STRATEGIC ANALYSIS REPORT ON EMAIL SCAMS

策略分析報告 - 電郵騙案

Joint Financial Intelligence Unit
聯合財富情報組

STRATEGIC ANALYSIS REPORT ON EMAIL SCAMS

策略分析報告 - 電郵騙案

OVERVIEW 概覽

策略分析是本組持續進行的工作，長遠而言，可提高各機構所呈報資料的質素，以及改善本組的情報分析及發布。

此策略分析報告針對本港的電郵騙案，對象是政府決策局、監管機構、執法機關、財富情報單位及私人界別之中，負責打擊洗錢及恐怖分子資金籌集的伙伴。

本報告重點介紹最新的類型學分析，並撮述就電郵騙案拓展的情報，謹望情報成果進一步促進情報交流，促成執法行動，並就制訂政策及規例提供意見。報告闡述現有/ 潛在的洗錢風險並提出可行建議，冀助拓展打擊洗錢及恐怖分子資金籌集方面的知識，能在政策和行動層面，應付現時和未來的需要。

To the JFIU, strategic analysis reflects its ongoing efforts to enhance the quality of information reported by entities as well as intelligence analysis and dissemination by the JFIU in the long run.

The JFIU presents this Strategic Analysis Report (Report) on email scams in Hong Kong to target Anti-Money Laundering/ Counter-Financing of Terrorism (AML/CFT) players in government policy bureaux, regulatory agencies, law enforcement bodies, FIUs and private sectors.

The Report highlights the latest typologies and summarizes the value-added intelligence cultivated on email scams. It is hoped that the intelligence product can further promote intelligence exchanges, trigger law enforcement actions and provide insights into policy and regulation formulation. It is also hoped that existing/ possible money laundering (ML) risks illustrated and observations proposed in the Report are conducive to the development of AML knowledge for current and future needs at both policy and operational levels.

KEY FINDINGS
主要結果

戶口詳情

- 2016年，有1,301宗欺詐交易涉及電郵騙案，共涉款22億港元，至於2017年(1月至6月)，則有337宗共涉款5.689億港元的欺詐交易；
- 源自電郵騙案的非法資金，於2016年至2017年6月期間存入香港1,119個銀行戶口；
- 約92%涉及電郵騙案的戶口屬公司戶口；
- 約78%董事持中國身分證明文件[1]，約16%董事持香港身分證；以及
- 約69%戶口在開設逾180天後始接收非法資金。

戶口活動

- 歐洲、北美洲和亞洲乃三大非法資金之來源；
- 以金額計算，約60%非法資金在接收當日移走[2]，約18%於收款次日移走；
- 接收非法資金後，近半資金以本地轉帳形式轉帳至本地銀行；以及
- 約40%資金經由海外匯款轉移。

主題分析

更換公司董事

- 更換公司董事是挪用已有公司銀行戶口以接收非法資金最常見的方法之一；以及
- 18%涉及電郵騙案的公司在接收非法資金前0至30日曾更換董事。

戶口簽署人

- 研究涵蓋的75個公司戶口之中，60%公司既不通知銀行更換董事，又不要求更新戶口簽署人。

試驗付款

- 約24%戶口錄得試驗付款交易(很可能用作測試戶口是否有效)；以及
- 金額大多少於500港元。

Account Information

- In 2016, 1,301 fraudulent transactions amounting to HKD2.2 billion were involved in email scams, whilst in 2017 (January to June), 337 fraudulent transactions amounting to HKD568.9 million were involved;
- All illicit fund originated from email scams was sent to 1,119 bank accounts in Hong Kong between January 2016 and June 2017;
- Around 92% of the accounts involved in email scams were corporate accounts;
- Around 78% of the directors were Chinese Identity Document holders[1] and about 16% of the directors were Hong Kong Identity Card holders; and
- Nearly 69% of the accounts were opened over 180 days prior to the receipt of illicit fund.

Account Activities

- Top three regions from which illicit fund was sent were Europe, North America and Asia;
- Around 60% of the fund dissipations[2], in terms of amount, were conducted within the same day as the day of receipt of illicit fund whilst around 18% of the same was conducted on the next day of following the receipt of illicit fund;
- Upon the receipt of the illicit fund, nearly half of the dissipated fund was transferred to domestic banks by means of local transfers; and
- Around 40% of the dissipated fund was sent via overseas remittances.

Thematic Analyses

Change of Company Directorship

- Changing company directorship is considered one of the most prevalent ways in appropriating readily available corporate bank accounts for the subsequent receipt of illicit fund; and
- 18% of the companies involved in email scams were found to have their directorships changed 0-30 days prior to the receipt of illicit fund.

Account Signatories

- 60% of 75 targeted corporate accounts neither informed the banks of the change of directorships nor requested for account signatory updates.

Test Payment

- About 24% of the accounts recorded test payment transactions (which were likely used to test the accounts' validity); and
- The amount of the test payment was mainly below HKD500.

1. 包括中國身分證/ 往來港澳通行證/ 中國護照持有人。
Including Chinese ID Card holders/ China Two-way Permit holders/ Chinese Passport holders.
2. 只包括每宗欺詐交易最主要的三次資金轉移。
Including only the main three fund dissipations in each fraudulent transaction.

INTRODUCTION 引言

本報告重點介紹本組就電郵騙案進行的策略分析，包括香港現況摘要及相關的主題分析。

本組仔細分析財富情報，向相關持份者提供增值成果。本報告所載資料，主要摘自本組接獲的資料、香港公司註冊處及其他來源。本報告檢視本組在2016年1月至2017年6月(檢討期)接獲的資料[3]，當中包括於戶口詳情、戶口活動、主題分析等。

This Report provides highlights of strategic analysis on email scams conducted by the JFIU, including a summary of the prevailing situation in Hong Kong and related thematic analyses.

The JFIU carries out detailed analysis of financial intelligence and delivers value-added outputs to relevant stakeholders. The information in this Report has been drawn primarily from information[3] received by the JFIU. It also contains information from the Companies Registry in Hong Kong and from other sources. This Report also examines information received by the JFIU from January 2016 to June 2017 (the review period), focusing on account information, account activities, thematic analyses, etc.

SUMMARY OF EMAIL SCAMS IN HONG KONG 本港電郵騙案摘要

表1
Table 1

	Total Number of Bank Accounts[4] Involved 涉及銀行戶口[4]總數	Total Number of Fraudulent Transactions 欺詐交易總數	Total Amount Involved[5] (HKD million) 涉及金額[5]總數 (百萬港元)	Average Amount Involved per Fraudulent Transaction (HKD million) 欺詐交易涉及金額平均數 (百萬港元)
2016	903	1,301	2,151.1	1.7
2017 (January to June) (1月至6月)	216	337	568.9	1.7

3. 由於發生電郵騙案至本組得悉事件存在時差，接獲的資料未必全面反映實情。2017年中發生的案件或未能涵蓋。
The information received by the JFIU may not completely reflect the situation as there is time difference between the occurrences of email scams and the receipt of information. Some of the email scams occurred in mid-2017 may not be covered.
4. 銀行戶口數目以首次接收欺詐交易者計算。
Only bank accounts receiving fraudulent transactions for the first time were counted.
5. 包括試圖進行但不成功的交易。
Including attempted but non-successful transactions.

Reported Suspicious Indicators in Email Scam Transactions

電郵騙案交易的可疑指標

可疑指標分析

「暫存款項」、「交易金額與背景不相稱」及「大額交易」，是涉及電郵騙案的戶口之中，最常見的三個可疑指標[6]。

Suspicious Indicator Analysis

'Temporary repository of fund', 'transactions incommensurate with the background' and 'large transaction' are three of the most prevalent suspicious indicators[6] in accounts involved in email scams.

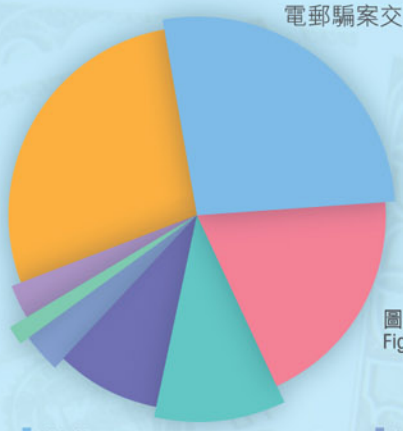


圖1
Figure 1

26.8%	暫存款項 Temporary repository of fund	2.9%	大額現金交易 Large cash transaction
19.1%	交易金額與背景不相稱 Transaction incommensurate with the background	1.6%	非直接交易 Indirect transaction*
10.3%	大額交易 Large transaction	2.7%	無商業目的之交易 Transaction with no business purpose
8.8%	非本地居民個人戶口 Non-resident personal account	27.8%	其他 Others**

* 間接交易指交易並非直接轉帳至指定的收款人，而是經一個或多個對手方轉折交易，加以掩藏。
**其他指i) 離岸公司、ii) 「掉頭式」交易、iii) 空殼公司、iv) 由簽署人控制的帳戶、v) 臨時帳戶、vi) 不合經濟原則的交易、vii) 鈔票帶家或未經註冊的匯款代理人、viii) 客戶堅持進行較不穩妥的交易，以及ix) 投保巨額保險/ 作出大筆投資後，迅速贖回。

* Indirect transaction refers to transaction that is not sent to the intended recipient directly, but layered by one or more counterparties.
**Others refer to i) Offshore company, ii) U-turn transactions, iii) Shell company, iv) Account operated by signatory, v) Transient account, vi) Uneconomical transaction, vii) Money courier or unlicensed money service operator, viii) Customer insisted to use less secured transactions and ix) Heavy insurance policy / investment followed by quick redemption.

ACCOUNT INFORMATION
戶口詳情

戶口種類

近92%涉及電郵騙案的戶口屬公司戶口。

Account Types

Nearly 92% of the accounts involved in email scams were corporate bank accounts.

表2
Table 2

	Corporate Accounts 公司戶口	Number of Companies Involved 涉及的公司數目	Personal Accounts[7] 個人戶口[7]	Number of Account Holders[8] Involved 涉及戶口持有人[8]數目
2016	825 (91.4%)	798	78 (8.6%)	84
2017 (January to June) (1月至6月)	200 (92.6%)	197	16 (7.4%)	16

6. 每宗欺詐交易或涉及多於一個指標。
More than one indicator may be used for each fraudulent transaction.
7. 包括個人聯名戶口。
Including personal joint accounts.
8. 包括個人聯名戶口持有人的實際人數。
Including the actual number of account holders of personal joint accounts.

Type of ID Documents held by Directors

董事所持的身份證明文件類型

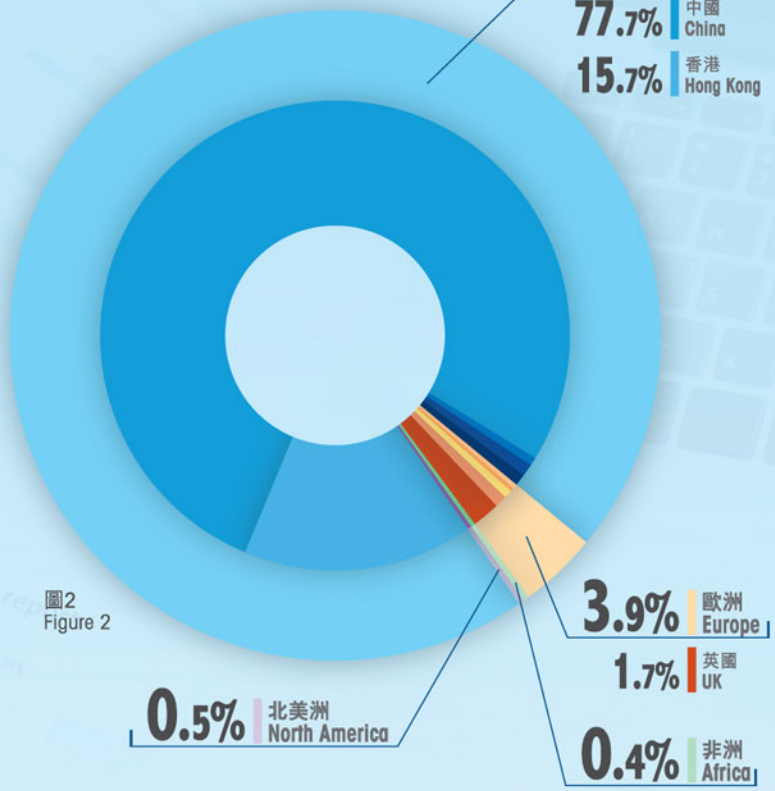


圖2
Figure 2

公司戶口

在涉及的公司戶口之中，即995間公司當中，約94%公司在香港註冊。

就2017年1月至6月涉及電郵騙案的公司分析其董事身分[9]，發現229名董事中，218名董事(95.2%)是亞洲人，9名(3.9%)是歐洲人。當中中國身分證明文件及香港身分證持有人佔總數逾90%。

Corporate Accounts

Among the corporate accounts involved, around 94% of 995 companies were Hong Kong incorporated.

Further analysis on the directorship[9] of the companies which accounts were involved in email scams in 2017 (January to June) indicated that 218 out of 229 directors (95.2%) were Asian whilst nine directors (3.9%) were European. Chinese Identity Document holders and Hong Kong Identity Card holders constituted over 90% of the total number.

個人戶口

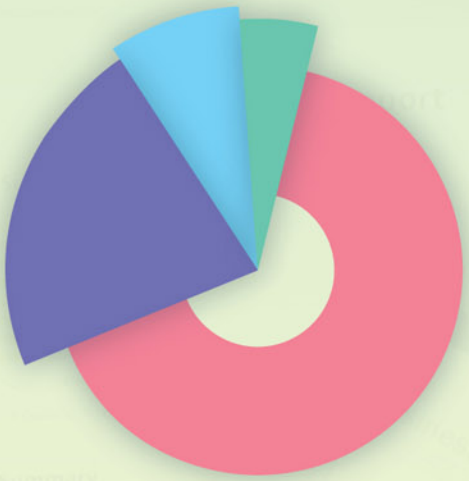
65%之個人戶口持有人乃香港身分證持有人，其次是中國身分證明文件持有人。

至於個人戶口持有人的年齡組別，2016年未見特定年齡組別佔多數，而2017年(1月至6月)涉及電郵騙局的個人戶口數目有限，未有定論。

Personal Accounts

65% of the personal account holders were Hong Kong Identity Card holders, followed by Chinese Identity Document holders.

Regarding the age group of the personal account holders, no particular age group dominated in 2016. Given the limited number of personal accounts involved in email scams in 2017 (January to June), no conclusive observation could be drawn.



65.0% 香港身分證 Hong Kong Identity Card
22.0% 中國身份証明文件 Chinese Identity Document
8.0% 其他旅遊證件 Travel Document of Other Jurisdictions
5.0% 資料未能提供 Information Not Available

* 其他司法管轄區包括澳洲、加拿大、印度、菲律賓及台灣。
Other jurisdictions include Australia, Canada, India, the Philippines and Taiwan.

圖3：身份證明文件種類
Figure 3: Type of ID Documents

9. 基於開設戶口時提供的資料作分析，重複的記錄已予以修正。
Analysis was based on the information provided at the time of account opening, with rectification on multiple entries.

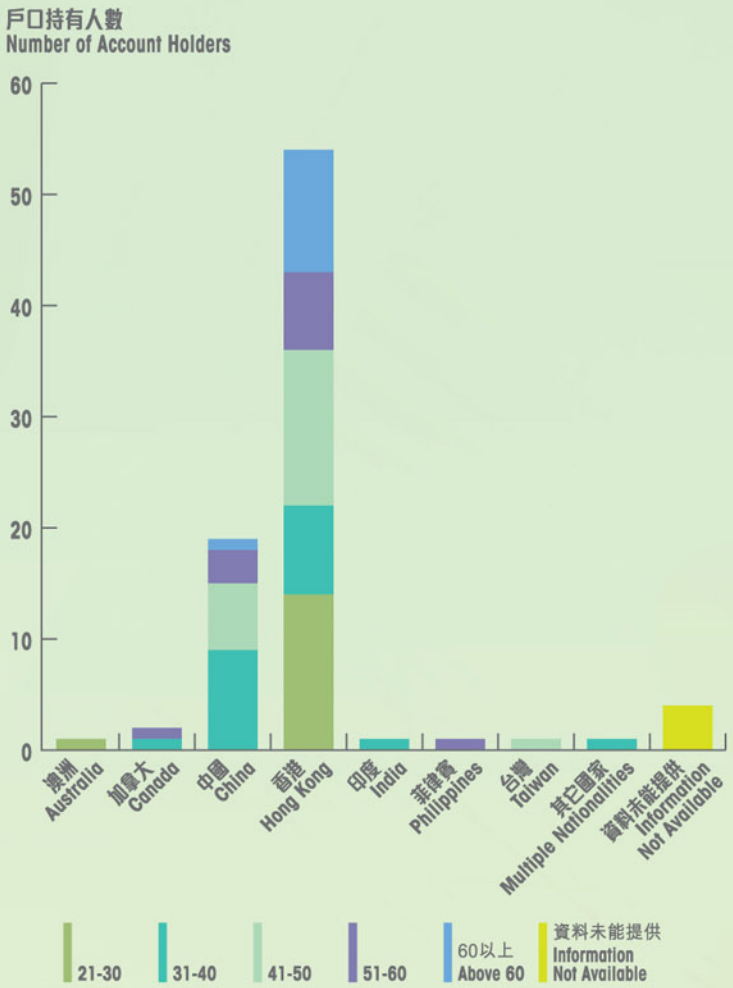


圖4：個人戶口持有人所持之身份證明文件及年齡組別 (2016年)
Figure 4: Type of ID Document held by and Age Group of Personal Account Holders (2016)

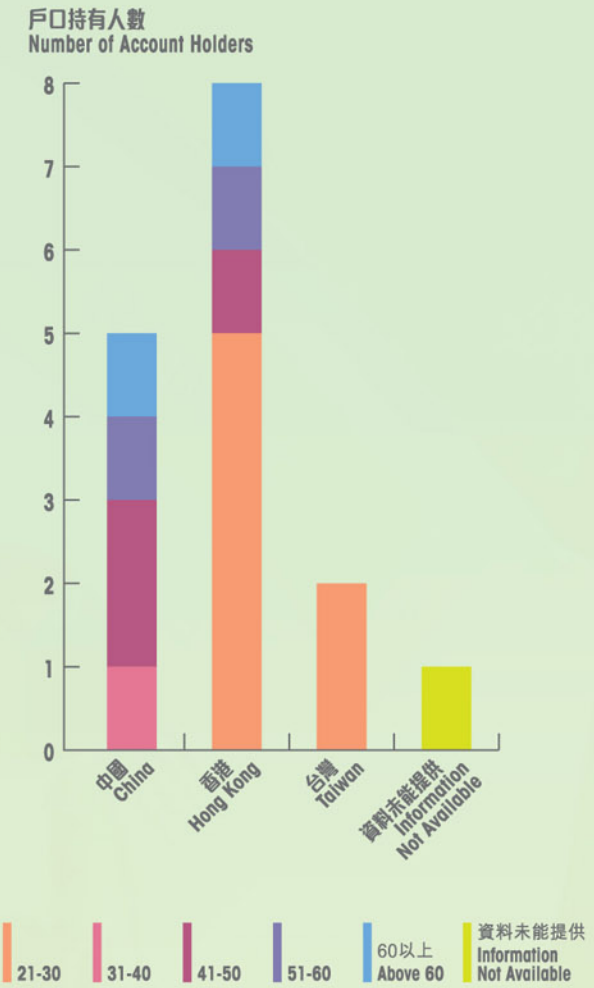


圖5：個人戶口持有人所持之身份證明文件及年齡組別 (2017年1月至6月)
Figure 5: Type of ID Document held by and Age Group of Personal Account Holders (2017 January to June)

開設戶口

檢討期內，在1,119個戶口之中，有770個(68.8%)在接收非法資金前逾180天開設。

Account Opening

During the review period, 770 (68.8%) out of 1,119 accounts were opened over 180 days prior to the receipt of illicit fund.

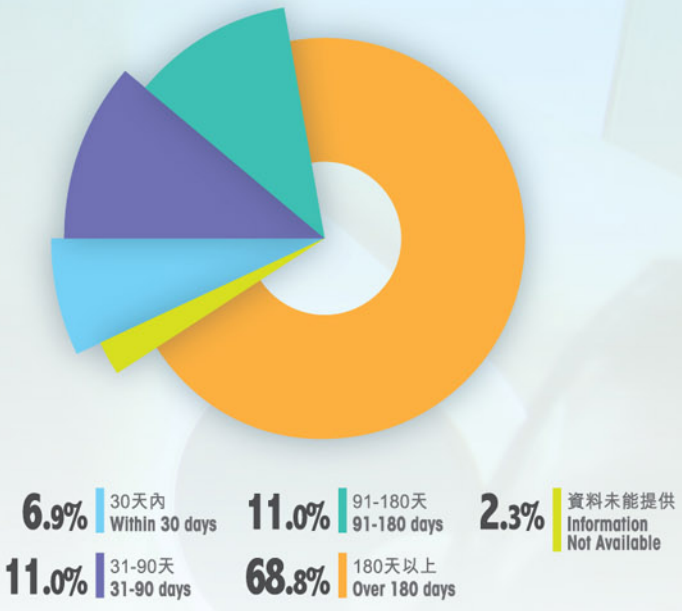


圖6：接收非法資金前開設戶口的時間
Figure 6: Periods of Account Opening Prior to the Receipt of Illicit Fund

ACCOUNT ACTIVITIES 戶口活動

按地區[10]劃分資金來源
Origin of Fund by Regions[10]

歐洲、北美洲和亞洲受害人的損失[11]，分別為10.666億港元、7.581億港元和4.995億港元，分別佔總額27.207億之39.2%、27.9%和18.4%。

The total amount of loss[11] from victims in Europe, North America and Asia were HKD1,066.6 million, HKD758.1 million and HKD499.5 million respectively, equivalent to 39.2%, 27.9% and 18.4% of the total amount HKD2,720.7 million.

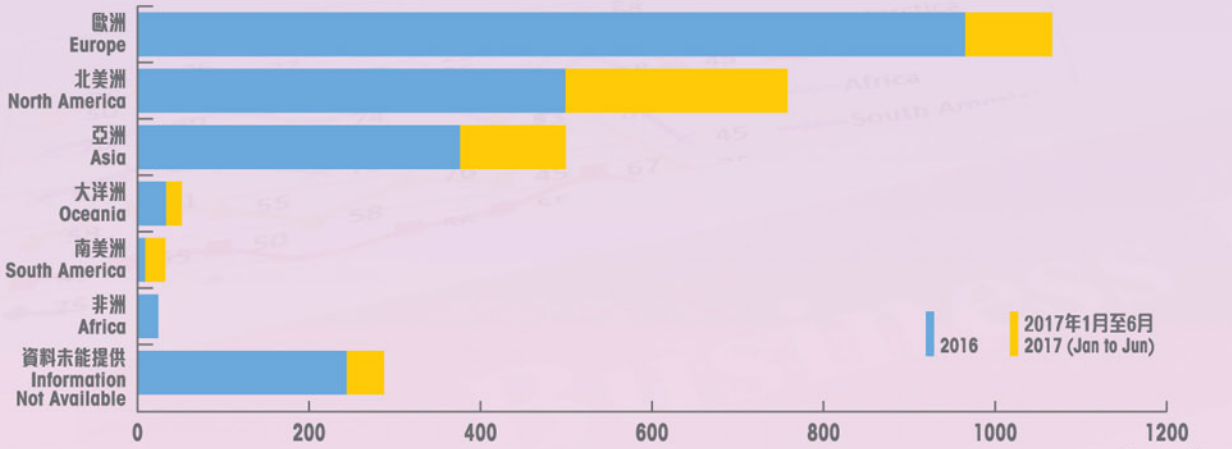


圖7：受害人損失金額(按地區劃分)
Figure 7: Amount of Loss Suffered by Victims (by Regions)

	Europe 歐洲	North America 北美洲	Asia 亞洲	Oceania 大洋洲	South America 南美洲	Africa 非洲	Information Not Available 資料未能提供
2016	965.2	499.2	376.4	33.6	9.1	24.3	244.0
2017 (Jan to Jun 1月至6月)	101.4	258.9	123.1	18	23.4	0.5	43.6

港元(百萬)
HKD (million)

按司法管轄區而言，2016年非法資金的三大來源(包括行騙未遂[12]的電郵騙案)，是美國(4.386億港元)、羅馬尼亞(3.408億港元)和香港(1.645億港元)，而2017年(1月至6月)的三大來源則是美國(2.37億港元)、西班牙(4,730萬港元)和中國(3,920萬港元)。

圖8至圖13，分項列出損失[11]最多的三個地區的損失總額百分比。

By jurisdiction, in 2016, the top three origins of illicit fund, including unsuccessful email scams[12], were the US (HKD438.6 million), Romania (HKD340.8 million) and Hong Kong (HKD164.5 million) whilst in 2017 (January to June), they were the US (HKD237 million), Spain (HKD47.3 million) and China (HKD39.2 million).

A breakdown of the total loss[11] in percentage of the top three regions is illustrated at Figures 8-13.

10. 參照特別組織的分區劃分(http://www.fatf-gafi.org/countries/World-Wide)。
Reference of Classification of Region was made to the FATF (http://www.fatf-gafi.org/countries/World-Wide).

11. 包括因電郵騙案致使非法資金存入疑犯香港戶口的交易，以及原本會進行但基於下列原因未有入帳的交易(行騙未遂的電郵騙案)：(i) 匯款銀行在欺詐款項存入疑犯戶口之前撤回，(ii) 受害人揭發騙案而沒有匯款，以及(iii) 在舉報電郵騙案前，疑犯戶口已遭封鎖。
Including those transactions that were actually made with illicit fund being credited to suspects' accounts in Hong Kong as a result of email scams, as well as transactions that would have been made (in 'attempted' email scams) but the fund eventually was not credited to the account (i) the fraudulent payments were recalled by remitting banks before reaching the suspects' accounts, (ii) victims unveiled the scam and did not remit the payment and (iii) the suspects' accounts were blocked prior to the report of email scams.

12. 以及原本會進行但基於下列原因未有入帳的交易(行騙未遂的電郵騙案)：(i) 匯款銀行在欺詐款項存入疑犯戶口之前撤回，(ii) 受害人揭發騙案而沒有匯款，以及(iii) 在舉報電郵騙案前，疑犯戶口已遭封鎖。
Transactions that would have been made (in 'attempted' email scams) but the fund eventually was not credited to the account (i) the fraudulent payments were recalled by remitting banks before reaching the suspects' accounts, (ii) victims unveiled the scam and did not remit the payment and (iii) the suspects' accounts were blocked prior to the report of email scams.

Top Three Regions 損失最多的三個地區
(in terms of the amount of total loss)

2016

36.6% 羅馬尼亞 Romania
15.3% 德國 Germany
12.9% 丹麥 Denmark
8.7% 瑞士 Switzerland
6.4% 比利時 Belgium
5.0% 愛爾蘭 Ireland
4.8% 土耳其 Turkey
2.9% 英國 UK
2.2% 荷蘭 The Netherlands
1.9% 法國 France
1.7% 西班牙 Spain
1.6% 澤西 Jersey

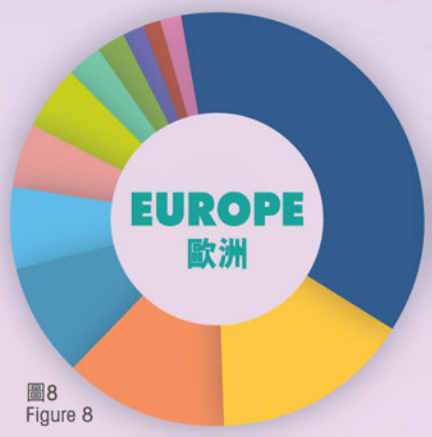


圖8
Figure 8

87.9% 美國 US
9.4% 加拿大 Canada
1.9% 開曼群島 Cayman Islands
0.8% 其它 Others

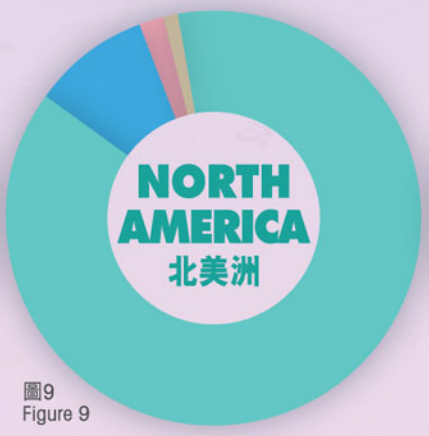


圖9
Figure 9

43.7% 香港 Hong Kong
17.9% 新加坡 Singapore
7.7% 台灣 Taiwan
7.3% 阿聯酋 UAE
3.3% 日本 Japan
3.2% 馬來西亞 Malaysia
3.0% 南韓 South Korea
2.8% 越南 Vietnam
2.5% 泰國 Thailand
2.2% 沙特阿拉伯 Saudi Arabia
1.3% 印尼 Indonesia
5.1% 其它 Others

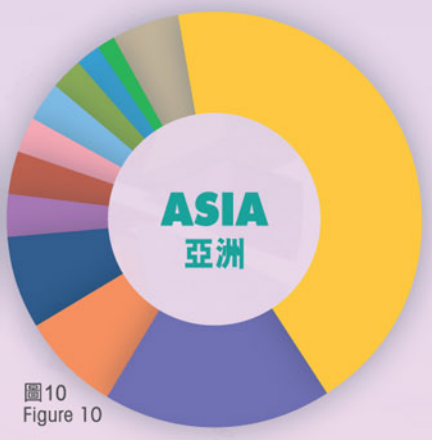


圖10
Figure 10

2017 (January to June) (1月至6月)

46.7% 西班牙 Spain
19.8% 德國 Germany
18.6% 法國 France
9.0% 英國 UK
2.6% 瑞士 Switzerland
3.3% 其它 Others

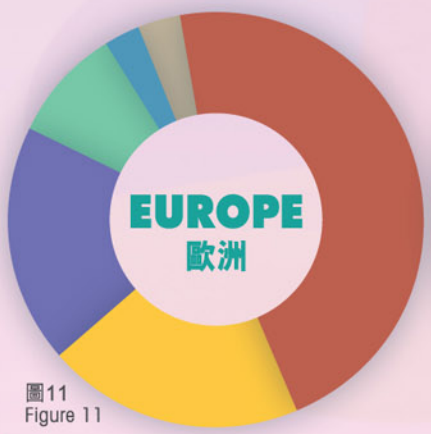


圖11
Figure 11

91.5% 美國 US
8.1% 加拿大 Canada
0.4% 其它 Others

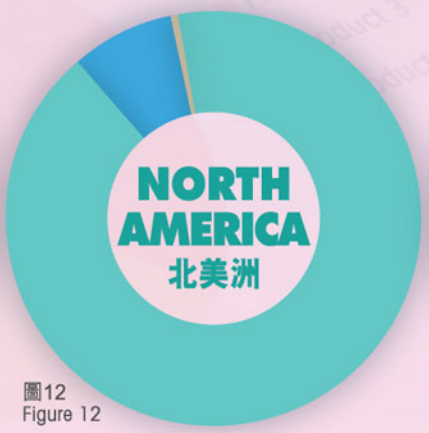


圖12
Figure 12

31.8% 中國 China
22.2% 香港 Hong Kong
15.3% 日本 Japan
8.3% 台灣 Taiwan
8.0% 阿聯酋 UAE
5.8% 新加坡 Singapore
5.0% 馬來西亞 Malaysia
1.9% 南韓 South Korea
1.7% 其它 Others

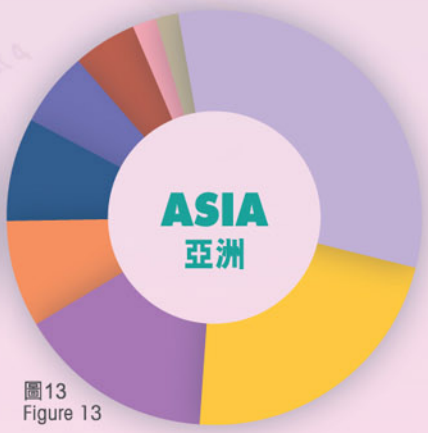


圖13
Figure 13

2016年，在1,301宗欺詐交易之中，364宗共涉款5.721億港元的行騙未遂交易(即交易總宗數的27.9%或涉及總額的26.6%)；至於2017年(1月至6月)，337宗欺詐交易中，70宗共涉款1.043億港元的行騙未遂交易(即交易總宗數的20.8%或涉及總額的18.3%)，資金未有轉來香港。

In 2016, 364 out of 1,301 fraudulent transactions amounting to HKD572.1 million (27.9% of the total number of transactions or 26.6% of the total amount involved) were unsuccessful whilst in 2017 (January to June), 70 out of 337 fraudulent transactions amounting to HKD104.3 million (20.8% of the total number of transactions or 18.3% of the total amount involved) were unsuccessful that fund was not transferred to Hong Kong.

資金轉移[13]
Fund Dissipation[13]

接收非法資金至移走資金的期間

以金額計算，61.6%資金轉移[14]在收款當日進行，約17.9%非法資金在收款次日移走。

Duration between the Receipt of Illicit Fund and Fund Dissipation

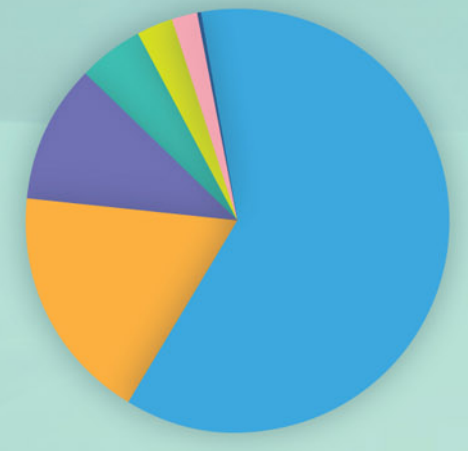
61.6% of the fund dissipations[14], in terms of amount, were conducted within the same day as the day of receipt of illicit fund whilst around 17.9% of the same was conducted on the day following the receipt of illicit fund.

資金轉移的方法

近50%資金以本地轉帳形式轉至本地銀行，少於40%經由海外匯款轉移。

Means of Fund Dissipation

Nearly 50% of the dissipated fund was transferred to domestic banks by local transfers whilst less than 40% of the same was dissipated via overseas remittances.



61.5% 同日 0 days (within the same day)
17.9% 1天 1 day
10.6% 2天 2 days
5.0% 3天 3 days
2.9% 4天 4 days
1.8% 5-10天 5-10 days
0.3% 11天或以上 11 days or above

圖14：接收非法資金至移走資金的期間
Figure 14: Duration between the Receipt of Illicit Fund and Fund Dissipation

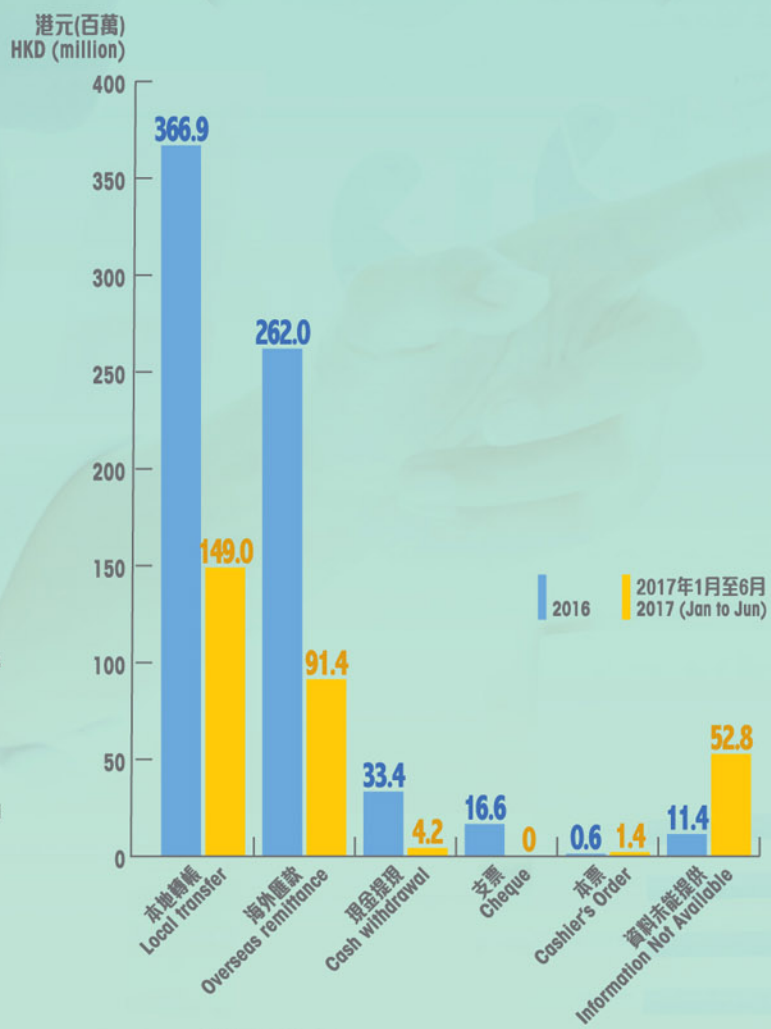


圖15：轉移資金的方法
Figure 15: Means of Fund Dissipation

13. 計算最多計算三個户口之第二層資金轉移。
The fund dissipation includes up to three destinations of second layer.

14. 包括以本地轉帳、海外匯款、現金提款、支票及銀行本票等方法轉移資金。
Including fund dissipation by means of local transfers, overseas remittances, cash withdrawals, cheques and cashier's orders.

轉移至其他司法管轄區

除了本地轉帳外，1.442億港元(14.6%)及1.416億港元(14.3%)之匯款分別轉至中國和阿聯酋。

Fund Dissipation by Jurisdictions

Other than local transfers, HKD144.2 million (14.6%) and HKD141.6 million (14.3%) were sent to China and UAE respectively.

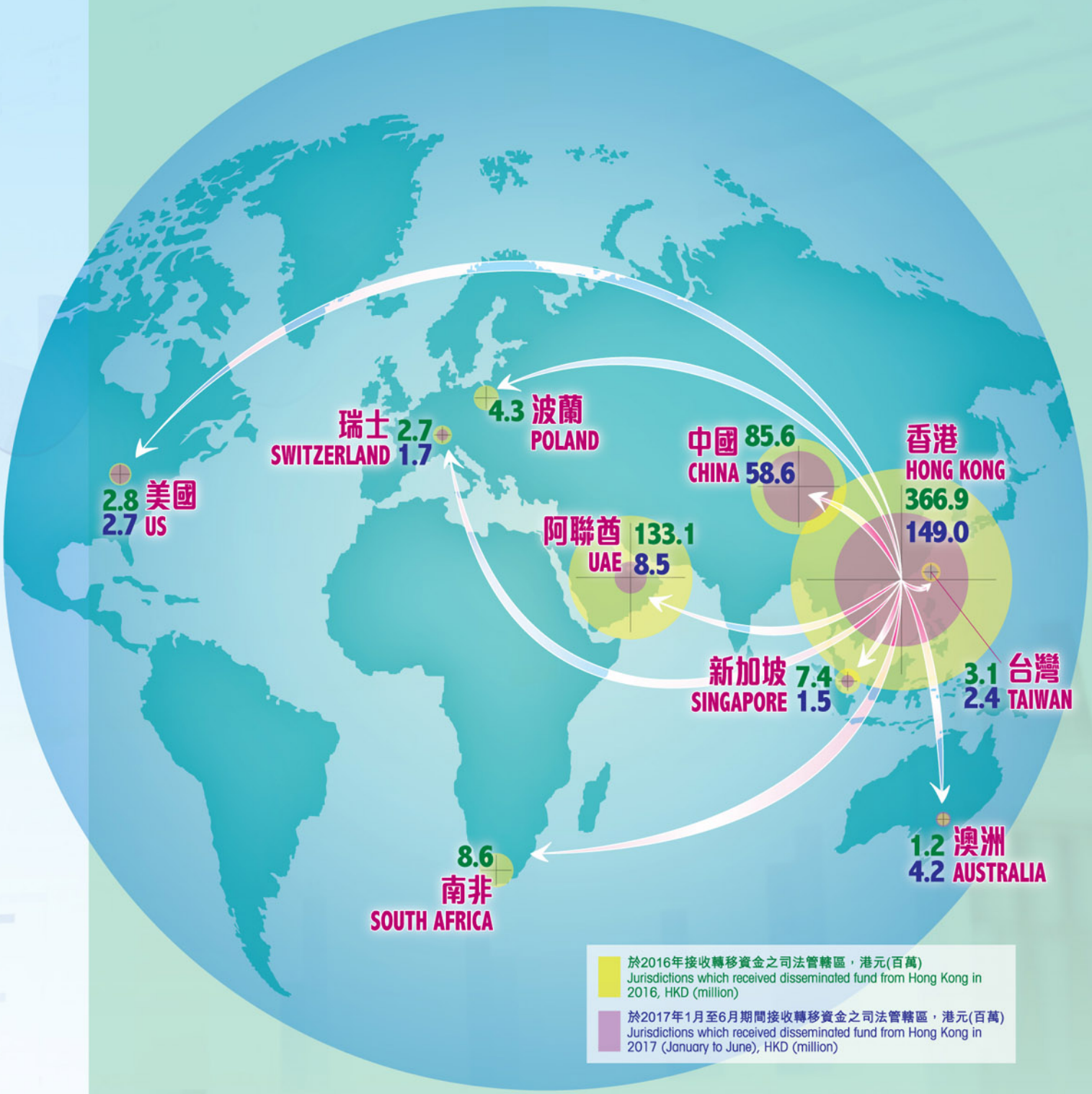


圖16：2016至2017年(1月至6月)的資金轉移情況(第二層交易十大司法管轄區)
Figure 16: Fund Dissipation in 2016 and 2017 (January to June) (Top 10 Jurisdictions, i.e. the Second Layer)

THEMATIC ANALYSIS 主題分析

主題分析1：更換公司戶口的公司董事以挪用戶口

(2017年1月至6月)

更換公司董事，是挪用已有公司銀行戶口以接收非法資金最常見的方法之一。涉及電郵騙案的178香港註冊公司[15]之中，75間(42.1%)在接收非法資金[17]前後180日內曾更換董事[16]，18%在接收非法資金前30日內曾更換董事。

在上述75間香港註冊公司之中，90.4%董事在更換董事前[18]，本為中國身分證明文件持有人。

Thematic Analysis 1: Change of Company Directorship for Corporate Account Appropriation

(2017 January to June)

Changing the company directorship is considered as one of the most prevalent ways in appropriating readily available corporate bank accounts for the subsequent receipt of illicit fund. 42.1% (75 out of 178 subject companies[15]) Hong Kong incorporated companies were found with their directorship changed[16] in fewer than 180 days before or after the receipt of illicit fund[17] in email scams. 18 % recorded a change of directorship 0-30 days prior to the receipt of illicit fund.

Out of the aforesaid 75 Hong Kong incorporated companies, 90.4% of the directors were Chinese Identity Document holders before the change of company directorships[18].

15. 在涉及電郵騙案的197間公司當中，178間公司在香港註冊並有公司註冊號碼。
Among 197 companies involved in email scams, 178 companies were Hong Kong incorporated with known Company Registration Number.

16. 以新董事替代、新增董事或刪減現有董事。
Either replacement by, addition of new director(s) or reduction of existing director(s).

17. 如某公司涉及多個戶口或多次接收非法資金，在專題分析1有關更換董事的研究中，只計算第一個戶口第一次接收非法資金。
If a company is involved in multiple accounts or multiple receipts of illicit fund, only the first account receiving the first transfer of illicit fund would be counted in the study of relationship of change of directorship in Thematic Analysis 1.

18. 根據開設戶口時提供的資料。
Referring to the information provided at the time of account opening.

Type of ID Documents held by Directors

Before

the Change of Directorship

更換公司董事前，董事所持
的身份證明文件類型

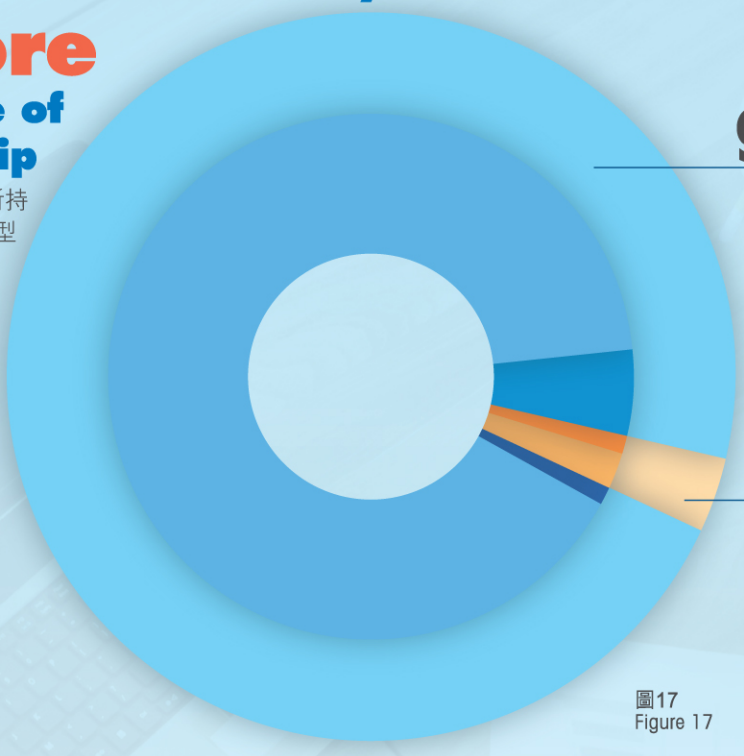


圖17
Figure 17

在更換董事後，新董事來自歐洲(49.4%)、亞洲(37.7%)和北美洲(11.7%)等地區。

After the change of directorship, the directors were from Regions of Europe (49.4%), Asia (37.7%), North America (11.7%), etc.

Type of ID Documents held by Directors

After

the Change of Directorship

更換公司董事後，董事所持
的身份證明文件類型

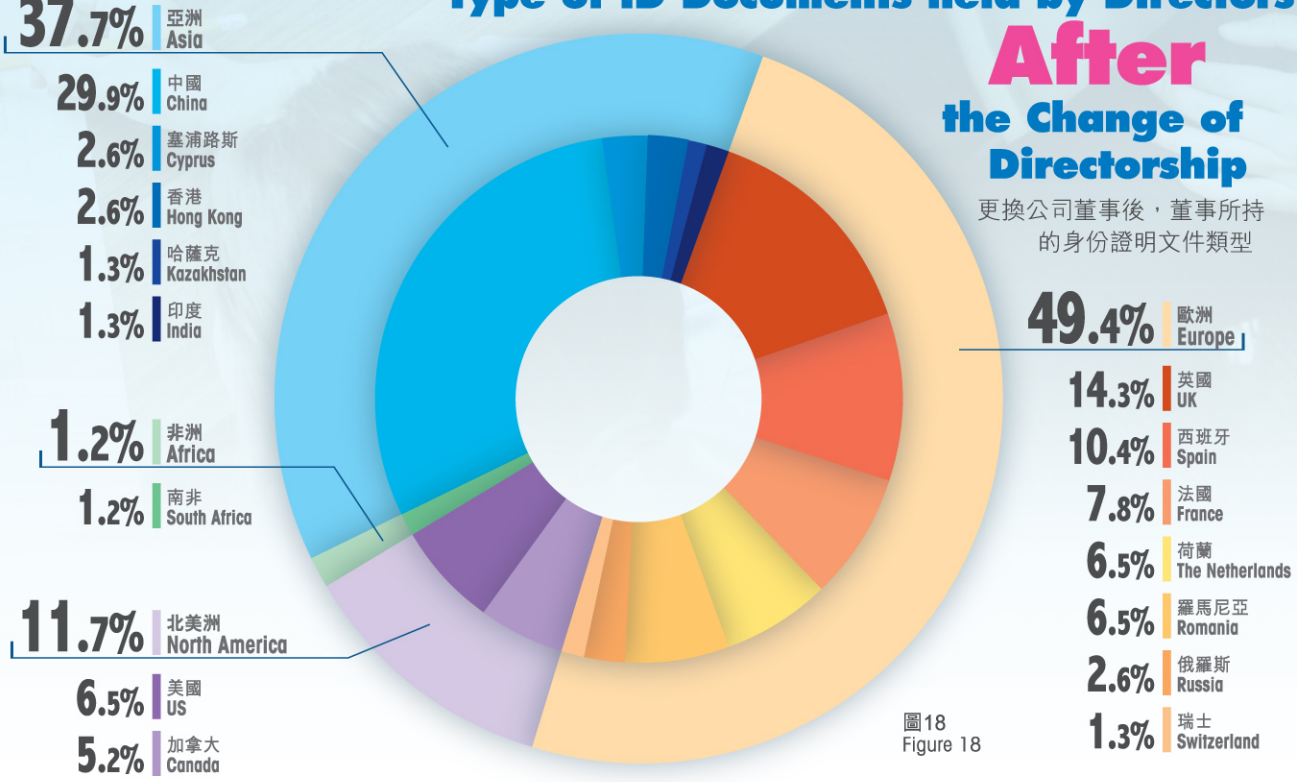


圖18
Figure 18

主題分析2：戶口簽署人
(2017年1月至6月)

在更換董事的75間香港註冊公司之中，8%在更換董事後，向相關銀行更新戶口簽署人。60%既沒有通知銀行更換董事，又不要求更新戶口簽署人。

Thematic Analysis 2: Account Signatories
(2017 January to June)

Among 75 Hong Kong incorporated companies with directorships changed, 8% had their account signatories updated at respective banks after the change. 60% neither informed the banks of the change of directorships nor requested for account signatories update.

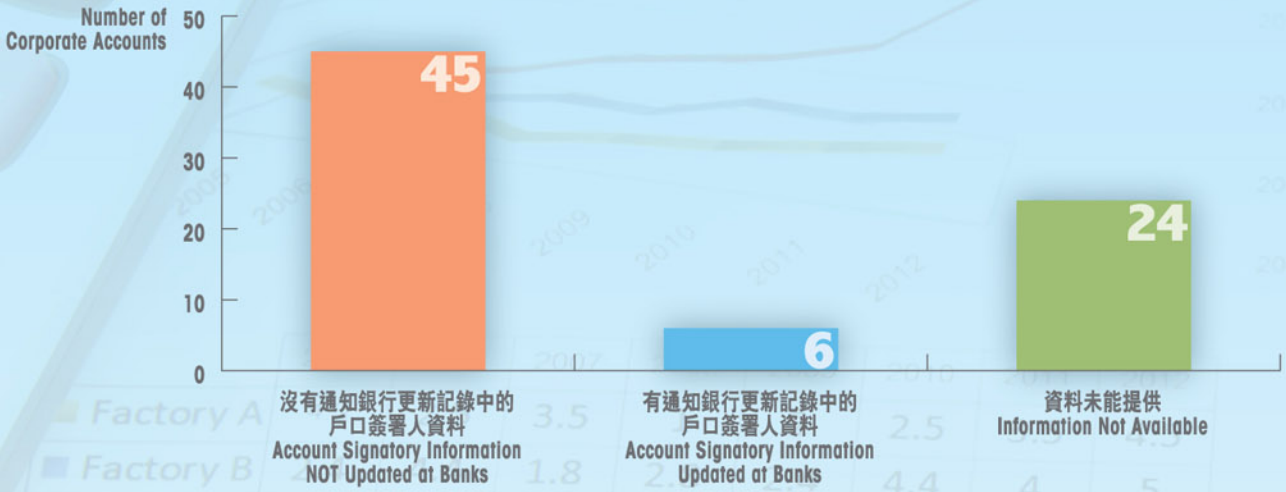


圖19：銀行記錄中的戶口簽署人資料
Figure 19: Account Signatory Information in Banks' Record

主題分析3：試驗付款

一些疑犯就電郵騙案接收非法資金前，會先與第三方或在其綜合貨幣戶口內進行交易[19]。此類交易相信是為了測試戶口是否有效，然後才用以接收非法資金。約24%戶口在接收非法資金前，曾錄得試驗付款交易。

Thematic Analysis 3: Test Payment

Some suspects would make transactions[19], either to or from third parties, or among self multi-currencies accounts, prior to the receipt of illicit fund in email scams. The purpose of such transactions was believed to test the accounts' validity before using them to receive illicit fund. About 24% of the accounts recorded test payments before the receipt of illicit fund.

圖20：戶口用作試驗付款之比例
Figure 20: Proportion of Accounts with Test Payment Observed

19. 在此分析中，試驗付款並不以數目衡量，而是指觀察到/ 認為異常，涉及細小金額、異於平常交易模式、於接收非法資金前一個月內進行的交易往來，很可能作測試用途。
The meaning of test payment in this analysis is not defined quantitatively. However, it is considered / observed to be abnormal incoming and/or outgoing transactions of trivial amounts which deviated from the normal transaction pattern and was recorded within one month before the receipt of illicit fund likely for testing purpose.

試驗付款的金額大多介乎50港元或以下(36.5%)至101至500港元(27.4%)，與準備接收的非法資金相比(檢討期內每宗欺詐交易的平均金額達170萬港元)，金額可謂微不足道。

76.7%試驗付款在其綜合貨幣戶口內進行，23.3%往來第三方戶口或以現金存款。

The amount of test payments mainly ranged from HKD50 or below (36.5%) to HKD101-500 (27.4%). The amounts were considered relatively insignificant when compared with the illicit fund to be received (the average amount involved per fraudulent transaction was HKD1.7 million during the review period).

76.7% of the test payments were made among their respective self multi-currencies accounts whilst 23.3% was sent to/ from third-parties or deposited by cash.

圖21：試驗付款的交易金額分布
Figure 21: Distribution of Amount of Test Payment

圖22：在綜合貨幣戶口內或以第三方戶口或現金存款作試驗付款
Figure 22: Test Payment via Self Multi-currencies Account or Third Parties/ Cash Deposits

結論

從上述分析，可見電郵騙案的各種趨勢和模式，以及其中的實質數據。經深入觀察所得的見解和意見，亦已提供予有關當局和銀行採取所需行動。

本組致力在最新的電郵騙案類型學分析方面，提供有用的分析成果。相關界別可藉報告中的增值情報，檢討打擊洗錢的政策和風險警報系統，以捍衛金融體系，免受不法之徒濫用。

免責聲明

本組致力在此報告提出全面而透徹的數據分析。然而，此報告之分析多建基於本組所接獲資料內容之準確及明確度，加上各方採用的觀點與定義或有不同，因此差異或會出現。本組不會對因使用本報告任何材料或關乎使用該等材料而直接或間接引致的任何損失、損害、費用或開支負上任何責任。

查詢

請致電 (852) 2866 3366，或以電郵 (jfiu@police.gov.hk) 與本組聯絡，亦可於本組網頁(www.jfiu.gov.hk)瀏覽資料。

意見回饋

你的意見有助我們訂定未來路向和專題項目，歡迎請把你的意見電郵至jfiu@police.gov.hk。

Overall Remarks

Different trends and patterns of email scams were observed, with concrete data, during the analysis. More in-depth observations and advice were provided to various competent authorities and banks for actions deemed necessary.

The JFIU strives to provide useful analytical products on the latest typologies of email scams. Relevant sectors are welcome to make use of the value-added intelligence in the Report in reviewing their AML policies and risk alert systems so as to safeguard the financial system from being misused by criminals.

Disclaimer

The JFIU aims at providing a thorough and comprehensive data analysis in this Report. That said, discrepancies might inevitably exist due to the availability/ accuracy/ explicitness of the information provided to the JFIU, different perceptions or definitions applied, etc. The JFIU accepts no responsibility for any loss, damage, cost or expense of whatever kind incurred directly or indirectly from or in connection with the use of any materials in this Report.

Enquiries

Please contact the JFIU at telephone: (852) 2866 3366 or via email: jfiu@police.gov.hk. Information is also available on the JFIU website at www.jfiu.gov.hk.

Feedback

Your feedback is important for us to shape our future directions and specific projects. You are welcome to email your comment(s) to jfiu@police.gov.hk.

聯合財富情報組出版 (2018)
Published by the Joint Financial Intelligence Unit (2018)

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