Anti-Money Laundering Webinar 2021

David Hsu – Head of Compliance Risk Management
Edgar Ma – Head of AML Compliance Risk Management

Use of Digital Footprints in Identifying Potential Mule Network

- With the increasing use of digital channels by customers to access banking products and services, their online / mobile footprint is an essential element to analyze and trace any suspicious behavior/pattern.
- The 2 cases are related to identification of potential mule network used for frauds/deceptions by analyzing customers' digital footprints.

Case 1 – IP Address

1. OBSERVATIONS

- Increase in STRs related to ***fraud/ deception***
- Majority of STR subjects are ***new-to-bank*** (NTB) individual customers holding ***Taiwan*** *ID/passport*

Investigation-led Approach

Targeted group of customers for analysis → **Taiwanese subjects**

2. COMMONALITIES

Some common indicators are noted on demographics and transactional pattern of the targeted customers.

- ✓ ***Correspondence address*** is non-residential building in HK, which some are commonly shared
- ✓ Enrolled a number of ***external payees***, some of whom are commonly shared
- ✓ Unusual ***email address*** (with random characters), some of which are commonly shared
- ✓ Declared not working or living in HK, but provided ***only HK contact channels*** – mailing address and only one HK mobile number
- ✓ New banking relationship established within 1-3 months
- ✓ Small amount of ***test fund*** movements among accounts
- ✓ ***Rapid movement of funds*** – Unrelated 3rd party fund deposits, followed by immediate transfer out to other 3rd parties
- ✓ Transfer out to external ***common beneficiaries***

Use of Digital Footprints in Identifying Potential Mule Network

3. IP Address Analysis

- Extract IP address of online/mobile banking login, dates, time and location.
- Identify linkage among the targeted customers through analysis.
- Noted that numerous attempts to access online banking shortly after the accounts were open.
- Findings include:
  - *i.* ***Common IP addresses*** used by the targeted group
  - *ii.* ***Same IP address used by different customers*** on the same day within proximate timeframe
  - *iii.* ***Same customer login at multiple jurisdictions*** on the same day

i. Top 5 Common IP Addresses

Ref#	IP Address	Location	Count of using IP
1	1*.2*.*1.3	China	174
2	1**.1*0.7*.2*5	China	41
3	1*3.3*.6*.15	China	36
4	10*.*4.1*5.5	Taiwan	34
5	**3.7*.22*.2*8	China	29

ii. Same IP Address Used by 7 Customers

Customer	Login Date	Login time	Login IP address
CU# 1	4/8/2020	12:25	1*.2*.*1.3
CU# 1	4/8/2020	15:21	1*.2*.*1.3
CU# 1	4/8/2020	17:07	1*.2*.*1.3
CU# 1	4/8/2020	18:13	1*.2*.*1.3
CU# 2	4/8/2020	12:22	1*.2*.*1.3
CU# 2	4/8/2020	15:19	1*.2*.*1.3
CU# 2	4/8/2020	17:06	1*.2*.*1.3
CU# 2	4/8/2020	18:10	1*.2*.*1.3
CU# 3	4/8/2020	9:59	1*.2*.*1.3
CU# 3	4/8/2020	15:54	1*.2*.*1.3
CU# 3	4/8/2020	16:57	1*.2*.*1.3
CU# 3	4/8/2020	18:52	1*.2*.*1.3
CU# 4	4/8/2020	17:39	1*.2*.*1.3
CU# 5	4/8/2020	11:44	1*.2*.*1.3
CU# 5	4/8/2020	12:31	1*.2*.*1.3
CU# 5	4/8/2020	15:22	1*.2*.*1.3
CU# 5	4/8/2020	17:08	1*.2*.*1.3
CU# 5	4/8/2020	18:19	1*.2*.*1.3
CU# 6	4/8/2020	17:34	1*.2*.*1.3
CU# 6	4/8/2020	18:23	1*.2*.*1.3
CU# 7	4/8/2020	10:56	1*.2*.*1.3
CU# 7	4/8/2020	17:47	1*.2*.*1.3

iii. Same Customer Login at Different Locations

Customer	IP Address	IP Location	Login Date	Login Time
CU# A	**3.7*.22*.2*8	China	3/19/2020	10:17
CU# A	**3.7*.22*.2*8	China	3/19/2020	10:48
CU# A	**3.7*.22*.2*8	China	3/19/2020	11:29
CU# A	**3.7*.22*.2*8	China	3/19/2020	12:45
CU# A	**3.7*.22*.2*8	China	3/19/2020	14:19
CU# A	**3.7*.22*.2*8	China	3/19/2020	15:38
CU# A	**3.7*.22*.2*8	China	3/19/2020	17:00
CU# A	*9.10.7*.20*	Taiwan	3/19/2020	17:04
CU# A	*9.10.7*.20*	Taiwan	3/19/2020	17:26
CU# A	*9.10.7*.20*	Taiwan	3/19/2020	17:31
CU# A	**3.7*.22*.2*8	China	3/19/2020	18:22

Customer	IP Address	IP Location	Login Date	Login Time
CU# B	1*2.6*.18*.2*8	India	4/3/2020	9:42
CU# B	*18.*3.3*.49	China	4/3/2020	10:41
CU# B	10*.*4.1*5.5	Taiwan	4/3/2020	12:10
CU# B	*18.*3.3*.49	China	4/3/2020	13:14
CU# B	1*.2*.*1.3	China	4/3/2020	14:19
CU# B	4*.1*0.1*5.78	India	4/3/2020	15:53

Use of Digital Footprints in Identifying Potential Mule Network

4. Analysis Results

- ~50 customers were included in the targeted analysis with risk indicators.
- Based on the IP address analysis, these accounts may not be controlled by the actual account holders.
- Together with the commonalities observed on their demographics and transaction pattern, it is believed that there is possibly a syndicate operating "behind the scene" to control these mule accounts.

5. Additional Review

- Conduct a sweep on new Taiwanese customers who opened accounts within 6 months with the common risk indicators.
- **12 more suspicious customers** were identified with similar background, pattern and IP address usage.

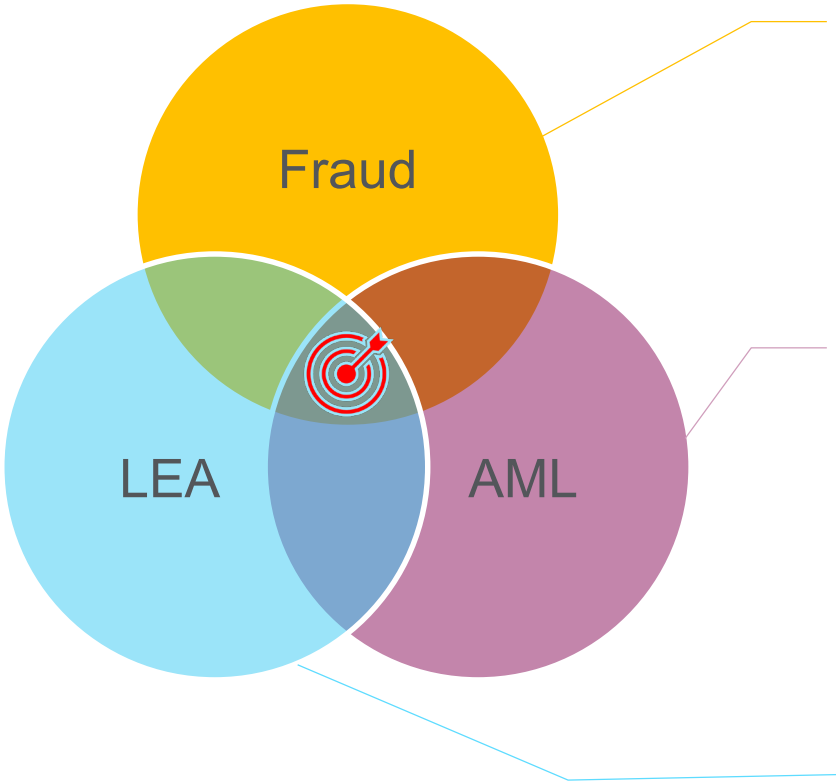
6. Risk Mitigating Actions

- Determine a proper account strategy on related accounts / customers

Use of Digital Footprints in Identifying Potential Mule Network

Case 2 – Device ID

- This case demonstrates the effective use of detecting **unusual Device ID behavior** followed by enhanced analysis to reveal suspicious accounts in a potential mule network.
- Strong internal collaboration between the **Fraud and AML** teams within the bank, and external public private partnership with the **Law Enforcement Agency** (LEA).



1. **Fraud Detection System – Unusual behavior** ***(Customer A)***
   - Online banking password reset by a different device ID
   - Frequent login with different IP locations

2. **AML Investigation – Transaction and Profile Review**
   - Frequent small amount transactions
   - Followed by large funds activities with different individuals
   - Some common counterparties are found
   - They share same Device ID

3. **LEA – Valuable Intelligence Exchange**
   - Customers are involved in telephone deception case

Use of Digital Footprints in Identifying Potential Mule Network

Findings:

- The Device ID used by Customer A was found to be the same as that used by a prior STR subject, who was a suspect of a telephone deception case, as informed by LEA.
- Frequent online banking logins at different IP locations (Guangzhou, Kwun Tong, Aberdeen, Macau, Shenzhen and Hubei).
- Account activities of Customer A were unusual:
  - Frequent small amount "test fund" transactions with different parties, followed by large amount transactions.
  - Rapid movement of funds in a temporary repository pattern
  - Share some common counterparties with prior STR subject
- Intelligence from LEA indicated Customer A was involved in a telephone deception case.

Enhanced Review:

- More customers were found to have used the same Device ID as Customer A.
- Their transactional activities also revealed linkage with other customers.
- Some common counterparties and payee registration setup
- Other Commonalities:
  - HKID card holders, local individual customers
  - New customers with banking relationship < 1 year
  - Residential address in public housing estates
  - No solid occupation – declared as unemployed, housewife, retired, self-employed or blue-collar work

Case Disposition:

- 22 customers were uncovered to have 'linkages' – common Device ID and/or common counterparties/payees.
- Intelligence from LEA revealed some of these customers' accounts were used to deal with suspected fraudulent proceeds.
- These observations indicate they are likely operating as mule accounts syndicate.
- Appropriate compliance actions and account strategy on these customers were performed and formulated.

Use of Digital Footprints in Identifying Potential Mule Network

Key Takeaway

- Authorised institutions should consider collecting relevant data on digital footprints and understand the data infrastructure.

- Work closely with law enforcement to share ideas and information.

- Consider establishing a firm-wide Regtech taskforce to explore ideas and opportunities, and be prepared to accept failure when implementing new ideas (failure in one project may help the team understand the data infrastructure better, which in turn may foster a successful adoption in the following plan).

- Support from Senior Management and Board of Directors needed, and they should be kept informed of industry and regulatory developments.

- Reference materials:
  - Regtech Watch Issue no. 3 on AML
    https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200612e1a1.pdf
  - Regtech Case Studies and Insights
    https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf
  - Regtech Adoption Practice Guide
    https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2021/20210617e5a1.pdf