the foreign judgement to confirm the conviction. In June 2018, a Restraint Order was successfully applied to withhold bank balances (totaling HKD 257 million) controlled by Ms. A and her associates.

案例8 成功限制從貪污所得的收益
Case 8 Successful Restraint of Proceeds of Corrupted Payments



7

儲值支付工具策略分析報告

STRATEGIC ANALYSIS REPORT ON STORED VALUE FACILITIES ("SVFs")

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。

[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。

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 DTROP, 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] 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.

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，它們分別為三三金融服務有限公司、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、通滙(香港)投資咨詢有限公司、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 licensees[2] 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。

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.

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

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

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.

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 statistics[3] of SVF sector published by the HKMA during the period from Q4/2016 to Q4/2018:

The quarterly number of SVF accounts in use[4] 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.

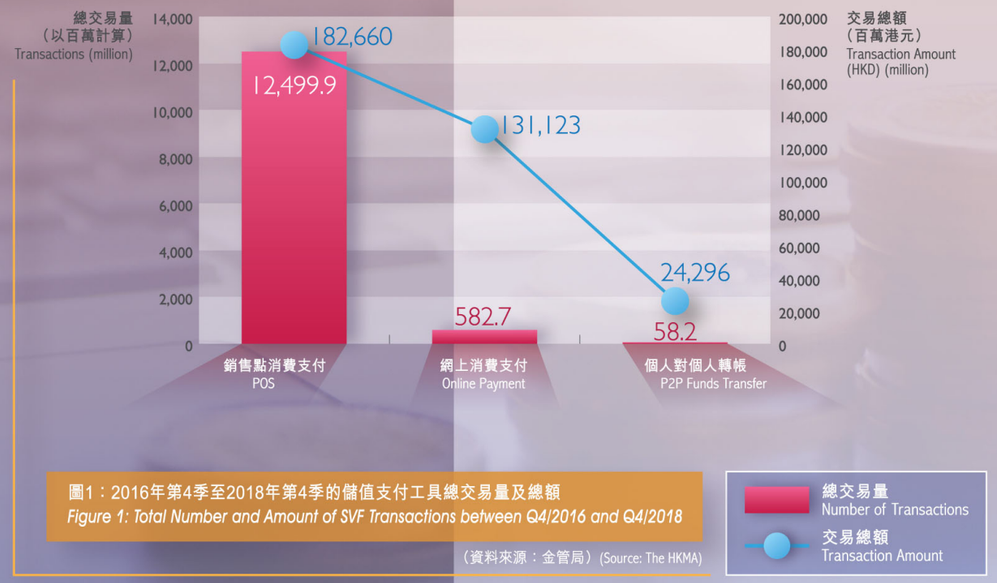


圖1：2016年第4季至2018年第4季的儲值支付工具總交易量及總額
Figure 1: Total Number and Amount of SVF Transactions between Q4/2016 and Q4/2018

（資料來源：金管局）(Source: The HKMA)

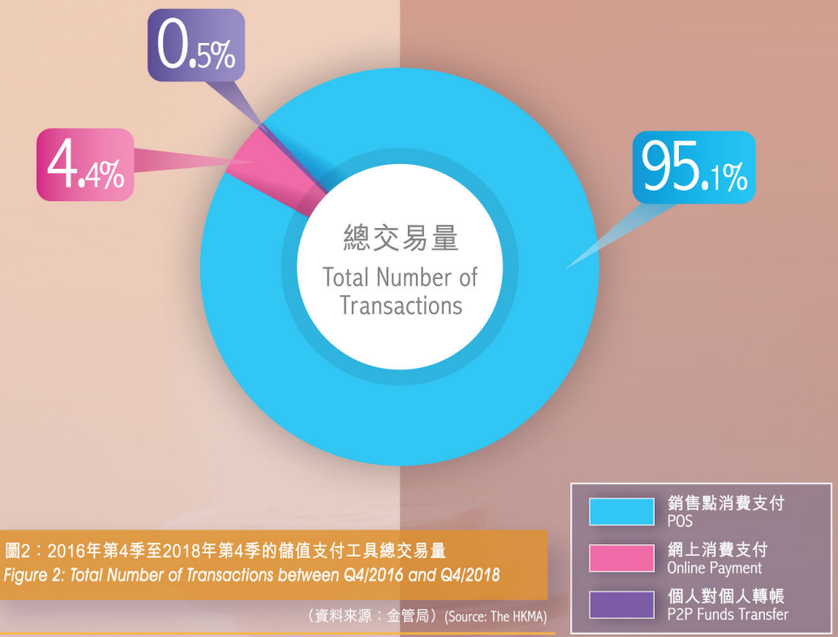


圖2：2016年第4季至2018年第4季的儲值支付工具總交易量
Figure 2: Total Number of Transactions between Q4/2016 and Q4/2018

（資料來源：金管局）(Source: The HKMA)

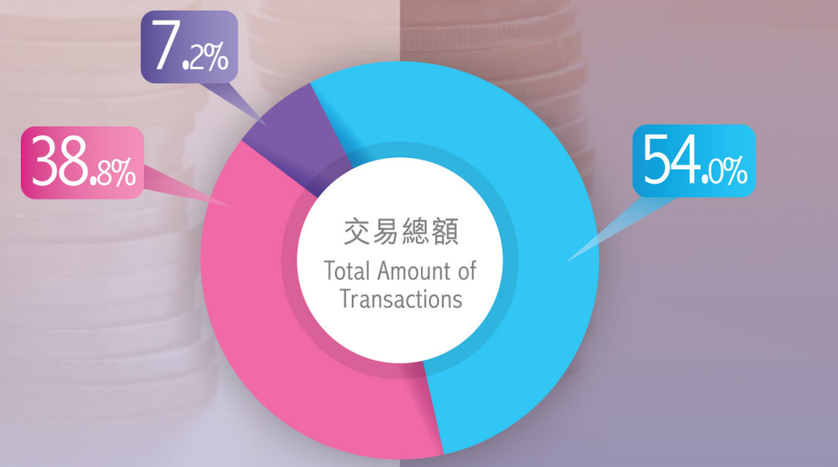


圖3：2016年第4季至2018年第4季的儲值支付工具總額
Figure 3: Total Amount of Transactions between Q4/2016 and Q4/2018

（資料來源：金管局）(Source: The HKMA)

[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.

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 30,262 million to HKD 48,099 million (+58.9%) respectively.

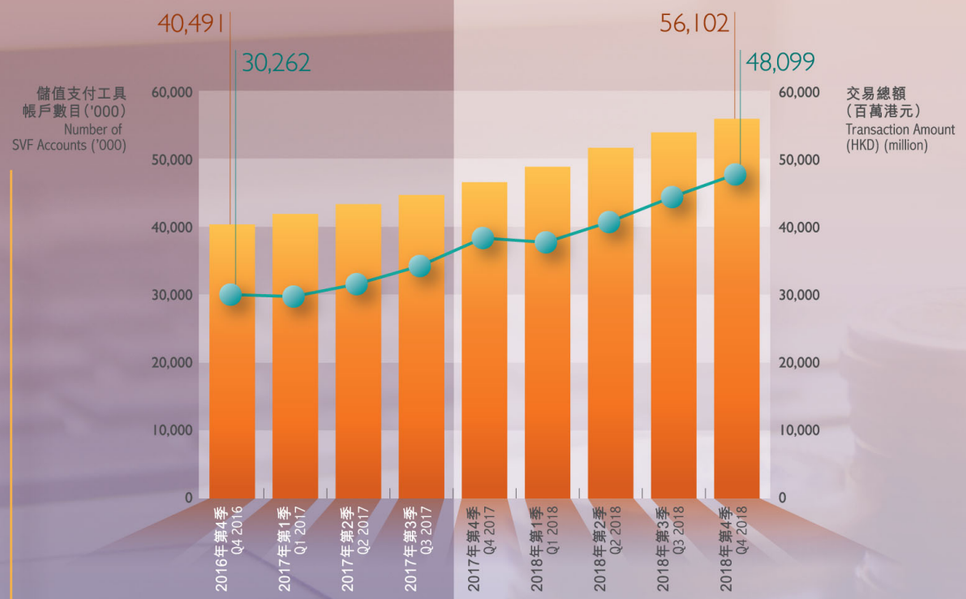


圖4：2016年第4季至2018年第4季的儲值支付工具帳戶總數，以及銷售點消費支付、網上消費支付和個人對個人轉帳之交易總額

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)

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 POS

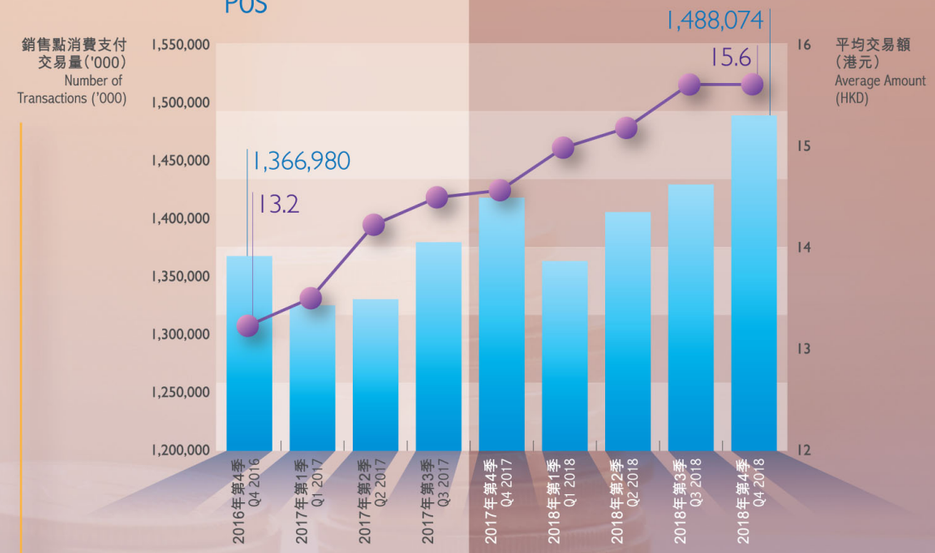


圖5：2016年第4季至2018年第4季的銷售點消費支付交易量及其平均交易額

Figure 5: Number of Point-Of-Sale Transactions and its Average Amount between Q4/2016 and Q4/2018

（資料來源：金管局）(Source: The HKMA)

銷售點消費支付是主要的交易方式，其交易總數由2016年第4季的14億，升至2018年第4季近15億。其2016年第4季至2018年第4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

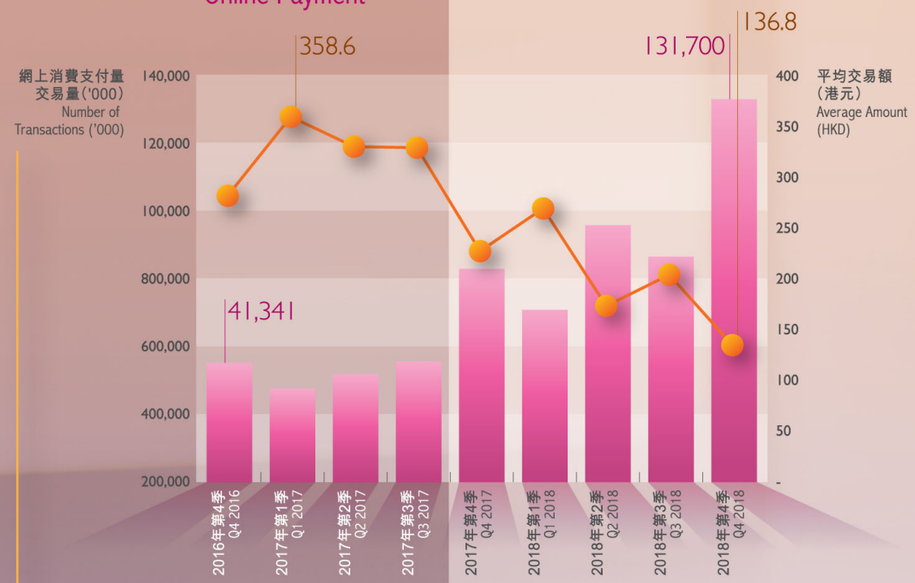


圖6：2016年第4季至2018年第4季的網上消費支付量及其平均交易額

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4季的4,130萬增加至2018年第4季的1億3,170萬（+218.6%）。平均交易額出現緩步下降趨勢，在2018年第4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

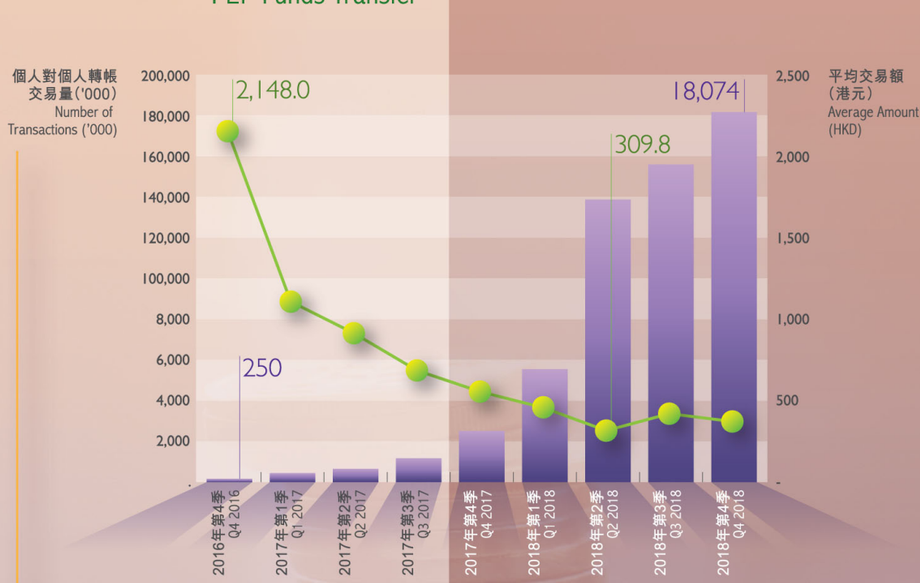


圖7：2016年第4季至2018年第4季的個人對個人轉帳交易量及其平均交易額

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4季的25萬大幅增加至2018年第1季接近560萬（+2,126.4%），並進一步急升至2018年第4季的約1,810萬（比2016年第4季+7,129.6%）。相反，個人對個人轉帳的平均金額由2016年第4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.

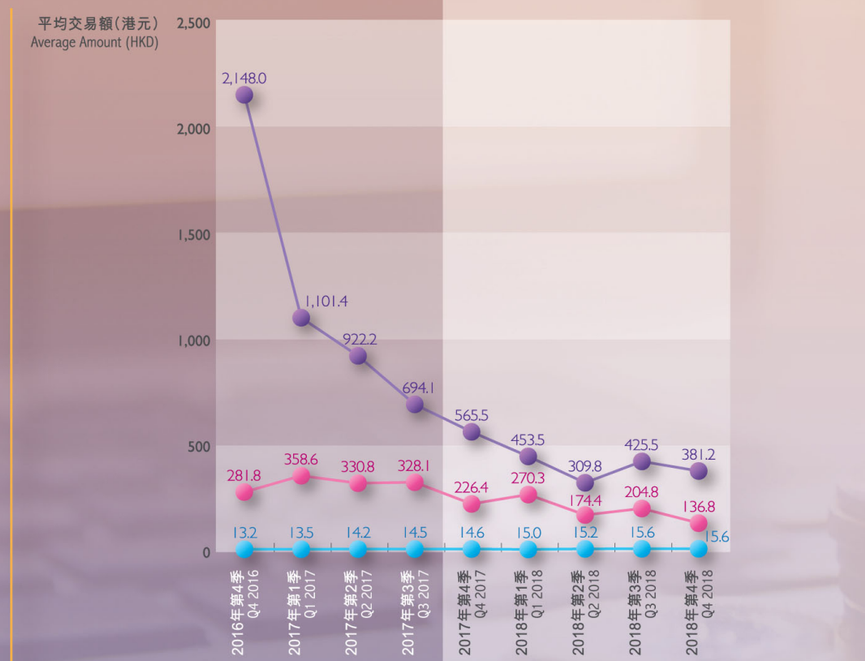


圖8：2016年第4季至2018年第4季的銷售點消費支付、網上消費支付及個人對個人轉帳的交易平均金額

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)

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 products[5]).

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

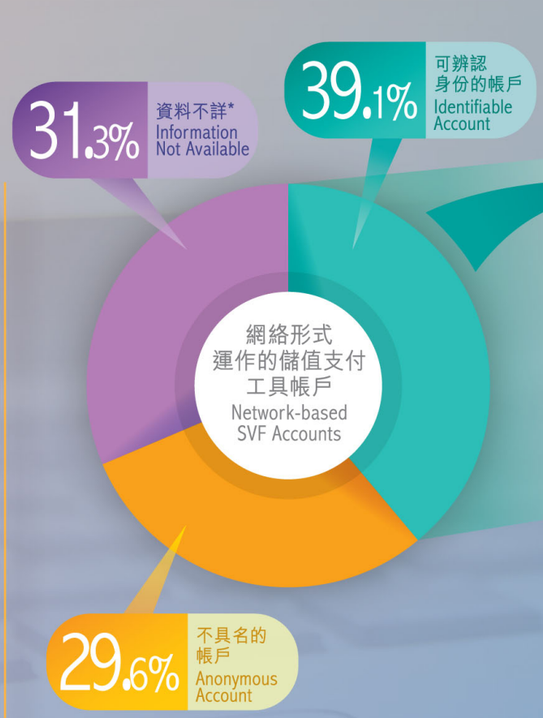
	所觀察的特點 Features Observed	已識別的風險 Risks Identified
「不具名」的儲值支付工具產品 **Anonymous SVF Products**	• 沒有客戶盡職審查的要求。 CDD is not required.	• 雖然部分儲值支付工具產品不需客戶盡職審查，但其不具名性質可能會潛在洗錢及恐怖分子資金籌集的風險或阻礙罪案偵查。 Although by default some SVF products are not required to conduct CDD, the anonymity of those products may still pose some ML/TF risk or hinder crime detection.
	• 部分只需流動電話號碼作登記。 Only mobile phone number suffices to register an SVF account.	• 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.
	• 服務範圍和帳戶限額均受限制。 The scope of services and the account limit are restricted.	• 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.
可辨認身份的儲值支付工具產品 **Identifiable SVF Products**	• 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戶盡職審查。 The identification information required depends on the ML/TF risk assessed on SVF products, and thus different level of CDD information is required accordingly.	• 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.
	• 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戶的個人資料，並參考來源可靠和獨立的文件[6]、數據和資料，以核實客戶身份。 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 sources[6] during on-boarding process.	
	• 部分服務或需要客戶綁定其銀行帳戶或信用卡，或獲取客戶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.).	

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 intelligence[7], 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 verification[8] 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

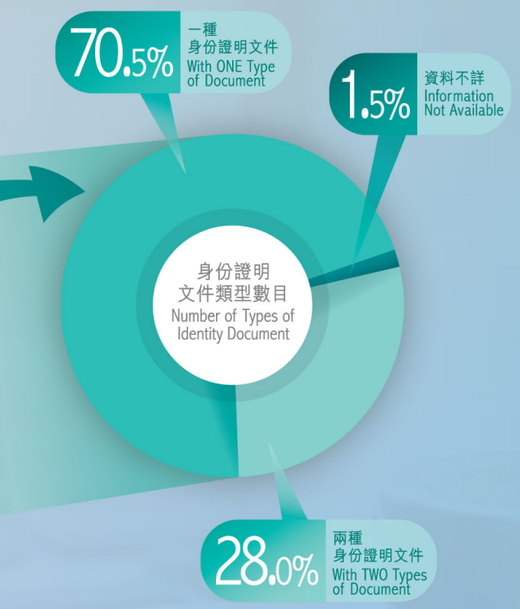


圖10：用於驗證可識別帳戶的身份證明文件類型數目
Figure 10: Number of Types of Identity Document Used for Verification for Identifiable Accounts

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)

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、商業登記等証明文件。

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

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	• 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") code[9] 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.	• 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，即通過掃描接收者的儲值支付工具二維碼以便於現金增值/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**	• 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優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 protection[10].)	• 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.
	• 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.	• 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**	• 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.	• 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**	• 接收來自儲值支付工具用戶的款項。 Receiving funds from SVF users.	• 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**	• 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。 Credit cards/ bank accounts bound or funds stored in SVF products can be used to settle online payments.	• 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**	• 商戶店內消費支付（本地/ 海外）。 In-store merchant payments (local/ overseas).	• 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**	• 向儲值支付工具用戶傳送款項。 Sending funds to other SVF users.	• 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)**	• 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。 Some SVF prepaid cards are reloadable by SVF accounts and vice versa via mobile application.	• 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。 Funds stored in SVF accounts could easily be transferred to anonymous SVF prepaid cards, and vice versa.
海外匯款 **Overseas Remittances**	• 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。 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.	• 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。 Funds may be channeled to other jurisdictions with higher ML/TF risk. • 執法機關進行海外調查時，資金難以追查。 It is difficult to trace funds during law enforcement agencies' investigation if an overseas jurisdiction is involved.
銀行帳戶轉帳 **Bank Account Transfers**	• 由儲值支付工具帳戶傳送款項至銀行帳戶。 Sending funds from SVF accounts to bank accounts.	/
提取現金 **Cash Withdrawals**	• 在本地/ 海外自動櫃員機或指定商戶提取現金。 Cash withdrawn at local/ overseas ATMs or designated merchants stores.	• 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。 Cash withdrawals at overseas ATM may facilitate cross-border ML and increase the difficulty in funds tracing. • 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代替品作非法用途。 The reloadable, portable and anonymous features of SVF prepaid cards may be misused by culprits as an alternative to cash in illegal activities.
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**	• 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。 Refunds of cash upon termination of SVF prepaid cards or SVF accounts.	• 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。 Anonymous SVF prepaid card holders may not be the genuine users if the SVF prepaid cards are stolen.

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.

案例 1 Scenario
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

「數據機池」是一組模擬數據機及軟件，允許連接大量智能卡，並控制該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。

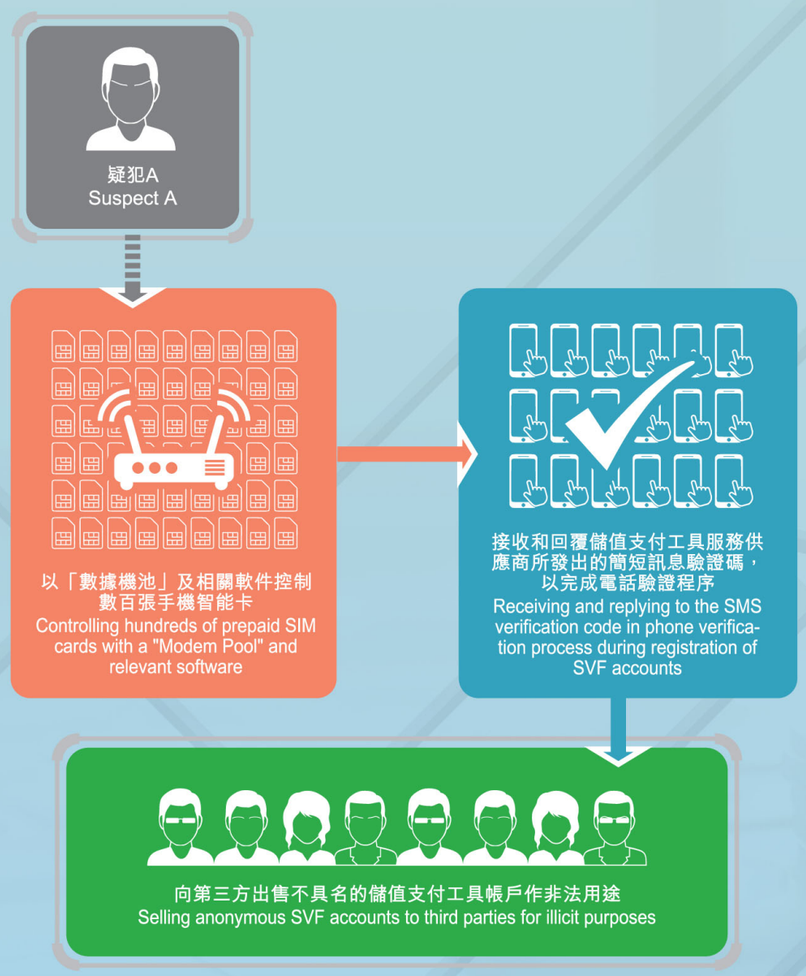
疑犯A購買數百張手機智能卡，並把卡插入數據機池，用來在登記儲值支付工具帳戶時接收和回覆短訊驗證碼，以完成大量帳戶的電話驗證程序。然而，這種登記並不需提供個人資料。該些以手機智能卡登記的不具名儲值支付工具帳戶其後被轉售予第三方作非法用途。

"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。
- 登記該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

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。

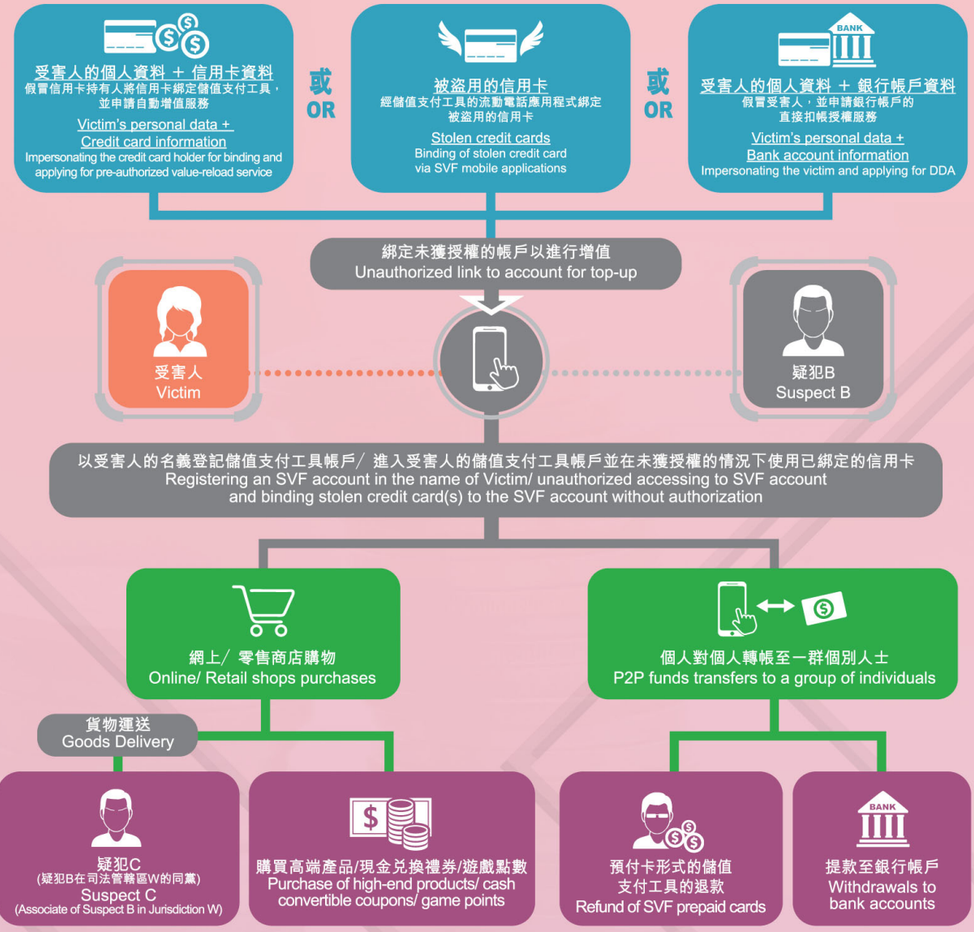
Suspect B then made purchases of high-end products/ cash coupons/ game points and settled payments through victim's linked credit card. The goods purchased were delivered to Suspect C (the associate of Suspect B) in Jurisdiction W. It is also noted that Suspect B would transfer funds that were withdrawn 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.]

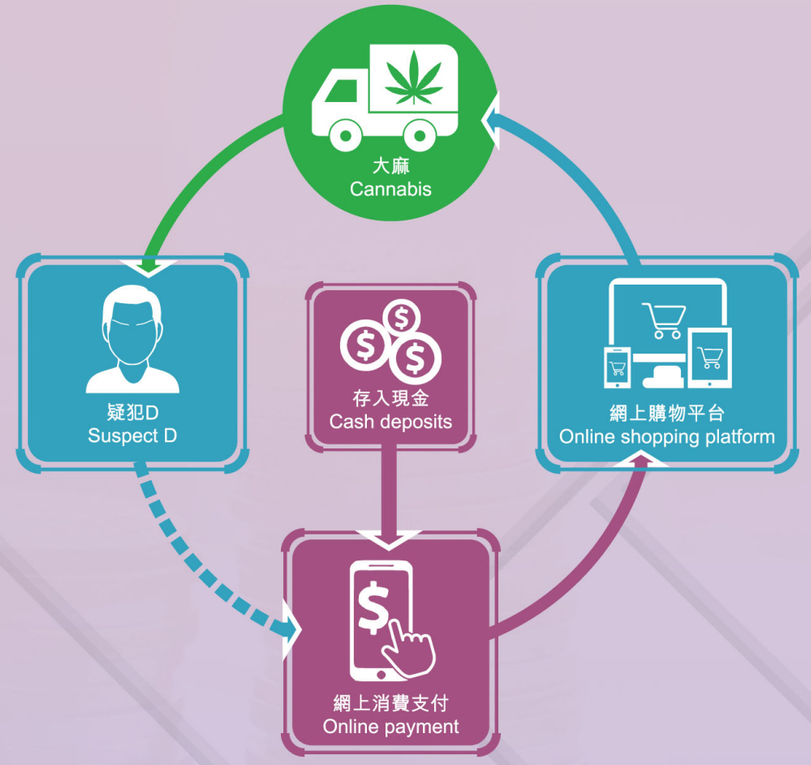
案例 Scenario 3

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.

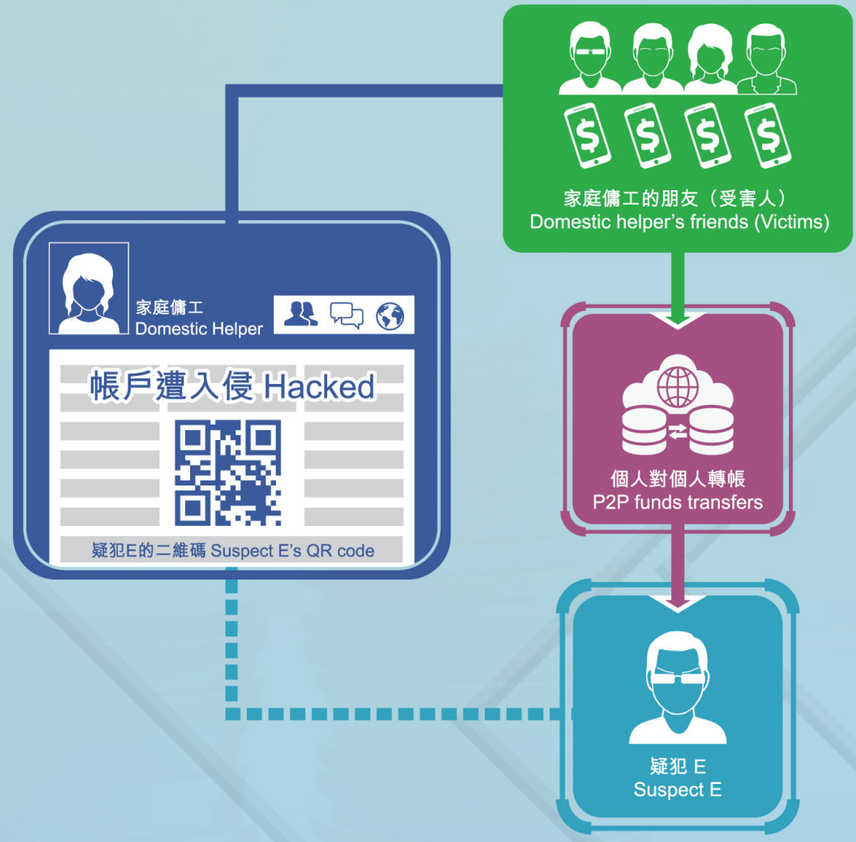
案例 Scenario 4

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。

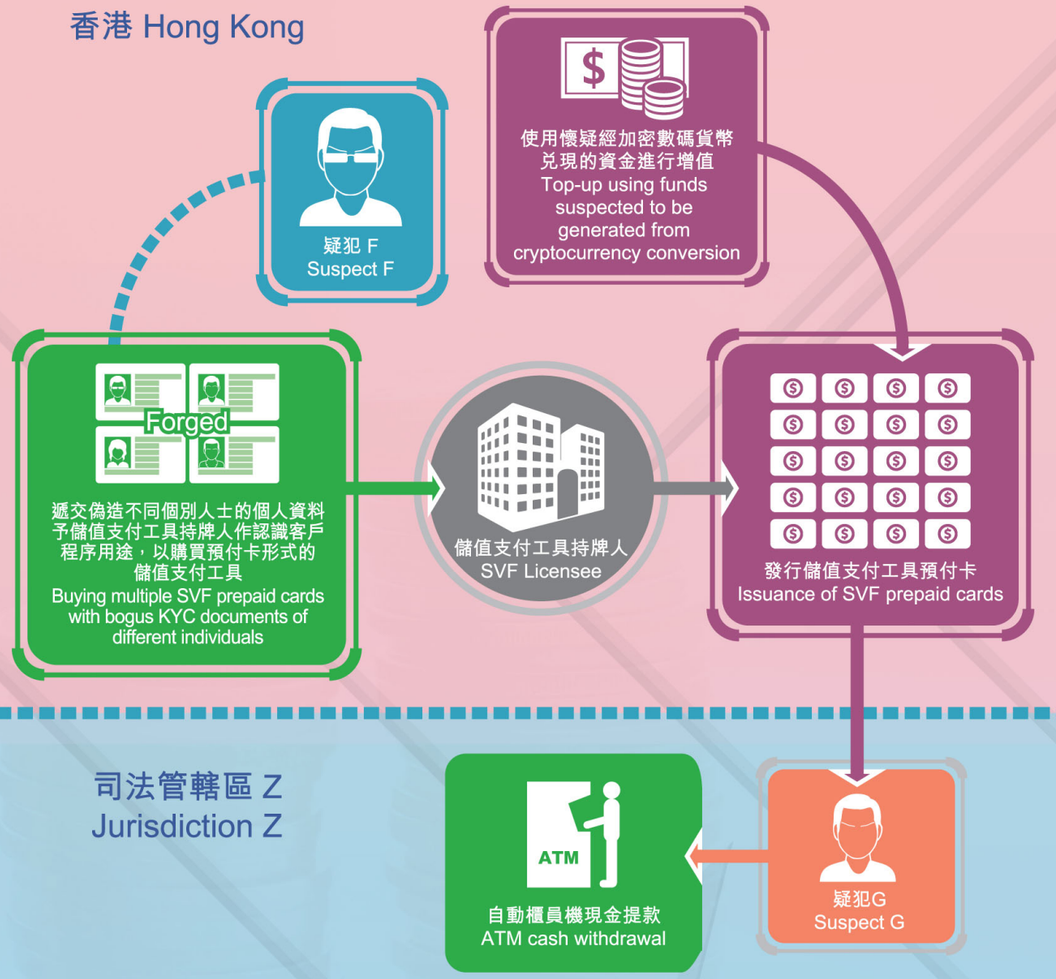
疑犯F使用大量預付卡形式的儲值支付工具作洗錢。他偽造不同個別人士的身份證明文件及住址證明，申請大量預付卡形式的儲值支付工具，以供相關儲值支付工具的持牌人作核實客戶程序用途。當申請獲批後，該些預付卡形式的儲值支付工具獲加密數碼貨幣相關行業的公司增值大額資金，並送付疑犯F在司法管轄區Z的同黨疑犯G。在政治不穩而貪污率高的司法管轄區（例如司法管轄區Z），這些預付卡形式的儲值支付工具被多次從自動櫃員機內提取現金。

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。

JFIU'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.

8

國際合作及參與

INTERNATIONAL COOPERATION AND REPRESENTATION

為了配合打擊洗錢及恐怖分子資金籌集的國際發展步伐，香港積極參與一些國際跨政府組織，監察世界各地的打擊洗錢及恐怖分子資金籌集標準，並評核該組織成員採用的標準是否全面或有何不足。同時，我們致力促進與策略同業伙伴的合作。本組人員亦主動參與不同種類的會議、工作坊及拜訪活動，而人員參加國際活動的熱忱，正好展現我們奮力加強伙伴合作，協力打擊跨國洗錢及恐怖分子資金籌集的決心。

打擊清洗黑錢財務行動特別組織（特別組織）

特別組織於1989年成立，屬跨政府組織，目的是促進國際合作，以制定有關打擊清洗黑錢及恐怖分子籌資活動的標準。特別組織現時由36個成員司法管轄區及兩個區域組織的代表組成。香港自1991年起一直是特別組織的成員。本組與其他政府機關，包括財經事務及庫務局緊密合作，致力為政策取得有效的成果。

In order to keep pace with international developments in the fight against ML and TF, Hong Kong takes part in a number of international intergovernmental organizations which oversee AML/CFT standards worldwide and thereupon to assess the extent to which the standards have been adopted by member jurisdictions. The JFIU is dedicated to fostering cooperation with our strategic counterparts as well. Officers of the JFIU actively participated in a wide range of conferences, workshops and visits. The participation of the JFIU officers in the international events demonstrated our commitment to boosting cooperation with our counterparts for combating transnational ML and TF.

Financial Action Task Force (FATF) on Money Laundering

FATF is an intergovernmental body and was established in 1989 to promote international cooperation on AML/CFT measures and it now consists of 36 member jurisdictions and two regional organizations. Hong Kong has been a member of the FATF since 1991. JFIU works in close partnership with other government agencies, including the Financial Services and the Treasury Bureau (FSTB), to contribute to effective policy outcomes within the FATF arena.

亞洲/ 太平洋反清洗黑錢組織（亞太反洗錢組織）

亞太反洗錢組織於1997年2月在泰國舉行的打擊清洗黑錢財務行動特別組織第4屆亞洲/ 太平洋反清洗黑錢座談會上協定成立，屬國際合作組織。鑒於亞洲/ 太平洋地區易受洗錢活動影響的風險增加，亞太反洗錢組織由41個司法管轄區組成，促進地區合作，倡議採用國際標準，以及向司法管轄區提供支援。香港於1997年成為亞太反洗錢組織的成員。

埃格蒙特組織（由世界各地的財富情報單位組成）

埃格蒙特組織於1995年4月成立，是一個現有159名成員的國際組織，負責加強全球財富情報單位在交換情報、培訓和分享專業知識等方面的合作，共同推行打擊洗錢及恐怖分子資金籌集的措施。本組主管於2017年7月4日在澳門特別行政區氹仔舉行的第24屆埃格蒙特組織全體會議獲選為亞洲/ 太平洋地區的其中一位地區代表。

Asia Pacific Group (APG) on Money Laundering

APG is an international cooperative body whose establishment was decided in February 1997 at the FATF 4th Asia/Pacific Money Laundering Symposium held in Thailand. In the context of increasing risks of vulnerability to ML in the Asia/Pacific region, the APG consists of 41 jurisdictions and was established to promote regional cooperation, adoption of the international standards, and to provide assistance to jurisdictions. Hong Kong has been a member of the APG since 1997.

The Egmont Group of FIUs (Egmont Group)

The Egmont Group consists of 159 members and is an international organization established in April 1995 with a mandate to improve cooperation on information exchange, trainings and expertise between FIUs around the world engaging in AML/CFT measures. The Head of JFIU was selected to be one of the Regional Representatives of the Asia /Pacific Region during the 24th Egmont Group Plenary Meetings in Taipa, Macao SAR on 4 July 2017.

研討會及工作坊

除了特別組織、亞太反洗錢組織及埃格蒙特組織的恆常全體會議外，本組代表亦出席各類研討會及工作坊，以擴展網絡，並就全球洗錢及恐怖分子資金籌集趨勢及相互評核的籌備工作，廣納其他司法管轄區的睿見以作深入了解。

Conferences and Workshops

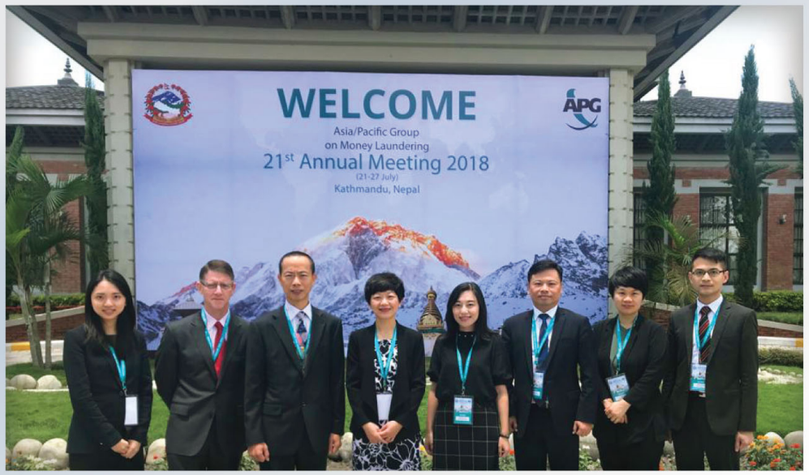
Apart from regular FATF, APG and Egmont Group plenaries, representatives from the JFIU attended various conferences and workshops to extend network and gain insights from other jurisdictions into global ML / TF trend and ME preparation work.

本組人員(右一)於2018年9月在澳洲悉尼出席第25屆埃格蒙特組織全體會議。

The JFIU officer (right one) attended the 25th Egmont Group Plenary Meetings in Sydney, Australia in September 2018.

2018年2月，時任毒品調查科高級警司(財富調查)(右一)及毒品調查科總督察(本組)(左三)與香港代表團在法國巴黎出席特別組織全體會議及工作小組會議。

In February 2018, the former Senior Superintendent of Police of Narcotics Bureau (NB) (Financial Investigation) (right one) and Chief Inspector of Police of NB (JFIU) (left three) joined the Hong Kong delegation to attend the FATF Plenary and Working Group Meetings in Paris, France.



2018年7月，時任毒品調查科總警司（左三）與香港代表團在尼泊爾加德滿都出席第21屆亞洲／太平洋反清洗黑錢組織周年會議。

In July 2018, the former Chief Superintendent of NB(left three) joined the Hong Kong delegation to attend the 21st APG Annual Meeting in Kathmandu, Nepal.

2018年8月，本組人員（左）在韓國釜山出席由特別組織舉辦的打擊擴散資金籌集訓練課程。

A JFIU officer (left one) attended the FATF Counter Proliferation Financing Training Course held in Busan, Korea in August 2018.

本組人員（中）於2018年9月在泰國曼谷出席由曼谷國際執法學院舉辦的反貪污及追討資產課程。

In September 2018, a JFIU officer (middle) attended the Anticorruption and Asset Recovery Workshop organized by ILEA in Bangkok, Thailand.

2018年10月，本組人員出席由經濟合作及發展組織舉辦題為「加密貨幣的現時趨勢、相關檢控及挑戰」的反清洗黑錢工作坊（專門課程）。

A JFIU officer attended the Anti-Money Laundering Workshop on Current Trends, Prosecutions and the Challenges around Cryptocurrencies (Specialty Programme) organized by OECD in October 2018.

本組人員於2018年10月在韓國首爾出席第5屆追討資產跨機構網絡—亞太國家追討資產培訓課程。

In October 2018, a JFIU officer attended the 5th Asset Recovery Interagency Network – Asia Pacific Asset Recovery Training in Seoul, Republic of Korea.

禮節性拜訪

本組向來重視世界各地的策略聯繫，並致力與國際伙伴建立和加強合作關係。回顧2018年，本組與中國內地、澳門特別行政區、法國及韓國安排禮節性拜訪，以及接待上述各地的代表團。透過此等訪問，各地人員可加深了解彼此的相互關係，並直接討論有關打擊洗錢及恐怖分子資金籌集的專項議題。

Courtesy Visits

JFIU treasures strategic international affiliation and committed to establish and strengthen the relations with international partners. In 2018, the JFIU arranged liaison visits and received delegations from France, Korea, Macao SAR and Mainland China. Such visits offered valuable opportunities for enhancing understanding mutual rapport and facilitating direct discussion on topical AML/CFT issues.

2018年10月，澳門金融情報辦公室訪問本組。
In October 2018, the Financial intelligence Office of Macao (GIF) visited the JFIU.

2018年12月，大韓民國警察廳及韓國財政經濟部金融情報分析院訪問本組。
In December 2018, the Korean National Police Agency and the Korea Financial intelligence Unit (KoFIU) visited the JFIU.

9

打擊清洗黑錢財務行動特別組織對香港進行的相互評核

FATF MUTUAL EVALUATION (ME) ON HONG KONG

作為香港的專門財富情報單位，本組一直不遺餘力，根據不斷演變的國際規定提升本港的相關標準，並與公私營機構的各類持份者合作，加強本組在打擊洗錢及恐怖分子資金籌集所充當的角色。

香港是特別組織的成員之一，須定期接受相互評核，而新一輪評核工作已於2018年展開。本組深信香港可藉此機會改善現行制度，務求符合各地財富情報單位均須遵從的國際標準為基準，以及提升打擊洗錢及恐怖分子資金籌集的能力。本組於2018年年中設立相互評核及國際政策組，並納入常設架構，這證明本組致力支持特別組織的相互評核機制。

全賴本港政策局協助統籌，本組與其他機構攜手合作，在相互評核過程中展示香港在打擊洗錢及恐怖分子資金籌集制度上的合規性及有效性。評核小組於2018年10月底至11月中在香港進行實地視察，其間，本組肩負重任，向評核小組小組成員全面且深入展示財富情報的使用情況，以及國際合作所付出的努力。

本組重視從相互評核所獲的國際見解和經驗，為未來發展制定可行的路線圖。在特別組織會員大會及亞太反洗錢組織周年會議取得香港的相互評核報告後，本組會繼續就相互評核的建議作出跟進。本組人員會不斷追求卓越，並持續參與本地或國際的打擊洗錢及恐怖分子資金籌集事宜，密切留意對財富情報單位的理想期望，以盡量發揮本組獨有的角色及功能。

As the designated FIU of Hong Kong, the JFIU spares no effort in advancing its standards as per evolving international requirements through collaborating with various stakeholders from public and private sectors to strengthen its role in the AML/CFT regime.

As one of the FATF members, Hong Kong commenced its ME process in 2018. The JFIU considers it as an invaluable opportunity to benchmark itself against global standards for FIUs and to enhance its AML/CFT capacity building. Since mid-2018, the JFIU has permanently created a new "ME and International Policy Team", as reflection to its commitment to supporting the ongoing peer review mechanism of implementation of FATF Recommendations among jurisdictions.

Through the coordination of local policy bureaux, the JFIU worked hand in hand with other agencies to demonstrate the level of technical compliance and effectiveness of Hong Kong's AML/CFT regime in the ME. To highlight, the JFIU played a pivotal role especially on showcasing the competent authorities' use of financial intelligence andFIU'sefforts on international cooperation during the onsite inspection held in Hong Kong between late October and mid November 2018.

The JFIU values the international insights and experience gained from the ME on the possible roadmap forbetter development in the future. It will continue to contribute to the follow-up process of ME after the adoption of Hong Kong's ME report at the FATF Plenary/ APG Annual Meeting. Personnel of the JFIU will also strive for excellence and keep in view the latest expectation and ideals on FIU through constant engagement with local/global AML/CFT community to leverage the unique role and function of the JFIU.

本組人員藉相互評核在香港舉行實地視察的機會，與國際評核小組就財富情報及打擊清洗黑錢及恐怖分子資金籌集等重要議題作積極交流。

The JFIU personnel took the opportunity of ME onsite inspection held in Hong Kong to exchange views on critical FIU and AML/CFT matters with the international assessment team.

10

打擊清洗黑錢及恐怖分子資金籌集的能力提升

AML/CFT CAPACITY BUILDING

有效的打擊洗錢及恐怖分子資金籌集措施亦包括能力建構和公眾教育。作為香港警務處加強打擊洗錢及恐怖分子資金籌集能力的一分子，本組負責為執法機關和其他伙伴舉辦財富調查訓練，並向金融機構和指定非金融企業及行業籌辦外展宣傳。所有能力建構措施旨在加強受訓人員在調查打擊洗錢及恐怖分子資金籌集時的知識和技巧，以及提高私營機構的認知，讓他們了解他們在香港打擊洗錢及恐怖分子資金籌集的機制擔當舉足輕重的角色和職責。

國際財富調查課程

本組每年舉辦兩次國際財富調查課程，為海外執法機關及其他同業伙伴安排特設的訓練。其中一個課程以英語授課，為世界各地打擊洗錢及恐怖分子資金籌集的伙伴而設，另一個則以普遍話授課，對象是大中華區的策略伙伴。課程旨在增進人員對打擊洗錢及及恐怖分子資金籌集方面的認知，涉獵課題包括法律和監管架構的發展、財富情報的交流、跨機構合作的重要性，以及最新罪案趨勢的風險。由於特別組織第四輪相互評核的實地訪問於2018年10月至11月進行，兩個原定在上述期間舉辦的國際財富調查課程相繼取消，但於2018年3月本組為印尼國家警察特意舉辦了一個以英語授課的國際財富調查課程。

Effective AML/CFT measures also include capacity building and public education. As an integral part of the HKPF's strategy to enhance AML/CFT capacity, JFIU assumed the responsibility for financial investigation training to LEAs and other counterparts, and external outreach to FIs and DNFBPs. All the capacity-building initiatives aim to strengthen participants with knowledge and skills in ML/TF investigations, and increase private sectors' awareness of their important roles and responsibilities in the AML/CFT regime in Hong Kong.

International Financial Investigation Course

JFIU organizes tailor-made training for overseas LEAs and other counterparts, through two international financial investigation courses which are to be conducted annually. One of these courses is conducted in English and targets AML/CFT partners worldwide while another one is conducted in Putonghua for our strategic partners within the Greater China Region. The courses aim to enrich participants' knowledge on AML/CFT issues, including the development of legal and regulatory framework, exchange of financial intelligence, inter-agency cooperation and the risks associated with the latest crime trends . Due to the 4th round of FATF ME onsite visit between October and November 2018, the two international financial investigation courses originally scheduled to be held during the period was suspended, while an additional international financial investigation course (English Class) was held in March 2018 with participants from Indonesian National Police.

內部財富調查課程

本組每年為香港警務處刑事單位的警務人員及法證會計辦事處同事舉辦四次財富調查課程，內容涵蓋打擊洗錢及恐怖分子資金籌集的最新國際標準、洗錢趨勢及案件類型、可疑交易報告，以及調查與洗錢相關案件的技巧。2018年，共有432名警務人員及3名來自法證會計辦事處人員接受訓練。

參與課程的印尼國家警察人員訪問香港金融管理局。
Participants from Indonesian National Police enjoyed their visit to the Hong Kong Monetary Authority.

Regional Financial Investigation Course

JFIU also provides four financial investigation courses annually for officers from the HKPF working in crime units and colleagues from the Forensic Accountants' Office (FAO). The courses cover the latest AML/CFT international standards, ML trends and typologies, suspicious transaction reporting and ML related investigation skills. The JFIU trained 432 police officers and three colleagues from FAO during the year.

來自香港警務處不同單位的學員在財富情報分析及洗錢調查的實踐環節積極互動。
Trainees from different formation of the HKPF actively interacted with each another during practical sessions on financial intelligence analysis and money laundering investigations.

打擊洗錢及恐怖分子資金籌集的外展宣傳

加強金融機構和指定非金融企業及行業的能力是有效打擊洗錢及恐怖分子資金籌集的最佳方法。就此，向市民大眾及策略伙伴籌備外展宣傳十分重要，可藉宣傳提高他們的認知，並爭取他們的支持，協力為香港建立穩健的打擊洗錢及恐怖分子資金籌集制度。

本組與財經事務及庫務局和保安局禁毒處通力合作，定期與其他持份者，例如香港證券業協會、香港證券及期貨從業員工會及地產代理監管局聯辦研討會。年內，本組以合辦或派員演講方式，參加了23場研討會，就可疑交易報告機制傳達重要訊息，並分享案例研究，以防止和偵查洗錢及恐怖分子資金籌集活動。

AML/ CFT Publicity Outreach

The best way to effectively combat ML and TF is capacity building in FI/DNFBP sectors. As such, it is vital to engage the general public and strategic partners through publicity outreach with a view to raising their awareness and enlisting their concerted support to build a robust AML/CFT regime in Hong Kong.

Working in partnership with the FSTB and Narcotics Division of Security Bureau (ND SB), the JFIU regularly co-organizes seminars together with other stakeholders such as Hong Kong Securities Association, Hong Kong Securities & Futures Employees Union and Estate Agents Authority. In 2018, the JFIU co-hosted or was invited as guest speakers in 23 seminars to address issues arising from the STR regime and share latest case studies with a view to preventing and detecting ML/TF activities.

本組人員獲香港不同的打擊清洗黑錢及恐怖分子資金籌集研討會邀請擔任演講嘉賓。

JFIU officers were invited to speak at different AML/CFT seminars in Hong Kong.

公布香港的洗錢及恐怖分子資金籌集風險評估報告（報告）

政府於2018年4月公布報告。

特別組織要求成員辨識及評估其洗錢及恐怖分子資金籌集風險，並採取相應的風險消減措施。該報告按特別組織的要求，評估香港有關行業及整體所面對的洗錢及恐怖分子資金籌集威脅及脆弱度。政府已根據風險評估的結果，採取了多項跟進措施。

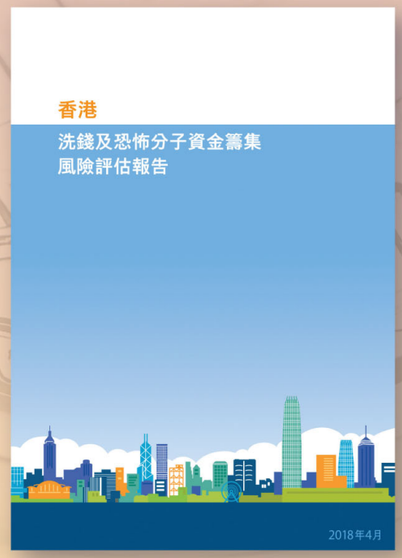
（詳情可在以下政府網頁瀏覽：https://www.fstb.gov.hk/fsb/aml/tc/risk-assessment.htm）

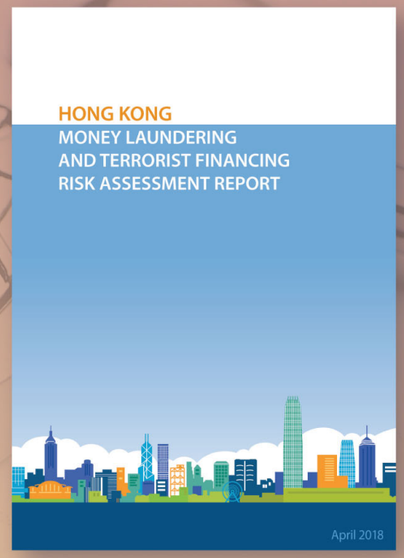
Publication of Hong Kong's Money Laundering and Terrorist Financing Risk Assessment Report (The Report)

The Government published the Report in April 2018.

Having regard to the recommendation of FATF for jurisdictions to identify and assess their ML/TF risks and to apply corresponding mitigating measures, the Report examines the ML/TF threats and vulnerabilities facing various sectors in Hong Kong and the city as a whole. The Report also identifies areas for further work and follow-up actions have been taken accordingly.

(Details can be referred from the government website: https://www.fstb.gov.hk/fsb/aml/en/risk-assessment.htm)





特別組織及反洗黑錢組織相互評核評估人員訓練工作坊

在財經事務及庫務局和香港警務處毒品調查科的協助下，特別組織及亞太反洗錢組織的秘書處人員於2018年1月8至12日期間在香港警察總部舉辦特別組織/ 亞太反洗錢組織相互評核評估人員訓練工作坊。

22名來自14個司法管轄區的執法機關、檢控、財富情報單位及監管人員參與工作坊；另有18名來自本港不同決策局、部門、金融監管機構及香港警務處的代表亦一同接受訓練。學員透過一系列單元課堂及實踐練習，進一步了解特別組織的⿴門評估方法和建議，並獲得資格成為特別組織和亞太反洗錢組織的相互評核評估人員。

FATF / APG Assessor Training Hong Kong

FSTB and NB of the HKPF supported and facilitated the FATF and the APG secretariats in the delivery of the FATF / APG Assessor Training Workshop from 8 to 12 January 2018 in the Hong Kong Police Headquarters.

A total of 22 representatives of LEAs, prosecutors, FIUs and regulatory practitioners from 14 jurisdictions as well as 18 Hong Kong participants from various policy bureaux, departments, financial regulators and the HKPF attended the Workshop. By acquiring the specialized knowledge of the FATF Assessment Methodology and Recommendations through a series of module presentations and practical exercises, participants thereafter are eligible as the assessors for the FATF and APG ME.

特別組織代表John Carlson及亞太反洗錢組織秘書處代表Eliot Kennedy向學員講述兩個組織的最新發展，並感謝財經事務及庫務局的合作和協助，以及就香港警務處所提供的招待和後勤支援，表示謝意。

Mr. John Carlson and Mr. Eliot Kennedy, representatives of the FATF and the APG secretariats shared the latest updates of FATF / APG and acknowledged the cooperation and assistance of the FSTB and expressed their appreciation to theHKPF for the hospitality and sound logistics support provided.

來自不同司法管轄區的學員在香港警察總部舉辦的特別組織/ 亞太反洗錢組織相互評核評估人員訓練工作坊踴躍交流意見。

Trainees from different jurisdictions actively participated in the FATF / APG Assessor Training Workshop held in the Hong Kong Police Headquarters.

11

常用詞彙

GLOSSARY

ABBREVIATIONS 簡稱	English	中文
ADCC	Anti-Deception Coordination Centre	反詐騙協調中心
AML	Anti-money Laundering	打擊清洗黑錢/ 打擊洗錢
AMLO 「《打擊洗錢條例》」	Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615 of the Laws of Hong Kong)	《打擊洗錢及恐怖分子資金籌集(金融機構) 條例》(香港法例第615章)
AML(A)O 「《打擊洗錢(修訂)條例》」	Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Ordinance (Cap. 615 of the Laws of Hong Kong)	《打擊洗錢及恐怖分子資金籌集(金融機構) (修訂) 條例》(香港法例第615章)
APG 「亞太反洗錢組織」	Asia/Pacific Group on Money Laundering (www.apgml.org)	亞洲／太平洋反清洗黑錢組織
C&ED	Customs and Excise Department	香港海關
CDD	Customer Due Diligence	客戶盡職審查
CFT	Counter-Financing of Terrorism	反恐籌資
DNFBPs	Designated Non-Financial Businesses and Professions	指定的非金融企業及行業
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405 of the Laws of Hong Kong)	《販毒 (追討得益) 條例》(香港法例第405章)
Egmont Group 「埃格蒙特組織」	The Egmont Group of Financial Intelligence Units (www.egmontgroup.org)	埃格蒙特金融情報組織
FATF 「特別組織」	Financial Action Task Force (www.fatf-gafi.org)	財務行動特別組織
FFMS	Federal Financial Monitoring Service (the Financial Intelligence Unit of the Russian Federation)	俄羅斯聯邦金融監督局(俄羅斯的財富情報單位)
FIs	Financial Institutions	金融機構
FID NB	Financial Investigation Division, Narcotics Bureau	毒品調查科財富調查組
FSTB	Financial Services and the Treasury Bureau	財務事務及庫務局
FIUs	Financial Intelligence Units	財富情報單位
HKPF	Hong Kong Police Force	香港警務處

ABBREVIATIONS 簡稱	English	中文
ICAC	Independent Commission Against Corruption	廉政公署
JFIU	Joint Financial Intelligence Unit (The Financial Intelligence Unit of Hong Kong)	聯合財富情報組 (香港的財富情報單位)
LEAs	Law Enforcement Agencies	執法機關
ME	Mutual Evaluation	相互評核
ML	Money Laundering	清洗黑錢／洗錢
MLA	Mutual Legal Assistance	相互法律協助
MOU	Memorandum of Understanding	諒解備忘錄
NB	Narcotics Bureau	毒品調查科
ND	Narcotics Division	禁毒處
OCTB	Organized Crime and Triad Bureau	有組織及三合會調查科
OSCO	Organized and Serious Crimes Ordinance (Cap. 455 of the Laws of Hong Kong)	《有組織及嚴重罪行條例》 (香港法例第455章)
RAU 「風險評估小組」	Money Laundering and Terrorist Financing Risk Assessment Unit	洗錢及恐怖分子資金籌集 風險評估小組
SB	Security Bureau	保安局
STRs	Suspicious Transaction Reports	可疑交易報告
STREAMS	Suspicious Transaction Report and Management System	可疑交易報告管理系統
SVF	Stored Value Facility	儲值支付工具
TCSPs	Trust & Company Service Providers	信託及公司服務提供者
TF	Terrorist Financing	恐怖分子資金籌集
UAE	United Arab Emirates	阿聯酋
UK	United Kingdom	英國
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575 of the Laws of Hong Kong)	《聯合國 (反恐怖主義措施) 條例》(香港法例第575章)
USA	United States of America	美國

12

年度交流活動
概覽

EVENT CALENDAR OF THE YEAR

第一季
1st Quarter

在香港出席打擊清洗黑錢財務行動特別組織/太平洋反洗黑錢組織相互評核評估人員訓練工作坊
Attendance at FATF and APG Assessor Training Workshop in Hong Kong

在深圳出席打擊清洗黑錢財務行動特別組織/太平洋反洗黑錢組織/歐亞反洗錢及反恐融資小組工作坊
Attendance at FATF/ APG/ Eurasian Group on Combating Money Laundering and Financial of Terrorism (EAG) Workshop in Shenzhen, China

在法國巴黎出席打擊清洗黑錢財務行動特別組織會議
Attendance at the FATF Plenary and Working Group Meetings in Paris, France

在香港出席受評國家培訓/相互評核事前工作坊
Attendance at the Assessed Country Training/ Pre-ME Workshop in Hong Kong

在阿根廷布宜諾斯艾利斯出席2018年埃格蒙特集團會議
Attendance at the 2018 Egmont Group Meetings in Buenos Aires, Argentina

法國司法學院訪問毒品調查科
Visit to the NB by the National School for the Judiciary, France

在泰國曼谷出席亞太經合組織反貪腐執法合作網絡追討資產訓練工作坊
Attendance at APEC Anti-Corruption Authorities and Law Enforcement Agencies Network Training Workshop on Asset Recovery in Bangkok, Thailand

第二季
2nd Quarter

荷蘭國家警察局訪問毒品調查科
Visit to the NB by the Netherlands Police

意大利財稅警察(隸屬財政及經濟部的軍事警察部隊) 訪問毒品調查科
Visit to the NB by the Italy Ministry of Economy & Finance

日本警察廳特別搜查幹部研修所訪問毒品調查科
Visit to the NB by the Highest Training Institute for Investigation Leaders of the Japanese National Police Agency

在英國倫敦出席財富情報交流前景會議
Attendance at the Future of Financial Intelligence Sharing Conference in London, The United Kingdom

在法國巴黎出席打擊清洗黑錢財務行動特別組織會議
Attendance at the FATF Plenary and Working Group Meetings in Paris, France

第三季
3rd Quarter

在尼泊爾加德滿都出席第21屆亞洲/太平洋反清洗黑錢組織周年會議
Attendance at the 21st APG Annual Meeting in Kathmandu, Nepal

在韓國釜山出席特別組織培訓及研究學院打擊擴散資金籌劃訓練課程
Attendance at the FATF Train Combating Proliferation Financing Training Course in Busan, Republic of Korea

法國警察訪問毒品調查科
Visit to NB by the French Police in Hong Kong

在澳洲悉尼出席第25屆埃格蒙特組織會議
Attendance at the 25th Egmont Group Plenary Meetings in Sydney, Australia

第四季
4th Quarter

澳門金融情報辦公室訪問聯合財富情報組
Visit to the JFIU by the Financial Intelligence Office of Macao

在法國巴黎出席打擊清洗黑錢財務行動特別組織全體會議及工作小組會議
Attendance at the FATF Plenary and Working Group Meeting in Paris, France

海南省公安廳訪問毒品調查科
Visit to NB by the Public Security Department, Hainan Province

打擊清洗黑錢財務行動特別組織就第四輪相互評核訪問香港警務處
Visit to HKPF by the FATF for 4th Round of FATF Mutual Evaluation on Hong Kong SAR

澳洲交易報告及分析中心訪問聯合財富情報組
Visit to JFIU by the Australian Transaction Reports and Analysis Centre

大韓民國警察廳及大韓民國財富情報組訪問聯合財富情報組
Visit to JFIU by the Korean National Police Agency and the Korean Financial Intelligence Unit

公安部經濟犯罪偵查局訪問毒品調查科
Visit to the NB by the Bureau of Economic Crime Investigation under Ministry of Public Security

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

http://www.jfiu.gov.hk/