



Financial Intelligence and Investigation Bureau  
Hong Kong Police Force

# Feedback on suspicious transaction reports (STRs) and money laundering trend

Presented by:

**Ms. Pauline WONG**

Chief Inspector of Police  
Joint Financial Intelligence Unit (JFIU)



More Information  
[www.jfiu.gov.hk](http://www.jfiu.gov.hk)

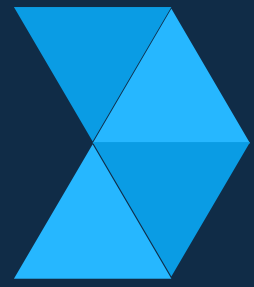


Email Address  
[jfiu@police.gov.hk](mailto:jfiu@police.gov.hk)



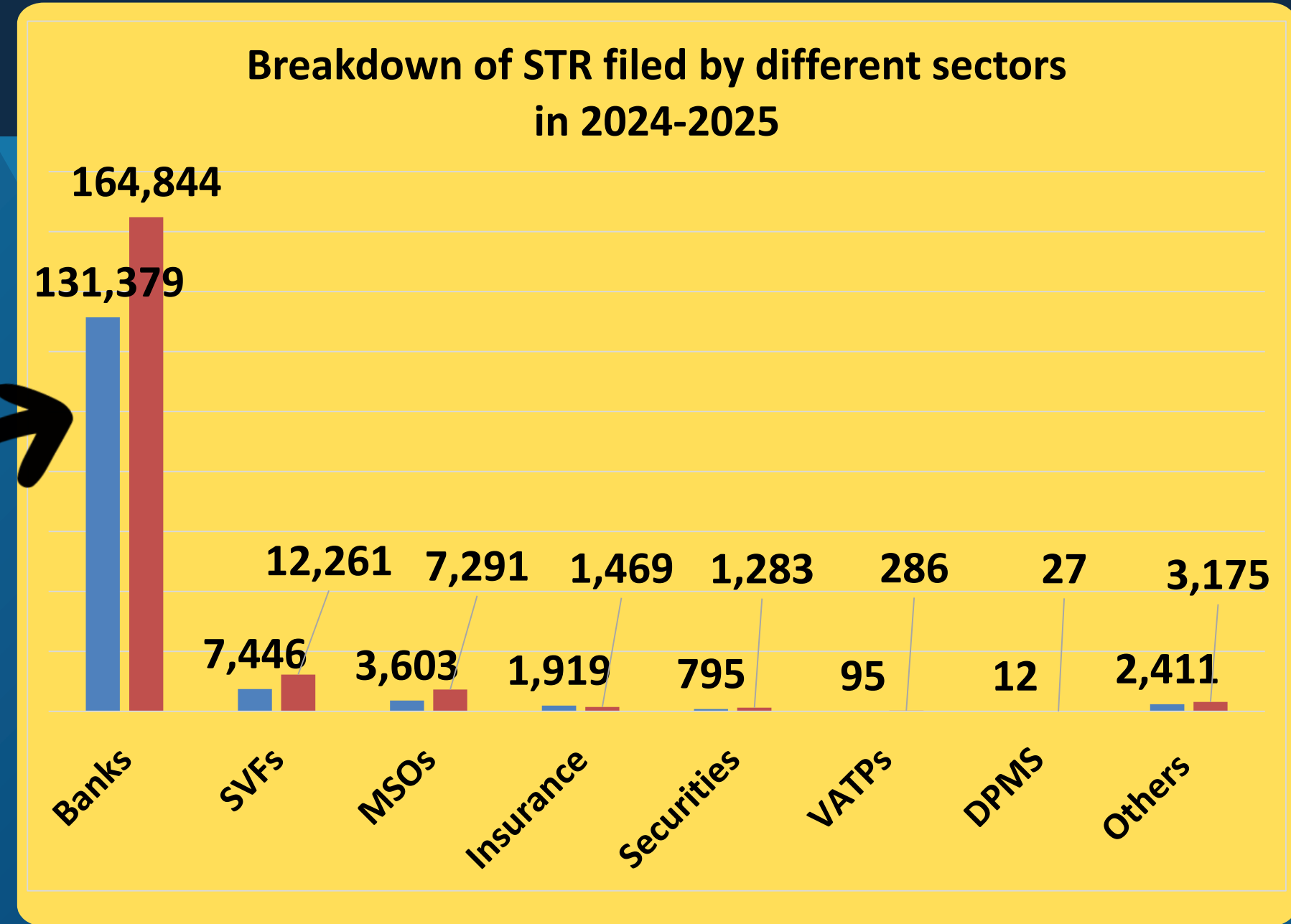
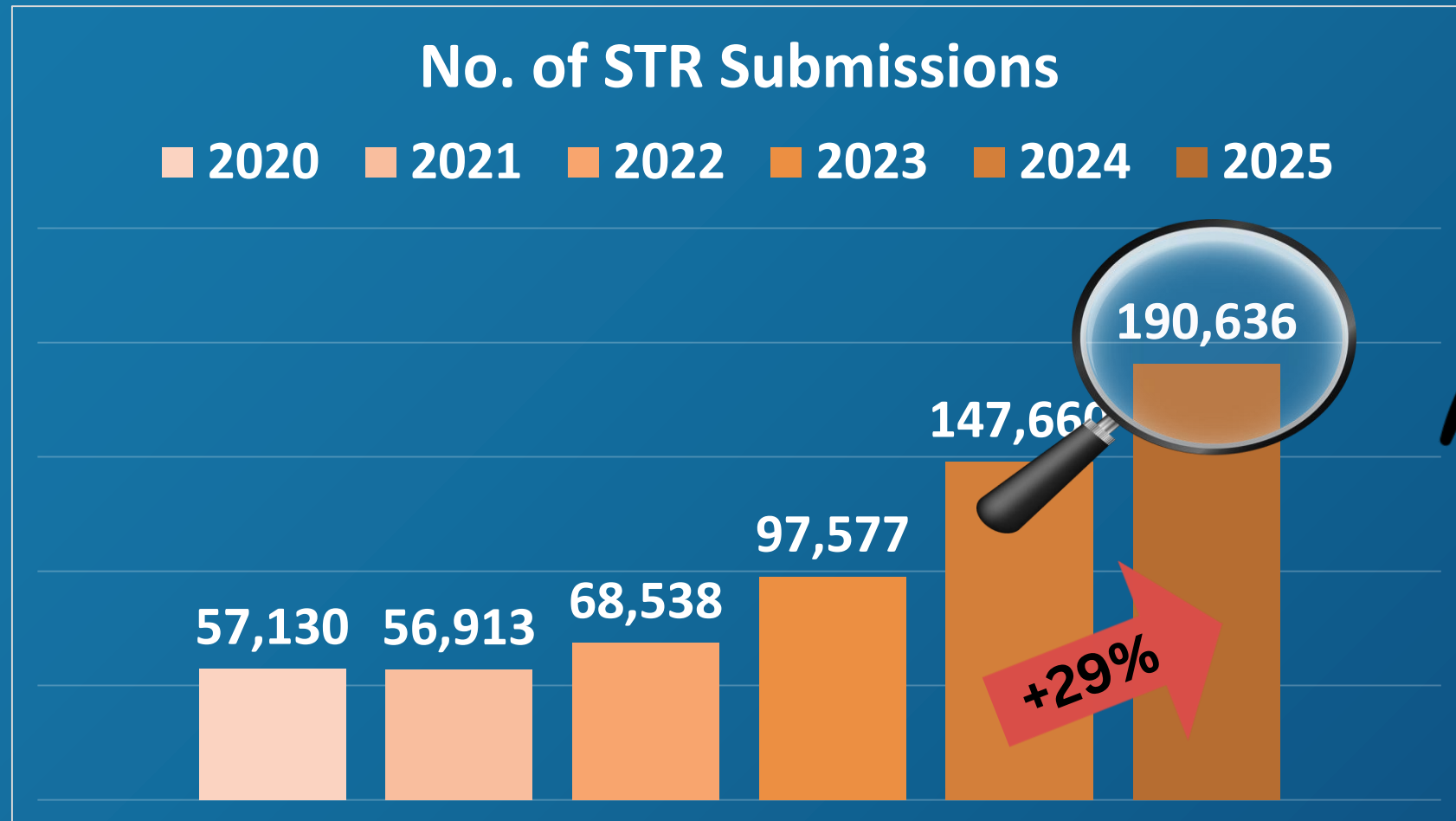
# Agenda

- 1. Trends and Observations on STR submission**
- 2. Money Laundering Trend**



# Trends of STR Submission

JFIU received a total of 190,636 STRs. Of which, 164,844 STRs and 12,261 STRs were submitted by banks and SVFs





# Observations on STR



## Good Quality (Clearly indicating LEA reference)

Reporting Party Subject Organisation Account Transaction Suspected C

Organisation Name Reporting Officer Name Your Reference Phon

Testing Company

**Disclosure-related Laws**

Drug Trafficking (Recovery of Proceeds) Ordinance [Cap.405]

Organized and Serious Crimes Ordinance [Cap.455]

United Nations (Anti-Terrorism Measures) Ordinance [Cap.575]

Hong Kong National Security Law

Other Information:

Report related to previous / other disclosure  Yes  No

“(1) STR triggered by internal monitoring”

Reporting Party Subject Organisation Account Transaction

Organisation Name Reporting Officer Name Your Reference

Testing Company

Industry Category \*  
Financial - Bank

**Disclosure-related Laws**

Drug Trafficking (Recovery of Proceeds) Ordinance [Cap.405]

Organized and Serious Crimes Ordinance [Cap.455]

United Nations (Anti-Terrorism Measures) Ordinance [Cap.575]

Hong Kong National Security Law

Other Information:

Report related to previous / other disclosure  Yes  No

Your Previous Reference [E.g. STR 2025000001] + -

Previous STR No. [E.g. ESPS 24/2025] + -

ADCC Ref. No. [E.g. MK RN 25000001] + -

Police Report No. [E.g. DIT 1 MKDIST] + -

Investigation Unit [E.g. TMCC 1234/2025] + -

Search Warrant (Writ No.) [E.g. ISR 2025001000] + -

FINEST ISR No. [E.g. FMLIT 1/2026] + -

Other LEA Reference No. + -

C&ED

ImmD

Others

IRD Reference No. + -

SFC Reference No. + -

“(2) STR triggered by LEA intelligence”



# Observations on STR

## Good Quality

(Showing all accounts belonging to the Subject)

Reporting Party   Subject   Organisation   **Account**   Transaction   Suspec

**+ Add**

**Account Create**

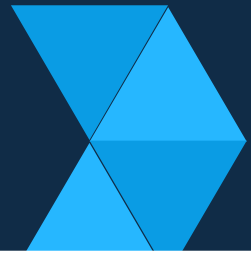
Crypto-transaction-related   OTC-Related  
 Yes    No    Yes    No

Name of Institution   If Others

Type \*   If Others

Opening Date   Closing Date  
yyyy-mm-dd   yyyy-mm-dd

- All-in-One Account - Savings
- All-in-One Account - Current
- All-in-One Account - Fixed Deposit
- Betting Account
- Credit Card Account
- Currency Account
- Currency Options Account
- Current Account
- Fixed Deposit Account
- FX Short Selling Account
- Investment Fund Account



# Observations on STR



## Good Quality

(Clearly indicating the Suspected Crime Type)

[Reporting Party](#)
[Subject](#)
[Organisation](#)
[Account](#)
[Transaction](#)
[Suspected Crimes](#)
[Suspicious Indicator](#)

**Suspected Crimes**

National Security

- Offence(s) Endangering National Security

Fraud

- Email Scam
- Investment Scam
- Romance Scam
- Telephone Deception
- Others (Please Specify) Purchase scam

Other Crimes

- Bookmaking
- Crime under Gambling Ordinance
- Corruption and Bribery
- Counterfeiting Currency
- Environmental Crime
- Extortion
- Forgery
- Illicit Arms Trafficking
- Illicit Trafficking in Dangerous Drugs / Psychotropic Substances
- Illicit Trafficking in Stolen and Other Goods
- Insider Trading and Market Manipulation
- Others (Please specify)

Illicit Trade Activities

- Counterfeiting and Piracy of Products
- Dealing in Precious Metals and Stones without a license
- Endangered Species Smuggling
- Illicit Cigarettes
- Smuggling (including in relation to customs and excise duties and taxes)
- Trade Based Money Laundering
- Unlicensed Money Service Operator (UMSO)
- Kidnapping, Illegal Restraint and Hostage-Taking
- Money Laundering
- Murder, Grievous Bodily Injury
- Participation in an Organized Criminal Group and Racketeering
- Robbery or Theft
- Sexual Exploitation (including Sexual Exploitation of Children)
- Tax Crimes (related to direct taxes and indirect taxes)
- Terrorism including Terrorist Financing
- Trafficking in Human Beings and Migrant Smuggling
- Weapon - Related
- No Crime Related

1) National Security

2) Fraud

a) Email Scam

b) Telephone Deception, etc

3) Other Crimes

a) Corruption

b) Insider Trading and Market Misconduct, etc

4) Illicit Trade, e.g.

• Weapon related

• UMSO

• TBML, etc



# Observations on STR



## Good Quality (Clearly indicating the Suspicious Indicator)

< Reporting Party Subject Organisation Account Transaction Suspected Crimes **Suspicious Indicator**

Please put a "✓" in the selected box(es).

**Fund Movement Pattern**

- Indirect Transaction / Transaction Intended to Break Audit Trail
- Large Cash Transaction
- Numerous Transaction Counterparties without Apparent Reasonable Cause
- Temporary Repository of Fund
- Transactions Involving High-Risk Jurisdiction / Region
- Uneconomical Transaction / Transaction with No Business Purpose
- N/A

**Accounts**

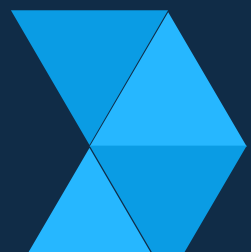
- Account Operated / Controlled by Third-Party Other Than Signatory / Account Holder
- Non Resident Personal Account
- Offshore Account (e.g. BVI Bank Account)
- Shell Company Account
- N/A

**National Security Related**

- A person is suspected of committing an offence endangering national security
- Transactions with specified absconders under Safeguarding National Security Ordinance

### Suspected Indicator:

- **Fund Movement Pattern**
- **Accounts**
- Customer Background / Behavior
- National Security Related
- Other Suspicious Indicator
- Narrative Comment



# Observations on STR

## Good Quality (Clearly indicating the Suspicious Indicator)

Reporting Party   Subject   Organisation   Account   Transaction   Suspected Crimes   **Suspicious Indicator**

Customer Background / Behaviour

- Civil Servant-related **NEW**
- Common IP Address **NEW**
- Customer Evasive / Reluctant to Provide Information
- Customer Insisted to Use Less Secured Transaction Methods
- Politically Exposed Persons (PEP)
- Sanctions-related
- Shared Device **NEW**
- Suspected Counterfeit Document Presented by the Customers
- Suspected Money Courier / Unlicensed Money Service Operator

Other Suspicious Indicator

- Transactions with specified absconders under Safeguarding National Security Ordinance
- Transactions with prohibited organisations under Safeguarding National Security Ordinance
- Transactions with high NS risk counterparties
- Others (Please Specify) \_\_\_\_\_
- N/A
- Casino-related Suspicious Transaction
- Charitable Organisation / NPO-related Suspicious Transaction
- Others (Please Specify) \_\_\_\_\_
- N/A

- Suspected Indicator:
- Fund Movement Pattern
  - Accounts
  - **Customer Background / Behavior**
  - National Security Related
  - Other Suspicious Indicator
  - Narrative Comment



# Observations on STR



## Good Quality (Clear report in respective fields)

Reporting Party Subject Organisation Account Transaction Suspected Crimes **Suspicious Indicator**

Narrative Comment about the Suspicious Transactions

1. Triggering Factors

- Commission / Types / Association of Offence
- Evidence of Suspicious Transaction Patterns
- Intelligence Received from LEAs
- Material from Publicly Available Information (e.g. adverse news, SFC alerts)
- Receipt of Search Warrant / Court Order
- Upstream Scam Intervention

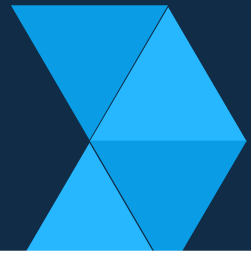
2. Background of Subject / Organisation

3. Details of Investigation / Transaction Analysis

4. Conclusions / Action Taken / Way Forward

Reporting Party Subject Organisation Account Transaction Suspected Crimes **Suspicious Indicator**

- **Offence** (Fraud, Corruption, Sanction, Terrorist Financing, National Security, etc.)
- **Suspicious Transaction Patterns** (Substantial Cash Deposits, Temporary Repository of Funds, etc.)
- **Intelligence / Enquiry from LEAs** (e.g. JFIU, CSTCB, ADCC)
- **Publicly available information** (Adverse News, ICAC Press Release, Sanction, etc.)
- **Receipt of Search Warrant / Court Order**
- **Upstream Scam Intervention** (Customer is victim)



# Observations on STR



## Good Quality (Clear report in respective fields)

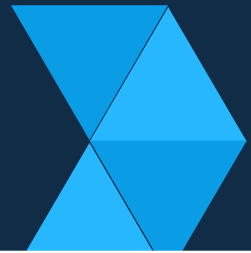
Reporting Party   Subject   Organisation   Account   Transaction   Suspected Crimes   **Suspicious Indicator**

2. Background of Subject / Organisation

3. Details of Investigation / Transaction Analysis

4. Conclusions / Action Taken / Way Forward

- Nationality, age, gender
- Type of ID document - HKID Holder, China Passport Holder, China ID and Exit-Entry Permit (C2P) etc.
- Occupation / business nature, source of wealth, source of income – include the date of last KYC
- Family background, if known - *e.g. wife/husband/daughter of the customer also maintained banking relationship with the bank and displayed similar suspicion.*
- Date of commencing banking relationship; also include account closing date if applicable



# Observations on STR



## Good Quality (Clear report in respective fields)

Reporting Party   Subject   Organisation   Account   Transaction   Suspected Crimes   **Suspicious Indicator**

2. Background of Subject / Organisation

3. Details of Investigation / Transaction Analysis

4. Conclusions / Action Taken / Way Forward

- Review Period
- Transactions and linkage with suspicious counterparts / third party, if any
- KYC / RFI result
- Open source information / details of the adverse news / sanction list with website links
- Findings on the digital footprints, if any
- Refrain from negative declarations of absence, *e.g. no PEP match, no search warrant, no sanction match*
- Further review  
Exit relationship

# Observations on STR

**Good Quality**  
(Timely and detailed reporting with supporting attachment)


Reporting Party   Subject   Organisation   **Account**   Transaction   Suspected Crimes   Suspicious Indicator

+ Add

Digital Footprint   **New**   Existing Digital Footprint

Event Type	Device Name	Device Model
Digital Footprint Create		
Event Type	Device Name	Device Model
Device ID	IP Address	Period From yyyy-mm-dd
SSID	BSSID	Geohash
Longitude		


**Digital Footprint**



**Transaction Records in Excel Format**



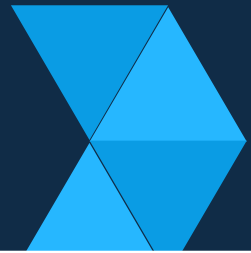
**Records of Digital Footprints**



**Relevant Documents obtained during CDD Process**



**Diagram of network relationships of wallet addresses**



# Observations on STR

**Good Quality**  
**(Include virtual asset related accounts)**

## Virtual Assets Related Accounts

- Transaction Platform
- Wallet Address
- Token Type
- Token Amount
- Equivalent Value in HKD

Reporting Party   Subject   Organisation   **Account**   Transaction   Suspected Crimes   Suspicious Indicator

+ Add

**Account Create**

Crypto-transaction-related   OTC-Related

Yes    No    Yes    No

Cancel   Confirm

**Wallet Details**

Transaction Platform \*   Platform User ID \*   Wallet Address \*

Opening Date   Closing Date

yyyy-mm-dd   yyyy-mm-dd

**Wallet Balance**   Add

Token Type   Token Amount   Correl

**Digital Footprint**   New   Link Existing Digital Footprint

Event Type	Device Name	Device Model	Device OS	IP Address

**Wallet Balance Create**

Token Type \*   If Others   Token Amount \*   Equivalent Value in HKD \*

\_\_\_\_\_   \_\_\_\_\_   \_\_\_\_\_   \$ \_\_\_\_\_

Date of Balance   yyyy-mm-dd

\_\_\_\_\_   \_\_\_\_\_

Cancel   Confirm

**Wallet Balance Create**

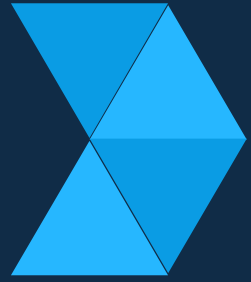
Token Type \*   If Others   Token Amount \*   Equivalent Value in HKD \*

\_\_\_\_\_   \_\_\_\_\_   \_\_\_\_\_   \$ \_\_\_\_\_

Date of Balance   yyyy-mm-dd

\_\_\_\_\_   \_\_\_\_\_

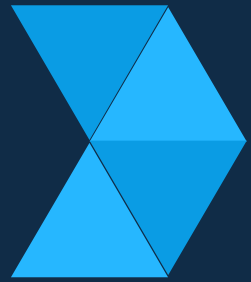
Cancel   Confirm



# Observations on STR



- Blank content / Narrative only in enclosure
- Entities with limited nexus in one STR
- Confusing Date of Account Opening
- “Streamlined STR”
- Misc. (e.g. difficult to comprehend, important data hidden, etc)



# Observations on STR



## Blank content/Narrative only in enclosure

Narrative Comment about the Suspicious Transactions

### 1. Triggering Factors

- Commission / Types / Association of Offence
- Evidence of Suspicious Transaction Patterns
- Intelligence Received from LEAs
- Material from Publicly Available Information (e.g. adverse news, SFC alerts)
- Receipt of Search Warrant / Court Order
- Upstream Scam Intervention

### 2. Background of Subject / Organisation

-

### 3. Details of Investigation / Transaction Analysis

-

### 4. Conclusions / Action Taken / Way Forward

-

### Attachment

Account Opening Mandate / Document(s)

No Data

No description of the Subject(s) / Account(s)

Only a consolidated Excel of some accounts available (but number of accounts different from STR)

### Detailed Transaction Record(s)

No.	Person / Account Holder	Name	Size
<input checked="" type="checkbox"/> 1	[Redacted]	[Redacted]	41 KB

### Other Bank / Institution Document(s)

No Data

### Other Document(s)

No.	Name	Size
<input checked="" type="checkbox"/> 1	[Redacted]	2129 KB

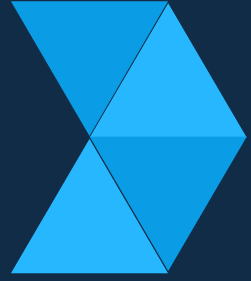
# Observations on STR

## Entities with limited nexus in one STR

### Focus on the Main Subject and be Concise

- 4.8 STRs should be precise and concise with sufficient information to establish suspicion and facilitate follow-up enquiries. Too much or irrelevant information will divert focus from the main subject, making timely understanding and assessment of the STR difficult. Entities involved in different layers of alleged fraud and ML, where known, should be included to give a full picture of the fund flows. Where entities are only remotely associated with the subject matter of an STR, AIs should assess their relevance and consider whether they should instead be covered in separate STRs.
- 4.9 Where a network of relationships or accounts has been identified, AIs should report the network in the same STR, as far as is reasonably practicable. To help the JFIU and LEAs conduct analysis and investigation more efficiently, AIs should include sufficient information to illustrate the connections among accounts, such as common attributes<sup>17</sup> and transaction counterparties.

**Source: Guidance Paper – Transaction Monitoring, Screening and Suspicious Transaction Reporting, published by the Hong Kong Monetary Authority (revised in February 2023)**



# Observations on STR



## Confusing Date of Account Opening

Account Entity [At least one highlighted field must be filled.]

Account Institution: [Redacted]

Account No.: [Redacted]

Type: Other Account (with description)

if others: [Redacted]

Opening Date: 2023-08-25

Closing Date: [Redacted]

Balance: HKD 26.47 Date: 2025-08-15

Related Person					
Name	HKID	ID No.	Country	DOB	Sex

### Suspicious Indicators

#### Fund Movement Pattern

N/A

#### Accounts

N/A

#### Customer Background

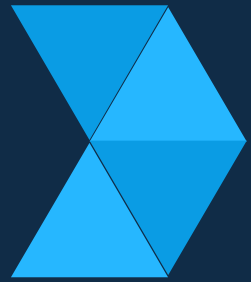
N/A

#### Others

Others(N/A)

#### Additional Information

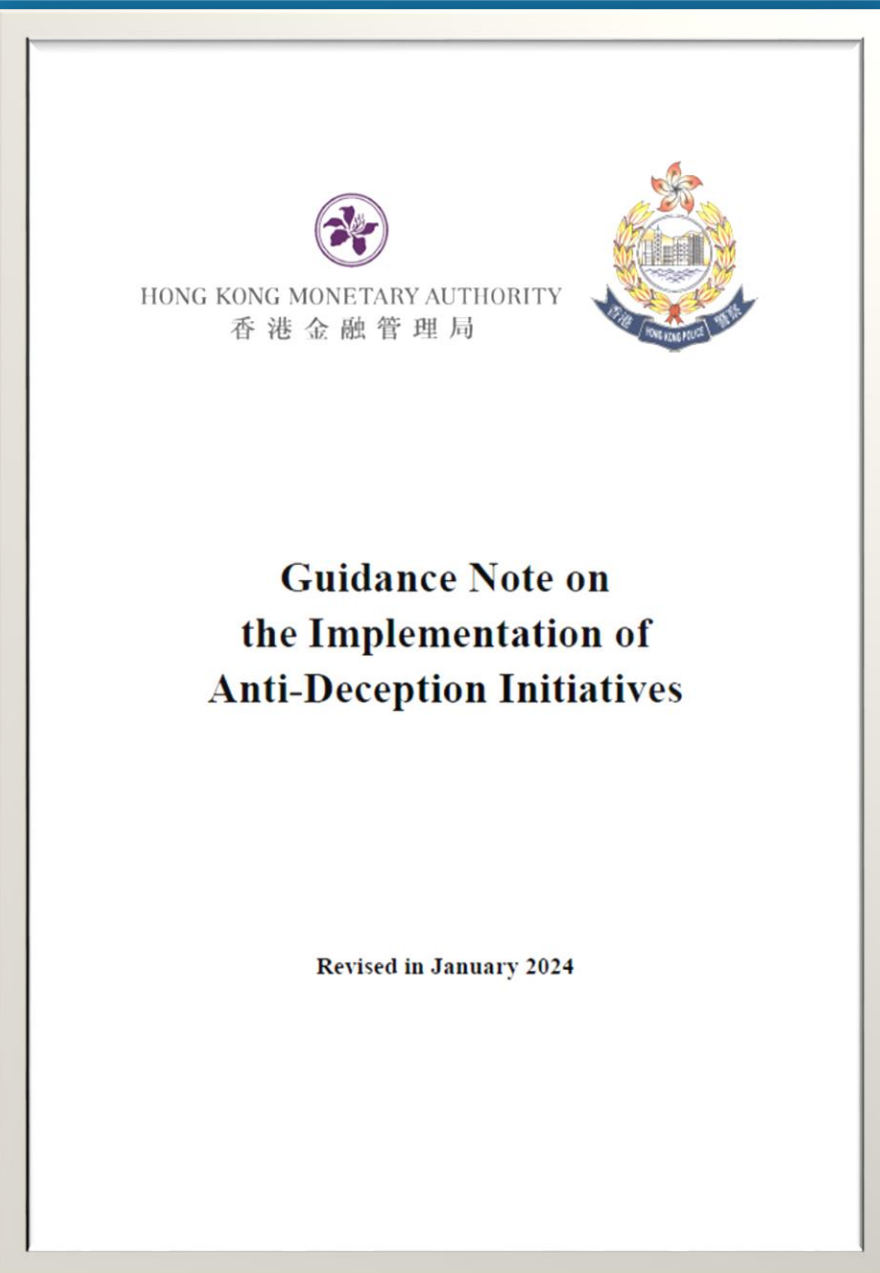
開戶日期2022-04-16



# Observations on STR

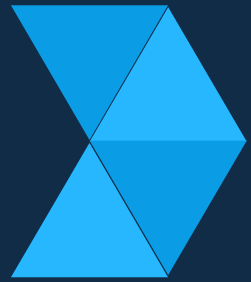


## “Streamlined STR”



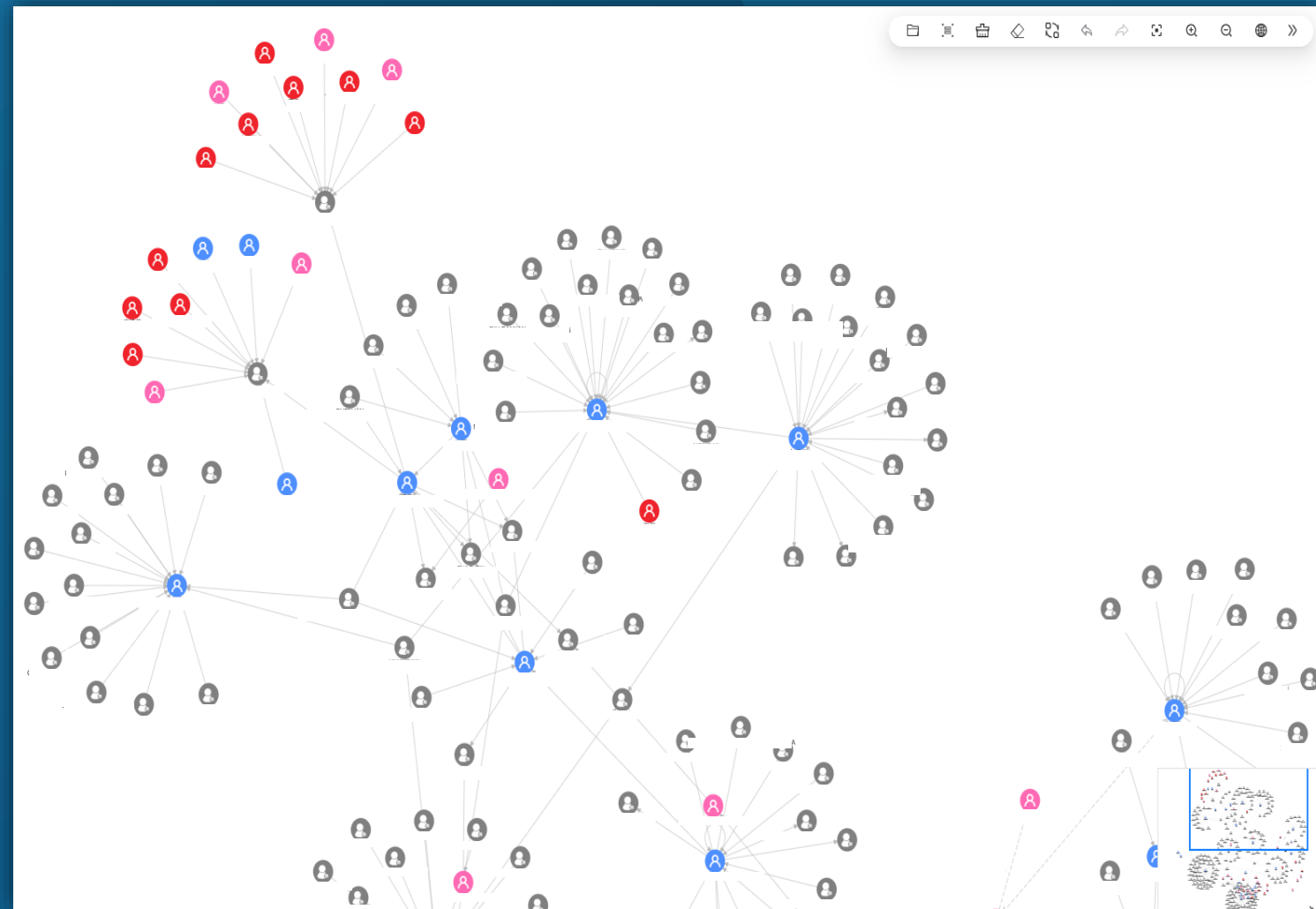
### **Initiative 2 – Real-Time Fraud Monitoring**

- ✧ A “streamlined” STR<sup>6</sup> could be filed to JFIU after passing information to ADCC or when the source of information provided in the STR is from law enforcement agencies or other sources<sup>7</sup> ;
- ✧ A full STR may be filed to JFIU if the source of information on potential suspects/syndicates provided in the STR is newly identified by the bank.



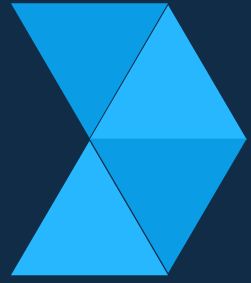
# Observations on STR

Misc. (e.g. Misc. (e.g. difficult to comprehend, important data hidden, etc)



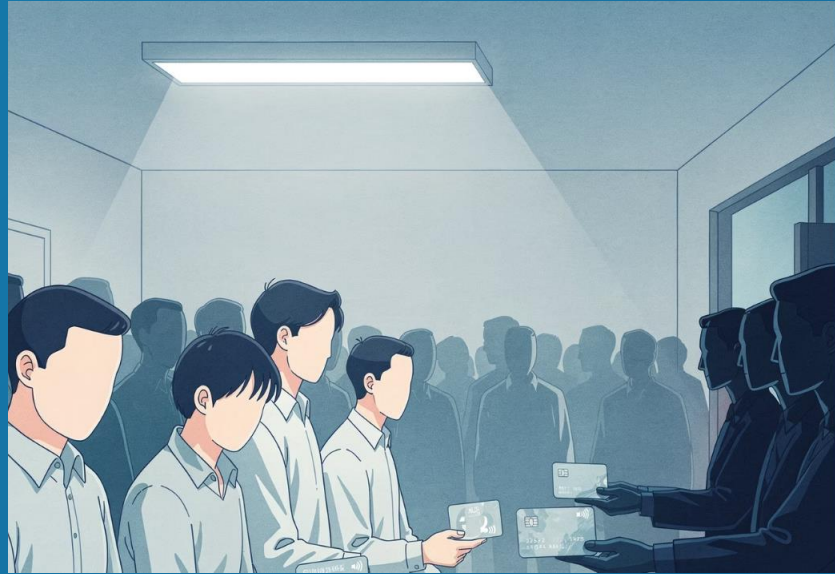
# Agenda

- 1. Trends and Observations on STR submission**
- 2. Money Laundering Trend**



# Money Laundering Trend

## - General Situation



1

**Recruitment of Mainlanders as Mules**



2

**Predicate Offence in Overseas**



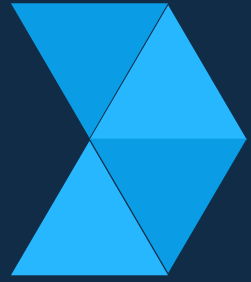
3

**Use of Advanced Technologies**



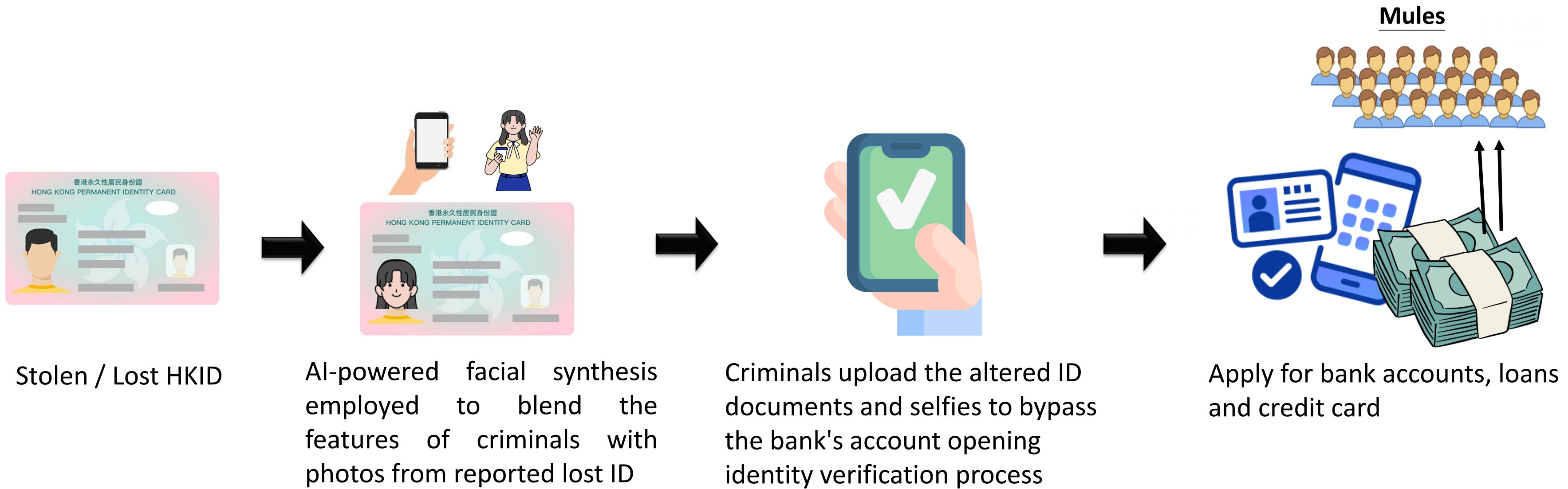
4

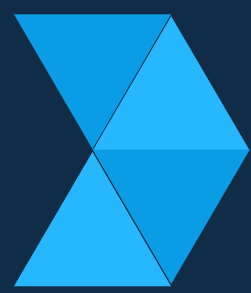
**Cross-sector Money Laundering**



# Money Laundering Trend

## - 3) Use of Advanced Technologies





# Money Laundering Trend

## - 3) Use of Advanced Technologies



Mobile applications automatically downloaded to phone without consent



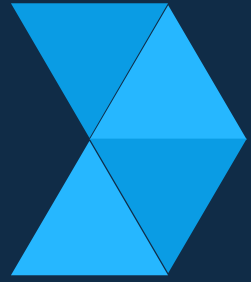
Hacker controlling the mobile phone



Hacker accessing victim's bank account via mobile app and requesting to change credential



Hacker using the two-factor authentication to change the security credential



# Money Laundering Trend

## - 3) Use of Advanced Technologies



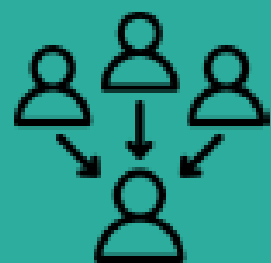
**Two aspects of risks:**

- 1) Installation by financial institution**
- 2) Usage by customers**



# Money Laundering Trend

## - 4) Cross-sector Money Laundering (Exploiting Securities Firm's Bank Account for ML)



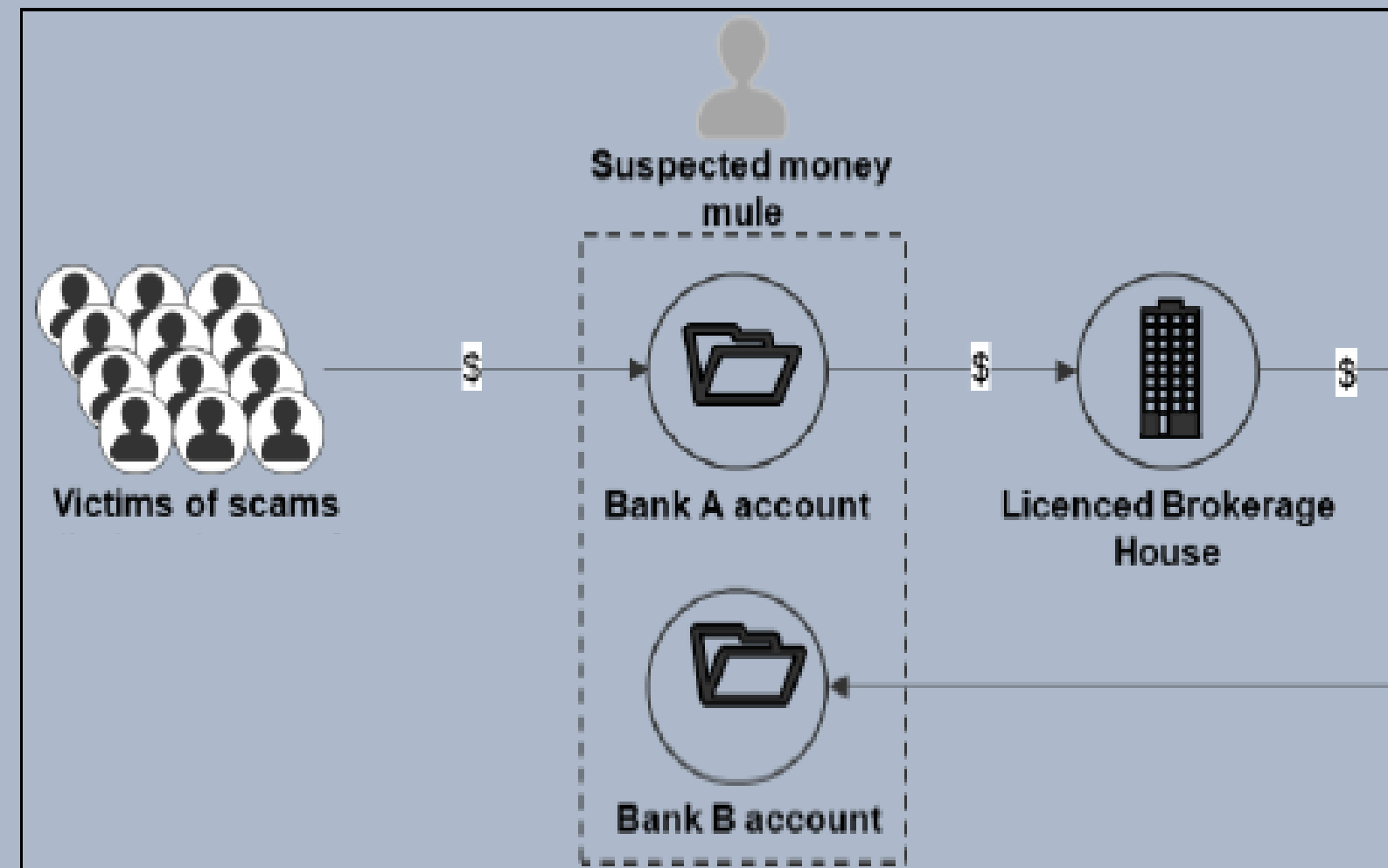
Money mules' bank account of Bank A received scam proceeds from victims (first layer account)



Funds were transferred from bank account to same-name brokerage house account (second layer account)



Funds withdrawn from brokerage house account to same-name bank account of Bank B (third layer account)





Financial Intelligence and Investigation Bureau  
Hong Kong Police Force

# THANK YOU FOR YOUR ATTENTION



More Information:  
[www.jfiu.gov.hk](http://www.jfiu.gov.hk)

