ANTI-MONEY LAUNDERING ANNUAL REPORT, 2020

Investigation Bureau, Ministry of Justice,
Republic of China (Taiwan)

法務部調查局一〇九年洗錢防制工作年報

Investigation Bureau, Ministry of Justice
Anti-Money Laundering Annual Report, 2020

PREFACE

The COVID-19 pandemic has impacted every aspect of life, including a wide range of living and working styles. Until today, COVID-19 has been continuing to spread around the world with waves of mutated virus. Even though the governments are making every effort to fight against the once-in-a-lifetime pandemic by carrying out measures such as raise vaccination rates, border controls, lockdown, social distancing, quarantine and economy-boosting plans, the lifestyle is still forever changed, and it also brings strong impacts on global financial systems, anti-money laundering (AML) and counter terrorism financing (CTF) framework.

Anti-Money Laundering Division (AMLD) of Ministry of Justice Investigation Bureau (MJIB) works closely with many international counterparts, public and private sectors in Taiwan, and appreciates the support and cooperation, even more valuable during the tough times of coronavirus pandemic. AMLD plays the role of financial intelligence unit (FIU) in Taiwan and builds tight relationships with relevant authorities/sections on AML/ CTF mechanism to detect and combat money laundering/ terrorism financing (ML/ TF) activities. In 2020, AMLD received a total of 24,406 Suspicious Transaction Reports (STRs), 3,052,856 Currency Transaction Reports (CTRs), and 269,841 International Currency and Securities Transportation Reports (ICTRs) in 2020. Additionally, AMLD, as a member of the Egmont Group, exchanges AML/ CTF intelligence with more than 160 FIUs within the global network, and there were 168 cases and 723 reports of international financial intelligence sharing through Egmont Secure Web in 2020.

As the COVID-19 wears on, it has caused many international events canceled or switched to online meeting/ virtual conferencing, for example, 2020 annual meeting of both Asia/ Pacific Group on Money Laundering (APG) and Egmont Group were canceled due to the coronavirus pandemic. Financial Action Task Force on Money Laundering (FATF) 3rd Plenary Meeting and Work Group Meeting of the 31st year (2020) were postponed and later switched to online meetings. Nevertheless, the AMLD seized opportunities to participate in events of AML/ CTF related international organization such as APG, so as to follow the international AML/ CTF trends and strengthen international cooperation.

Moreover, for reinforcing the domestic public-private partnership (PPP), the AMLD not only assigned specialists for reporting entities (e.g. financial institutions, designated non-financial businesses and professions) onsite to promote AML/ CTF awareness, but also held physical workshops/ meetings with law enforcement agencies and competent authorities, namely, Financial Supervisory Commission, National Police Agency, Agency Against Corruption, Coast Guard Administration, Customs Administration and Tax authorities in 2020. Those workshops/ meetings enhanced AMLD's function by coordinating and discussing practical needs with relevant authorities.

In December 2020, the AMLD organized "Conference on Criminal Cash Flow Analysis and Abnormal Transaction Patterns" and more than 140 AML specialists from public and private sectors were attended. The Conference highlighted on ML/ TF case studies and annual reports, and more importantly, it provided a platform for domestic AML/ CTF professions to communicate face to face.

In response to readers' need to further understand ML/ TF criminal activities, trends and typology, this annual report includes more case studies than before. These cases, which were investigated by MJIB, revealed the emerging trends of latest ML tactics used by criminals. Furthermore, the AMLD has been receiving STRs filed by several financial institutes (FIs) with similar descriptions of suspicious transactions and account opening patterns since November 2019; thus the AMLD noticed that the risk of dummy e-banking accounts was increasing and conducted "AML/ CFT Strategic Analysis Report on Dummy E-Banking Accounts" in 2020. The report is included in this annual report as a reference for future policy making and STRs reporting.

FATF has published and renewed a number of documents related to virtual assets due to the misuse of virtual assets is springing up. After the Money Laundering Control Act (MLCA) being amended in November 2018, virtual asset service providers (VASPs) are officially regulated by MLCA, and are required to comply AML regulations similar with FIs. Therefore, in order to better understand virtual assets and raise public awareness, the AMLD, with the consent of FATF, translated FATF paper "Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets" into Chinese and included the paper as part of this annual report. Another FATF report "Trade-based Money Laundering: Trends and Developments" is also included, it gives a comprehensive overview of trade-based money laundering, which provides businesses sectors a guideline of detecting such suspicious activities.

Weng-Jong LEU
Director General
MJIB

August 2021

Editorial Notes

I. Purpose

Recommendation 33 of FATF 40 amended in February 2012 states; "Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/ CFT systems. This should include keeping statistics on: STRs, received and disseminated; ML/ TF investigations, prosecutions and convictions; property frozen, seized and confiscated; and mutual legal assistance or other international requests for co-operation made and received." Therefore, the statistics and analysis of annual data regarding AML/ CFT performed by reporting entities are summarized in this report.

II. Contents

This annual report is divided into the following five parts:

(I) About AMLD.

(II) Work overview (including statistical chart and data).

(III) Significant case studies.

(IV) Strategic analysis report.

(V) Event Calendar of 2020.

III. Notes

(I) The years quoted in this annual report refer to the Gregorian calendar. The numbers of Suspicious Transaction Reports (STRs), Currency Transaction Reports (CTRs), and International Currency and Securities Transportation Reports (ICTRs) are based on the numbers of reports. The value of money is calculated in New Taiwan Dollar (NTD). Special cases are noted in corresponding figures (charts).

(II) MJIB is an acronym which stands for Ministry of Justice Investigation Bureau, and AMLD is an acronym which stands for Anti-Money Laundering Division of MJIB.

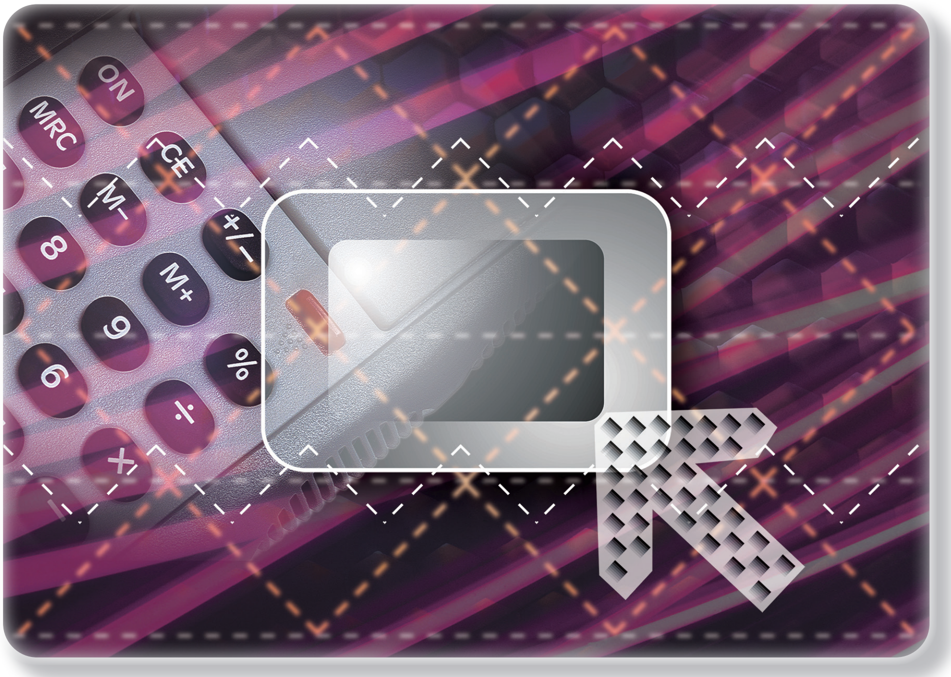
(III) The percentage of each figure is rounded off and the integer is slightly different from the decimal point.

(IV) Date of data collection in work overview statistics, as presented in the second part of this annual report, is 13 July 2021.

Table of Contents

Part I

Introduction to the organization



A criminal group can penetrate and corrode government agencies at all levels, legitimate commercial or financial enterprises, and all sectors of society with the huge profits and wealth obtained through drug crimes. Therefore, at the 1988 Vienna Conference, the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) was enacted to request States members to legislate penalizing ML associated with drug trafficking. The Group of Seven (G7) recognized the drug crimes related to ML, which caused serious threats to the banking system and FIs, and determined to set up the FATF in the 1989 summit meeting. The 40 Recommendations on AML were formulated in 1990 and amended in 1996 that further expanded the predicate offences of ML to other serious offences other than drug trafficking. After 2001, FATF expanded its mission that introduced combat measures against terrorism financing and PWMD.

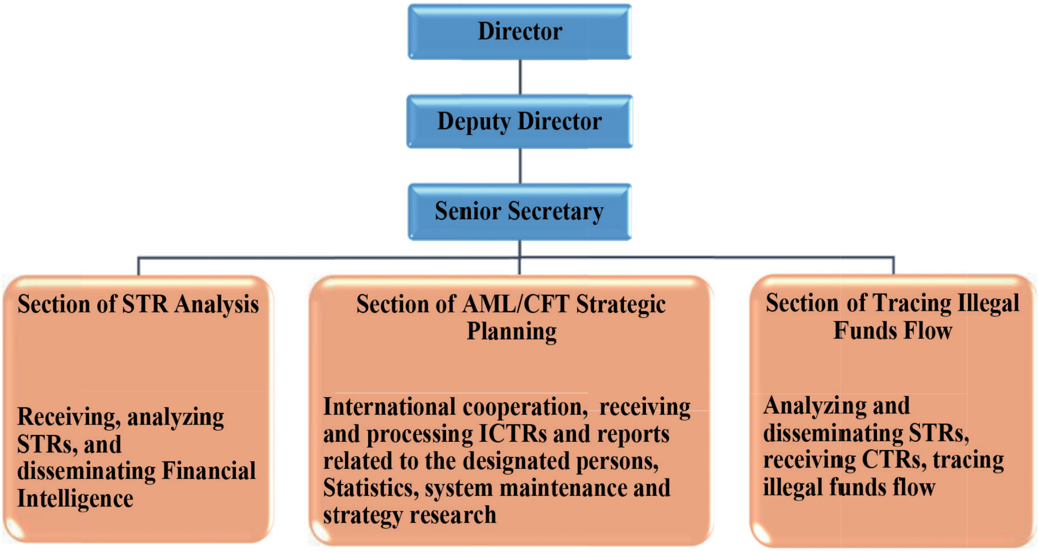
In response to the global trends to curb the detriment caused by ML, the Taiwan's government drafted the Money Laundering Control Act (MLCA), which was passed by the Legislative Yuan on October 23, 1996 and took effect on April 23, 1997 upon presidential decree. During the past years of implementation and practice, it has been recognized by the international organization of AML. Also the MLCA underwent amendments in 2003, 2006, 2007, 2008, 2009, 2016 and 2018 respectively to tackle the practical problems encountered for reacting to the requirements of the FATF Recommendations and the practical need in implementation.

In order to prevent criminals from misusing FIs for ML purposes and to detect major crimes and ML scheme at the point of the transaction, AML legislations around the world require all FIs to file CTRs and STRs. Based on the definition of the AML international organizations, an authority responsible for receiving and analyzing STRs is called FIU. In accordance with the MLCA and the "Key Points for the Establishment of the Money Laundering Prevention Center MJIB", the Investigation Bureau, Ministry of Justice (MJIB) was assigned by the Executive Yuan to receive STRs filed by FIs, and the

Money Laundering Prevention Center (MLPC) was established in 1997 to act as the Taiwan's FIU. In addition, the Legislative Yuan passed the "Organic Act for the MJIB" in 2007. It is clearly enacted in Article 2, Paragraph 7, which the MJIB is in charge of "the AML related matters." Pursuant to Article 3 of the same Act, the MLPC changed the name to the "Anti-Money Laundering Division" (AMLD) and kept on the same functions of Taiwan's FIU. Moreover, Article 7 of the CTFA promulgated in July 2016 stipulates that the MJIB shall receive reports related to TF. The AMLD currently has a Section of STR Analysis, a Section of AML/CFT Strategic Planning, and a Section of Tracing Illegal Funds Flow setup with 26 personnel assigned. Organization and workflow, as shown in Figures A and B. According to Article 9 of the "Regulations for Departmental Affairs of Investigation Bureau under the Ministry of Justice, AMLD is responsible for the following matters:

1. Researching AML strategies and providing consultation in the formulation of relevant regulations;
2. Receiving, analyzing, and processing STRs filed by FIs and disseminating the analysis result;
3. Receiving, analyzing and processing CTRs filed by FIs, and ICTRs forwarded by the Customs and disseminating the analysis result;
4. Assisting other domestic law enforcement partner agencies in matching the AMLD database for investigating ML cases and coordinating/contacting with respect to AML operations
5. Liaison, planning, coordination and implementation of information exchange, personnel training and co-operation in investigating ML cases with foreign counterparts;
6. Compilation and publication of Annual Report on AML work and the data management;
7. Other AML related matters.

Figure A: Organizational Chart of the AMLD



Director

Deputy Director

Senior Secretary

Section of STR Analysis

Receiving, analyzing STRs, and disseminating Financial Intelligence

Section of AML/CFT Strategic Planning

International cooperation, receiving and processing ICTRs and reports related to the designated persons, Statistics, system maintenance and strategy research

Section of Tracing Illegal Funds Flow

Analyzing and disseminating STRs, receiving CTRs, tracing illegal funds flow

FATF GAFI

FINANCIAL ACTION TASK FORCE
GROUPE D'ACTION FINANCIÈRE

◎ FATF（Financial Action Task Force）

At the 1989 Summit in Paris, the Group of Seven (G7) had recognized that activities of ML poses a serious threat to the banking system and FIs. Therefore a decision was reached to set up the FATF. The FATF is responsible for understanding ML techniques and trends, and checking whether each country had adopted international standards and enacted preventive measures to prevent money laundering from occurring. For establishing a generally applicable anti-money laundering infrastructure dedicated to preventing money laundering perpetrators from taking advantage of the financial system, FATF had 40 Recommendations enacted in 1990, and amended in 1996 and 2003, respectively, in order to grasp the development of money-laundering threat. In response to the terrorist attacks in the United States in 2001, 9 special recommendations for countering the financing of terrorism were enacted in 2001.The "Anti-money laundering, countering terrorist financing, and the proliferation of weapons international standards" was passed in the General Assembly of the FATF in February 2012 to have the original 40 anti-money laundering recommendations and 9 special recommendations on countering terrorist financing integrated and amended. In addition, the recommendations on countering the proliferation of large-scale destructive weapons were included.

FATF Member States and FATF-Style Regional Bodies (FSRBs) members exercise Self-assessment or Mutual Evaluation to ensure the effective execution of the aforementioned recommendations.

Currently, FATF has 39 members (37 members of jurisdictions body and 2 organization members, including Gulf Co-operation Council and the European Commission), 9 Associate Members that are regional anti-money laundering organizations, and 1 observers that can participate in the General Assembly and working group meetings fully.

◎ Financial Intelligence Unit (FIU)

Pursuant to the amended FATF Recommendation 20: "If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF, it should be required, by law, to report promptly its suspicions to the FIU." According to the Recommendation 29: "Countries should establish a FIU with responsibility for acting as a national center for receipt and analysis of suspicious transaction reports and other information relevant related to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis." The FIU should serve as the central agency for the receipt of disclosures filed by reporting entities, including:

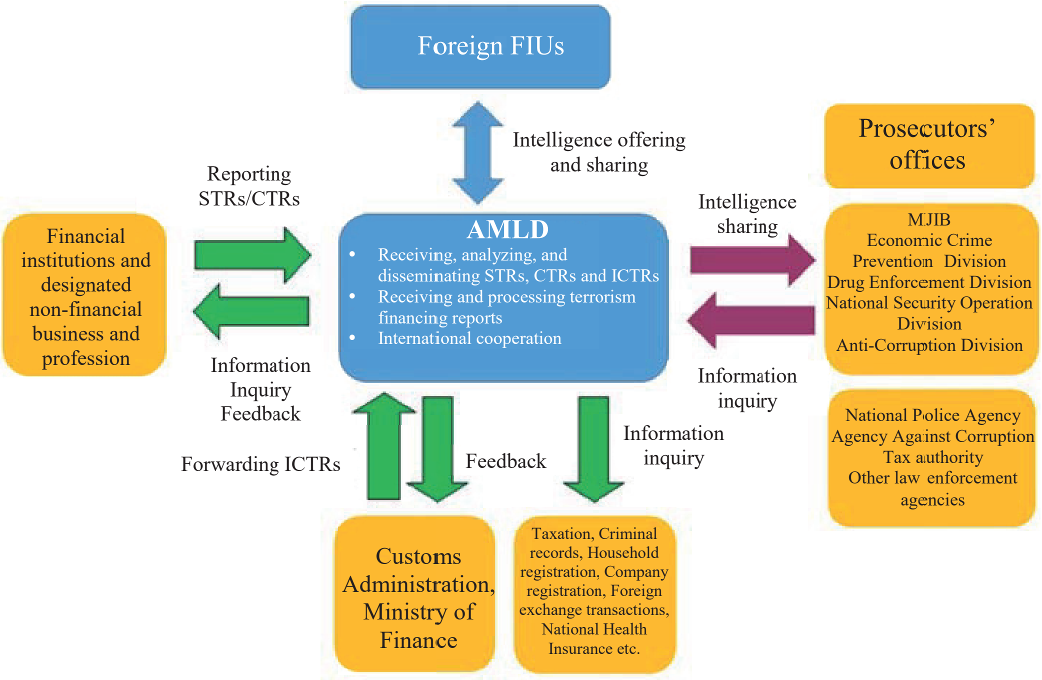
(i) Suspicious transaction reports filed by reporting entities as required by Recommendation 20 and 23; and

(ii) any other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures)

Article 10, Paragraph 1, of the MLCA stipulates: “FIs and designated nonfinancial businesses or professions shall report to the MJIB all suspicious transactions, including attempted transactions, which may involve any of the offenses described in Articles 14 and 15.” Articles 9 and 12 of the same Act stipulate:” FIs and designated nonfinancial businesses or professions shall report currency transactions equal to or above the applicable designated threshold ($500,000 currently) to the MJIB” and “Passengers or crew members entering or leaving the country along with the vehicle and carry the following items shall make declarations at Customs; the Customs should subsequently file a report to the MJIB”

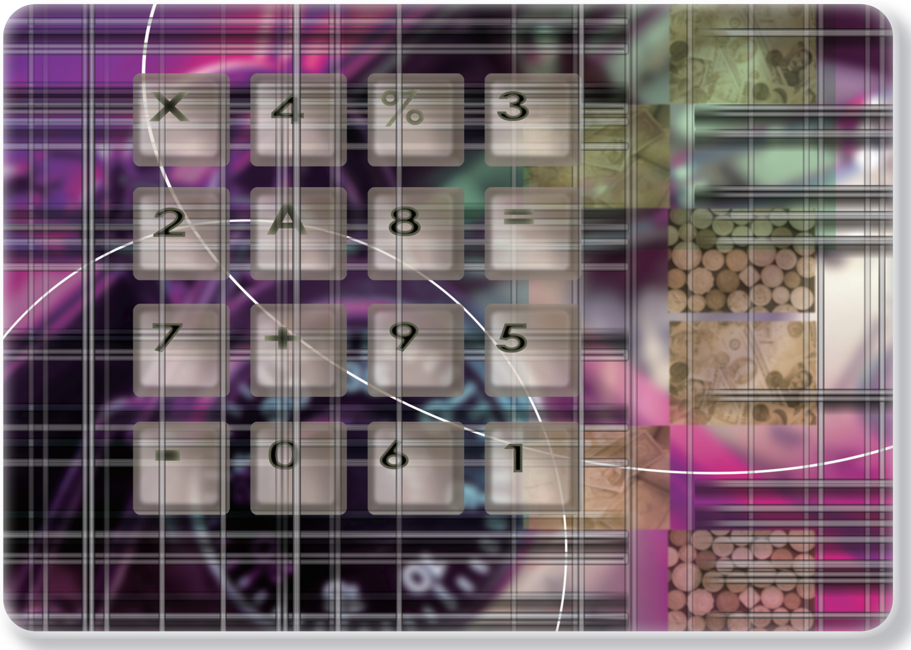
According to Article 2 of the “Organic Act for MJIB” and Article 9 of the “Regulations of the MJIB,” the MJIB is in charge of the AML related matters, and the AMLD actually has taken over the running of Taiwan FIU.

Figure B: Operational flow chart of the AMLD


Foreign FIUs
Intelligence offering and sharing
Prosecutors’ offices
Reporting STRs/CTRs
Intelligence sharing
Financial institutions and designated non-financial business and profession
AMLD
• Receiving, analyzing, and disseminating STRs, CTRs and ICTRs
• Receiving and processing terrorism financing reports
• International cooperation
MJIB
Economic Crime Prevention Division
Drug Enforcement Division
National Security Operation Division
Anti-Corruption Division
Information Inquiry Feedback
Information inquiry
National Police Agency
Agency Against Corruption
Tax authority
Other law enforcement agencies
Forwarding ICTRs
Feedback
Information inquiry
Customs Administration, Ministry of Finance
Taxation, Criminal records, Household registration, Company registration, Foreign exchange transactions, National Health Insurance etc.

Part II

Work Overview



One. Processing STRs

According to FATF Recommendation 20: “If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF, it should be required to report promptly its suspicious to FIUs.” The requirement should be set out in law.

Article 10, Paragraph 1, of the MLCA stipulates: “FIs and DNFBPs shall report to the MJIB all suspicious transactions, including attempted transactions, which may involve any of the offenses described in Articles 14 and 15.” AMLD of MJIB will analyze and disseminate STRs to other Divisions of MJIB or other competent authorities. AMLD received a total of 24,406 STRs in 2020, which was 7.84% less than the 26,481 cases in the last year (2019). After sorting and analyzing the reported data by reporting entities, processing progress, place of occurrence, month of report, subject's age and transaction amount, it was found that 79.56% of reports were raised by local banks, 28.15% of suspicious transactions took place in Taipei City, 53.53% of transaction counterparties were within the 31 to 60 age group, whereas 14.46% of transactions were below NTD 500,000 (detailed statistics and analysis are presented in Tables 01 to 07 and Figures C to F). All STRs received by AMLD have been made accessible to competent authorities such as Ministry of Justice and National Police Agency (NPA), Ministry of the Interior, via online inquiry.

I. Statistics of STRs

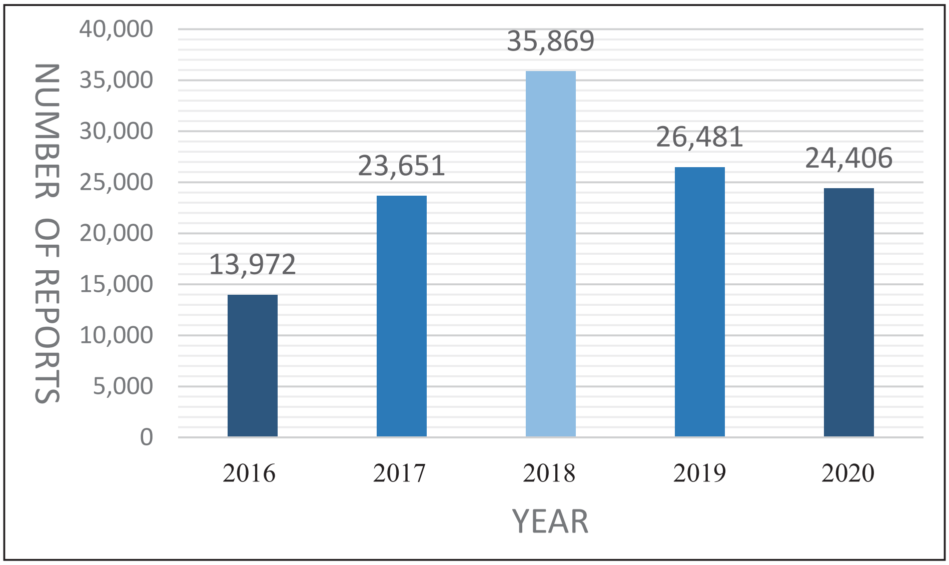
Table 01: Statistics of STRs reported in 2020

Reporting Entities	Number of Reports
Domestic banks	19,417
Foreign banks	20
Trust investment companies	0
Credit cooperative associations	558
Credit departments of farmers’ and fishmen’ s associations	679
Postal remittances and savings	1,816
Bills finance companies	2
Credit card companies	39
Insurance companies	1,221
Securities companies	271
Securities investment trust enterprises	40
Securities finance enterprises	8
Securities investment consulting enterprises	1
Centralized securities depository enterprises	10
Futures commission merchants	85
Designated non-financial businesses and professions	94
Chinese banks	19
Electronic stored value card issuers	106
Foreign currency collection/ exchange agencies	0
Fintech innovative experimentation businesses	3
Finance leasing companies	15
	Total: 24,406

Table 02: Statistics of STRs reported in the last 5 years

Year	2016	2017	2018	2019	2020
No. of STRs	13,972	23,651	35,869	26,481	24,406

Figure C: Statistics on STRs in the last 5 years



II. Dissemination of STRs

Table 03: Statistics of STRs disseminated by AMLD in 2020

	Number of STRs
Refer to MJIB's investigation unit	1,398
Refer to police, prosecutor and other accountable agencies	1,440
International cooperation	47
Add to database	21,429
Analyzing	92
	Total: 24,406

III. Distribution of Suspicious Transactions by Region

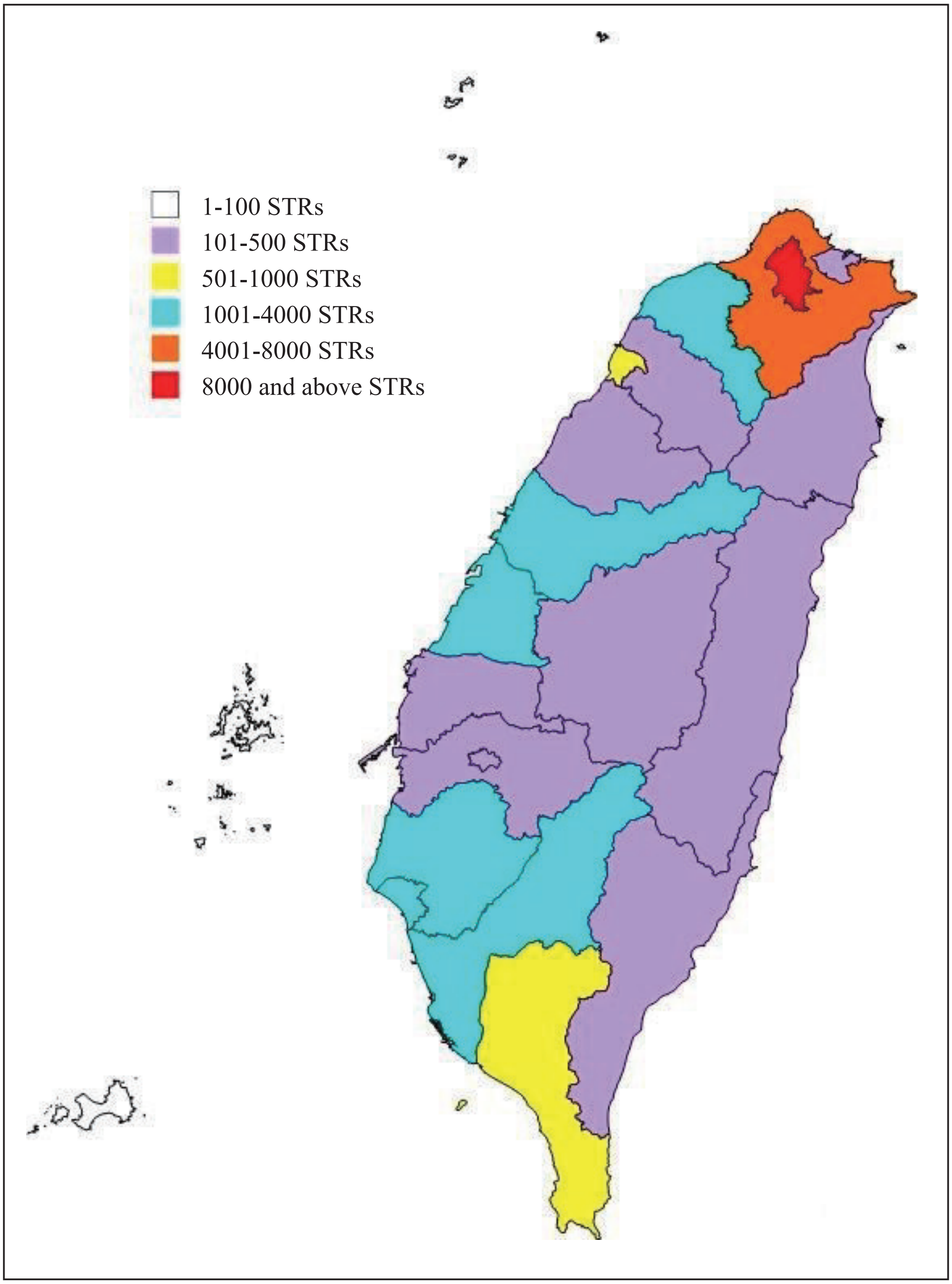
Table 04: Statistics of suspicious transactions by region in 2020

Trading area	Number of STRs	Trading area	Number of STRs
Taipei City	8,585	Chiayi City	438
New Taipei City	4,765	Chiayi County	260
Keelung City	351	Tainan City	1,680
Yilan County	277	Kaohsiung City	2,951
Taoyuan City	2,470	Pingtung County	659
Hsinchu City	673	Hualien County	210
Hsinchu County	468	Taitung County	109
Miaoli County	399	Penghu County	20
Taichung City	3,858	Kinmen County	42
Changhua County	1,050	Lienchang County	3
Nantou County	327	Others[1]	542
Yunlin County	361		
			Total: 30,498

Note: One STR may cover occurrences in more than one area.

[1] Refer to foreign countries, etc.

Figure D: Distribution of STRs Reported by Region in 2020



IV. Distribution of STRs by Month

Table 05: Statistics of STRs reported by month in 2020

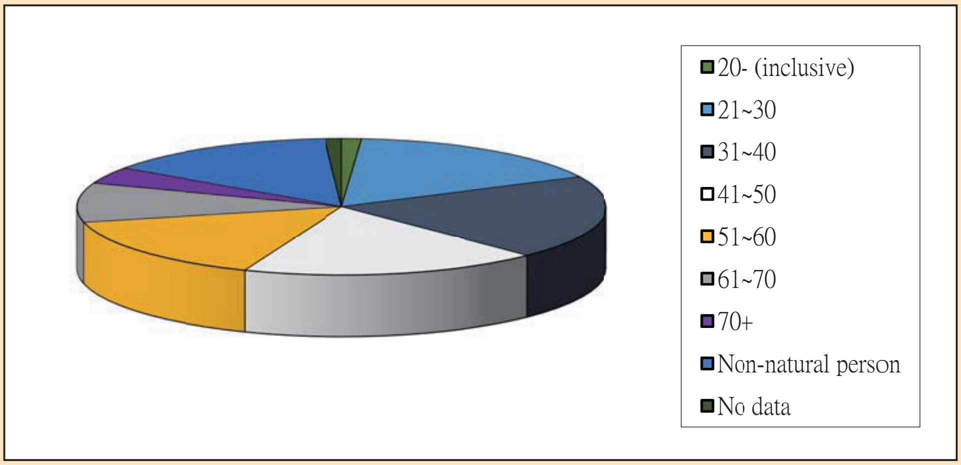
Month	January	February	March	April	May	June	July	August	September	October	November	December
Number of STRs	1,861	1,953	2,097	1,823	1,783	2,121	2,096	2,034	2,417	1,858	2,091	2,272

V. Distribution of STRs by Subjects' Age Group

Table 06: Distribution of STRs by subjects' age group in 2020

Age groups	Number of persons
Aged under 20 (inclusive)	295
Aged 21~30	4,042
Aged 31~40	4,864
Aged 41~50	4,458
Aged 51~60	3,743
Aged 61~70	2,268
Aged 71 and over	972
Non-natural person	3,516
No data	248
	Total: 24,406

Figure E: Pie Chart of STRs Distribution by Subjects’ Age Group in 2020



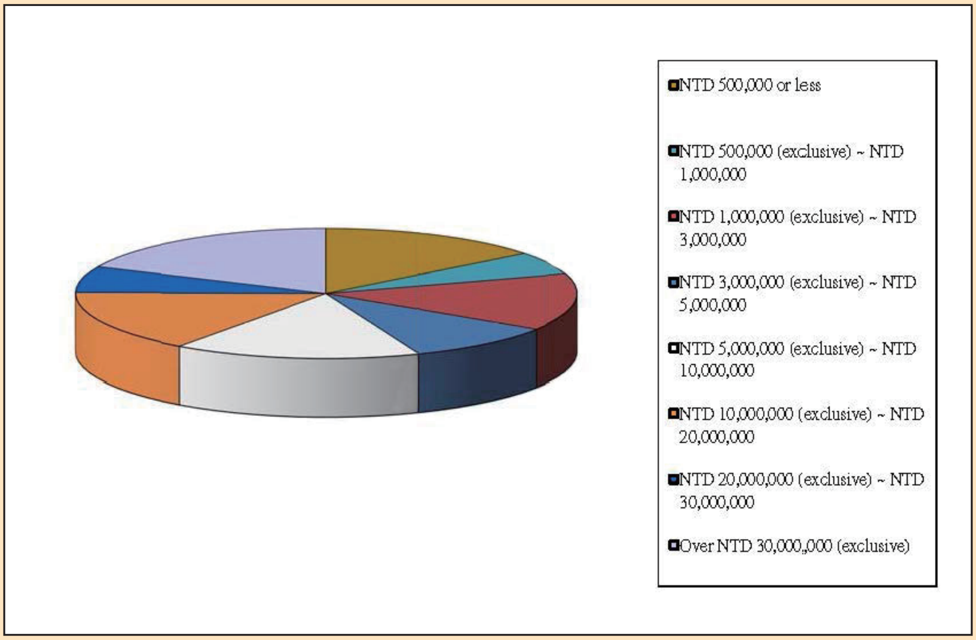
□ Aged under 20 (inclusive) 1.20%
□ Aged 21~30 16.56%
□ Aged 31~40 19.93%
□ Aged 41~50 18.27%
□ Aged 51~60 15.33%
□ Aged 61~70 9.30%
□ Aged 71 and over 3.98%
□ Non-natural person 14.41%
□ No data 1.02%

VI. Distribution of STRs by Amount

Table 07: Distribution of STRs by amount in 2020

Amount	Number of STRs
Below NTD 500,000 (including NTD 500,000)	3,528
NTD 500,000 ~ NTD 1 million (excluding NTD 500,000)	1,392
NTD 1 million ~ NTD 3 million (excluding NTD 1 million)	3,450
NTD 3 million ~ NTD 5 million (excluding NTD 3 million)	2,363
NTD 5 million ~ NTD 10 million (excluding NTD 5 million)	3,887
NTD 10 million ~ NTD 20 million (excluding NTD 10 million)	3,715
NTD 20 million ~ NTD 30 million (excluding NTD 20 million)	1,613
Over NTD 30 million (excluding NTD 30 million)	4,458
	Total: 24,406

Figure F: Pie Chart of STRs Distribution by Amount in 2020



□ Below NTD 500,000 (inclusive) 14.46%
□ NTD 500,000 ~ NTD 1 million (excluding NTD 500,000) 5.70%
□ NTD 1 million ~ NT3 million (excluding NTD 1 million) 14.14%
□ NTD 3 million ~ NTD 5 million (excluding NTD 3 million) 9.68%
□ NTD 5 million ~ NTD 10 million (excluding NTD 5 million) 15.93%
□ NTD 10 million ~ NTD 20 million (excluding NTD 10 million) 15.22%
□ NTD 20 million ~ NTD 30million (excluding NTD 20 million) 6.61%
□ Over NTD 30 million (excluding NTD 30 million) 18.27%

Two. Receiving CTRs

According to Article 9 of the MLCA, FIs and DNFBPs shall report currency transactions equal to or above the applicable designated threshold to the MJIB The term “the applicable designated threshold” shall mean NTD 500,000 (including the foreign currency equivalent thereof) pursuant to Article 2 of Regulations Governing Anti-Money Laundering of Financial Institutions and Regulations Governing Anti-Money Laundering of Agricultural Financial Institutions. After receiving CTRs, AMLD will update and maintain data on the database, and accept large cash transaction inquiries from MJIB field offices, law enforcement agencies, judiciary, and prosecutor offices and policies agencies based in Regulations under Art 5 of MJIB Operation Regulations on Matters relevant to AML/CFT. AMLD received 3,052,856 CTRs in 2020, and according to the statistics and analysis of those reports, 78.74% of CTRs were reported by domestic banks; 73.13% of CTRs were with an amount of NTD 500,000 ~ NTD 1 million; and 38,704 transactions in CTRs database had been accessed in 2020 (Please refer to Table 8 ~ Table 11 and Figure G ~ H for detailed statistics and analysis)

I. Statistics of CTRs

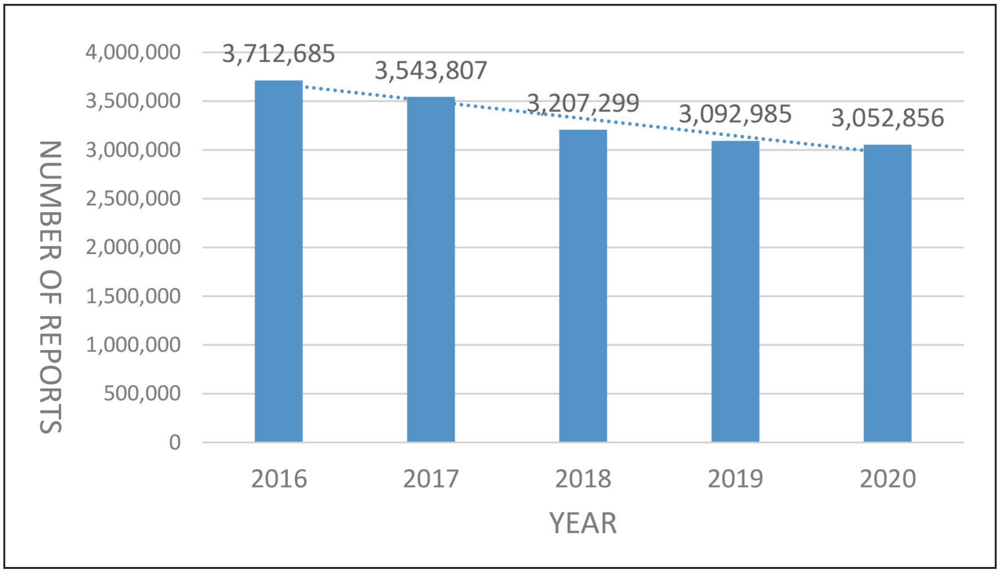
Table 08: Statistics of CTRs in 2020

Reporting entities	Number of Reports
Domestic banks	2,403,839
Foreign banks	8,471
Chinese banks	0
Trust investment companies	0
Credit cooperative associations	116,983
Credit departments of farmers' and fishmen's associations	252,256
Postal remittances and savings	265,466
Insurance companies	5,560
Reports in writing (Securities investment trust and consulting companies)	8
Reports in writing (Electronic stored value card issuers)	1
Reports in writing (Other financial institutions)	9
Reports in writing (Jewelry businesses)	272
	Total: 3,052,856

Table 09: Statistics of CTRs in the last 5 years

Year	2016	2017	2018	2019	2020
Number of Reports	3,712,685	3,543,807	3,207,299	3,092,985	3,052,856

Figure G: Statistics on CTRs in the last 5 years

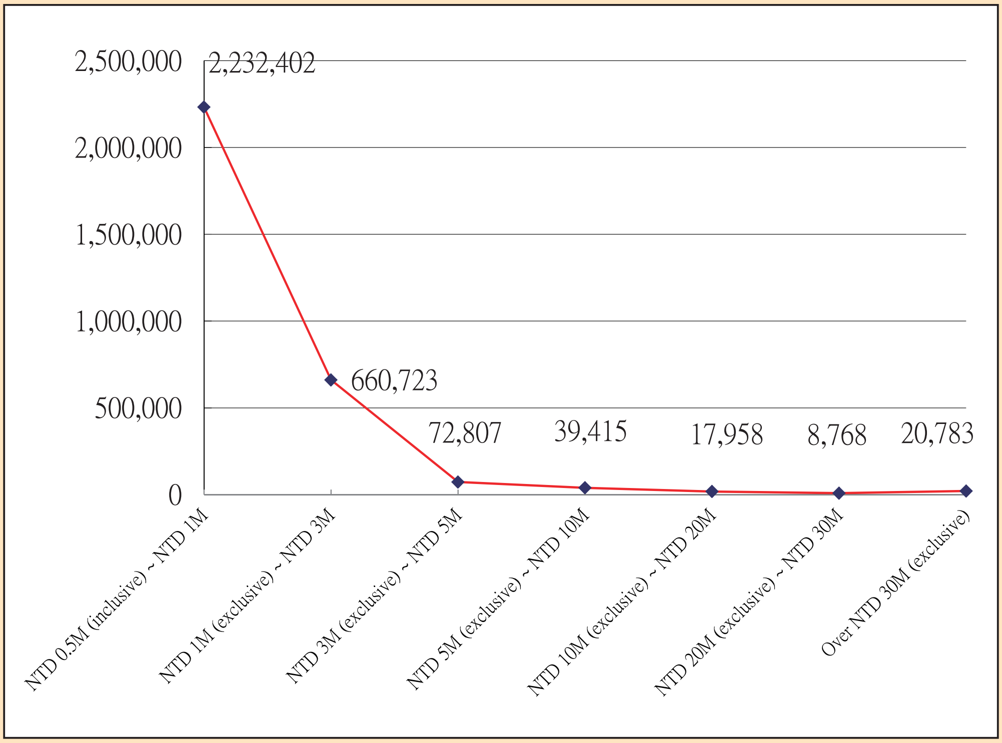


II. Distribution of CTRs by Amount

Table 10: Distribution of CTRs by Amount in 2020

Amounts	Number of Reports
NTD 500,000 ~ NTD 1 million (including NTD 500,000)	2,232,402
NTD 1 million ~ NTD 3 million (excluding NTD 1 million)	660,723
NTD 3 million ~ NTD 5 million (excluding NTD 3 million)	72,807
NTD 5 million ~ NTD 10 million (excluding NTD 5 million)	39,415
NTD 10 million ~ NTD 20 million (excluding NTD 10 million)	17,958
NTD 20 million ~ NTD 30 million (excluding NTD 20 million)	8,768
Over NTD 30 million (excluding NTD 30 million)	20,783
	Total: 3,052,856

Figure H: Line Graph of CTRs Distribution by Amount in 2020



□ NTD 500,000 ~ NTD 1 million (including NTD 500,000) 73.13%
□ NTD 1 million ~ NT3 million (excluding NTD 1 million) 21.64%
□ NTD 3 million ~ NTD 5 million (excluding NTD 3 million) 2.38%
□ NTD 500,000 ~ NTD 1 million (excluding NTD 500,000) 1.29%
□ NTD 10 million ~ NTD 20 million (excluding NTD 10 million) 0.59%
□ NTD 20 million ~ NTD 30 million (excluding NTD 20 million) 0.29%
□ Over NTD 30 million (excluding NTD 30 million) 0.68%

III. Statistics of Accessing CTRs Database

Table 11: Statistics of accessing CTRs database in the last 5 years

Year	2016	2017	2018	2019	2020
Investigation Bureau of the Ministry of Justice	21,413	32,402	30,717	21,609	23,472
Other law enforcement agencies	13,012	17,929	29,153	19,236	13,047
Prosecution and court	5,186	9,051	6,628	3,252	2,185
Total	39,611	59,382	66,498	44,097	38,704

Three. Receiving ICTRs

According to FATF Recommendation 32: “Countries should implement a declaration system or a disclosure system for incoming and outgoing cross-border transportation of currency and bearer negotiable instruments (BNIs). Countries should ensure that a declaration or disclosure is required for all physical cross-border transportations, whether by travelers or through mail and cargo, but many use different system for different modes of transportation.”

According to Article 12, Paragraph 1, of the MLCA: “Passengers or crew members entering or leaving the country along with the vehicle and carry the following items shall make declarations at Customs; the Customs should subsequently file a report to the MJIB: I. Cash in foreign currency or currencies issued by Hong Kong or Macau, and cash in NTD, totaling over an applicable designated threshold. II. Negotiable securities with a face value totaling over an applicable designated threshold. III. Gold with a value totaling over an applicable designated threshold. IV. Other items with a value totaling over an applicable designated threshold and might be used for the purpose of money laundering.” and Article 12, Paragraph 2, of the MLCA: “Acts to deliver items prescribed in the preceding paragraph by shipment, express delivery, mail, or other similar means, across the border, would also be subject to the preceding provisions.”

In addition, according to Article 3, Paragraph 1 and 2, of the Anti-Money Laundering Regulations for Cross-border Declaration and Reporting: “A passenger or a service crew member arriving into or departing from the country on a flight/voyage within the same day, holding the following items in his/her possession, shall be required to declare said items to the Customs pursuant to Article 4 of the Regulations.” Thereafter, the Customs shall report the said declarations to the MJIB pursuant to Article 5 of the Regulations. “I. Cash in foreign currencies, including currencies issued by Hong Kong or Macau, in an aggregate value exceeding ten thousand US dollars. II. Cash in NTD in an aggregate value exceeding one hundred thousand. III. Securities bearing a total face value more than ten thousand US dollars IV. Gold in an aggregate value exceeding twenty thousand US dollars. V. Items, might be used for the purpose of ML, in an aggregate value exceeding five hundred thousand NTD." Affected by COVID-19 pandemic, the number of passenger/crew member to enter or exit the border was significantly decreased in 2020, comparing to the last few years. A total of 7,364 ICTRs were filed to the MJIB in 2020, which is a lot less than 39,855 ICTRs in 2019. In terms of the declared value, 84.08% of ICTRs were below NTD 1 million (Please refer to Table 12 to Table 15 and Figure I for detailed statistics and analysis).

Meanwhile, Article 3, Paragraph 3, of the Anti-Money Laundering Regulations for Cross-border Declaration and Reporting states that "An Exporter/Importer or a Sender/Receiver delivers items prescribed in the preceding paragraph across the border on a flight/shipment within the same arriving/post day by shipment, express delivery, mail or other similar means, shall also be subjected to provisions of preceding paragraph." In 2020, the customs had reported to MJIB 262,477 ICTRs (delivered items) with the total value of more than NTD 255 billion; 51.23% of which were import declaration (please refer to Table 16 to Table 19).

I. Volume of passengers' reports (including crew member)

Table 12: Volume of passengers' reports (including crew member) in 2020

Departure and arrival	Count
Arrival	1,342
Departure	6,022
Total	7,364

Table 13: Volume of passengers' reports (including crew member) in the last 5 years

Year	2016	2017	2018	2019	2020
Count	33,555	45,165	47,383	39,855	7,364

II. Passengers' reports (including crew member) by Month

Table 14: Passengers' reports (including crew member) by month for 2020

Month	January	February	March	April	May	June
No. of Reports	3,220	1,887	468	116	125	127
Violations[2]	17	5	5	0	0	1
Subtotal	3,237	1,892	473	116	125	128
Month	**July**	**August**	**September**	**October**	**November**	**December**
No. of Reports	210	226	216	272	261	236
Violations	0	1	2	2	0	4
Subtotal	210	227	218	274	261	240

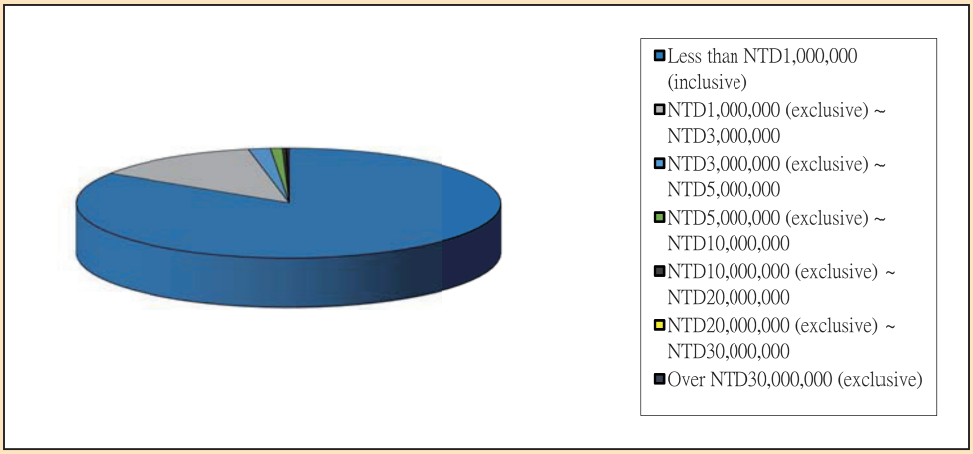
III. Passengers' reports (including crew member) by Value

Table 15: Passengers' reports (including crew member) by value in 2020

Amount	Count
Below NTD 1 million	6,192
NTD 1 million ~ NTD 3 million (excluding NTD 1 million)	946
NTD 3 million ~ NTD 5 million (excluding NTD 3 million)	122
NTD 5 million ~ NTD 10 million (excluding NTD 5 million)	66
NTD 10 million ~ NTD 20 million (excluding NTD 10 million)	19
NTD 20 million ~ NTD 30 million (excluding NTD 20 million)	6
Over NTD 30 million (excluding NTD 30 million)	13
	Total: 7,364

[2] Unreported or false reports.

Figure I: Pie Chart of ICTRs Distribution by Value in 2020



- □ Below NTD 10 million 84.08%
- □ NTD 1 million ~ NT3 million (excluding NTD 1 million) 12.85%
- □ NTD 3 million ~ NTD 5 million (excluding NTD 3 million) 1.66%
- □ NTD 5 million ~ NTD 10 million (excluding NTD 5 million) 0.90%
- □ NTD 10 million ~ NTD 20 million (excluding NTD 10 million) 0.26%
- □ NTD 20 million ~ NTD 30 million (excluding NTD 20 million) 0.08%
- □ Over NTD 30 million (excluding NTD 30 million) 0.18%

IV. Statistics of ICTRs (delivered items)

Table 16: Statistics of ICTRs (delivered items) in 2020

Import/export	No. of reports
Export	51,538
Import	210,939
Total	262,477

Table 17: Statistics of ICTRs (delivered items) in recent years

Year	2018	2019	2020
Count	290,084	320,481	262,477

V. Statistics of the Value of ICTRs (delivered items)

Table 18: Statistics of the value of ICTRs (delivered items) in 2020

Import/export	Value (NT dollar)
Export	133,275,188,200
Import	122,518,919,465
Total	255,794,037,665

VI. Distribution of ICTRs (delivered items) by Month

Table 19: Distribution of ICTRs (delivered items) by month in 2020

Month	January	February	March	April	May	June
No. of reports	18,360	17,945	20,989	16,993	13,860	20,427
Month	July	August	September	October	November	December
No. of reports	24,675	21,324	28,417	26,000	26,773	26,714

Four. Publicity Outreach and Training

I. Publicity Outreach

In an attempt to raise the general public's awareness toward money laundering to effectively deter illegal activities, MJIB has been organizing a series of AML promotion programs through its field division that are targeted at local institutions, universities and private organizations. Through the use of fun quizzes and rewards, the audience is made aware of the nation's AML framework as well as the negative effects of money laundering and the importance of combating it.

MJIB's Taichung City Field Division promoting AML awareness at "2020 Employment Fair" in Taichung City.

MJIB's Taipei City Field Division promoting AML awareness on self-designed posters.

II. AML/CFT Capacity Building Training

According to FATF Recommendation 34: "The competent authorities, supervisors and SRBs shall establish guidelines, and provide feedback, which will assist FIs and designated non-financial businesses and professions in applying national AML/CFT measures and, in particular, in detecting and reporting suspicious transactions." In this respect, the AMLD has been addressing the requests of FIs by assigning specialists to promote AML awareness, provide personnel of FIs with the information needed to strengthen AML and CTF skills, improve the quality of STRs, and enhance the abilities to identify suspicious transactions. AMLD specialists would share their experiences on how to detect crimes such as illegal remittance, stock price manipulation, insider trading, corporate embezzlement, fraud and online gambling. Through these efforts, AMLD hopes to improve FIs' abilities to identify abnormal transactions and enhance risk-based customer due diligence practices.

Table 20: Statistics on AML and CFT training for reporting institutions in 2020

Name of institution		Subtotal	
		Session	Participants
Banks	Local banks (including financial holding companies)	16	1,781
	Foreign banks	1	23
Credit departments of farmers' and Fishmen's Associations		4	297
Securities investment trust and consulting companies		2	112
Securities companies		1	75
Futures commission merchants		3	205
Insurance companies		10	602
Credit card companies		2	47
Electronic payment companies		1	8
Virtual asset service providers		1	30
Designated non-financial businesses and professions		1	52
Total		42	3,232

Five. Public-private sector coordination and strategic studies

I. Organized coordination meeting with law enforcement agencies and competent authorities

To strengthen the capacity of the national FIU in supporting the operational requirements of the competent authorities of law enforcement and supervision, enhance the effectiveness of the use of financial intelligence, and respond to the recommendations proposed by the APG in the mutual evaluations, AMLD actively exchanged ideas with competent authorities and law enforcement agencies in 2020. In the first half of 2020, AMLD organized coordination meetings with the Coast Guard Administration of Ocean Affairs Council and Taxation Administration of Ministry of Finance (including the Fiscal Information Agency, National Taxation Bureau of Taipei, and

Coordination meeting between AMLD and the Taxation Administration, Ministry of Finance on February 2020

National Taxation Bureau of the Northern Area). The key issues discussed in the meetings include how to improve cross-agency information sharing mechanism, how to identify and detect illegal activities through financial intelligence more effectively, and other affairs related to cross-agency cooperation. In the second half of 2020, AMLD organized coordination meetings with the Customs Administration of Ministry of Finance, National Taxation Bureau of the Northern Area, Criminal Investigation Bureau of National Police Agency, National Taxation Bureau of Taipei, Agency Against Corruption of Ministry of Justice, National Taxation Bureau of the Central Area, Financial Examination Bureau of Financial Supervisory Commission (FSC), National Taxation Bureau of the Kaohsiung and National Taxation Bureau of the Southern Area. The meetings were focused on case studies, ML risks, typologies and trends. The meetings provided opportunities for different agencies to communicate with each other face to face, making it more efficient for coordination and cooperation between the authorities.

Attendees to meetings between the AMLD and Criminal Investigation Bureau on September 2020

II. Organized Conference on Criminal Cash Flow Analysis and Abnormal Transaction Patterns

To develop a better framework of public-private partnership in Taiwan, and to enhance the understanding on ML/ TF/ proliferation financing of relevant sectors, the AMLD and Banking Bureau of FSC co-organized "2020 Conference on Criminal Cash Flow Analysis and Abnormal Transaction Patterns" on 10 December 2020. A total of 140 AML supervisors and specialists from 86 FIs had participated in the conference. The conference opened with remarks from Leu Weng-Jong, Director-General of the MJIB, and Huang Kuang-Hsi, Deputy Director of the Banking Bureau. Invitees included the following individuals from the MJIB: Chen Hsi-Chieh, investigation specialist at the National Security Division; Chen Ya-Wen, special agent at the Anti-Corruption Division; Chang Chieh-Chen, section chief at the Economic Crime Prevention Division; Li Wei-Chun, senior special agent at the Drug

Scene of the 2020 Conference on Criminal Cash Flow Analysis and Abnormal Transaction Patterns

Hosting officers at the 2020 Conference on Criminal Cash Flow Analysis and Abnormal Transaction Patterns

Enforcement Division; and Chen Chi-Ming, special agent at the AMLD. Also, Captain Chao Shang-Chen from the Criminal Investigation Bureau was invited to share ML related cases. These invitees briefly explained important cases in law enforcement, 2019 annual report, and future enforcement focuses of their respective units. The AMLD Director Wu Jung-Chun hosted the post-conference symposium, in which attendees raised questions and participated in the discussions, thereby gaining deeper understanding of criminal and ML methods. In doing so, it is hoped that professionals in relevant industries can improve their ability to identify suspicious transaction patterns and optimize the efficacy of reporting mechanisms.

IIII. Compilation of strategic analysis report on "dummy e-banking account"

To understand the ML risks and trends in Taiwan, and also to provide assistance to competent authorities and FIs for reinforcing AML framework, the AMLD had conducted “AML/CFT Strategic Analysis Report on Dummy E-Banking Accounts” after been receiving STRs filed by several FIs with similar description of suspicious transactions and account creation patterns. By reviewing and analyzing those STRs, the AMLD noticed that the risk of dummy e-banking accounts was increasing. Afterwards, the AMLD started initial investigation and assigned several MJIB field divisions to interview some holders of the bank accounts. The strategic analysis report was disseminated by the AMLD to the relevant authorities and reporting entities for reference of policy making and refining the existing AML/CFT mechanism.

IV. Issued AMLD Press

Taiwan had been through APG's 3rd round of Mutual Evaluation in 2019 and was awarded a favorable rating of "Regular follow-up." However, the assessment team did make several emphases in its recommendation about the importance of information sharing, cooperation and coordination between FIU, law enforcement, supervisory authority, reporting entities of the private sector. As a national FIU, AMLD bears the critical responsibility of delivering information to designated agencies. To further enhance AMLD's role and functionality as an FIU, AMLD issued its first press in November 2019 and took steps toward creating a common platform that would facilitate exchange of knowledge and information relating to AML, CTF and anti-PWMD. In 2020, the AMLD had published 3 issues of the AMLD Press, and both Chinese and English versions are available on the AMLD official website. In the meantime, AMLD continues to expand relationship with the public sector, private sector and industry partners, which provides it with access to valuable information such as statistics, crime trends, transaction patterns, prevention measures and professional opinions that can be shared with competent authorities, partners and the general public. With improved risk identification capacity, the nation as a whole will be able to adopt preventive measures that are commensurate with risks, and allocate limited resources to high-risk activities for more effective AML, CTF and anti-PWMD.

◎ APG（Asia/ Pacific Group on Money Laundering）

The APG was established in 1997 to assist its state members in accepting and fulfilling the international standards set by the FATF on preventing money laundering, combating terrorism financing, and preventing weapon proliferation financing.

Taiwan had previously undergone two rounds of APG Mutual Evaluations, once in 2001 and once in 2007; both evaluation reports were approved in APG annual meetings, and Taiwan has been favorably recognized for its AML system. As Taiwan's FIU, the AMLD received the highest rating that affirmed its competent functions. While undergoing APG's 3rd round of Mutual Evaluation, the evaluators were impressed with AMLD's ability to perform as a FIU and collaborate with international counterparts despite Taiwan's diplomatic challenges.

At present, the APG has 41 members, 8 observers, and 32 observer organizations, and is an associate members of FATF. Taiwan is a founding member of the APG under the name of "Chinese Taipei", and is allowed to participate in the FATF's affairs with the APG membership.

Six. International co-operation and exchange

I. International intelligence exchange

FATF's Recommendation 40 states that: "Countries shall ensure that their competent authorities can rapidly provide the widest range of international co-operation in relation to money laundering, associated predicate offences and terrorist financing. Such exchanges of information should be possible both spontaneously and upon request. Competent authorities should have a lawful basis for providing co-operation; be authorized to use the most efficient means to co-operate; have clear and secure gateways, mechanisms or channels that will facilitate and allow for the transmission and execution of requests; have clear processes for the prioritization and timely execution of requests; and have clear processes for safeguarding the information received.” The AMLD makes use of Egmont Group's channels to exchange intelligence on money laundering, terrorism financing and PWMD with 167 countries/ FIUs worldwide. The statistics of AMLD’s international intelligence exchange in the last 5 years are listed as table 21.

Table 21: Statistics of international intelligence exchange in the last 5 years

Task	Year	2016	2017	2018	2019	2020
Requests from overseas FIUs	Cases	50	55	47	71	58
	Reports	169	161	162	279	197
Requests to overseas FIUs	Cases	34	26	23	38	32
	Reports	165	94	107	292	110
Sponstaneous exchange from overseas FIUs	Cases	25	53	99	81	66
	Reports	44	100	198	198	132
Sponstaneous exchanges to overseas FIUs.	Cases	26	45	20	17	12
	Reports	45	94	46	50	23
Questionnaire and others	Cases	0	0	0	0	0
	Reports	262	354	339	248	261
Total	Cases	135	179	189	207	168
	Reports	685	803	852	1,067	723

II. Concluding Agreement/MOUs with Other FIUs

Money laundering is a crime that often takes place across borders, therefore it requires consensus, cooperation, mutual trust and mutual benefit among governments to effectively combat cross-border money laundering, terrorism financing, and financing of PWMD. On 1 June 2020, the AMLD completed signing of the “Memorandum of understanding for cooperation of information-sharing regarding money laundering, crimes of relevant preparations and financing of terrorism” with the Republic of Kosovo by signing the agreement in separate locations due to the coronavirus pandemic. The MOU will be hugely beneficial for cooperation for combating transnational money laundering crimes, felonies, and financing of terrorism operations. By 31 December 2020, the AMLD had signed agreements or memorandums with 51 countries or regions, and the AMLD is still looking for more opportunities to cooperate with the members in international society.

III. Participation in Working Group Meeting of Egmont Group

The 2020 Egmont Group Working Group and Egmont Committee Meetings was held at the Ravenala Attitude Hotel in Balaclava, Mauritius from January 27 to January 31, 2020. More than 300 representatives from countries and international organizations attended the event. The delegation from AMLD was participated in meetings of the "Membership, Support and Compliance Working Group" and the "Asia Pacific Regional Group". Since 1998, the AMLD has been a member of the Egmont Group. The AMLD has provided technical support to assist in operations of the meetings, and the Division is currently co-sponsoring the entry of FIU Vietnam with FIU France to actively create opportunities for interactions with members while deepening Taiwan's participation in international organizations.

Scene of the 2020 Egmont Group Working Group and Egmont Committee Meetings

◎ Egmont Group

On June 9, 1995, the financial intelligence units of various countries met up at Egmont-Arenberg Palace in Brussels, Belgium, to set up the Egmont Group, which was an important platform for intelligence exchange of the financial intelligence units around the world for the prevention of money laundering jointly, especially the scope of intelligence exchange, training, and technology sharing.

Taiwan had joined Egmont Group since its 6th annual meeting in June 1998 and is currently named as Anti-Money Laundering Division (AMLD), Taiwan. Egmont Group has 167 members so far that exchange financial intelligence through a secure network. The AMLD regularly participates in the plenaries and working group meetings organized by Egmont Group and also conducts intelligence exchange and promotes signing an agreement or memorandum of intelligence exchange on anti-money laundering and countering terrorism financing in order to comply with the FATF Recommendation and the mission of the Egmont Group.

IV. Participation in APG Activities

Due to the COVID-19 outbreak, the 2020 APG Annual Meeting in July was canceled, and other APG meetings, including Governance Committee (GC), Mutual Evaluation Committee (MEC), Operations Committee and Donors and Providers Group, were switched to online meeting. The MEC meeting approved follow-up reports of Palau, Samoa, Solomon Islands, Bangladesh, Sri Lanka, Cook Islands, Fiji and Vanuatu. The GC meeting discussed and approved APG Priorities in 2020 to 2022, including strengthen technical assistance and training, build up public-private partnership platform, and strengthen analysis of typologies and the supporting of APG Secretariat. Moreover, the FATF officially approved the revised Recommendation 1 and 2 and their interpretive notes related to weapon proliferation financing. These recommendations require countries and private sectors to comprehensively identify, assess, manage, and mitigate risks related to proliferation financing and evasion of targeted financial sections, as well as to strengthen the coordination, cooperation, and information sharing among the competent authorities within each country. Since the above-mentioned revised Recommendation 1 and 2 will be adopted in APG fourth round mutual evaluation, relevant authorities, associations, FIs and DNFBPs in Taiwan should start to evaluate risks and review policies and measures regarding weapon proliferation financing.

Part III

Significant Case Studies

One. “Chuang” Group’s Online Gambling and Money Laundering Scheme

Two. Fraud and Money Laundering Scheme

Three. Virtual Asset Arbitrage Platform Fraud and Money Laundering Scheme

Four. "Wang" Group's Online Gambling and Money Laundering Scheme

Five. Fraud, Ponzi Scheme and Money Laundering

Six. Violation of Counter-Terrorism Financing Act

One. "Chuang" Group's Online Gambling and Money Laundering Scheme

I. Case summary

(I) Source of intelligence

Following an analysis of financial intelligence in August 2020, AMLD found that: "Company A" and its related company "B" and "C" are believed to be an illegal group of online gambling. The bank accounts controlled by the Group had frequent cash deposits with amounts slightly below the NTD 500,000 reporting requirement. Oversea shell companies, offshore bank accounts and underground banking system were used by the group to launder the illicit proceeds from online gambling platforms. And the funds were then used for real estate investment and company mergers. Thus, the AMLD produced an analysis report and disseminated it to law enforcement agencies.

(II) Suspect

Chuang: president of "Company A"; Lee: vice president of "Company A"; Hong: president of "Company B"; Wen: president of "Company C".

(III) Involvement

Since 2014, Chuang and his accomplices used "Company A" and more than 10 related companies to operate online gambling business with several platforms, and they recruited platform managers from China and South East Asia countries. The managers were responsible for attracting online gamblers. Chuang's Group, on the other hand, were responsible for providing servers, designing and maintaining online gambling games, and bet/ cash exchanges and transfers. Service payments and commission were paid by platform managers to Chuang's Group monthly. "Company C" of Chuang's Group was specifically responsible for financial management of the group and transferred illegal proceeds from overseas to Taiwan, and

"Company A" used the funds on legal investment to make illicit money to have clean appearance. Money laundering techniques used by Chuang's Group were as below:

1. Chuang's Group established several offshore companies under the names of owners of "Company A" and related companies. Lots of bank accounts located in foreign jurisdictions were used by "Company A", and transferred illegal proceeds, in the name of "information service", from overseas to Taiwan and used for real estate investment and company mergers.
2. When Chuang or the relevant companies had fund needs, Hong, the president of "Company B", and Wen, the president of "Company C", would ask their employees to exchange illicit proceeds from RMB to NTD through underground banking systems. Employees from "Company A" then made cash deposits to bank accounts of Chuang or the relevant companies for personal spending.
3. At the time when Chuang and his accomplices were fleeing from the investigation, they sold land properties, buildings and cars, which were purchased with illicit proceeds, in prices much lower than market prices, in order to disguise the origin of funds.

"Company A" had made an illegal profit of NTD 59,493,551,920 by operating online gambling platforms. The law enforcement agency was able to seize NTD 750,078,292 of cash and properties owned by Chuang and associates, and was success to recover assets worth NTD 1,004,600,000.

II. Signs of suspicious money laundering

Customers who make frequent transfers of funds between different accounts above a certain amount; customers who make frequent transactions with different offshore bank accounts for a certain amount and above; customers who make frequent cash deposits or withdrawals with amounts slightly below the reporting requirement.

III. Indictment

On March, 2021, Taichung District Prosecutors Office prosecuted Chuang and associates for violations against gambling under the criminal code, violations against Organized Crime Prevention Act and Money Laundering Control Act.

IV. Experience reference

(I) A number of employees from Chuang's Group were responsible for operating all the bank accounts under companies of Chuang's Group, and they frequent make cash deposits or withdrawals with amounts slightly below the reporting requirement. This implied criminals' intention of avoiding being reported from banks. Moreover, there was no outward transfer in any of the account controlled by the group besides salary, utility bill, labor and health insurance the suspects claimed the funds was used for. The transaction patterns were very different from regular companies.

(II) Chuang's Group created many accounts at offshore banking unit (OBU) located in Samoa and British Virgin Islands, in order to hide and disguise origin of funds and fund flows through those bank accounts. FIs shall gain insight into customers' business operations and conduct due diligence assessments when detecting unusual transactions and suspicious funds, especially for those transactions include multiple OBU accounts, and have suspicious transaction reports filed to AMLD timely. The awareness from FIs would help the law enforcement authorities to investigate criminal activities, follow the fund flows and conduct asset recovery of criminal proceeds more effectively.

Two. Fraud and Money Laundering Scheme

I. Case summary

(I) Source of intelligence

AMLD has received a STR indicated that a Taiwan national, Huang, the president of "Company D", frequently used his bank accounts and other relevant accounts to make cash withdrawals or transfer funds to another parties, and the transactions often happened right after receiving large amount of proceeds in cash or foreign currencies. The source and application of funds were unknown.

(II) Suspect

Huang, Su and Hsieh.

(III) Involvement

Huang pretended to be a core family member of "Group B" and also the chief attorney of a law firm, and claimed to X who owns a company that he was able to offer X a VVIP service in the bank of "Group B" with higher deposit rate and better exchange rate. Moreover, Huang told X that he can help X with her dispute at the court if she paid him a large amount of money. Therefore, X was taken in and paid a total amount of NTD 50,000,000 and 228,000,000 Japanese yen, which were later transferred to bank accounts controlled by Huang. Huang created 16 bank accounts and 4 safe deposit boxes under the name of himself, Su and Hsieh to disguise the origin and application of funds.

After Huang told X that he can offer a VVIP service in the bank of "Group B" with higher deposit rate and better exchange rate, Huang and his accomplices accompanied X and assisted her to carry Japanese yen from Japan to Taiwan for several times. Huang declared 228,000,000 Japanese yen in cash, which was withdrew from a bank located in Japan, to Taiwan Customs Administration in the names of "Payment fee for legal services", "Cash bail" and "Funds for company establishment". Huang then instructed

Su to deposit the funds into the above-mentioned accounts and safe deposit boxes.

Huang claimed that he can help X with her dispute at the court once NTD 30,000,000 legal fee was paid. X then transferred NTD 30,000,000 from her company’s bank account to Huang’s legal firm’s bank account on 8 April 2020. On the same day, Huang instructed Su to withdraw NTD 10,600,000 in cash from the bank account and the money was handed to Huang to purchase properties.

Cash in NTD and Japanese yen was found and seized by MJIB during the search at Huang's residence; and 3 properties purchased by illicit funds were seized. Furthermore, to prevent illegal proceeds in the bank being transferred, emergency seizure was activated and the related bank accounts were frozen. A sum of amount NTD 101,985,366 of illegal proceeds was seized by MJIB.

II. Signs of suspicious money laundering

Customers who make significant amounts of cash deposits and inward remittances immediately after the accounts were created, and transfer significant funds to other bank accounts very quickly; customers who make frequent transactions with different offshore bank accounts for a certain amount and above; customers who use safe deposit boxes frequently with unusual patterns.

III. Indictment

In August 2020, Taiwan Taipei District Prosecutors Office prosecuted Huang and Su for fraud under the criminal code and for violations of Money Laundering Control Act, The Company Act and Business Entity Accounting Act.

IV. Experience reference

(I) Huang often instructed Su to make cash deposits, with NTD 5,000,000 and NTD 10,000,000 each transaction, into bank accounts owned by Su and others. Su then immediately deposited cash (that he withdrew from his and his associates' bank accounts) or transferred the funds to mule accounts controlled by Huang. The unusually intensive transactions among different accounts were intended to disguise the source of funds, which could be considered as red flags of money laundering.

(II) During 2019, Huang asked Su and Hsieh to open 16 bank accounts with different holders' name, those accounts were deposited with large amounts of cash (in NTD and Japanese yen) and received significant funds (in USD and Hong Kong dollar) from X's foreign bank accounts immediately after the accounts were created. The transactions were related to money laundering red flags such as frequent inward remittances and cash deposits immediately after the accounts opened, and quickly transferred to other bank accounts; customers who frequent received funds from different offshore bank accounts, and often followed with immediate cash withdrawals for a certain amount and above.

Three. Virtual Asset Arbitrage Platform Fraud and Money Laundering Scheme

I. Case summary

(I) Source of intelligence

In March 2019, MJIB field office found out that Tong and his associates were operating online virtual assets trading platforms, where the suspects attracted investors to invest on virtual assets. Tong and his associates accessed to victims' accounts in virtual asset exchanges and transferred virtual assets to accounts under Tong's control. The suspects used lots of cold and online wallets to transfer cryptocurrencies, and they also used different virtual asset exchanges to convert the crypto money to different types of cryptocurrencies. Moreover, Tong and his accomplices often withdrew money in cash to make the funds untraceable, which largely increased the difficulties for law enforcement authorities.

(II) Suspect

Tong and Tsai.

(III) Involvement

Tong was the director of "Platform C", an online virtual assets trading platform. Tsai was the computer engineer of "Platform C". In 2018, Tong and Tsai claimed that they had created a fully automated crypto arbitrage system in "Platform C", which showed the price gaps and trading information for different exchanges and different types of cryptocurrencies, and it allowed investors to easily take advantage of arbitrage trading. Therefore, many investors started to believe that "Platform C" can really make profits for themselves, and they voluntarily transferred Ether to those wallets controlled by suspects. A total of 284.77 ethers was transferred from victims to Tong in this stage of criminal activity. Next, Tong and

Tsai used the dis-functional arbitrage system, and false investing data and transaction records in “Platform C” to attract investors. More than 200 people were deceived and another 12,565.92 ethers were transferred to Tong and his associates afterward. The illicit proceeds of “Platform C” was approximately NTD 145,758,037. MJIB was able to seize 900 ethers (approximately NTD 25,072,347), properties, vehicles and money remained in bank accounts, with a total value of NTD 40,977,445.

II. Signs of suspicious money laundering

Multiple and frequent cash deposits and withdrawals from ATMs, and each inward transaction usually followed with a similar amount of cash deposit.

III. Indictment

In October 2021, Taiwan New Taipei District Prosecutors Office prosecuted Tong and Tsai for fraud and offenses against the computer security under the criminal code and for violations of Money Laundering Control Act.

IV. Experience reference

(I) Tong, Tsai and their associates claimed the success of developing virtual asset arbitrage system in “Platform C”, and they also claimed that the system was able to automated detect price gaps and trading information in different exchanges and different types of cryptocurrencies to benefit investors. In recent years, arbitrage platforms have become a commonly seen criminal activity links to virtual assets. Criminals promote automated arbitrage system and profit guarantee to attract investors, but it often ends with closure of online platform, lost contact with owners or operators of platform, and huge financial losses for investors and victims.

(II) In this case, the offenders used traditional financial institutions, and also local/overseas exchanges or virtual asset service providers (VASPs) in turns or in combinations, in order to process the layering technique of money laundering. The criminals frequently transferred virtual assets among different exchanges and wallets, which added extra hurdles for law enforcement agencies to trace the original source of funds and follow the fund flows. Financial institutions and VASPs should enhance their ability to detect suspicious transactions which indicate their customers' involvement of purchasing different types of virtual assets and transferring assets very frequently and rapidly without reasonable explanations. In such circumstances, reporting entities should consider to file STRs to FIU when noticing the above-mentioned red flags of money laundering.

Four. "Wang" Group's Online Gambling and Money Laundering Scheme

I. Case summary

(I) Source of intelligence

Following an analysis of financial intelligence in December 2019, AMLD found that Wang, the president of “Company E”, frequently withdrew cash from his bank accounts, or transferred funds to other bank accounts under his control and made cash withdrawals. Wang received funds from specific bank accounts without clear and reasonable explanation for fund sources, which made his financial transactions suspicious. AMLD then conducted analysis reports and disseminated the intelligence to law enforcement agency.

(II) Suspect

Wang and Chu.

(III) Involvement

Since June 2017, Wang and Chu had been operating online gambling websites, and recruiting gamblers from China. In order to disguise illegal proceeds of online gambling websites, Wang purchased and collected lots of mule accounts in China, and categorized those accounts into different layers for online top up and betting payment. Wang and his associates instructed their employees to use USBKey and internet banking to transfer funds. Take the incoming funds for example, the first-layer accounts functioned as receiving gamblers’ money directly, and when those accounts reached balance of NTD 20,000, those money would be transferred to the next layer accounts, which were called “collecting accounts”. At the time when balance of “collecting accounts” were more than NTD 10,000, those money would again be transferred to “in-middle layer 1”, “in-middle layer 2”, and “in-middle layer 3” accounts. Once “in-middle layer 3” accounts reached balance of NTD 30,000, the funds would then be transferred to the ultimate accounts. On the other hand, the fund flows of outward transaction were contrary to inward transactions, moreover, the fund would be transferred to gamblers' designated accounts to avoid being detected from financial institutions and law enforcement agencies.

Wang instructed Chu to create a "fund department" in the group to manage "fourth-party payment", which linked online gambling websites and third-party payment companies. When a gambler asked for topping up its member account through website, the "fund department" would choose a suitable third-party payment company to receive money from the gambler. Once the third-party payment company received the money from gambler, it then informed the "fund department" and balance of the gambler's member account would be updated. Wang added service fee for each payment of gamblers, which was a major profit for Wang and his associates. All of the service fee was transferred to Chinese mule accounts designated by Wang, and remitted to Taiwan through underground banking system.

Wang used "fourth-party payment" and mule accounts to layer and transfer the illegal proceed. From June 2017 to January 2020, the total earnings of "Company E" was NTD 5,356,657,060.

II. Signs of suspicious money laundering

The aggregation of cash deposited into a customer's account, or the aggregation of cash withdrawn from a customer's account, which reaches a specific amount within a certain period. Accounts with significant amount of inward funds and transfer to other accounts rapidly. Customers often transfer money among specific accounts with significant amount of funds.

III. Indictment

In July 2020, Taiwan Qiaotou District Prosecutors Office prosecuted

Wang and his associates for violations against gambling under the criminal code and Money Laundering Control Act.

IV. Experience reference

(I) Financial intelligence analysis of Wang and his wife indicated that significant amount of illegal proceed was transferred among few accounts controlled by Wang, which was a sign of money laundering. A financial institution found the suspicious transactions and filed several reports, which helped the law enforcement agency to understand the fund flow and seize the illicit proceed.

(II) Third-party payment has become a new trend of money laundering technique. Online gambling websites are able to receive and pay gambling related payments through third-party payment companies by using ATMs in convenient stores, credit cards and virtual accounts. Tracing anonymous, fake accounts and fund flows in third-party payment can be very challenging. Mule accounts in this case frequently received small amount of fund and then made cash withdrawals via ATMs, which was a sign of money laundering and an abnormal pattern for business accounts.

Five. Fraud, Ponzi Scheme and Money Laundering

I. Case summary

(I) Source of intelligence

MJIB have received an intelligence indicated that Shen, a Taiwan national, and his associate Lee, a China national, obtained illegal money from Chen and many others by attracting them to invest in oil futures. Shen and Lee also laundered money from Taiwan to China via jewelry business and underground banking system, in order to disguise the financial flows and the origins of illicit money.

(II) Suspect

Shen, Jiang, Yeh, Wang, Fang, Gu, Lian, Lin and Lee.

(Ⅲ) Involvement

Shen met Lee, a Chinese citizen, on internet when doing business in China in 2018. Since August 2019, Shen had been providing mule accounts under the names of Fang and others in Taiwan to Lee for illegal uses such as transferring proceeds of fraud investment. Shen was responsible for withdrawing money from accounts located in Taiwan and conducting fraud investment of Hong Kong oil futures. The investors transferred money to mule accounts of Fang, Gu, Lian and Lin, which were controlled by Shen. Shen then asked Fang, Gu, Lian and Lin to withdraw money in cash from those accounts, and hand over cash to Shen or his associate, Jiang. Fang, Gu, Lian and Lin were paid 1% to 3% of amount they processed as service fee.

Jiang had been operating underground banking system between Taiwan and China for many years. He linked Chinese underground banking operators, Taiwanese jewelry shop owners and a Taiwanese travel agency, to transfer illegal proceed from Taiwan to China, specifically to Chinese accounts designated by Lee. Shen and his associates had raised a total of NTD 15,111,636 from investors through illegal means, and a total of NTD 62,632,189 was transferred via underground banking system.

II. Signs of suspicious money laundering

Bank accounts receive significant amount of money intensively and transfer the fund frequently that are inconsistent to the account holders' identity and income. Exchange currencies illegally through DNFBPs (jewelry businesses) with unclear sources and final destinations of funds.

III. Indictment

In August 2020, Taiwan Qiaotou District Prosecutors Office prosecuted Shen and his associates for fraud under the criminal code and for violations against Organized Crime Prevention Act and Money Laundering Control Act.

IV. Experience reference

(I) When receiving unknown information of investment on social media or internet websites, people should be awarded that it may involve illegal investment activities. In this case, MJIB found offenders controlled more than 10 mule accounts and large-scale organized crimes located in both Taiwan and China. The criminal group transferred illicit proceed via jewelry shops and travel agencies in Taiwan and underground banking operators in China, and send money from Taiwan to China.

(II) Fraud techniques used by criminals are continually developing. In this case, criminals attracted investors by linking the investing project with overseas financial products and making investors to believe that the investment could really make profits for themselves. While more victims were involved and the amount of money received from investors got higher, the offenders suddenly closed the relevant accounts. At the time the victims realized they were scammed and reported it to law enforcement agency, most illegal proceed had been transferred to overseas through underground banking system.

Six. Violation of Counter-Terrorism Financing Act

I. Case summary

(I) Source of intelligence

Intelligence from foreign counterparts in 2018 shows that an Panama-flagged oil tanker “Vessel A”, which departed from Kaohsiung Port (Taiwan) on 27 April 2018, sold oil to a North Korean vessel and another vessel registries in unknown country on 18 May 2018 and 2 June 2018.

(II) Suspect

Huang, Wen, Wu and Liu.

(III) Involvement

Because of violating the UN Security Council Resolution 1718, Huang, Wen, Wu and Liu was included in “Sanctions List of UNSCR 1718”. Huang and his associates ignored the regulation of Counter-Terrorism Financing Act and UN Security Council Resolution, and schemed to transport oil from “Vessel A” to North Korean vessels with the intention of increasing their profits. Wen purchased oil from “Company S” and provided forged documents, which involved falsely described export destination as Hong Kong. Those oil which should be landed in Hong Kong was in fact transported to “Vessel A” (owned by Huang) on the high seas and then sold to a North Korean vessel “B”. Huang and Wen made a profit of NTD 26,000,000 from selling oil to the North Korean vessel “B”.

Wen and his associates conducted a similar scheme again few days later. Wen purchased oil from “Company S” and declared it to be exported to Hong Kong, but the oil was transported to “Vessel A” and sold to a North Korean vessel “C”. Liu was the broker of the oil transportation trading. Huang and Wen made another profit of NTD 30,340,000 from selling oil to the North Korean vessel “C”.

II. Signs of suspicious money laundering

(I) Media coverage on account holders' activities.

(II) The goods were shipped to or from countries or regions with high ML/TF risks.

(III) Customers were suspected of involving in ML/TF activities, including importing and exporting embargoed or restricted products.

III. Indictment

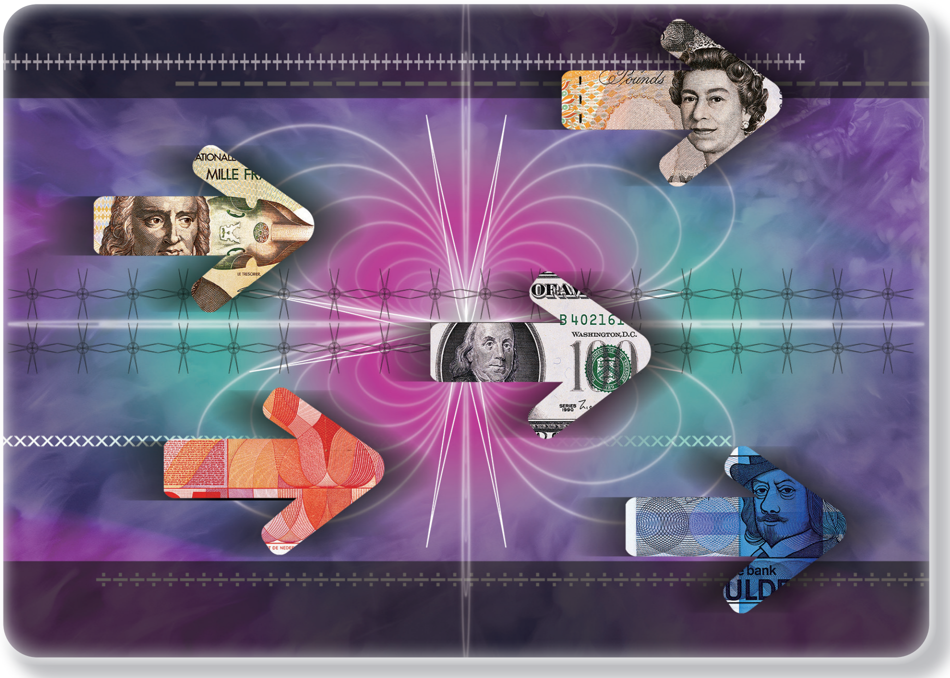
In October 2020, Taiwan Kaohsiung District Prosecutors Office prosecuted Huang and his associates for providing forged documents under the criminal code and for violations against Counter-Terrorism Financing Act.

IV. Experience reference

Huang created 3 offshore companies registries in Hong Kong, and opened several OBU accounts in different financial institutions. When filing STRs, FIs provided complete registration certificates, shareholders and directors' lists, which assists in clarifying the existence of offshore companies and the movement of funds.

Part IV

Strategic Analysis Report



AML/CFT Strategic Analysis Report on Dummy E-Banking Accounts

AML/CFT Strategic Analysis Report on Dummy E-Banking Accounts

I. Introduction

i. Motivation and Purpose

The Anti-Money Laundering Division (AMLD), Ministry of Justice Investigation Bureau (MJIB), Republic of China (Taiwan), as well as the financial intelligence unit (FIU) of Taiwan, has been receiving suspicious transaction reports (STRs) with the same or very similar red flags from several financial institutes (FIs), especially from the banks, since November of 2019. According to the above-mentioned STRs, many banks found their customers set up the same or very similar usernames with the same pre-designated receiving accounts after checking their cellphones when opening e-banking accounts. Moreover, small amount on-line/ATM transactions were being found soon after the electronic banking (e-banking) function activated, also reported in the STRs. To perform the FIU's function of value-added analysis, AMLD checked the money flows, criminal records, and any other information thus finding strong ties among some reported dummy accounts, beneficiaries and criminal cases being detected by the law enforcements (LEAs) during the same period such as illegal on-line gambling, cyber-fraud and underground banking. In the beginning of the investigation, AMLD conducted initial random inspections on the STRs and assigned several MJIB field divisions to interview some owners of the bank accounts. Most of the interviewees confessed that via social media, such as Facebook, and/or communication apps, e.g., Line, WeChat, etc., they sold the said bank accounts to some unknown criminal group or gangs instructing them to apply for activating the e-banking accounts. The bank accounts mentioned in the STRs are mostly dummy accounts with e-banking function facilitating money laundering (ML) and terrorist financing (TF), concluded by AMLD after the initial inquiry.

AMLD found the money flow breakpoints of the “back end accounts” were usually created by withdrawing cash from the automated teller machines (ATMs) while money flows complicatedly relayed in the “front end accounts” and the “relay accounts” docking to e-banking and third-party payment providers by using mobile phones or any other digital transaction vehicles with floating IPs. The above trend reveals that the criminal groups seems already adapted to the regulations on the daily ATM cash withdrawing limits. AMLD calls for the banking sectors to review or reconsider adjusting the relevant ATM regulations in accordance with the risk-based approach (RBA) and financial inclusion.

E-banking account is one of the money/value transfer vehicles with the character of non face-to-face transactions and all the account holders have to do is key in the usernames and passwords and press “Enter”. The acquisition cost to obtain e-banking dummy accounts is lower and the transaction speed is much faster without boundaries and jurisdictions, comparing with traditional bank accounts. Therefore, the harmfulness of e-banking dummy accounts is more significant than that of traditional dummy accounts. AMLD recognized the above-mentioned threats and vulnerabilities of e-banking accounts and the problem aroused from the complicated money flows connecting directly to the third-payment providers, having similar threats and vulnerabilities, resulting in the “multiplier effect” of ML/FT. The existing regimes of anti-money laundering (AML) and combating the financing of terrorism (CFT) seems insufficient to effectively mitigate or address the risk of ML/TF caused by the said threat multipliers. AMLD encourages the competent authorities to review and adjust the existing AML/CFT regimes in accordance with RBA.

In view of the former practices of AML/CFT, focusing on combating or identifying accomplished or ongoing serious offences instead of crime prevention, the AMLD played the role of national FIU in preventing crimes and assisting financial supervisory authorities concerned, and timely disseminated the above-mentioned ML/FT trend analysis to the Financial Supervisory Commission (FSC) for reference on December 11, 2019. The

Banking Bureau of FSC immediately forwarded the information disseminated by the AMLD to the Bankers Association and the National Federation of Credit Co-operatives to remind their members to pay more attention to the new ML/FT trends and red flags. The FIs could not only timely report STRs to the AMLD but also adopt appropriate AML/CFT countermeasures that commensurate with the risk identified. As per April 30 of 2020, the AMLD had received a total of 338 STRs from at least 15 FIs with the same or similar red flags due to the general warning to FIs. The number of the owners of bank accounts in the STRs is 1,435, including 1,429 natural persons and 6 legal entities and the total number of the dummy account is up to 1,500. There seems to be a lack of systematic reviews and empirical studies on this issue by the LEAs or academic institutes. From the strategic height and the point of view of the national FIU, the AMLD not only tried her best to conduct value-added analysis on the above-mentioned 238 STRs, but also took the 1,435 account owners and 1,500 dummy e-banking accounts in the STRs as research population and conducted big data analytics to identify the red flags and build typologies. Consequently, the AMLD could successfully disseminate the analytic results to the LEAs for reference and timely give feedback to the FIs and competent authorities for refining existing AML/CFT regimes and policies.

ii. Population, Method and Research Limit

As mentioned above, the AMLD took the 1,435 account owners and 1,500 dummy e-banking accounts in the 238 STRs as the research population. The method is to analyze the background information of the account owners by comparing databases of the AMLD, build the typologies of the money flows, and identify the predicate offenses in the criminal cases detected by the LEAs or disseminated by the AMLD. The AMLD also tries to find the threats and vulnerabilities of the new means of payment connecting directly to the dummy e-banking accounts and identify the corresponding risks based on RBA in order that the readers of this report, e.g., LEAs, FIs, bankers associations, financial supervisory authorities and policy making agencies, could take the best advantage of limited AML/CFT resources. Therefore, the LEAs could put more effort in the high risk offenses and the FIs could focus more on the high risk customers and money flows to enforce the countermeasures to prevent or mitigate ML/FT commensurate with risks identified and the competent authorities could also take actions by making suitable policies or regulations.

The research population in this report, as mentioned above, includes those dummy e-banking accounts with specific characteristics and/or red flags. Given that the proceeds of crime (POC) are value transferable and launderable by using any kind of dummy bank account including but not limited to e-banking accounts, this report is going to review the types of ML/TF cases disseminated by the AMLD in 2019 to let the users of this report get a general understanding of the risk profiles before undertaking the quantitative analysis of the research population. The research of this report is not only subject to the collection of research population and the limit of sampling but also subject to other impact factors beyond the AMLD's control such as the time constraint for the LEAs, the prosecutor offices and the courts to go through all cases disseminated by the AMLD. The accuracy of the statistics data of this report is consequently influenced to some extent but the AMLD does believe this report is of reference value for the readers to quickly build a profile of the trend of dummy e-banking accounts and their weaknesses as well as vulnerabilities. The AMLD takes this report as an official pioneer research on dummy e-banking accounts and welcomes any follow-up research from the sectors of LEAs, FIs and academia to refine the outcomes and address the deficiencies.

Besides, this report is also subject to the types of predicate offence such as corruption and corporate fraud that cannot be fully explained by this report. Because the dummy bank accounts used as criminal tools in these criminal cases are usually obtained from the criminals' family members and /or close associates instead of massively buying from the lower middle class.

II. Types of ML/TF Cases Disseminated by AMLD in 2019

Table 1. Types of ML/TF Cases Disseminated by AMLD in 2019

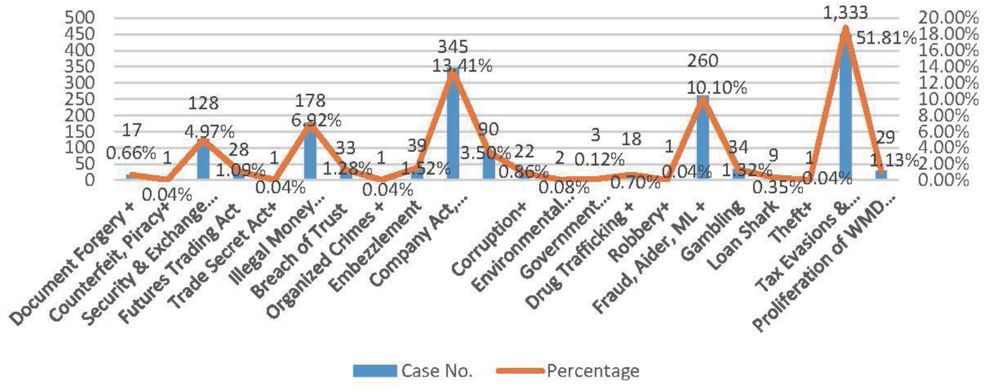
Predicate Offence	Case No.	Percentage
Document Forgery +	17	0.66%
Counterfeit, Piracy+	1	0.04%
Security & Exchange Act (Insider Dealing, Market Manipulation, Corporate Fraud, Securities Fraud+）	128	4.97%
Futures Trading Act	28	1.09%
Trade Secret Act+	1	0.04%
Illegal Money Gathering	178	6.92%
Breach of Trust	33	1.28%
Organized Crimes +	1	0.04%
Embezzlement	39	1.52%
Company Act, Business Entity Accounting Act	345	13.41%
Underground Banking/Hawala	90	3.50%
Corruption+	22	0.86%
Environmental Crimes +	2	0.08%
Government Procurement Act	3	0.12%
Drug Trafficking +	18	0.70%
Robbery+	1	0.04%
Fraud, Aider, ML +	260	10.10%
Gambling	34	1.32%
Loan Shark	9	0.35%
Theft+	1	0.04%
Tax Evasions & Administrative Sanctions	1,333	51.81%
Proliferation of WMD & Financing	29	1.13%
STRs Disseminated by AMLD in 2019	2,573	100.00%
Total Numbers of STRs Received by AMLD in 2019	26,481	

In 2019, the AMLD received a total of 26,481 STRs from the FIs and disseminated 2,573 cases to the competent authorities for reference after value-added analysis. The largest case number, accounting for 51.81%, is 1,333 of tax evasions and administrative sanctions. Most of the cases were forwarded to National Taxation Bureaus for overdue tax recovery while other small parts of the cases were forwarded to FSC and Central Bank for administrative sanctions. To evade family members' estate/gift tax, personal income tax and profit-seeking enterprise income tax were the most reported probable transaction reasons in the STRs with red flags of using cash transaction to set money flow breakpoints, using personal bank accounts to run business of profit-seeking enterprise, and using foreign SPVs' OBU accounts to receive payments from foreign clients. Liang, Ching-Tao(梁建道), section chief of National Taxation Bureau of Taipei, also an attorney and a theorist, pointed out in his thesis that some typologies of tax crime ML in the circumstances of e-commerce and digital economy nowadays can usually be identified, such as to build websites beyond jurisdiction, to use dummy accounts to access service, and to use foreigners' dummy accounts to disguise or conceal revenue. And he consequently called for actions to refine counter measures against foreigners' dummy accounts and to enhance customer due diligence (CDD) on them. He also reiterated to reinforce cross-agency communication and information sharing and encouraged tax authorities concerned to cooperate with the AMLD, prosecutors' offices, Investment Commission and FSC to build a regular platform to share best practices to address the problems mentioned above.

The types of ML/FT cases disseminated by the AMLD and the common criminal cases using dummy bank accounts detected by the LEAs are in positive correlation. The case numbers of the most common seen types in descending order are respectively as follows: 345 cases (13.41%) of violating Company Act and Business Entity Accounting Act; 260 cases (10.10%) of fraud (including aider and ML); 178 cases (6.92%) of illegal money gathering (Ponzi Scheme); 128 cases (4.97%) of violating Security & Exchange Act (including insider dealing, market manipulation, corporate fraud, securities fraud, etc.); 90 cases (3.50%) of underground banking/Hawala; 39 cases (1.52%) of embezzlement; 34 cases (1.32%) of gambling; 33 cases (1.28%) of breach of trust; 29 cases (1.13%) of proliferation of WMD & financing; 28 cases (1.09%) of violating Futures Trading Act; 22 cases (0.86%) of corruption; and 18 cases (0.70%) of drug trafficking (see Table 1).

If we focus on the distribution of types, we can find tax evasion, violating Company Act and Business Entity Accounting Act, fraud (including aider and ML), illegal money gathering (Ponzi Scheme), and violating Security & Exchange Act (including insider dealing, market manipulation, corporate fraud, securities fraud, etc.) are the top 5 types. Underground banking/ Hawala, embezzlement, gambling, breach of trust are also very significant afterwards (see Figure A).

Figure A: Distribution Graph of Types of ML/TF Cases Disseminated by AMLD in 2019



III. Trend Analysis on Owners of Dummy E-Banking Accounts

i. Distribution of Research Population by Nature Person and Legal Entity

Table 2: Statistics of Nature Persons and Legal Entities

Categories of Owner	No. of Bank Account	Percentage
1,429Nature Persons	1,494	99.60%
Citizen	1,494	99.60%
Foreigner	0	0%
6 Legal Entities	6	0.40%
Local Company	6	0.40%
Foreign Company	0	0%
1,435 Owners	1,500	100.00%

The research population in the 238 STRs includes 1,429 natural person owners holding 1,494 (99.60%) bank accounts and 6 (0.4%) legal entities holding 6 bank accounts (see Table 2). No foreign company owners were found in the STRs. This may be due to the language and geographical barriers of criminal gangs collecting/buying these dummy bank accounts, the parameter setting of risk assessment, the characteristics of predicate offenses and/or the limit of population sampling.

Even though only 6 local companies and the owners identified in this report were underrepresented, the AMLD still noticed that the owners had similar criminal records (eg., drug and/or fraud), the companies had just been founded for no more than 6 months, running software service and/or third-party payment with very small registered capitals not correspond to the huge transactions, and the owners also opened dummy e-banking accounts under their names. These red flags or trends do deserve our attention.

ii. Distribution of Nature Persons by Age Group

Table 3: Statistics of Age Group

Age Group (in Years)	No. of Nature Person	Percentage
>20	19	1.33%
21~30	892	62.42%
31~40	363	25.40%
41~50	98	6.86%
51~60	39	2.73%
61~70	15	1.05%
>71	3	0.21%
Total	1,429	100.00%

There are 19 (1.33%) natural persons aged 20 years and under; 892 (62.42) aged 21 to 31; 363 (62.42%) aged 31 to 40; 98 (6.86%) aged 41 to 50; 39 (2.73%) aged 51 to 60; 15 (1.05%) aged 61 to 70; and only 3 (0.21%) aged 71 and over (see Table 3). The 21 to 31 is the largest group and the second one is 31 to 40 (see Figure B).

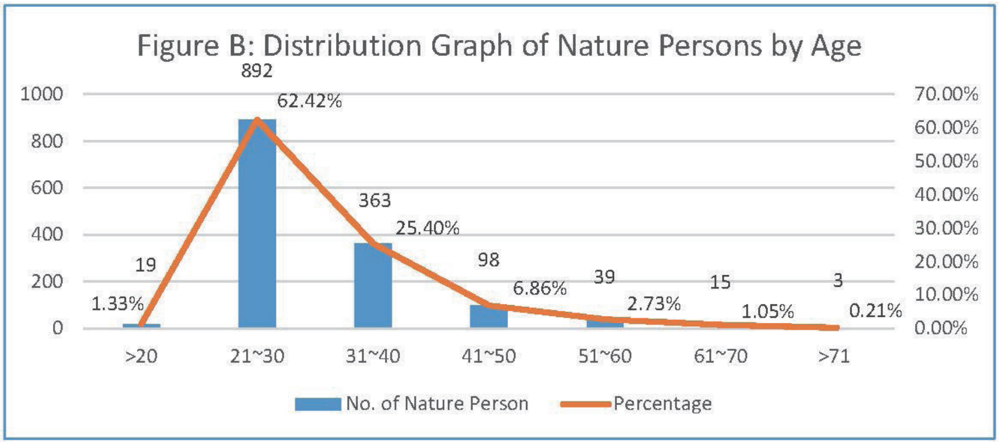


Figure B: Distribution Graph of Nature Persons by Age

Focusing on the group aged 21 to 30, most of the group members just graduated from colleges or retired from compulsory military service (see Figure C). No suitable job opportunities, the low-wage condition and even unemployment are the main reasons why those group members sold their bank accounts for making money.

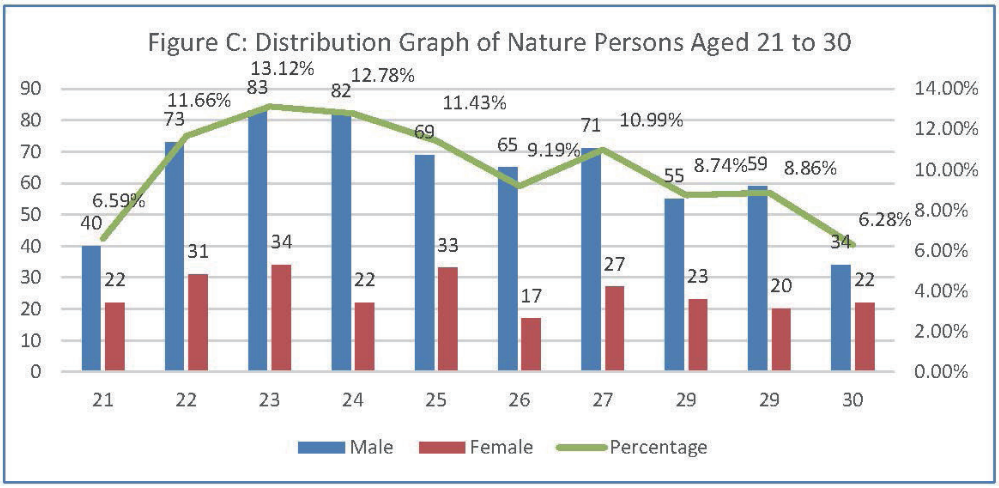


Figure C: Distribution Graph of Nature Persons Aged 21 to 30

iii. Distribution of Nature Persons by Criminal Records

Table 4: Statistics of Criminal Records

Type of Offenses	Offense	No.	Percentage
Violent Crimes	Homicide	11	0.77%
	Against Public Safety	66	4.60%
	Against Freedom	34	2.37%
	Causing Injury	51	3.55%
	Illegal Possession of Guns, Ammunition and Knives	23	1.60%
	Subtotal	185	12.89%
Property Crimes	Loan Shark/Usury	19	1.32%
	Embezzlement	21	1.46%
	Fraud, Aider, ML+	216	15.05%
	Gambling	92	6.41%
	Theft+	63	4.39%
	Robbery+	32	2.23%
	Subtotal	443	30.87%
Drug Crimes	Drug	228	15.89%
Etc.	Sex Offenses	53	3.69%
	Against Intellectual Properties	23	1.60%
	Subtotal	76	5.30%
No Criminal Records		707	49.27%
Remarks	Some of the research population have more than one criminal records. The denominator in percentage terms is 1,435 (1,429 nature persons + 6 owners of the local companies).		

There are 707 (49.27%) natural persons without criminal records. In terms of those having criminal records, 185 (12.89%) have records of violent crimes; 443 (30.87%) have records of property crimes; 228 (15.89%) have records of drug crimes; and 76 (5.30%) have records of sex offenses, against intellectual properties, etc. (see Table 4). The risk of the type of offenses in descending order are respectively property crimes, drug crimes and violent crimes.

Focusing on the specific offenses, 216 (15.05%) have records of fraud (including Aider & ML) while 228 (15.89%) have records of drug crimes, which can be inferred that the 2 offenses have the highest risks, and by the way, 92 (6.41%) with records of gambling still draw our attention (see Figure D).

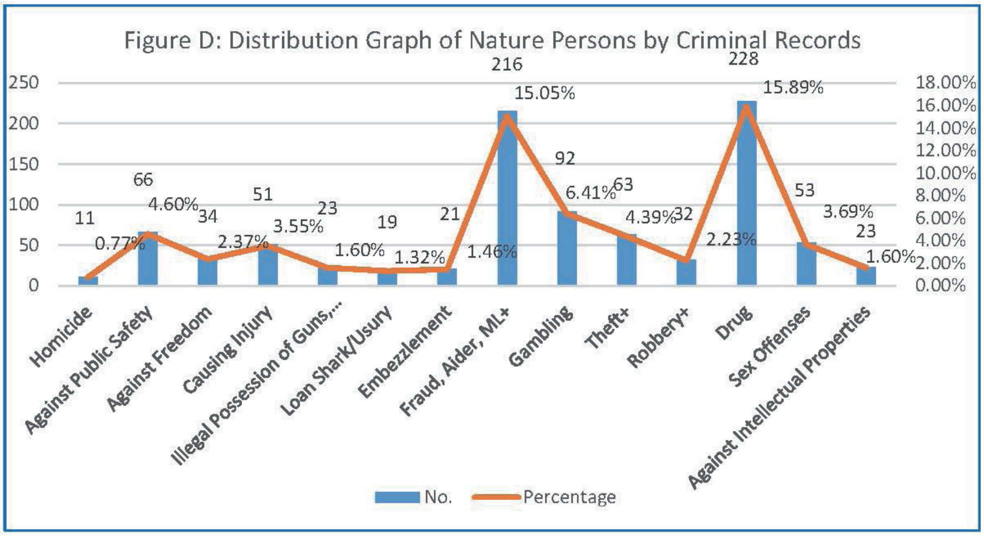


Figure D: Distribution Graph of Nature Persons by Criminal Records

Table 5: Cross Analysis on Criminal Records of Fraud & Drug

Offense	Fraud	Drug	Subtotal	Percentage
Fraud	86	130	216	60.19%
Drug	130	98	228	57.02%

After running cross analysis on the criminal records, a very significant phenomenon can be noticed that the overlapping rate of the natural persons selling the dummy bank accounts having criminal records of both fraud and drug crimes is much more higher than those of any other crimes. 130 (60.19%) of 216 natural persons having criminal record of fraud also have criminal record of drug while 130 (57.02%) of 228 having criminal record of drug also have criminal record of fraud (see Table 5). The actual reason why those natural persons who have criminal records of drug also have the records of fraud cannot be proven directly. It is probably because for those who already have criminal records of drug, to sell their bank accounts to the fraud gangs is the fastest way to gain money for buying drugs. Despite the probable reason mentioned above needs more proof to stand for, the coexisting rate of the criminal records on drug and fraud is approximately 60% (see Table 5). In other words, those natural persons who have criminal records of drug that also have the records of fraud are the group with the highest risk.

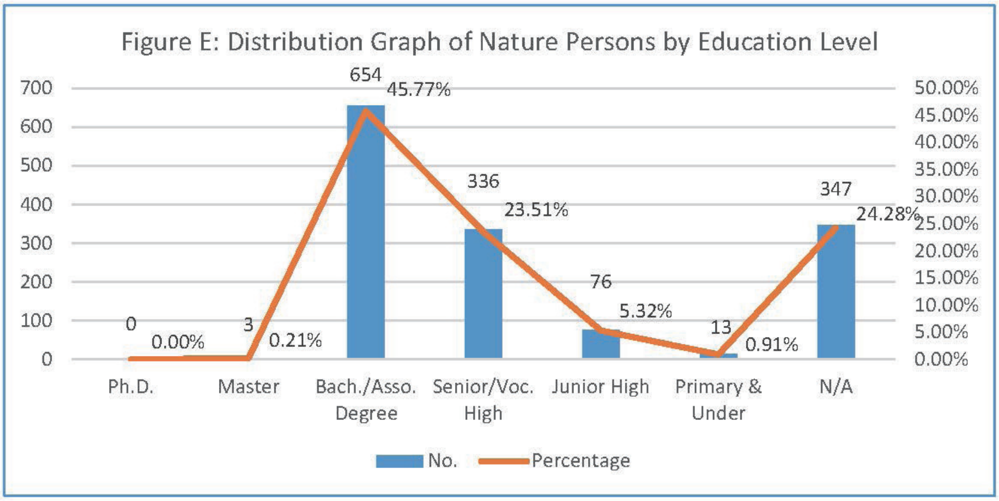
iv. Distribution of Nature Persons by Education Level

Table 6: Statistics of Education Level

Highest Academic Degree	No.	Percentage
Ph.D.	0	0.00%
Master	3	0.21%
Bachelor/Associate Degree	654	45.77%
Senior/Vocational High	336	23.51%
Junior High	76	5.32%
Primary and Under	13	0.91%
N/A	347	24.28%
Total	1,429	100.00%

Among the 1,429 nature persons, there is no one with Ph.D. degree found while there are 3 (0.21%) with master's degree; 654 (45.77) with bachelor/associate degree; 336 (23.51%) graduated from senior high school; 76 (5.32%) graduated from junior high school; 13 (0.91%) graduated from primary school and under; 347 (24.28%) academic information not available (see Table 6).

Theoretically or at least from the common sense point of view, the risk to sell bank accounts for criminal use is inversely related to the education level of the bank account owners. However, the hypothesis seems to be defeated by the conclusion of this study (see Figure E). This phenomenon does not mean the higher educational degrees the bank account owners possess, the higher the risk to sell their bank accounts for criminal use. This illusion is probably because the education curve and the age curve have significant conformity (see Figure B & Figure E). And there is consequently no question that we need to enhance the legal education in campus.



v. Distribution of Nature Persons by Occupation

Table 7: Statistics of Occupation

Occupation	No.	Percentage
Unemployed/Contractor	255	17.84%
Clerk	217	15.19%
Salesperson	140	9.80%
Online Business/Streamer	127	8.89%
Manual Laborer	126	8.82%
Operational Level	83	5.81%
Security Guard	72	5.04%
Driver/Logistics Clerk/Deliveryman	66	4.62%
Street Vendor	63	4.41%
Entertainment/Sexual Industry	54	3.78%
Student	52	3.64%
Gas Station Staff	45	3.15%
Owner of Claw Machine	42	2.94%
Administration	23	1.61%
Cook/Chef	18	1.26%
Beautician/Hairdresser	14	0.98%
Solider	12	0.84%
Nanny	7	0.49%
Supervisor/Owner of Business	6	0.42%
Seafarer	5	0.35%
Farmer	2	0.14%
Total	1,429	100.00%

Regarding the statistics of natural persons by occupation, the research team of this report did not have the intention to make a conclusion on the relation between the types of careers and the risk of ML or selling bank accounts for criminal use. To avoid occupational discrimination, this report just make a statistical table without description for reference (see Table 7). Actually, the supply to sell bank accounts comes from the demand of money. Even though this report assumed the statistical data of annual income is more suitable to explain the conclusion than that of the types of careers (see the next paragraph & Table 8), there are still some types of careers drawing our attention such as the 225 (17.84) unemployed/contractors. Those who are unemployed or temporary contractors may be considered the group with very high risk because they are almost paid by cash or even do not need any bank accounts to receive monthly salary, which will arouse some concern during KYC process when opening bank accounts. Besides, online business/streamer, entertainment/sexual industry and owner of claw machines are also very special and eye-catching types of careers found in this report. And lastly, soldiers found in this report are all retired or just retired mandatory soldiers as no voluntarily active soldiers with regular monthly payment were found.

vi. Distribution of Nature Persons by Annual Income

Table 8: Statistics of Annual Income

Income Bracket per Year (NTD)	No.	Percentage
N/A	972	68.02%
>500K	457	31.98%
510K-990K	0	0.00%
>1M	0	0.00%
Total	1,429	100.00%

Among the 1,429 natural person account owners, there are 972 (68.02%) without income information available (including the owners of the 6 companies) while the other 457 (31.98%) are under NTD 500 thousands per year (see Table 8). There are many theorists insisting poverty is not the mother of crime but they still have no objection that there are some correlation between poverty and crime such as relative deprivation and social exclusion, etc. As the statistics shows, most of the nature persons selling their bank accounts for criminal use are those whose annual income is below NTD 500 thousands or income information is not available. They can easily gain many thousands from the criminal gains by selling their bank accounts or even renting them for ML. The higher annual income the bank account owners earn, the lower they will be at risk to sell their bank accounts for criminal use, which can be concluded in this report.

vii. Distribution of Bank Accounts by Opening Region

Table 9: Statistics of Bank Account Opening Region

Region	No.	Percentage	Region	No.	Percentage
Taipei City	78	5.20%	Yunlin County	22	1.47%
New Taipei City	195	13.00%	Chiayi City	7	0.47%
Keelung County	35	2.33%	Chiayi County	11	0.73%
Yilan County	10	0.67%	Tainan City	57	3.80%
Taoyuan County	50	3.33%	Kaohsiung City	326	21.73%
Hsinchu City	18	1.20%	Pintung County	41	2.73%
Hsinchu County	7	0.47%	Hualien County	6	0.40%
Miaoli County	35	2.33%	Taitung County	3	0.20%
Taichung City	418	27.87%	Penghu County	0	0.00%
Changhua County	136	9.07%	Kinmen County	0	0.00%
Nantou County	45	3.00%	Lienjiang County	0	0.00%
Total	1,500		100.00%		

In terms of the 1,500 dummy bank accounts, the bank account numbers in the opening region in descending order are respectively as follows: 418

(27.87%) bank accounts opened in Taichung City; 326 （21.73%）in Kaohsiung City; 195(13.00%) in New Taipei City; 136 (9.07%) in Changhua County; 78 (5.20%) in Taipei City; 57 (3.80%) in Tainan City; 50 (3.33%) in Taoyuan City; 45 (3.00%) in Nantou County; 41 (2.73%) in Pintung County; 35 (2.33%) in Keelung County; 35 (2.33%) in Miaoli County; 22 (1.47%) in Yunlin County; 18 (1.20%) in Hsinchu City; 11 (0.73%) in Chiayi County; 10 (0.67%) in Yilan County; 7 (0.47%) in Hsinchu County; 7 (0.47%) in Chiayi City; 6 (0.40%) in Hualien County; 3 (0.20%) in Taitung County; and 0 (0.00%) found in Penghu County, Kinmen County and Lienjiang County (see Table 9).

The 3 hotspots of opening bank accounts indicates a trend of concentrating distribution among the metropolitans from Northern to Southern Taiwan: the Greater Taipei Area (Taipei City & New Taipei City), Taichung City & Changhua County, and Kaohsiung City (see Figure F). The urbanization degree and the risk to sell bank accounts for criminal use have a positive correlation. It is probably because the predicate offences of using dummy E-banking bank accounts are more related to the metropolitan crimes. Therefore, the farther distance to the metropolitan, the fewer case number can be found. Moreover, no cases were found in the areas of outlying islands.

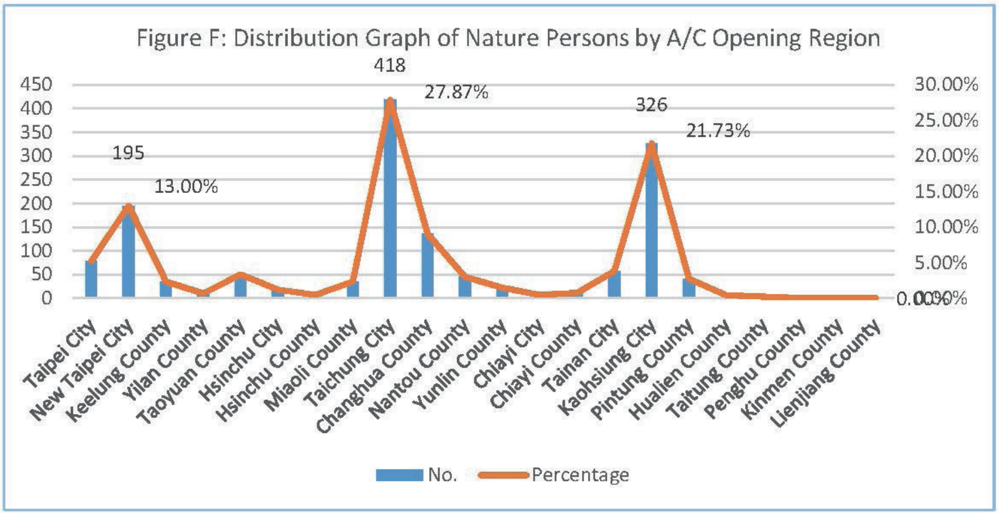


Figure F: Distribution Graph of Nature Persons by A/C Opening Region

IV. Trend Analysis on Clients of Bank Accounts

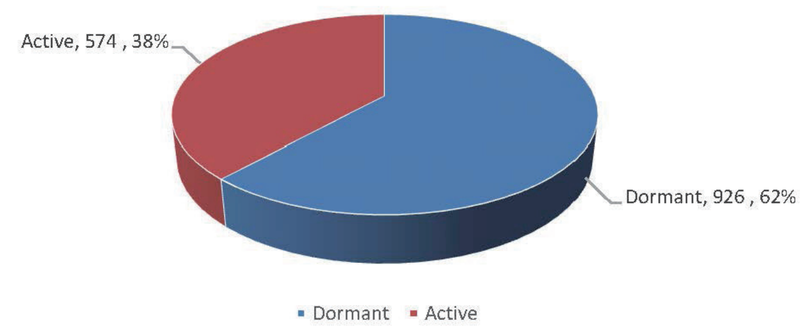
i. Distribution of Active and Dormant Bank Accounts

Table 10: Statistics of Active and Dormant Bank Accounts

Status	No.	Percentage
Dormant	926	61.73%
Active	574	38.27%
Total	1,500	100.00%

There are 926 (61.73%) of 1,500 dummy bank accounts that were found dormant after activating the e-banking function with NTD 1, 100, 1,000 or other small amount testing transactions while another 574 (38.27%) accounts are still in active status with intensive transactions (see Table 10 & Figure G). This indicates that the criminal gangs are collecting e-banking accounts as they are collecting cellphone SIM cards. According to the follow-up STRs, the average period length of using a dummy bank account is only 1 to 6 months, which multiplies the difficulties to investigate the criminal cases for the LEAs.

Figure G: Distribution Graph of Active and Dormant Bank Accounts



ii. Distribution of Active Bank Accounts by Country/Area

Not all the FIs provided the IP data or any other activity information of the e-bank accounts in the STRs. Due to the technical limit and time constraint, a few FIs only provided some login data during specific periods of time. Even though the AMLD could not conduct a comprehensive analysis on all 574 active bank accounts, the main locations of the active bank accounts were still roughly identified as follows: Taiwan, Mainland China, Hong Kong, the Philippines, Malaysia, Vietnam, Cambodia, the US and Canada, etc. The functions of the locations where the IPs appeared still could not be exactly identified as the proxy/relay servers or the actual tele-fraud offices or ML centers of the criminal gangs. But in most of the cases, the proxy/relay servers were usually located in the U.S. or Canada while the actual offices of the criminal gangs were found in Southeast countries.

As per the IP activity information of the dummy e-banking accounts, the IPs of the active accounts had been appearing in each country/area 24/7 with intensive large amount transactions and the amount balances were also being checked afterwards. Most of the criminal gangs set up the same or very similar usernames and the same pre-designated receiving accounts to facilitate ML and to save remittance fees. These red flags are very common as well as very unusual for internet/mobile payments but have not been included in the list of suspicious signs of ML.

It is because the traditional development of suspicious signs of ML focused on the amounts and the frequencies of transactions and on whether the transactions are commensurate with the remitters' financial background. The AMLD calls for the competent authorities to take more consideration on the characteristics of the e-banking and any other similar new payment instruments to address the deficiencies of the existing suspicious signs of ML.

iii. Distribution of Active Bank Accounts by Function

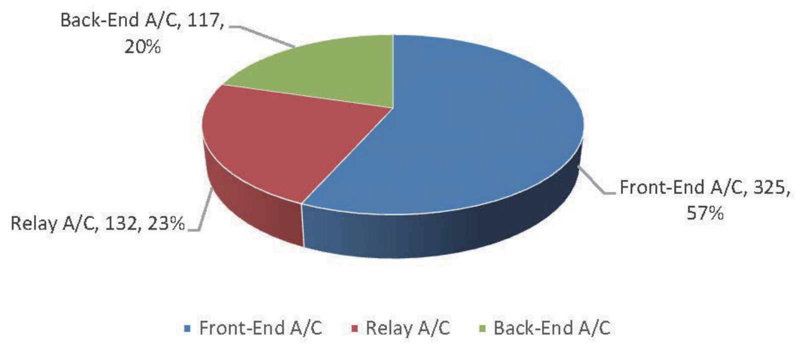
Table 11: Statistics of Active Bank Accounts by Function

Function	No.	Percentage
Front-End Account	325	56.62%
Proxy/Relay Account	132	23.00%
Back-End Account	117	20.38%
Total	574	100.00%

The 1,500 dummy bank accounts set up 538 (25.33%) pre-designated receiving accounts as 926 (61.73%) of them are dormant. The AMLD could not directly identify the function of each bank account but some transaction methods and specific characteristics still could be reliable references. In most of the cases, the front-end accounts usually have very intensive and small integer amount of inward transactions from those buying online gambling credits. If the amount of single inward transaction is large, the bank account might probably be used for tele-fraud. If the amount is large with lower frequency, it might probably be used as a relay account. If each amount is over NTD 100K, or up to Millions, it might probably be used for underground banking/hawala. And if the amount is intensively withdrawn by the ATMs, it might probably be used as a back-end account. The cash mules/couriers usually bring the cash withdrawn from the ATMs to the ML center or some specific area temporarily and then the money will be laundered cross-border via business payment, investment, loan or any other legal ways.

According to the abovementioned initial criteria, regarding the 574 active bank accounts, there are 325 (56.62%) front-end accounts, 132 (23%) relay accounts and 117 (20.38%) back end accounts (see Table 11 & Figure H). But in some cases, some accounts have multiple functions.

Figure H: Distribution Graph of Active Bank Accounts by Function



iv. A Trend That Dummy E-Banking Accounts Connect to Third Party Payment

Table 12: Statistics of Dummy E-Banking Accounts Connecting to Third Party Payment

Function	No.	Connecting to 3rd Party Payment	Percentage
Front-End Account	325	287	88.31%
Proxy/Relay Account	132	98	74.24%
Back-End Account	117	79	67.52%
Total	574	464	80.84%

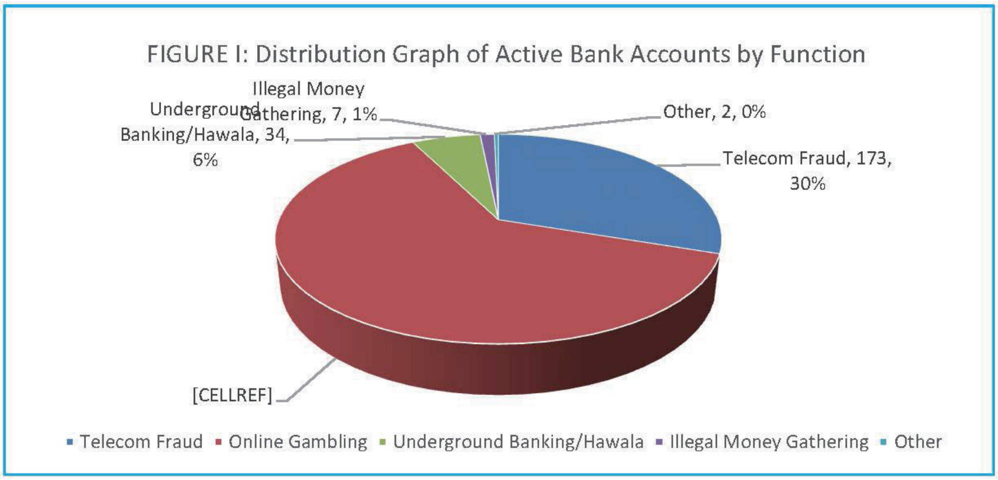
There are 287 out of 325 (88.31%) front-end accounts, 98 out of 132 (74.24) proxy/relay accounts and 79 out of 117 (67.52%) back-end accounts have money flows directly connecting to the third party payment accounts. And a total of 464 out of 574 (80.84%) active accounts were found connecting to the third party payment accounts (see Table 12). The AMLD identified a trend that the dummy bank accounts have intensive money flows directly connecting to the third party payment accounts.

v. Probable Predicate Offences Involved

Table 13: Statistics of Probable Predicate Offences Involved

Predicate Offence	No.	Percentage
Telecom-Related Fraud	173	30.09%
Illegal Online Gambling	358	62.37%
Underground Banking/ Hawala	34	5.91%
Illegal Money Gathering	7	1.22%
Other	2	0.35%
Total	574	100.00%

There are 926 out of 1,500 dummy e-banking accounts that are dormant and therefore the probable predicate offences involved are unable to be identified. In the other 574 active dummy e-banking accounts, 173 (30.09) accounts are identified involving in telecom-related fraud, 359 (62.43) involving in illegal online gambling, 34 (5.91%) involving in underground banking/hawala, 7 (0.35%) involving in illegal money gathering (see Table 13 & Figure I)



V. Conclusions and Recommendations

i. To Enhance Dynamic KYC and Counter Measures on Internet/ Fintech Transactions to Meet Requirements of AML/CFT Regimes and Financial Inclusion

Convenience, anonymity, low cost and fast speed are the characteristics of online transactions, also accompanied by uncertainties and risks on technical and trading matters, which arouses new modus operandi. Fintech, both now and in the future, has shown an inevitable trend of development and it can only be regulated but not completely prohibited. Otherwise the country’s global competitiveness and market opportunities will be harmed. However, the above-mentioned characteristics also bring the criminal groups some opportunities to take advantage of them, which makes it more difficult for financial supervision and law enforcement agencies to check and verify. Moreover, both online banking accounts and related fintech payment tools are highly non-face-to-face transaction vehicles. After two or more high-risk payment tools are connected through the internet transactions, the "multiplier effect" of ML/TF risks will be exacerbated.

In mainland China and some European and American countries, all payment vehicles through non-banking systems are collectively referred to as third-party payment. But in Taiwan, the third-party payment industry is divided into 3 sectors: electronic payment institutions (EPIs), electronic stored value card companies (ESVCCs) and third party payment companies (TPPCs). According to the official statistics of the FSC, there are 28 EPIs including 5 dedicated EPIs and 23 concurrent operation banks, 5 ESVCCs including 4 dedicated ESVCCs and 1 concurrent operation bank while there are 9,154 TPPCs based on the database of the Ministry of Economic Affairs (see Table 14). The total numbers of the EPIs and ESVCCs under the supervision of the FSC are not as much as that of the TPPCs and the AML/CFT legal regimes are also very sufficient to meet the requirements of the international AML/CFT standards, including technical compliance and effectiveness. But for the FIU and the LEAs, the main difficulty lies in the effectiveness of intelligence analysis and investigation. The TPPCs' transaction speed and the frequency are beyond the capacity of traditional analysis or investigative manpower. This report encourages the private sectors to be willing to cooperate and assist in the establishment of complete log files and any databases to facilitate the LEAs to develop big data investigation techniques to overcome this problem.

TABLE 14: Comparison Table Among 3 Sub-Sectors of Third Party Payment Industry

<table>
<tr><td>Sector</td><td colspan="2">Electronic Payment Institutions</td><td colspan="2">Electronic Stored Value Cards Companies</td><td>Third Party Payment Companies</td></tr>
<tr><td>No.</td><td colspan="2">28 (5 dedicated+ 23 concurrent operation)</td><td colspan="2">5(4 dedicated+ 1 con. operation)</td><td>9,154</td></tr>
<tr><td>Competent Authority</td><td colspan="2">FSC</td><td colspan="2">FSC</td><td>MOEA</td></tr>
<tr><td>Rules and Regulations</td><td colspan="2">1. The Act Governing Electronic Payment Institutions
2. Rules Governing the Administration of Electronic Payment Business
3. Template for Guidelines Governing Anti-Money Laundering and Countering Terrorism Financing of Electronic Payment Institutions
4. Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission
5. Guidelines Governing Money Laundering and Terrorist Financing Risk Assessment and Relevant Prevention Program Development by the Electronic Payment Institutions …</td><td colspan="2">1. Act Governing Issuance of Electronic Stored Value Cards
2. Rules Governing the Business of Electronic Stored Value Card Issuers
3. Regulations Governing the Security of Electronic Stored Value Cards
4. Template for Guidelines Governing Anti-Money Laundering and Countering Terrorism Financing of Electronic Stored Value Cards
5. Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission
6. Regulations Governing Reporting on the Properties or Property Interests and Locations of Designated Sanctioned Individuals or Entities by Financial Institutions
7. Guidelines Governing Money Laundering and Terrorist Financing Risk Assessment and Relevant Prevention Program Development by the Electronic Stored Value Cards Companies ……</td><td>1. The Self-Regulatory Standards of Credit Card Acquirers Executing Contracts with “Payment Collection Platform Service Providers” as Merchants
2. Mandatory Provisions to be Included in and Prohibitory Provisions of Standard Form Contract for Third Party Payment Companies</td></tr>
<tr><td>Minimum Paid-In Capital</td><td colspan="2">NTD 500M</td><td colspan="2">NTD 300M</td><td>No Limit</td></tr>
<tr><td>Maximum Storable Value</td><td colspan="2">NTD 50K</td><td colspan="2">NTD 10K</td><td>Non Storable</td></tr>
<tr><td>Transaction Limit</td><td>1St Type: For purposes of personal use, payment and value storing only.</td><td>Monthly accumulative upper limit of receipt and payment is NTD 30K, and the upper limit of stored value balance is NTD 10K.</td><td>1St Type: For paying government fees, taxes, etc.</td><td>No Limit</td><td>No Limit</td></tr>
</table>

	2nd Type: For purposes of both personal & non-personal use, collection, payment and value storing.	Monthly payment limit is NTD 300K.	2nd Type	Single transaction maximum is NTD 1K, and single-day cumulative maximum is NTD 3K.	
	3rd Type: For purposes of both personal & non-personal use, collection, payment and value storing and should be handled at the counter.	Monthly payment limit for individuals is NTD 1M, and the maximum for non-individuals is NTD 10M and should be handled at the counter.			

In order to address the deficiencies of the AML/CFT regimes aroused by the third party payment sector, the Ministry of Justice (MOJ) and the Ministry of Economic Affairs (MOEA) had officially made a joint announcement that the sector is also mandatorily applicable to the Money Laundering Control Act (MLCA) in February 2013. Therefore, the TTPCs also have the responsibilities to implement KYC, record keeping and STRs/CTRs reporting based on the MLCA. The competent authority of the TPPCs is the MOEA instead of the FSC and that is because the TPPCs are only "payment collection platform service providers". The MOEA's existing business itself is quite heavy and complicated which results in the lack of its AML/CFT expertise, experience and supervisory synergies, comparing with the FSC. As we can see in the Table 14, there are currently 9,154 TPPCs and the quality of them also varies, and there is a lack of complete AML/CFT regimes for the MOEA to provide sufficient supervision. As mentioned above, even though the payment collection platform service run by the TPPCs is not actually bank remittance business, the need of value transfer can be satisfied by the design of internal virtual accounts. And it is also fast, convenient, and has no transaction limit, which naturally degenerates into weaknesses that the criminal groups intend to take advantage of.

This report found that the connection between the dummy e-banking accounts and the third-party payment accounts is quite intensive. The registered owners of certain TPPCs also have a lot of criminal records and they are even the provider of some dummy accounts. The TPPCs are non-special permission companies, there are no restrictions on its founder qualifications, capital amount thresholds and transaction limits. The regulations/rules for AML/CFT technical compliance are only very simple self-regulatory provisions and administrative guidance, which are also insufficient. To address the above-mentioned deficiencies, the MOEA had started to hold a series of special meetings on the draft AML/CFT countermeasures for the TPPCs since September, 2020, inviting competent authorities, scholars and experts, major industry players and stakeholders to participate in the discussions. This report expresses a high recognition and affirmation of the efforts and contributions made by the MOEAs and the participants to fill the gaps between the third-party payment sector and AML/CFT regimes. And we do believe that the technical compliance gaps in relevant laws and regulations should be greatly addressed in the coming future.

ii. The Current Red Flags of ML/TF Could Not Cover Major Abnormalities of E-Banking Accounts

Table 15: Statistics of the ML/TF Red Flags for the Banking Sector

Reported Red Flags	No.	Percentage
A11: Cash deposit and withdrawal transactions in the same account within a certain period of time, each of which accumulates to a specific amount or more	9	2.72%
A12: The same customer handles multiple cash deposit and withdrawal transactions in his account within a certain period of time, each of which has accumulated a certain amount or more	8	2.42%
A14: Customers who have deposits exceeding a certain amount suddenly (such as depositing multiple promissory notes and cheques into the same account)	2	0.60%
A15: Sudden transfer of funds from an inactive account to a certain amount or more	15	4.53%
A16: After the customer opens an account, there is deposit or remittance of a certain amount or more immediately after the account is opened, and it is transferred quickly	12	3.63%

A17: The deposit account has intensively deposited multiple sums of a certain amount or more, or the number of transactions reach to a certain amount or more, and they are transferred quickly	84	25.38%
A18: Clients often transfer funds of more than a certain amount between several different clients’ accounts	30	9.06%
A1A: The amount of each deposit and withdrawal of the customer is equal and the time is short, and the amount exceeds a certain amount	22	6.65%
A1B: The customer often deposits or withdraws on behalf of others, or a specific account is often deposited or withdrawn by a third person for a specific amount or more	1	0.30%
A1C: The customer remits multiple payments in cash at one time, or requests to issue bills (such as bank cheques, or money orders), apply for negotiable time deposit certificates, traveler's cheques, beneficiary certificates and other securities, and the total amount reaches a certain amount or more	1	0.30%
A83: Several people go to the bank together to proceed deposit, withdrawal or remittance transactions	2	0.60%
A91:The customer has the red flags provided by Regulations Governing the Deposit Accounts and Suspicious or Unusual Transactions, Template for Guidelines Governing Anti-Money Laundering and Countering Terrorism Financing of Banking Sector and/or any other situations where it is not possible to complete the required procedures for confirming identity	4	1.21%
A92: There are a large number of customers registered at the same address, the resident frequently changes, or the address is not the real residential address	1	0.30%
AB1: Customers who often remit money abroad for a certain amount or more	1	0.30%
AZZ: Other red flags regarding ML/TF	139	41.99%
Total	331	100.00%

The research population, 1,500 dummy e-banking accounts, in this report are derived from 238 STRs reported by the banking sectors. However, since each report can select more than two red flags, the number of red flags is 331 as the number of STRs is 238. The most reported red flag is "AZZ: Other red flags regarding ML/TF ", being reported for 139 times, accounting for 41.99%. This is mainly because most of the accounts are in dormant status and could not be verified by the same user name, password, or IP location in a short period of time in different countries or regions. The second highest reported red flag (10 times or more) is "A17: The deposit account has intensively deposited multiple sums of a certain amount or more, or the number of transactions reach to a certain amount or more, and they are transferred quickly ", for 84 times, accounting for 25.38%. And the third to the sixth one are respectively as follows: "A18: Clients often transfer funds of more than a certain amount between several different clients' accounts", for 30 times, accounting for 9.06%; "A1A: The amount of each deposit and withdrawal of the customer is equal and the time is short, and the amount exceeds a certain amount ", for 22 times, accounting for 6.65%; "A15: Sudden transfer of funds from an inactive account to a certain amount or more ", for 15 times, accounting for 4.53%; and "A16: After the customer opens an account, there is deposit or remittance of a certain amount or more immediately after the account is opened, and it is transferred quickly ", for 12 times, accounting for 3.63% (see Table13).

From the above information, the current red flags of ML/TF can no longer cover the major abnormalities of e-banking accounts. Because the development of traditional ML/TF red flags mainly focuses on indicators such as the amount, the frequencies of transactions, and whether the transactions are commensurate with the dealers' financial backgrounds. In order to adapt to the advent of the era of e-banking and new payment vehicles, this report urges the banking sectors to consider the characteristics of e-banking and any other related new payment vehicles as developing new ML/TF red flags in the future.

iii. Fully Implement the Existing Mechanisms for Notification of Suspicious Dummy Accounts and Risk Control Countermeasure

There have been some research reports on the issue of dummy security accounts, suggesting that when finding the transactions abnormal, securities firms may voluntarily send "warning letters" to inform the account owners regarding the abnormal transaction situations and the possible legal responsibilities that the owners may face, in order to receive the effect of vigilance and deterrence. The current legal regime has roughly conformed to the spirit of the proposal. The Paragraph 4, Article 1 of the Checklist of Money Laundering Prevention Measures for Banks provides that if the situation meets the legal requirements of the Paragraph 12, Article 12 of the Regulations Governing the Deposit Accounts and Suspicious or Unusual Transactions, the banks should reject the client's application for opening an account; for those who are suspected of applying for opening dummy accounts, they may tactfully refuse or temporarily not accept automated services including financial cards, telephone and voice banking, online banking, etc. The Subparagraph 3, Paragraph 1, Article 2 of the Template for Guideline Governing Account Opening Review Procedure and Risk Control on Abnormal Account of Financial Institutes also provides that when accepting account opening, the customer should be informed, if the account is provided for illegal use, the customer should take the relevant legal responsibilities. And the Article of the same Template also provides that financial institutions should establish a post-tracking management mechanism for deposit accounts. Suspicious customers found after opening an account should be reconfirmed by telephone, written statements or on-site inspections, and handled appropriately. The above-mentioned regulations have already had related risk control, prevention and aftermath management mechanisms.

However, the AMLD, in the process of accepting a large number of STRs of suspected dummy e-banking accounts, found that the reporting FIs had different practices on how to "appropriately handle" the suspected dummy e-banking accounts. Some FIs directly refused to continue the account opening procedure, some just stopped the e-banking function, some refused to issue an ATM card, and a large number request the AMLD to give specific instructions or approve the countermeasures recommended by the FIs. In fact, the AMLD is only an FIU accepting STRs in accordance with the MLCA, and does not have the power or legal privilege to instruct or approve to any countermeasures recommended by the FIs. This report recommends and reiterates that FIs take the specific countermeasures listed in Article 5 of the Regulations Governing the Deposit Accounts and Suspicious or Unusual Transactions, and take into account the spirit of Recommendation 1 of the International AML/CFT Standards, the FATF 40 Recommendations. Based on the spirit of risk-based approach and the above-mentioned regulations, implement countermeasures corresponding to the risk level so that the ML/TF risks can be effectively reduced.

iv. Encourage FIs to Conduct Informal Cooperation and Information Exchange

In practice of the banking sectors, FIs usually conduct informal cooperation and exchange some level of information with each other in response to specific events or suspicious accounts and/or transactions, but the scope and depth of information exchange are different. This practice of informal cooperation and information exchange helps to expand the perspective of the STRs, and is conducive to improving the qualities and the subsequent analysis and judgment of the FIU. As a result, the FIs that are notified can also be vigilant about the suspicious accounts and/or transactions and timely file relevant STRs to the FIU for further analysis.

Therefore, this report encourages the FIs to conduct related formal and/or informal information exchanges without violating relevant laws and regulations without affecting the investigation by the LEAs. However, for the third-party payment sector, this report holds a reservation or even a negative attitude. This report recommends the FIs at least conduct a certain degree of research or understanding of the specific TPPCs before deciding whether to proceed the above-mentioned cooperation or information exchange. Otherwise, the specific TPPCs themselves are maybe members of some criminal groups, badly affecting the investigation by the LEAs.

v. Encourage FIs to Attach Any Additional Documents or Information Helpful for Analysis and Investigation When Filing STRs

In the process of receiving a large number of STRs regarding suspicious dummy e-banking accounts, the AMLD found that most FIs only provide account opening information and transaction details for a certain period of time, and describe the relevant suspicious reasons, but they seldom provided other supporting documents and/or information to stand for the STRs. For example, some FIs described in the STRs that unknown persons are remotely controlling the account opening person to fill in the necessary KYC information at the bank door or even in the car outside the banks, or the IP addresses of the accounts are abnormally appearing in different countries/ regions in a short period of time, if the masterminds' telephone numbers, car plate numbers, related CCTV records and the relevant IP login information are attached at the same time, it will speed up the analysis of the FIU and expedite the LEAs to trace the cash flow and the proceeds of crimes, and take the best opportunity to avoid the loss of evidence. Therefore, this report also encourages the FIs to provide any additional documents or information that is helpful for subsequent analysis and investigation.

Part V

Event Calendar of 2020

2020/1/8	Participated in “Meeting on Reviewing Targeted Financial Sanctions”.
2020/1/14	Coordination meeting with the Coast Guard Administration of Ocean Affairs Council.
2020/1/24-2/1	Participated in “2020 Egmont Group Working Group and Egmont Committee Meetings” at Mauritius.
2020/2/14	Participated in "Meeting on Development of Crime Prevention".
2020/2/18	AMLD organized “Workshop on Enhancing Financial Intelligence Sharing and Using” with law enforcement agencies and competent authorities.
2020/6/1	Signed “Memorandum of understanding for cooperation of information-sharing regarding money laundering, crimes of relevant preparations and financing of terrorism” with the Republic of Kosovo.
2020/7/13	Coordination meeting with Customs Administration of Ministry of Finance.
2020/7/20、8/3	Participated in “Meeting on Deficiency Improvement of APG's 3rd Mutual Evaluation”.
2020/8/4	Coordination meeting with National Taxation Bureau of the Northern Area.
2020/8/5、12/7	Participated in "Meeting on amendments of the Regulations Governing the Prevention of Money Laundering and Terrorist Financing by Land Administration agents and real estate agencies”.
2020/9/2	Participated in “37th Coordination meeting between Ministry of Justice and Financial Supervisory Commission”.

2020/9/17	Coordination meeting with Criminal Investigation Bureau of National Police Agency.
2020/9/25	Coordination meeting with National Taxation Bureau of Taipei.
2020/9/25、10/19	Participated in "Meeting on amendments of the Regulations Governing the Prevention of Money Laundering and Terrorist Financing by Third-party Payment Providers”.
2020/10/13	Coordination meeting with Agency Against Corruption of Ministry of Justice.
2020/10/14	AMLD organized “2020 Workshop of AML Specialists in Financial Institutions”
2020/10/14、12/8	Participated in “Meeting on Deficiency Improvement of DNFBPs”.
2020/10/23	Coordination meeting with National Taxation Bureau of the Central Area.
2020/11/26	Participated in “Meeting on Transparency of Ultimate Beneficial Owners”
2020/12/10	AMLD organized “Conference on Criminal Cash Flow Analysis and Abnormal Transaction Patterns”
2020/12/18	Coordination meeting with Financial Examination Bureau of Financial Supervisory Commission.
2020/12/23	Participated in “Preliminary Meeting on Publicizing Guides of Trading with Iran”.
2020/12/28	Coordination meeting with National Taxation Bureau of the Kaohsiung.
2020/12/29	Coordination meeting with National Taxation Bureau of the Southern Area.

ANTI-MONEY LAUNDERING ANNUAL REPORT, 2020

Published by: Investigation Bureau, Ministry of Justice, Republic of China (Taiwan)

Issuer: LEU, Weng-Jong

Editor: Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice

Address: No.74, Zhonghua Rd., Xindian Dist., New Taipei City 23149, Taiwan

Phone: 886-2-29112241

Website: http://www.mjib.gov.tw/en/

Publishing Date: October 2020

ANTI-MONEY LAUNDERING
ANNUAL REPORT, 2020
INVESTIGATION BUREAU, MINISTRY OF JUSTICE,
REPUBLIC OF CHINA (TAIWAN)

http://www.mjib.gov.tw/mlpc