

# ANTI-MONEY LAUNDERING ANNUAL REPORT, 2019



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

法務部調查局一〇八年洗錢防制工作年報

Investigation Bureau, Ministry of Justice

Anti-Money Laundering Annual Report, 2019



# PREFACE

---

Under the collaboration of 37 government agencies and 31 private businesses, Taiwan had successfully completed its 3rd APG (Asia/Pacific Group on Money Laundering) Mutual Evaluation. A Mutual Evaluation report was released on October 2, 2019 following APG's global review, in which Taiwan was awarded the best rating of "Regular follow-up," which marked a significant milestone in the nation's efforts toward anti-money laundering (AML) and counter terrorism financing (CTF) while making it a role model for other members in Asia Pacific. Anti-Money Laundering Division (AMLDD) of the Investigation Bureau, Ministry of Justice (MJIB) has been designated as the financial intelligence unit (FIU) of Taiwan and entrusted with the tasks of receiving, analyzing and disseminating financial intelligence since April 23, 1997, and its competence and value as a national FIU had impressed the assessment team during the 3rd Mutual Evaluation, earning a performance rating of "SE" (Substantial level of effectiveness) across all relevant categories that contributed significantly to the nation's "Regular follow-up" rating.

Serving as the nation's financial intelligence hub, AMLDD not only receives financial intelligence reports from financial institutions and designated non-financial businesses and professions (DNFBPs), but also performs the necessary analysis, shares findings with law enforcement agencies and tax authorities, and cooperates with relevant authorities in the investigation of terrorism financing (TF), money laundering (ML), and proceeds of predicate offences. With respect to the gathering of financial

intelligence, MJIB received a total of 26,481 suspicious transaction reports (STRs), 3,092,985 reports on cash transactions above a certain amount, and 360,336 customs reports on passengers' (and crew members') possession of valuable goods and attempts to transport valuable goods via shipment, express delivery, mail etc. in 2019. As for sharing of financial intelligence, the AMLD has proven competent in analyzing and adding value to the reports gathered, thereby enabling MJIB to compile 2,512 pieces of financial intelligence from 2,881<sup>1</sup>STRs and disseminate them to relevant authorities.

The AMLD actively engages in international AML/CTF organizations such as Financial Action Task Force on Money Laundering (FATF), APG, Egmont Group, and Asset Recovery Inter-Agency Network of Asia/Pacific (ARIN-AP) in various events to learn the latest AML trends and strengthen international collaboration. AMLD also takes this opportunity to discuss with representatives of other nations on issues that can be cooperated upon. Through Egmont Secure Web, AMLD exchanges AML/CTF intelligence with more than 160 foreign FIUs, and has been praised favorably for the quality, volume and effectiveness of its intelligence. In addition, Taiwan signed agreements/memorandums of understanding with FIUs of the Republic of Guatemala, Democratic Republic of Timor-Leste, Kingdom of Tonga, Independent State of Papua New Guinea, and Hashemite Kingdom of Jordan on the sharing of financial intelligence relating to ML, predicate offences and TF in 2019 for

---

<sup>1</sup> Time of data: 9:50 am, July 13, 2020.

enhanced bilateral cooperation.

Terrorism financing and proliferation of weapons of mass destruction (PWMD) have evolved in complexity around the world due to incorporation of new financing practices and new technologies, which exacerbate the threat on world peace and regional security. AMLD remains dedicated in the fight against terrorism financing and PWMD; it received more than 300 STRs on terrorism financing and PWMD in 2018 and 2019, and assigned representatives to participate in the 2019 "No Money for Terror Ministerial Conference on Counter-Terrorism Financing" organized by the Australian government, where it gained knowledge on the trends, strategies and successful experiences of counter-terrorism around the world to further improve counter-terrorism practices within Taiwan. AMLD also invited MJIB investigator Kai-Ting Ho to produce a written report addressing international rules on counter financing against PWMD as well as regulatory system and actual case studies within Taiwan, which will provide useful reference to the counter PWMD efforts of both the public and private sectors.

Year 2019 marked the beginning of a digital era for financial service industry of Taiwan, as three online-only banks passed review and had business licenses issued by Financial Supervisory Commission. However, more convenient and efficient financial services bring greater risk of information security, ML, and TF, which financial institutions (FIs) are required to respond with more intensive customer due diligence and mitigation measures when

promoting inclusive financial technologies. FATF published a Guidance on "Digital Identity" in this regard in March 2020 to help FIs adopt a risk-based approach toward digital identity verification and conform with FATF Recommendation 10 on customer due diligence. With the consent of FATF, AMLD translated the Guidance into Chinese and included it as part of this annual report, which will serve as reference to relevant authorities and the private sector.

Although this annual report has been carefully proofread and revised, there remain some omissions, mistakes, or incomplete sections; therefore, your comments and suggestions are welcome and appreciated.



Weng-Jong LEU  
Director General  
MJIB

August 2020

## 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 six parts:

- (I) Introduction to the organization.
- (II) Work overview (including statistical chart and data).
- (III) Significant case studies.
- (IV) Project research.
- (V) Strategic analysis report.
- (VI) Event Calendar of 2019.

### III. Notes

- ( I ) The year quoted in this annual report refer to the solar calendar; references to Project Research are presented in Gregorian calendar. The numbers of Suspicious Transaction Reports (STRs), Cash 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

- (NT). Special cases are noted in corresponding figures (charts).
- (II) The percentage of each figure is rounded off and the integer is slightly different from the decimal point.
- (III) Work overview statistics, as presented in the second part of this annual report, is dated March 2, 2020.
- IV. This annual report has been rushed to print; therefore, please feel free to point out the mistakes and incompletions for our correction.



## Table of Contents

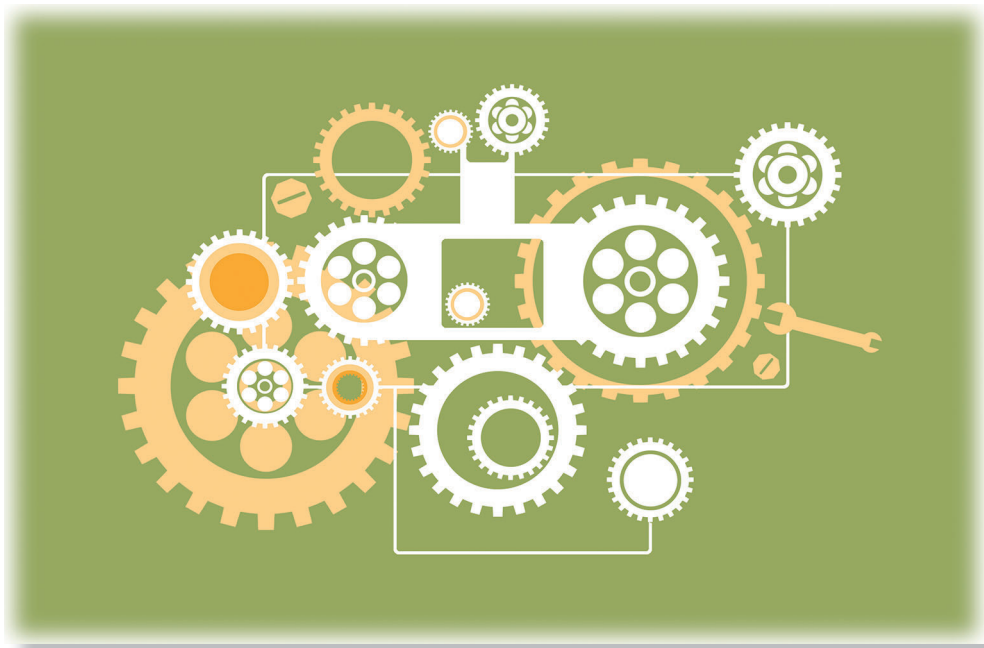
<b>Preface</b> .....	<i>II</i>
<b>Editorial Notes</b> .....	<i>VI</i>
<b>Part I Introduction to the organization</b> .....	<i>1</i>
<b>Part II Work Overview</b> .....	<i>7</i>
<b>One. Processing STRs</b> .....	<i>8</i>
I. Statistics of STRs.....	<i>9</i>
II. Dissemination of STRs.....	<i>10</i>
III. Distribution of STRs by Region.....	<i>11</i>
IV. Distribution of STRs by Month.....	<i>13</i>
V. Distribution of STRs by Subjects' Age Group.....	<i>13</i>
VI. Distribution of STRs by Amount.....	<i>14</i>
<b>Two. Receiving CTRs</b> .....	<i>16</i>
I. Statistics of CTRs.....	<i>17</i>
II. Distribution of CTRs by Amount.....	<i>18</i>
III. Statistics of Accessing CTRs Database.....	<i>19</i>
<b>Three. Receiving ICTRs</b> .....	<i>20</i>
I. Volume of passengers' reports (including crew member).....	<i>21</i>
II. Passengers' reports (including crew member) by Month.....	<i>22</i>
III. Passengers' reports (including crew member) by Value.....	<i>23</i>
IV. Statistics of ICTRs (delivered items).....	<i>23</i>
V. Statistics of the Value of ICTRs (delivered items).....	<i>24</i>
VI. Distribution of ICTRs (delivered items) by Month.....	<i>24</i>
<b>Four. Publicity Outreach and Training</b> .....	<i>25</i>
I. Publicity Outreach.....	<i>25</i>
II. AML/CFT Capacity Building Training.....	<i>26</i>
<b>Five. Public-private sector coordination and strategic studies</b> .....	<i>27</i>
I. Participated in APG's 3rd Mutual Evaluation and received rating of “Regular follow-up”.....	<i>27</i>
II. Assisted associations in the establishment of practical guidelines to improve the quality of STRs across different	

industries .....	29
III. Organized conferences on criminal cash flow analysis and abnormal transaction patterns.....	31
IV. Organized coordination meeting with Financial Examination Bureau, Financial Supervisory Commission.....	33
V. Compilation of strategic analysis report on “corruption crime” .....	33
VI. Issued AMLD Press.....	34
<b>Six. International co-operation and exchange .....</b>	<b>35</b>
I. International intelligence exchange .....	35
II. Concluding Agreement/MOUs with Other FIUs .....	36
III. Participation in the 26th annual meeting of Egmont Group .....	39
IV. Participation in No Money for Terror Ministerial Conference on Counter-Terrorism Financing .....	40
V. Participation in the 6th annual conference of “Asset Recovery Inter-Agency Network of Asia/ Pacific” .....	42
VI. Participated in FATF's 3rd Plenary Meeting and Work Group Meeting of the 30th year .....	43
<b>Part III Significant case studies .....</b>	<b>45</b>
<b>One. Violations against the Banking Act of Republic of China and Money Laundering Control Act- Loan Fraud .....</b>	<b>46</b>
<b>Two. Violations against the Banking Act of Republic of China and Money Laundering Control Act- Illegal Remittance.....</b>	<b>51</b>
<b>Three. Violations against the Banking Act- Illegal Fundraising.....</b>	<b>54</b>
<b>Four. Violations against the Criminal Code- Unredeemable Checks .....</b>	<b>57</b>
<b>Part IV Project Research .....</b>	<b>61</b>
<b>The International Trends on Counter Proliferation Financing and the Current Implementation of Taiwan- The Case Studies with the Investigation on the Taiwanese Citizen Who Becomes a Financier for North Korea .....</b>	<b>62</b>
<b>Part V Strategic Analysis Report .....</b>	<b>93</b>
<b>Strategic analysis report on corruption crime .....</b>	<b>94</b>
<b>Part VI Event Calendar of 2019 .....</b>	<b>117</b>

Table 01: Statistics of STRs reported in 2019.....	9
Table 02: Statistics of STRs reported in the last 5 years .....	10
Table 03: Statistics of STRs disseminated by AMLD in 2019 .....	10
Table 04: Statistics of suspicious transactions by region in 2019 .....	11
Table 05: Statistics of STRs reported by month in 2019.....	13
Table 06: Distribution of STRs by subjects' age group in 2019 .....	13
Table 07: Distribution of STRs by amount in 2019 .....	14
Table 08: Statistics of CTRs in 2019 .....	17
Table 09: Statistics of CTRs in the last 5 years .....	17
Table 10: Distribution of CTRs by Amount in 2019.....	18
Table 11: Statistics of accessing CTRs database in the last 5 years.....	19
Table 12: Volume of passengers' reports (including crew member) in 2019.....	21
Table 13: Volume of passengers' reports (including crew member) in the last 5 years .....	21
Table 14: Passengers' reports (including crew member) by month for 2019 .....	22
Table 15: Passengers' reports (including carrier service crew) by value in 2019.....	23
Table 16: Statistics of ICTRs (delivered items) in 2019.....	23
Table 17: Statistics of ICTRs (delivered items) in recent years.....	23
Table 18: Statistics of the value of ICTRs (delivered items) in 2019 .....	24
Table 19: Distribution of ICTRs (delivered items) by month in 2019 .....	24
Table 20: Statistics on AML and CTF training for reporting institutions in 2019.....	26
Table 21: Statistics of international intelligence exchange in the last 5 years.....	35
Figure A: Organizational chart of the AMLD .....	4
Figure B: Operational flow chart of the AMLD.....	6
Figure C: Statistics on STRs in the last 5 years .....	10
Figure D: Distribution of STRs reported by region in 2019 .....	12
Figure E: Pie chart of STRs distribution by subjects' age group in 2019.....	14
Figure F: Pie chart of STRs distribution by amount in 2019 .....	15
Figure G: Statistics on CTRs in the last 5 years .....	18
Figure H: Line graph of CTRs distribution by amount in 2019 .....	19
Figure I: Pie chart of ICTRs distribution by value in 2019.....	22

# 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 7 (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 abusing FIs as a vehicle for ML and to detect major crimes and ML at the point of the transaction, AML legislations around the world require all FIs to file Cash Transaction Reports (CTRs) and STRs. Based on the definition in the related international organizations, an authority responsible for receiving and analyzing STRs is 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” (AML/D) 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 AML/D currently has a Section of STR Analysis, a Section of AML/CFT Strategic Planning, and a Section of Tracing Illegal Funds Flow setup with 27 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, AML/D 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 AML/D 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



FINANCIAL ACTION TASK FORCE  
GROUPE D'ACTION FINANCIÈRE

### © FATF (Financial Action Task Force)

The Group 7 had realized at the 1989 Summit in Paris 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 centre 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

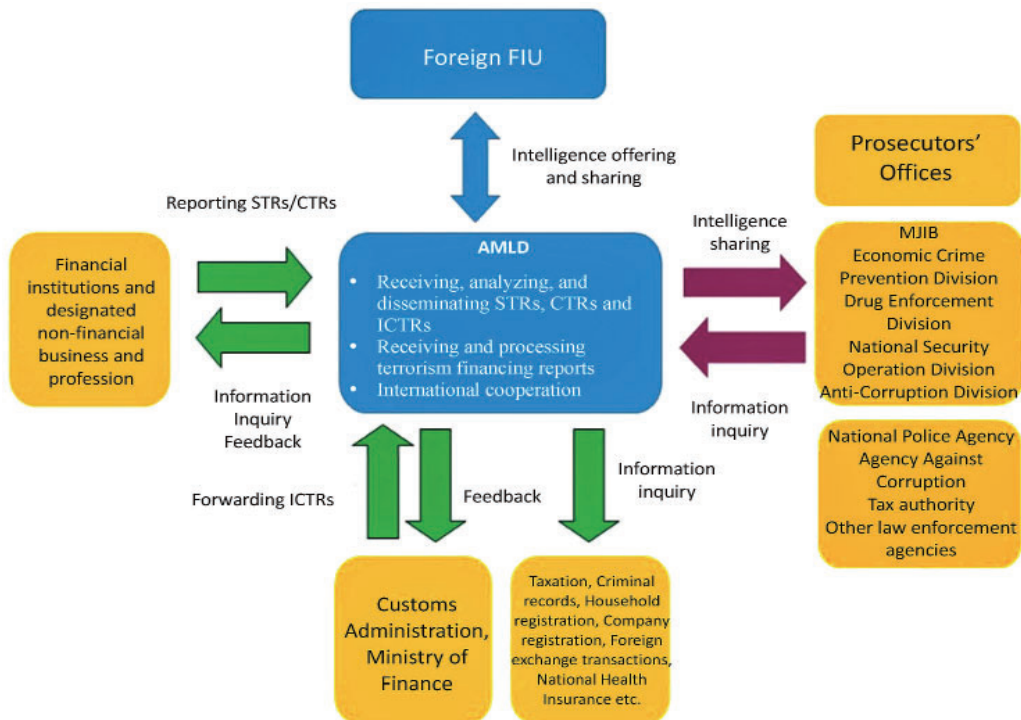


declarations/disclosures)

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



## Part II

# Work Overview



**One. Processing STRs**

**Two. Receiving CTRs**

**Three. Receiving ICTRs**

**Four. Publicity Outreach and Training**

**Five. Public-private sector coordination and strategic studies**

**Six. International co-operation and exchange**

## 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 26,481 STRs in 2019, which was 26.17% less than the 35,869 cases a year ago (2018). 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 72.49% of reports were raised by local banks, 27.3% of suspicious transactions took place in Taipei City, 52.66% of transaction counterparties were within the 31 to 60 age group, whereas 18.29% of transactions were below NT\$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

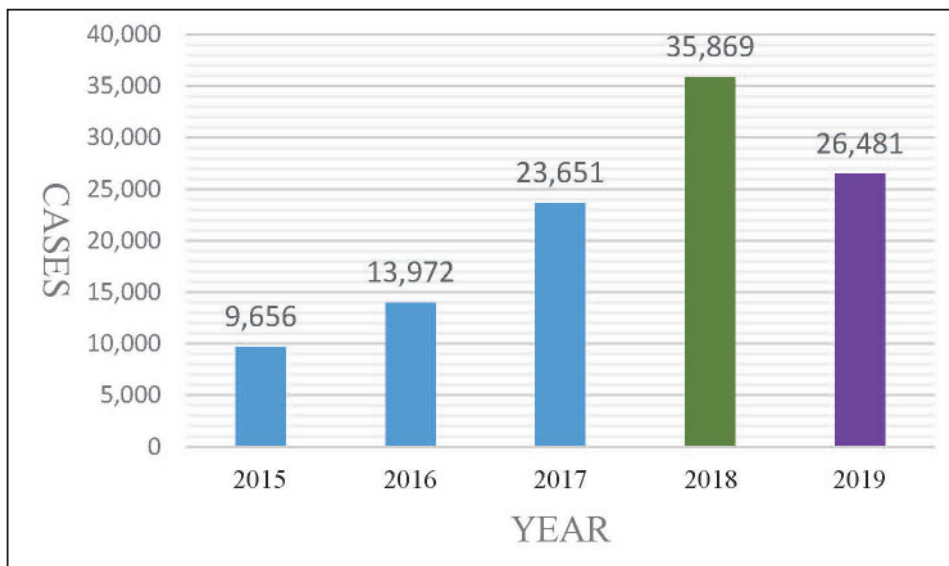
Table 01: Statistics of STRs reported in 2019

Reporting Entities	Number of STR reported
Domestic banks	19,196
Foreign banks	22
Trust investment company	0
Credit unions	831
Credit Department of National Farmers' and Fishman's Associations	824
Postal remittances and savings	3,679
Bills finance companies	2
Credit card companies	30
Insurance companies	1,202
Securities firms	371
Securities investment trust enterprises	34
Securities finance enterprises	5
Securities investment consulting enterprises	0
Centralized securities depository enterprises	21
Futures Commission Merchants	49
Designated non-financial business and profession	68
China's banks	35
Electronic payment and electronic stored value card issuers	107
Foreign currency collection/exchange agencies	2
Fintech innovative experimentation businesses	2
Finance leasing companies	1
<b>Total: 26,481</b>	

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

Year	2015	2016	2017	2018	2019
No. of STRs	9,656	13,972	23,651	35,869	26,481

Figure C: Statistics on STRs in the last 5 years



## II. Dissemination of STRs

Table 03: Statistics of STRs disseminated by AMLD in 2019

	Number of STRs
Refer to MJIB's investigation unit	1,355
Refer to police, prosecutor and other accountable agencies	1,340
International cooperation	11
Add to database	23,648
Analyzing	127
Total: 26,481	

### III. Distribution of Suspicious Transactions by Region

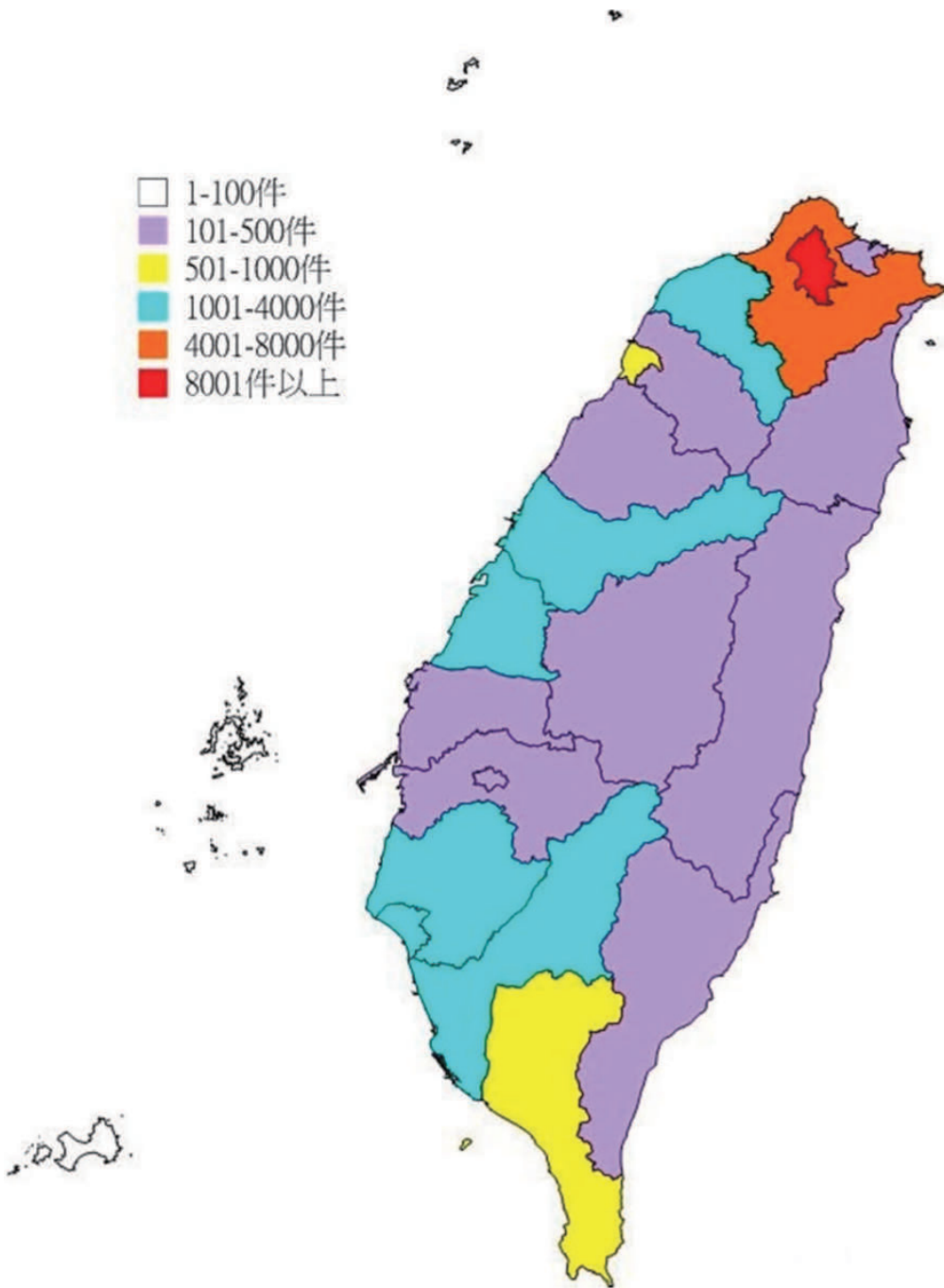
Table 04: Statistics of suspicious transactions by region in 2019

Trading area	Number of STRs	Trading area	Number of STRs
Taipei City	8,270	Chiayi City	436
New Taipei City	4,632	Chiayi County	264
Keelung City	332	Tainan City	1,770
Yilan County	294	Kaohsiung City	3,298
Taoyuan City	2,362	Pingtung County	511
Hsinchu City	678	Hualien County	201
Hsinchu County	482	Taitung County	149
Miaoli County	367	Penghu County	25
Taichung City	3,829	Kinmen County	39
Changhua County	1,220	Lienchang County	4
Nantou County	300	Others <sup>2</sup>	484
Yunlin County	344		
			Total: 30,291

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

<sup>2</sup> Refer to foreign countries, etc.

Figure D: Distribution of STRs Reported by Region in 2019



## IV. Distribution of STRs by Month

Table 05: Statistics of STRs reported by month in 2019

Month	January	February	March	April	May	June	July	August	September	October	November	December
Number of STRs	2,497	1,532	2,056	2,127	2,325	2,054	2,353	2,434	2,178	2,145	2,328	2,452

## V. Distribution of STRs by Subjects' Age Group

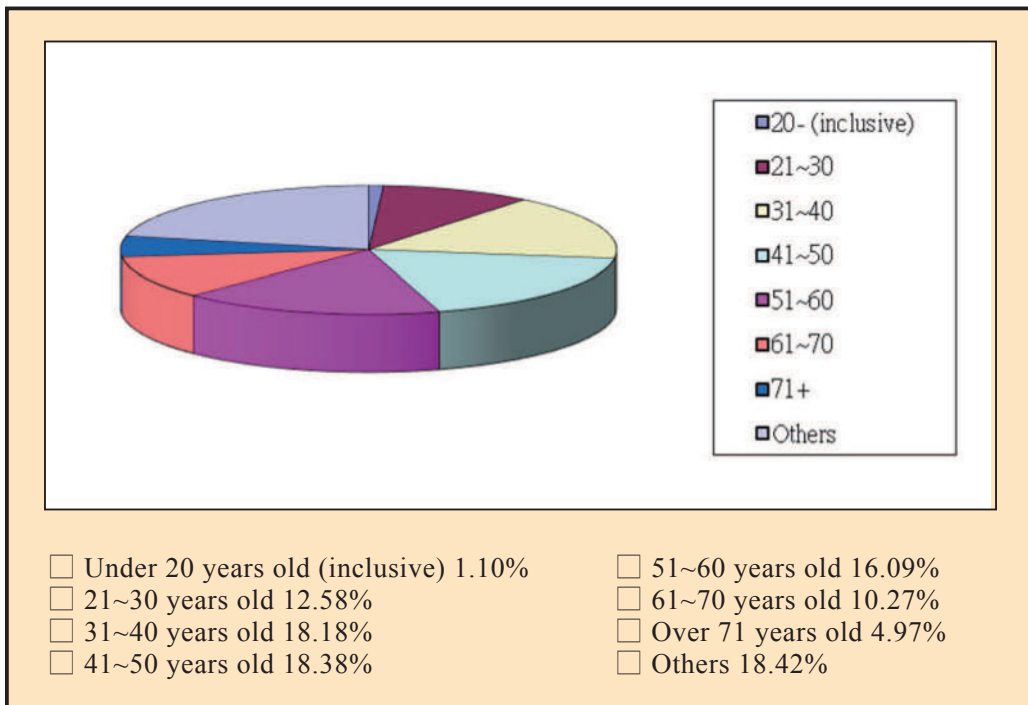
Table 06: Distribution of STRs by subjects' age group in 2019

Age groups	Number of persons
Under 20 years old (inclusive)	291
21~30 years old	3,330
31~40 years old	4,815
41~50 years old	4,868
51~60 years old	4,262
61~70 years old	2,719
Over 71 years old	1,317
Others <sup>3</sup>	4,879
Total: 26,481	

<sup>3</sup> Others: Non-natural person.



Figure E: Pie Chart of STRs Distribution by Subjects' Age Group in 2019

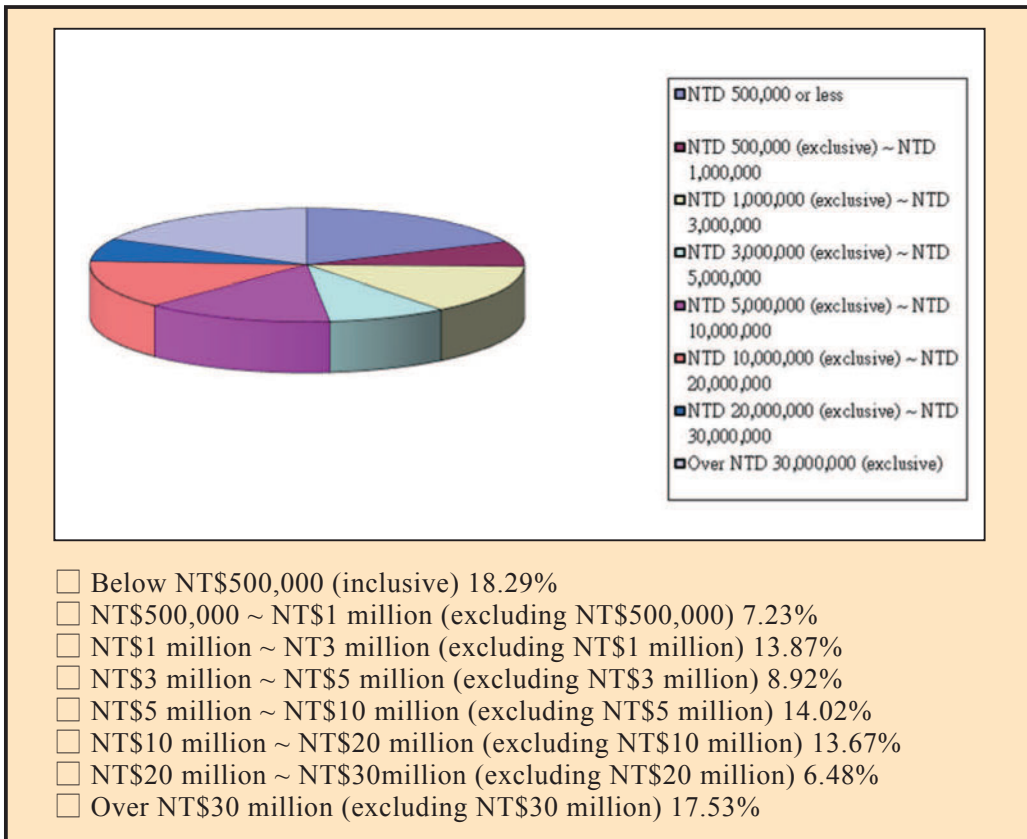


## VI. Distribution of STRs by Amount

Table 07: Distribution of STRs by amount in 2019

Amount	Number of STRs
Below NT\$500,000 (including NT\$500,000)	4,844
NT\$500,000 ~ NT\$1 million (excluding NT\$500,000)	1,914
NT\$1 million ~ NT\$3 million (excluding NT\$1 million)	3,674
NT\$3 million ~ NT\$5 million (excluding NT\$3 million)	2,362
NT\$5 million ~ NT\$10 million (excluding NT\$5 million)	3,712
NT\$10 million ~ NT\$20 million (excluding NT\$10 million)	3,619
NT\$20 million ~ NT\$30 million (excluding NT\$20 million)	1,715
Over NT\$30 million (excluding NT\$30 million)	4,641
Total: 26,481	

Figure F: Pie Chart of STRs Distribution by Amount in 2019



## 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 NT\$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, prosecutor offices and policies agencies based in Regulations under Art 5 of MJIB Operation Regulations on Matters relevant to AML/CFT. AMLD received 3,092,985 CTRs in 2019, and according to the statistics and analysis of those reports, 78.24% of CTRs were reported by domestic banks; 73.39% of CTRs were with an amount of NT\$500,000 ~ NT\$1 million; also, 44,097 transactions in CTRs database had been accessed in 2019. (Please refer to Table 8 ~ Table 11 and Figure G ~ H for detailed statistics and analysis).

## I. Statistics of CTRs

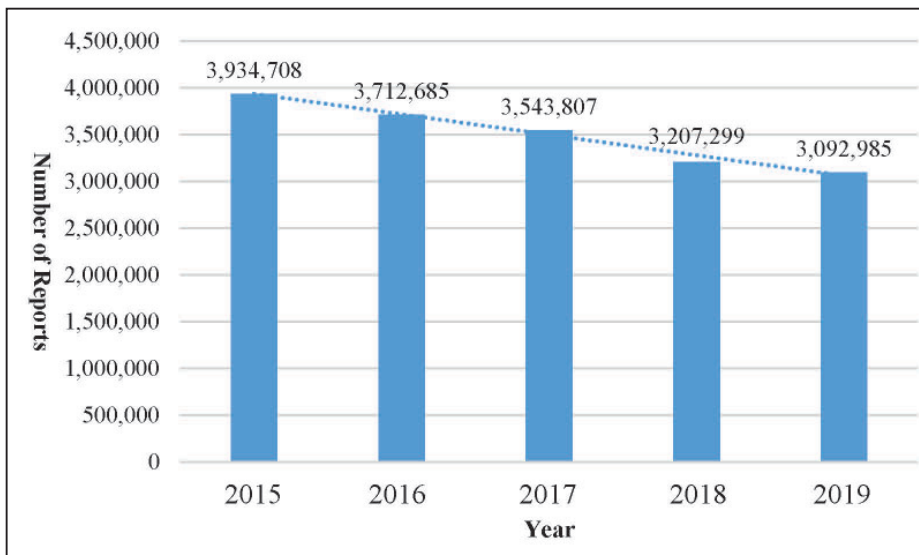
Table 08: Statistics of CTRs in 2019

Reporting entities	Number of Reports
Domestic banks	2,420,092
Foreign banks	10,892
China's banks	0
Trust investment company	0
Credit cooperative	123,450
Credit Department of National Farmers' and Fishman's Association	260,886
Postal remittances and savings	271,642
Reports in writing (Financial institution - local bank)	0
Reports in writing (Financial institution - foreign bank)	0
Reports in writing (Financial institution - China's bank)	0
Reports in writing (Financial institution - Farmers' association)	0
Reports in writing (Financial institution - Fishermen's association)	0
Reports in writing (Financial institution - Others)	11
Insurance company	5,876
Reports in writing (Insurance)	1
Reports in writing (Jewelry shop)	135
Other financial institutions	0
Total: 3,092,985	

Table 09: Statistics of CTRs in the last 5 years

Year	2015	2016	2017	2018	2019
Number of Reports	3,934,708	3,712,685	3,543,807	3,207,299	3,092,985

Figure G: Statistics on CTRs in the last 5 years

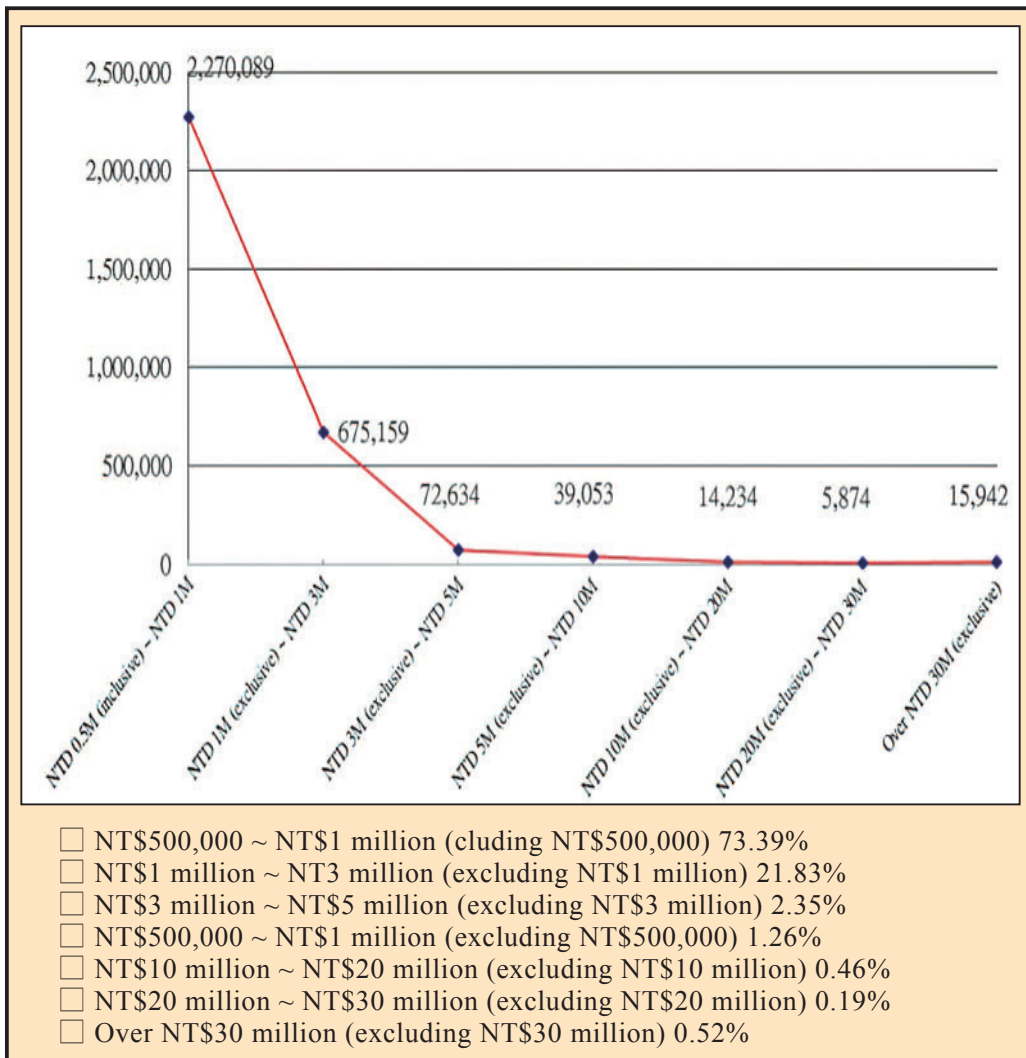


## II. Distribution of CTRs by Amount

Table 10: Distribution of CTRs by Amount in 2019

Amounts	Number of Reports
NT\$500,000 ~ NT\$1 million (including NT\$500,000)	2,270,089
NT\$1 million ~ NT\$3 million (excluding NT\$1 million)	675,159
NT\$3 million ~ NT\$5 million (excluding NT\$3 million)	72,634
NT\$5 million ~ NT\$10 million (excluding NT\$5 million)	39,053
NT\$10 million ~ NT\$20 million (excluding NT\$10 million)	14,234
NT\$20 million ~ NT\$30 million (excluding NT\$20 million)	5,874
Over NT\$30 million (excluding NT\$30 million)	15,942
Total: 3,092,985	

Figure H: Line Graph of CTRs Distribution by Amount in 2019



### III. Statistics of Accessing CTRs Database

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

Year	2015	2016	2017	2018	2019
Investigation Bureau of the Ministry of Justice	36,040	21,413	32,402	30,717	21,609
Other law enforcement agencies	5,641	13,012	17,929	29,153	19,236
Prosecution and court	8,987	5,186	9,051	6,628	3,252
Total transactions	50,668	39,611	59,382	66,498	44,097

## 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. 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.” A total of 39,855 ICTRs were reported to the MJIB in 2019. In terms of the declared value, 87.02% of ICTRs were below \$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.” The customs had reported 320,481 ICTRs (delivered items) to AMLD in 2019; 79.23% of which were imports, the total value of import declaration was over NT\$213 billion (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 2019

Departure and arrival	Count
Arrival	5,371
Departure	34,484
Total	39,855

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

Year	2015	2016	2017	2018	2019
Count	27,725	33,555	45,165	47,383	39,855

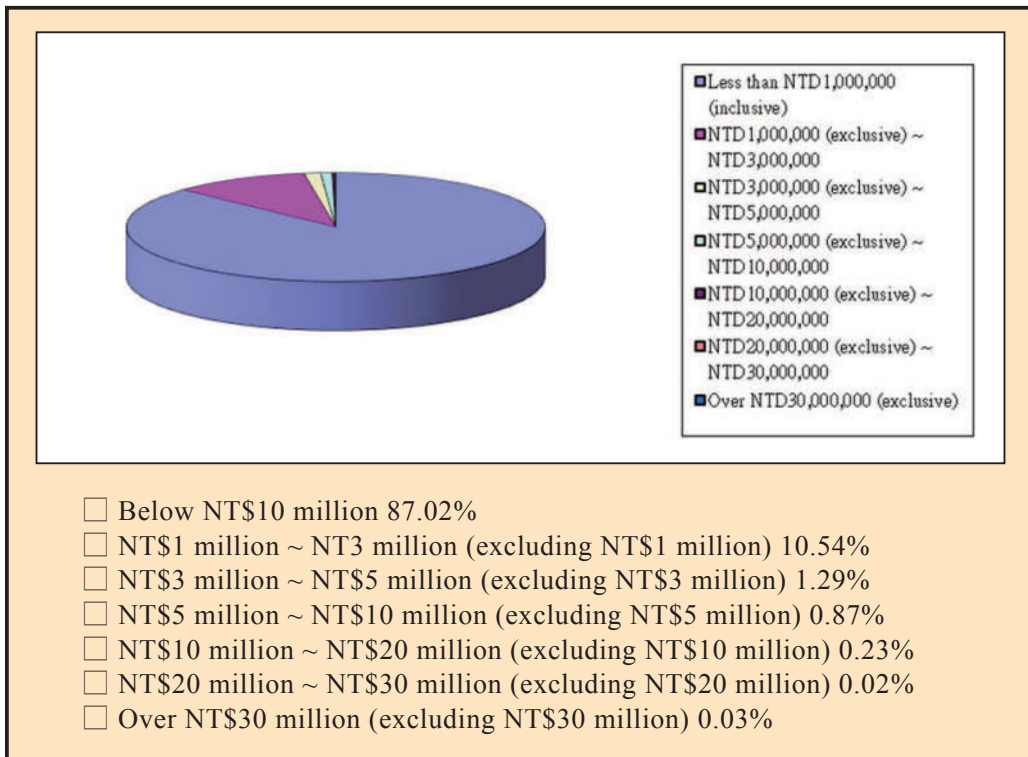


## II. Passengers' reports (including crew member) by Month

Table 14: Passengers' reports (including crew member) by month for 2019

Month	January	February	March	April	May	June
No. of Reports	3,318	3,603	3,534	3,690	3,952	3,367
Violations <sup>4</sup>	26	13	18	16	14	16
Subtotal	3,344	3,616	3,552	3,706	3,966	3,383
Month	July	August	September	October	November	December
No. of Reports	3,221	2,869	2,931	3,537	3,272	2,561
Violations	15	14	9	4	8	15
Subtotal	3,236	2,883	2,940	3,541	3,280	2,576

Figure I: Pie Chart of ICTRs Distribution by Value in 2019



<sup>4</sup> Unreported or false reports.

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

Table 15: Passengers' reports (including crew member) by value in 2019

Amount	Count
Below NT\$1 million	34,680
NT\$1 million ~ NT\$3 million (excluding NT\$1 million)	4,200
NT\$3 million ~ NT\$5 million (excluding NT\$3 million)	515
NT\$5 million ~ NT\$10 million (excluding NT\$5 million)	348
NT\$10 million ~ NT\$20 million (excluding NT\$10 million)	92
NT\$20 million ~ NT\$30 million (excluding NT\$20 million)	9
Over NT\$30 million (excluding NT\$30 million)	11
Total: 39,855	

### IV. Statistics of ICTRs (delivered items)

Table 16: Statistics of ICTRs (delivered items) in 2019

Import/export	Count
Export	66,574
Import	253,907
Total	320,481

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

Year	2017 (since June 28)	2018	2019
Count	151,657	290,084	320,481

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

Table 18: Statistics of the value of ICTRs (delivered items) in 2019

Import/export	Value (NT dollar)
Export	117,379,546,222
Import	213,004,843,477
Total	330,384,389,699

## VI. Distribution of ICTRs (delivered items) by Month

Table 19: Distribution of ICTRs (delivered items) by month in 2019

Month	January	February	March	April	May	June
Count	29,572	14,556	26,186	28,004	24,640	25,845
Month	July	August	September	October	November	December
Count	29,169	28,297	24,812	27,674	36,379	25,347

## 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, schools 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 money laundering has on the society and the importance to combat it.



■ MJIB's Taipei City Field division promoting AML awareness at "2019 Campus Recruitment Exposition of National Taipei University of Technology."

## 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 perform AML and CTF, improve the quality of STRs, and enhance identification of suspicious transaction patterns. 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 2019

Name of financial institution		Subtotal	
		Session	Participants
Banks	Local banks (including financial holding companies)	42	2,868
	Foreign banks	2	33
Credit cooperative		1	30
Credit Department of National Farmers' and Fishman's Association		9	854
Securities firms		9	1,661
Futures Merchant		3	425
Chunghwa Post for postal remittances and savings		1	128
Insurance companies		12	730
Designated non-financial business and profession		2	362
Total		81	7,091

## Five. Public-private sector coordination and strategic studies

### I. Participated in APG's 3rd Mutual Evaluation and received rating of "Regular follow-up"

The Asia/Pacific Group on Money Laundering (APG) held its 22nd annual meeting from August 17 to August 23, 2019, in Canberra, the capital of Australia, which saw participation of 520 representatives from 46 countries (regions) and 13 international organizations in total. Taiwan mission comprised representatives from Anti-Money Laundering Office (Executive Yuan), Financial Supervisory Commission, Ministry of Foreign Affairs, Central Bank, National Police Agency (Ministry of the Interior), and MJIB Hung-Chin Lee, former Director of AMLD, led a team of AMLD staff to represent MJIB in the mission.

Taiwan was one of the four nations, including Pakistan, Solomon Islands and the Philippines, to have Mutual Evaluation report adopted during the meeting, and in the morning of August 22, Taiwan received an unanimous approval of the 3rd Mutual Evaluation report and was awarded the rating of "Regular follow-up." According to the Mutual Evaluation report, "Largely Compliant" (LC) in 36 of the 40 Technical Compliance Ratings, and achieved "Substantial level of effectiveness" (SE) in 7 of the 11 Effectiveness Ratings. Amongst the 11 Effectiveness Ratings, IO 6 pertains to the effectiveness of a nation's FIU, and being the FIU of Taiwan, AMLD has demonstrated its competence throughout the assessment period on many different aspects, including the ability to provide the law enforcement agencies and administrative departments with adequate financial intelligence, the ability to bring value to analyses by incorporating new information technologies, and the ability to strengthen horizontal communication with the private sector. The assessment team and all APG members were highly impressed with the performance of Chinese Taipei's FIU, and therefore awarded the rating of "SE."

The "Regular follow-up" rating was not something that could be achieved in a short period of time; it involved as many as 37 institutions/departments from the public sector and 31 associations/institutions from the private sector, and took extensive level of preparation including 4 national risk assessment meetings, 2 public/private sector simulated evaluation meetings, preparation of Taiwan's "National Risk Assessment Report," "Technical Compliance Report" and "Effectiveness Evaluation Report," and successful completion of Mutual Evaluation pre-meeting, on-site evaluation and face-to-face meeting to accomplish. Taiwan will be submitting its first follow-up report in 2021 and undergoing official follow-up assessment in 2024. As the nation's FIU, AMLD will continue engaging local and foreign law enforcement agencies, supervisory authorities, and private sector reporting entities in more active exchange of information, while at the same time promote business innovation and create synergies through inter-department cooperation for better results.



- Taiwan mission at APG's 22nd Plenary Meeting, during which Taiwan received the outcome of its 3rd Mutual Evaluation and was awarded the best rating of "Regular follow-up."



## © 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 APG Mutual Evaluations, once in 2001 and once in 2007; both evaluation reports were approved in APG annual meeting, and Taiwan has been favorably recognized for its AML system. As Taiwan's FIU, AMLD received the highest rating that affirmed its competent functions. While undergoing APG's 3rd Mutual Evaluation, the evaluators were impressed with AMLD's ability to perform as an FIU and collaborate with international counterparts despite 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 "Chinese Taipei," and is allowed to participate in the FATF's affairs as an APG member.

## II. Assisted associations in the establishment of practical guidelines to improve the quality of STRs across different industries

To help reporting entities of different industries adopt risk-based approach and identify suspicious money laundering and terrorism financing signs, AMLD assigned personnel to participate in the "Legal Affairs and Compliance Committee Meeting" organized by Taiwan Securities Association on October 16, 2019, during which it offered advices on the amendment of Appendix - "Signs of Money Laundering, Terrorism Financing and Proliferation" contained within "Template for Guidelines Governing Anti-Money Laundering and Countering Terrorism Financing of Securities Firms"



and assisted in the amendment of AML/CTF practical guidelines. The newly revised "Signs of Money Laundering, Terrorism Financing and Arms Proliferation" is scheduled to be implemented on October 1, 2020. AMLD also assigned personnel to participate in the "2019 3rd Risk Division Meeting of Credit Card Business Committee" held by Bankers Association on October 17, 2019, during which it offered opinions on signs that are subject to STR and appropriate reporting practices for credit card issuers. These opinions were taken into consideration for the amendment of "Template for Guidelines Governing Anti-money Laundering and Counter Terrorism Financing for Credit Card Issuers," and the amended version was implemented in September 2020 with the approval of the Financial Supervisory Commission. On November 29, 2019, Taiwan Securities Association hosted its "Anti-money Laundering and Counter Terrorism Financing Compliance Forum Conference for Securities Firms" for a trainee size of approximately 300, and AMLD was invited to offer feedback on the STRs submitted by securities firms with the intention of improving the quality of reports submitted by securities firms.



■ Section Chief Chih-Cheng Chen of AMLD participated in the "Anti-money Laundering and Counter Terrorism Financing Compliance Forum Conference for Securities Firms" organized by Taiwan Securities Association on November 29, 2019.

### III. Organized conferences on criminal cash flow analysis and abnormal transaction patterns

According to the 2018 National Money Laundering and Terrorism Financing Risk Assessment Report, there were 8 major crime categories that posed very high level of money laundering risks to Taiwan, namely: drug trafficking, corruption/bribery, fraud, securities-related crime, third-party money laundering, tax-related crime, smuggling, and organized crime. Meanwhile, APG's 3rd Mutual Evaluation Report in 2019 highlighted the importance for government agencies such as FIU, law enforcement and customs to continually cooperate with FIs and DNFBPs on the sharing of threats, weaknesses and risk trends, and to assist the private sector in the adoption of risk-based approach. For this reason, AMLD coordinated with Banking Bureau of the Financial Supervisory Commission (FSC) and Taiwan Financial Services Roundtable and hosted "Conference on Criminal Cash Flow Analysis and Abnormal Transaction Patterns" on May 24, 2019 as a means to promote understanding toward high-risk crimes and raise AML capacity among FIs and reporting entities. A total of 140 AML specialists from 63 FIs had participated in the meeting. The conference began with opening speeches delivered by Deputy Director Hsiu-Yuan Chuang of FSC's Banking Bureau and Director Hung-Chin Lee of AMLD at the time. Former head of Financial Crime Prevention Division Jung-Chun Wu (currently Director of AMLD), investigator Shou-Yuan Kuo from Drug Prevention Division, and investigator Yi-Chun Lin from Anti-corruption Division then shared their practical experience on crime investigation, briefly explained the typical cash flow and abnormal transaction patterns involved in the 8 major crime categories that pose very high money laundering risks in Taiwan, including: share price manipulation, fraudulent cash issue, misstatement of financial report, illegal fundraising, illegal remittance, tax-related crime, drug-related crime, and corruption crime (e.g.: fraudulent claim of assistants' allowance, embezzlement, and bid-rigging), and gave an indication on the emphasis and

direction of MJIB's future investigation efforts. Deputy Director General Hsiu-Yuan Chuang hosted a Q&A session after the conference, during which the participants demonstrated a more in-depth understanding of crime and money laundering in the questions raised. Overall, the conference was deemed helpful toward identifying signs of suspicious transaction and improving the effectiveness of the reporting system.



- Group photo of former Director Hung-Chin Lee of AMLD (3rd from right), head of Financial Crime Prevention Division Jung-Chun Wu (currently Director of AMLD, 2nd from left), Section Chief Chih-Cheng Chen of AMLD (2nd from right), former Deputy Director General Hsiu-Yuan Chuang (currently the Director General) of Banking Bureau, Financial Supervisory Commission, and Deputy Secretary General Ming-Chi Hsu of Taiwan Financial Services Roundtable.

## IV. Organized coordination meeting with Financial Examination Bureau, Financial Supervisory Commission

On December 4, 2019, FSC's Financial Examination Bureau hosted a coordination meeting with AMLD to exchange opinions on the categories of STRs raised by FIs, the quality of reports, risk trends, and major defects discovered in Target examinations. The following issues were highlighted during the meeting and will be the focus of attention and discussion between the two parties in the future: (I) Investigate the reasons why "Other suspicious money laundering signs" remains one of the top-3 signs of suspicious transaction for banks, securities firms, and insurance companies; and (II) Develop signs of money laundering for OBU (Offshore Banking Unit) accounts, and help reporting entities improve the ability to identify money laundering, terrorism financing and financing of PWMD involving OBU accounts. AMLD maintains regular contact with Financial Examination Bureau and facilitates communication between the competent authorities, reporting entities, and law enforcement agencies. It has made noticeable contributions to the implementation of risk-based AML and CTF practices within the public and private sectors.

## V. Compilation of strategic analysis report on "corruption crime"

Corruption is one of the 8 very high risk crimes that Taiwan is prone to, but the number of related STRs has been low over the years. To help reporting entities develop the capacity needed to identify signs of corruption crime and money laundering activities, AMLD took the initiative to analyze the facts of crime and money laundering activities/cash flow in major corruption cases involving civil servants that MJIB and Agency Against Corruption, Ministry of Justice (AAC) had referred to prosecution between 2016 and 2018, assess the risk of FIs or DNFBPs being exploited for money laundering, analyze/

summarize STRs that AMLD had previously received on the abovementioned cases, and was able to produce a comprehensive list of suspicious signs and common money laundering patterns for different types of corruption, along with useful suggestions. The outcome was shared with reporting entities to provide reference for their STR filing.

### VI. Issued AMLD Press

Taiwan passed APG's 3rd 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 users. To further enforce 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 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.

## 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." AMLD makes use of Egmont Group's channels to exchange intelligence on money laundering, terrorism financing and PWMD with 163 countries worldwide. All intelligence gathered is analyzed and disseminated to accountable authorities for further actions. AMLD made 1,067 international exchanges of intelligence (including questionnaire) in 2019, up 20.15% from the 852 cases in 2018.

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

Task	Year	2015	2016	2017	2018	2019
Requests from overseas FIUs	Cases	51	50	55	47	71
	Reports	152	169	161	162	279
Requests to overseas FIUs	Cases	45	34	26	23	38
	Reports	222	165	94	107	292
Spontaneous exchange from overseas FIUs	Cases	32	25	53	99	81
	Reports	44	44	100	198	198
Spontaneous exchanges to overseas FIUs.	Cases	9	26	45	20	17
	Reports	18	45	94	46	50
Questionnaire and others	Cases	0	0	0	0	0
	Reports	201	262	354	339	248
Total	Cases	137	135	179	189	207
	Reports	637	685	803	852	1,067

## 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 between governments to effectively combat cross-border money laundering, terrorism financing, and financing of PWMD. On July 3rd, 2019, AMLD signed “Agreement Concerning Cooperation in the Exchange of Information Related to Money or Other Assets laundering, Associated Predicate Offences and Terrorism Financing” with the Superintendency of Banks through the Special Verification Intendancy (IVE), Republic of Guatemala in Hague, The Netherlands. Later in August 2019, AMLD traveled to Canberra, Australia, to take part in APG's 22nd annual meeting, during which it signed "Memorandum of Understanding Concerning Cooperation in the Exchange of Financial Intelligence Related to Money Laundering, Associated Predicate Offences and Terrorism Financing" with Independent State of Papua New Guinea, Democratic Republic of Timor-Leste, and Kingdom of Tonga. On October 4, 2019, AMLD signed "Memorandum of Understanding Concerning Cooperation in the Exchange of Financial Intelligence Related to Money Laundering, Associated Predicate Offences and Terrorism Financing" with Hashemite Kingdom of Jordan at an alternative location. By December 31, 2019, Taiwan had signed memorandums or agreements of similar nature with 50 countries or regions, which is a strong indication for the efforts and progress the nation has made to cooperate with international counterparts on AML/CTF matters.



- July 3, 2019 - Taiwan signed “Agreement Concerning Cooperation in the Exchange of Information Related to Money or Other Assets laundering, Associated Predicate Offences and Terrorism Financing” with the FIU of the Republic of Guatemala.

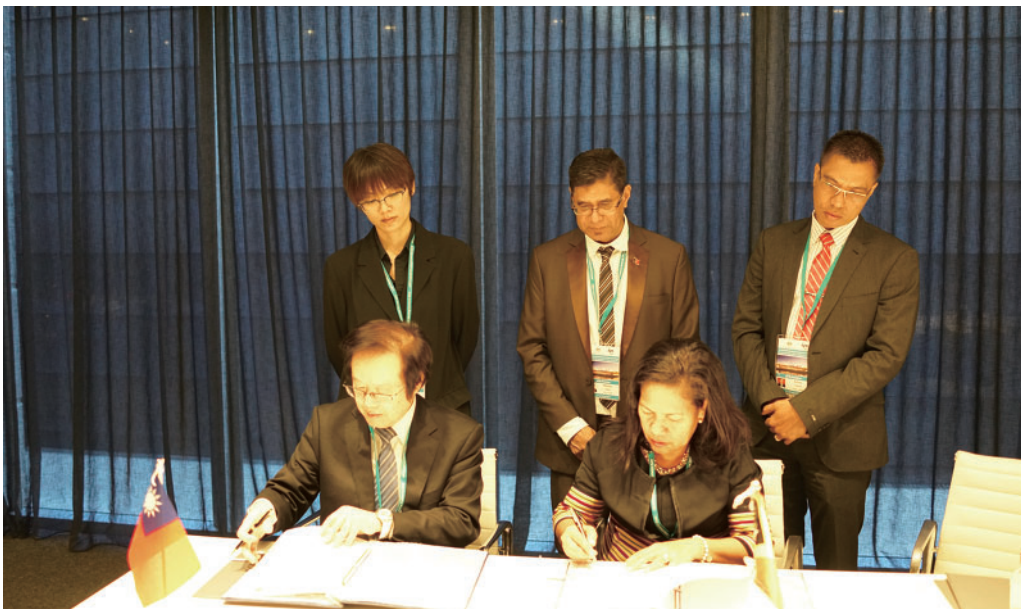


- August 20, 2019 - Hung-Chin Lee, former Director of AMLD, signed "Memorandum of Understanding Concerning Cooperation in the Exchange of Financial Intelligence Related to Money Laundering, Associated Predicate Offences and Terrorism Financing" with Kingdom of Tonga in Canberra, Australia.





- August 20, 2019 - Hung-Chin Lee, former Director of AMLD, signed "Memorandum of Understanding Concerning Cooperation in the Exchange of Financial Intelligence Related to Money Laundering, Associated Predicate Offences and Terrorism Financing" with Independent State of Papua New Guinea in Canberra, Australia.



- August 20, 2019 - Hung-Chin Lee, former Director of AMLD, signed "Memorandum of Understanding Concerning Cooperation in the Exchange of Financial Intelligence Related to Money Laundering, Associated Predicate Offences and Terrorism Financing" with Democratic Republic of Timor-Leste in Canberra, Australia.

### III. Participation in the 26th annual meeting of Egmont Group

Being a member of Egmont Group, Taiwan participates in Egmont Group Plenary each year. In 2019, AMLD represented Taiwan and participated in the 26th Egmont Group Plenary Meeting held at the World Forum in Hague, Netherlands, from July 1 to July 4. The theme of the meeting was: "Enhancing Public-Public cooperation from the perspective of an FIU" during which AMLD was invited by Egmont Group's Asia Pacific representative to make a special presentation on "The Operation, Benefits and Challenges of Coordinated Investigation between Prosecution, Police and FIU" and share with Asia Pacific members on AMLD's successful experiences, practices, challenges and opportunities in assisting the prosecution and police with cash flow analysis. This presentation was highly regarded among Egmont Group members. AMLD is actively involved in Egmont Group's missions; it helps the organization review eligibility for candidate FIUs in Asia Pacific, and works with FIU of France to provide the necessary guidance to bring FIU of Vietnam into the organization. With Egmont Group, AMLD is constantly looking for opportunities to cooperate and exchange intelligence with other member countries.



### © 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 since the 6th annual meeting in June 1998 and is currently named as Anti-Money Laundering Division (AMLAD), Taiwan. The organization has 163 state members so far that initiate intelligence exchange through a secure network. The AMLAD regularly participates in the plenaries and working group meetings organized by the organization; 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. As of the end of December 2019, an agreement or a memorandum had been signed with 50 countries.

## IV. Participation in No Money for Terror Ministerial Conference on Counter-Terrorism Financing

The Department of Home Affairs of Australia held its 2019 "No Money for Terror Ministerial Conference on Counter-Terrorism Financing" between November 7 and 8, 2019 at Melbourne Convention and Exhibition Centre, and a total of 65 missions were invited to participate, including ministers from 20 countries. Hung-Chin Lee, former Director of AMLAD, not only participated in the conference as head of FIU of Taiwan, but also made a presentation that

explained the nation's "public, private and partnership" framework on AML/CTF and introduced the audience to how AMLD has been assisting FIs with STR tracking and supporting supervisory authorities in the update of signs for money laundering and terrorism financing. Lee received high level of response from the audience for the presentation. AMLD kept up with the latest development of terrorism around the world by participating in all five main topics discussed throughout the conference, namely: "The evolving terrorist threat," "Global responses to terrorism financing," "Emerging technologies and terrorism financing risks," "Enhancing public-private partnerships" and "Not-for-profit organisations." It exchanged opinions with foreign ministers and staff on the topics discussed, and made pro-active efforts to learn successful experiences of other nations in combating terrorism, which will provide useful reference to the establishment of counter terrorism policies within Taiwan.



■ Hung-Chin Lee, former Director of AMLD, was invited to the 2019 "No Money for Terror Ministerial Conference on Counter-Terrorism Financing."

### V. Participation in the 6th annual conference of "Asset Recovery Inter-Agency Network of Asia/ Pacific"

"Asset Recovery Inter-Agency Network of Asia/ Pacific" (ARIN-AP) was founded in Seoul, Korea, on November 19, 2013 for the purpose of helping countries exchange intelligence on judicial matters and improving the overall outcome of judicial aid. As one of the founding members, Taiwan has designated Ministry of Justice as the secretariat responsible for maintaining contact with the organization. ARIN-AP's 6th annual conference was held in Ulaanbaatar, Mongolia, from September 23 to 24, 2019, which AMLD had participated. During the meeting, representatives from Taiwan, Australia and Pakistan made presentations and shared experience on the trace of criminal proceeds, whereas AMLD staff also exchanged opinions with representatives of other countries on issues such as cross-border collaboration and seizure of criminal proceeds. Through participation in various discussions, AMLD was able to learn useful techniques and experiences from other countries in their fight against new crimes, such as money laundering with crypto currency. This level of interaction and exchange helps strengthen communication with foreign counterparts and expands law enforcement reach of Taiwan.



■ Staff of AMLD at the 6th (2019) annual conference of "Asset Recovery Inter-Agency Network of Asia/ Pacific."

## VI. Participated in FATF's 3rd Plenary Meeting and Work Group Meeting of the 30th year

Financial Action Task Force (FATF) is an international organization founded during the 1989 G7 Summit in Paris with the responsibilities of setting global standards on AML and CFT. FATF's 3rd Plenary Meeting and Work Group Meeting for the 30th year was held between June 16 and June 21, 2019 at the International Conference Room of Wyndham Hotel in Orlando, USA. This meeting took place at a time when Taiwan was preparing for APG's 3rd Mutual Evaluation, and due to the prominent nature of this international meeting, AMLD participated for the entire duration of the plenary and work group meetings, and kept up to date with the latest international standards on CFT, anti-proliferation of arms, supervision of virtual assets, and financial investigation guidelines on virtual assets. AMLD also took into consideration how FATF members had reviewed the Mutual Evaluation Reports of Greece and Hong Kong to develop responses for Mutual Evaluation of Taiwan in the future.



## Part III

### Significant Case Studies



- One. Violations against the Banking Act and Money Laundering Control Act- Loan Fraud**
- Two. Violations against the Banking Act and Money Laundering Control Act- Illegal Remittance**
- Three. Violations against the Banking Act- Illegal Fundraising**
- Four. Violations Against the Criminal Code- Unredeemable Checks**



# One. Violations against the Banking Act and Money Laundering Control Act- Loan Fraud

## I. Case summary

### (I) Source of intelligence

Following an analysis of financial intelligence in June 2019, AMLD found that: A group of related companies A, B, C and D (collectively referred to as Corporate Group A) had been defaulting on accounts receivable financing repayments since May 2019, and there were instances where transactions of different companies were handled by one employee or made under the name of a different payer. Due to the suspicious nature of such transactions, AMLD produced an analysis report and disseminated it to law enforcement agencies.

### (II) Suspect

O-Hu Yang, O-Chih Wang, and O-Ju Lin of Corporate Group A; O-Tang Huang of Company E; O-Ming Chiang of Company F; O-Kang Li of Company G; O-Lung Yao of Company H; O-Ta Liu of Company I; O-Ting Ou of Company J; O-Ching Hsieh of Company K; O-Hsien Tsai of Company L; O-Cheng Hsiao of Company M; O-Kuei Hsiao of Company N; and O-Hsi Huang of Law Firm P.

### (III) Involvement

Person-in-charge, managers, directors and employees of Corporate Group A including O-Hu Yang had conspired with people who had fiduciary duties to shareholders in Company E (domestic) and Subsidiary Q of Company F (offshore), and used offshore paper company R that O-Hu Yang and O-Chih Wang had registered in Belize in an attempt to defraud banks, while knowing that no actual transaction took place between Corporate Group A and the abovementioned companies. The scheme began with O-Hu Yang and O-Chih Wang instructing employees to

forge documents including fictitious sales contracts, invoices and shipping orders between Corporate Group A and Company E et al., which created the illusion that the group was doing business with Company E and others. Company E then assisted Corporate Group A by issuing fictitious bills of lading. With sales contracts, invoices and bills of lading in place, O-Chih Wang and O-Hu Yang presented the above documents and applied for accounts receivable financing and export loan facilities from a total of 9 banks including Bank X. In addition, O-Chih Wang issued a letter of guarantee in favor of the negotiating bank under the name of Corporate Group A, promising to repay the full outstanding balance if customers fail to make payment, while O-Tang Huang et al. of Company E helped complete the bank's standard procedures including plant visit, transfer of debt entitlement, and due diligence. The above steps were taken to deceive employees of Bank X into believing that real transactions had taken place between the companies, and loans were disbursed as a result. When the accounts receivable that Corporate Group A and Company E et al. claimed to have existed between them were due to be collected for repayment to the bank, O-Hu Yang and O-Chih Wang either withdrew or instructed employees to withdraw cash from Corporate Group A's account and had it wire-transferred by Company E et al. as repayment for loan principals owed to the bank; alternatively, employees were sometimes instructed to wire-transfer funds to the account of an overseas company, from which they were used to repay loan principals. All above arrangements were made to create fictitious transaction and cash flow between Corporate Group A and its counterparties. In May 2019, Corporate Group A began exhibiting signs of default such as failure to repay domestic L/C and export loan balance, late collection of financed receivables etc. It was when the lending bank started collecting debt from business partners of Corporate Group A that it discovered the absence of underlying transaction, at which time the bank had lost contact with O-Hu Yang and O-Chih Wang et al. and Corporate Group A had ceased operations.

Corporate Group A had defrauded the bank for proceeds totaling

NT\$38.6 billion using the above method. In an attempt to conceal illegitimate proceeds gained from fraudulent loans, O-Chih Wang purchased 16 real estate properties located in Nantou County, Taipei City and Hsinchu County under the names of O-Chen Yang, O-Hai Yang, O-O Yang Liao, O-Cheng Hsiao, and O-Ju Lin, while at the same time retained actual ownership over such assets. In addition, law practitioner O-Hsi Huang was found to have discussed with O-Chih Wang et al. in regards to the fraudulent loan on several occasions since April 2019, and accepted NT\$12.5 million of fraudulent loan proceeds from O-Chih Wang et al. in April and May 2019 using Huang's own account and the account of Law Firm P in which Huang served as the lead attorney, while having knowledge of Corporate Group A's scheme to defraud multiple banks. After O-Chih Wang and O-Hu Yang had fled the country in early June 2019, O-Chen Yang, O-Ru Lin, and O-Fen Chuang assisted in the concealment of fraudulent loan proceeds by making consecutive cash withdrawals from Corporate Group A's account over counter, and transferred more than NT\$20 million of criminal proceeds to various accounts owned by Law Firm P, Company M, O-Chen Yang, O-Ju Lin, and O-Jung Hsiao (controlled by O-Kuei Hsiao). Furthermore, NT\$6 million of cash was placed inside the safe deposit box leased by O-Cheng Wang (O-Chen Yang's boyfriend) at Bank Y as part of the attempt to conceal criminal income and avoid investigation.

After conducting thorough investigations, searches and interrogations, the law enforcement department was able to seize properties in various forms including cash, bank deposit, real estate, and vehicle. An order of arrest was issued on O-Hu Yang and spouse, who had fled the country before the fraud was uncovered. In early January 2020, the prosecutor prosecuted O-Hu Yang and spouse for violation against the Banking Act, Business Entity Accounting Act and Money Laundering Control Act, and criminal breach of trust. Through assistance in different channels, the law enforcement department was able to extradite O-Hu Yang and spouse back to Taiwan for trial between January and March 2020.

## II. Signs of suspicious money laundering

Customers who make frequent transfers of funds between different accounts above a certain amount; customers who make frequent deposits or withdrawals on behalf of others, or accounts that are frequently deposited or withdrawn by a third party for a certain amount and above; customers who make unusual deposit above a certain amount; customers who frequently transfer funds to another party in the same country or region, or to the payer's account in another country or region, immediately after receiving proceeds above a certain amount from a foreign source; a party who has been reported on TV, newspaper, magazine or online media for having involved in an extraordinary event approaches a bank for transactions such as deposit, withdrawal or remittance, and the transactions conducted are apparently unusual; other suspicions for involvement of money laundering activity.

## III. Indictment

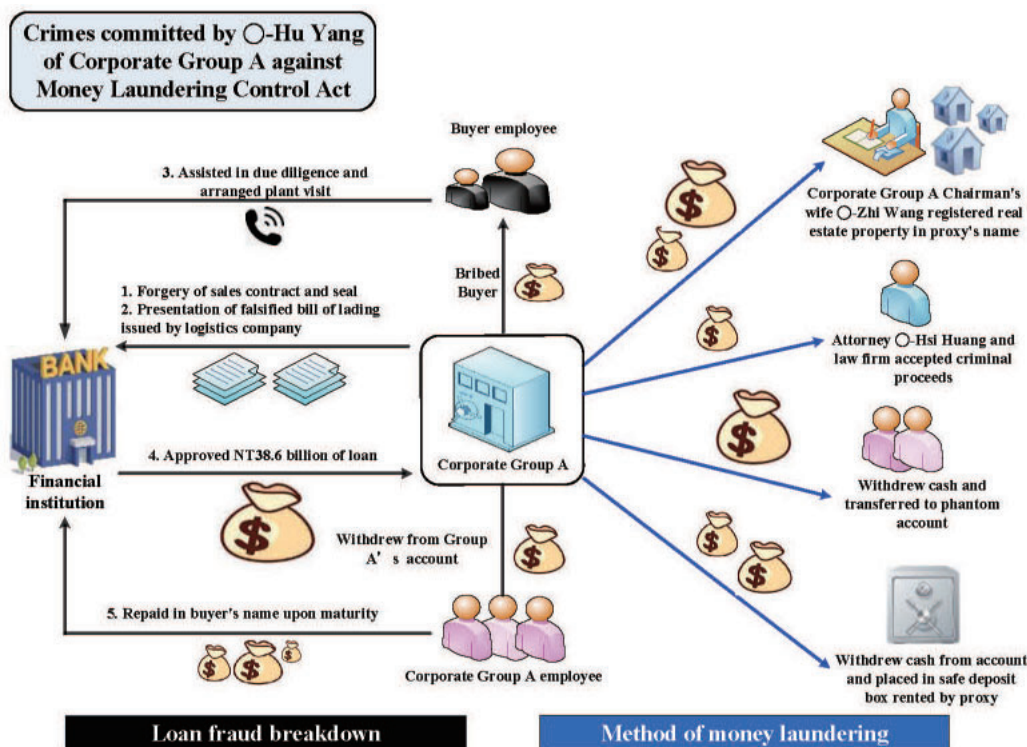
On January 9, 2020, Taipei District Prosecutors Office prosecuted O-Hu Yang, O-Chih Wang and associates for violations against the Banking Act, Business Entity Accounting Act, Securities and Exchange Act and Money Laundering Control Act, and for criminal breach of trust.

## IV. Experience reference

The case involved frequent withdrawal of cash from Corporate Group A's bank account followed by immediate transfer of proceeds through a related company to another account at a different bank held in the same as that of the origin account. These transactions were part of Corporate Group A's attempt to disguise its capital as proceeds received from outsiders, and the fact that transactions of different companies were handled by the same person conformed with the following signs of money laundering: customers who make frequent transfers of funds between different accounts above a certain amount; and customers who make frequent deposits or withdrawals on behalf of others, or accounts that are frequently deposited or withdrawn by a third

party for a certain amount and above.

The attempt by Corporate Group A to conspire with wrongdoers at renowned enterprises and logistics companies in defrauding FIs had been reported as suspicious transactions, as some reporting entities noticed abnormality in Corporate Group A's repayment pattern and fictitious details in some of the transaction documents presented for financing. After the news was covered by media, other reporting entities began contributing financial intelligence, which conformed with the following signs of money laundering: a party who has been reported on TV, newspaper, magazine or online media for having involved in an extraordinary event approaches a bank for transactions such as deposit, withdrawal or remittance, and the transactions conducted are apparently unusual; and other suspicions for involvement of money laundering activity.



## Two. Violations against the Banking Act and Money Laundering Control Act- Illegal Remittance

### I. Case summary

#### (I) Source of intelligence:

MJIB received report that: O-Chen Sun had received package from the Mainland containing information such as online banking login and password, as well as items including UnionPay Cards and USBKey, for a large number of phantom accounts that could be used to engage in illegal remittance service.

#### (II) Suspect:

O-Lin Wu, O-Jui Chen, O-Hung Huang, O-Chen Sun, O-Fu Liu and O-Feng Peng

#### (III) Involvement

O-Lin Wu and spouse O-Jui Chen, along with O-Lin Wu, O-Jui Chen, O-Hung Huang, O-Chen Sun, O-Fu Liu and O-Feng Peng, had been conducting the following illegal remittance activities since December 2017 despite knowing that non-banking institutions are not permitted to perform currency exchange service locally or abroad unless otherwise specified by law:

1. O-Lin Wu instructed O-Chen Sun and O-Fu Liu to purchase bank accounts (along with online login, password, UnionPay Cards and USBKey) in the Mainland at NT\$15,000 or above per account for the purpose of illegal remittance.
2. Customers who wished to remit funds from Taiwan into the Mainland would first make rate inquiries with O-Lin Wu, O-Jui Chen, O-Chen Sun, and O-Fu Liu over WhatsApp; O-Lin Wu et al. then replied with a quotation for the amount (in NTD) payable by applying a 2%

margin on top of current day's RMB board rate quoted by FIs. Once an agreement is reached between two parties, O-Lin Wu et al. would instruct O-Jui Chen, O-Chen Sun and O-Hung Huang to collect NTD payment and details of the destination account in the Mainland from customer. O-Lin Wu then instructed O-Feng Peng through O-Hung Huang to have funds transferred from a Mainland account that they had acquired into customer's designated account over online banking, and completed the currency exchange without going through proper channels. For customers who wished to remit funds from a foreign location into Taiwan, O-Lin Wu et al. would withhold a 2% margin from the calculated exchange rate and notify customers the amount of NTD currency they may receive. Once O-Feng Peng confirmed having received customer's RMB payment into one of the Mainland accounts that O-Lin Wu et al. had acquired, O-Lin Wu would instruct O-Jui Chen, O-Chen Sun, O-Fu Liu, and O-Hung Huang to deliver the agreed amount of NTD to customer in cash and in person.

3. O-Lin Wu's crime syndicate had completed approximately NT\$12,400,890,512 of illegal remittance and earned 2% of illegal income from the above sum. All NTD cash that O-Lin Wu et al. had collected from customers seeking to remit funds into the Mainland from all over Taiwan was placed under the custody of O-Jui Chen, and was used to meet NTD payments for customers seeking to remit funds from the Mainland into Taiwan. In an attempt to conceal criminal proceeds, O-Lin Wu et al. stashed NT\$239,992,600 of cash at the residence of O-Chin Wang (O-Jui Chen's mother) in Chiayi County. This cash was found and seized by MJIB during the search at O-Chin Wang's residence, and the prosecutor later prosecuted O-Lin Wu et al. for violations against the Banking Act and Money Laundering Control Act.

### II. Signs of suspicious money laundering

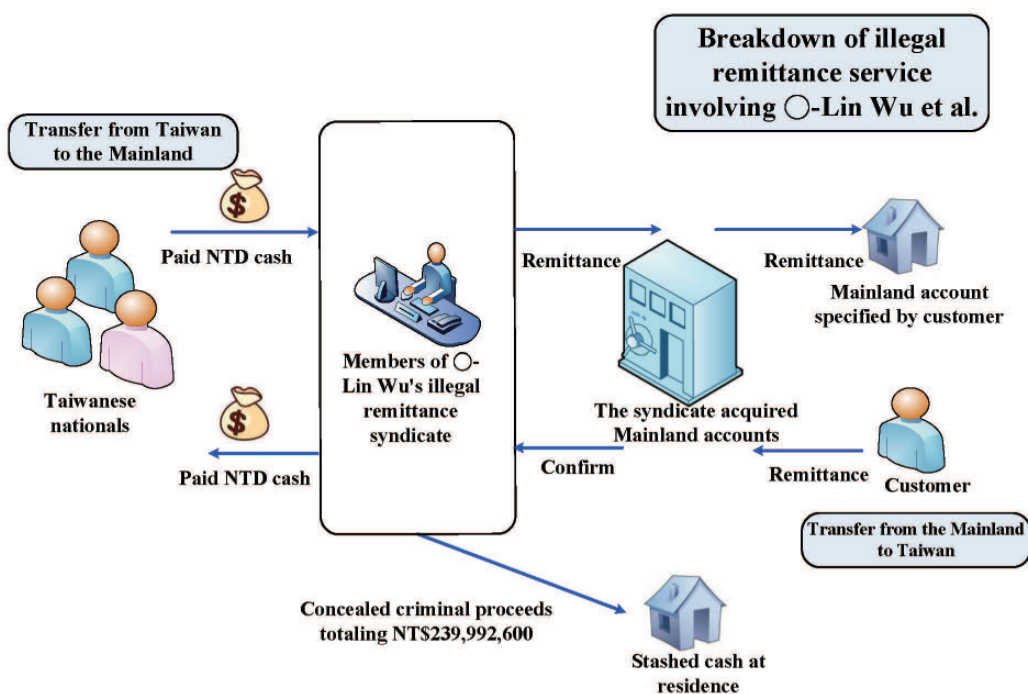
O-Lin Wu et al. possessed large sums of cash of unknown purpose and origin, which was a sign of money laundering.

### III. Indictment

In December 2019, Taiwan Chiayi District Prosecutors Office prosecuted O-Lin Wu et al. for violations against Paragraph 1, Article 29 of the Banking Act, Paragraph 1, Article 3 of Organized Crime Prevention Act, and Paragraph 1, Article 14 of Money Laundering Control Act.

### IV. Experience reference

The fight against money laundering or other crime requires coordination from different law enforcement agencies and FIs, as intelligence provides the grounds while authority provides the means to act against crime. In this case, the criminal activities were first uncovered during a regular customs inspection; the inspection led to the discovery of one suspicious package from the Mainland that contained information and UnionPay Cards relating to dozens of phantom accounts in the Mainland. After conducting a series of investigations, MJIB was able to establish involvement of O-Lin Wu et al. in illegal remittance. This case had been an example of successful collaboration between law enforcement departments.





# Three. Violations against the Banking Act- Illegal Fundraising

## I. Case summary

### (I) Source of intelligence

When analyzing financial intelligence in December 2018, AMLD discovered that: Taiwan nationals O-Cheng Chiu and spouse O-Chun Chiu, who served as persons-in-charge for Construction Companies B and C, respectively, exhibited frequent large cash deposits and frequent cash inflows of unknown origin in their accounts, and were suspected of abnormal transactions after multiple records of returned check. AMLD then produced an analysis report and distributed it to accountable units for reference.

### (II) Suspect

O-Cheng Chiu and O-Chun Chiu.

### (III) Involvement

Despite knowing that non-bank institutions and individuals are not permitted to accept deposits or raise funds from multiple, random parties by agreeing to pay dividends or interests that are disproportionate to the principals, whether in the form of investment or loan, O-Cheng Chiu and O-Chun Chiu had intentionally committed violation against the Banking Act solely to raise funds for payment of construction expenses and credit card bills. Between 2010 and 2018, the above parties raised funds from more than 30 random individuals, claiming that the capital would be invested into construction projects with the promise to pay interests at 18% to 27.75% per annum. In addition to hosting investor seminars and soliciting capital from investors personally, O-Cheng Chiu also paid commissions as encouragement for company employees and investors to bring others into the scheme. They even designed investment packages of different tiers and profit profile. O-Cheng Chiu and O-Chun Chiu would

accept proceeds from investors through account transfer or cash, and issue post-dated checks for the promised principal and interest. When an investment matured, investor would first confirm with O-Cheng Chiu on the method of principal and interest payment, and either present the check to O-Cheng Chiu for cash or deposit the check into bank account as per instruction. For investors that had no urgent need for cash, O-Cheng Chiu would convince investors to continue investing principal for interest or retain principal and interest while top up for higher tier of investment package. For this reason, O-Cheng Chiu incurred no cash outlay and was able to raise additional capital from investors simply by replacing old checks with new ones. In December 2018, the banks denied O-Cheng Chiu's loan request, causing liquidity shortage followed by a cascade of check returns. At which time, O-Cheng Chiu and O-Chun Chiu had raised a total of NT\$312,850,000 from investors through illegal means.

## II. Signs of suspicious money laundering

Multiple and frequent cash deposits aggregating to a certain amount or volume that were quickly transferred afterwards; and deposits that are shortly followed by withdrawals of equivalent amount aggregating to a certain sum and above.

## III. Indictment

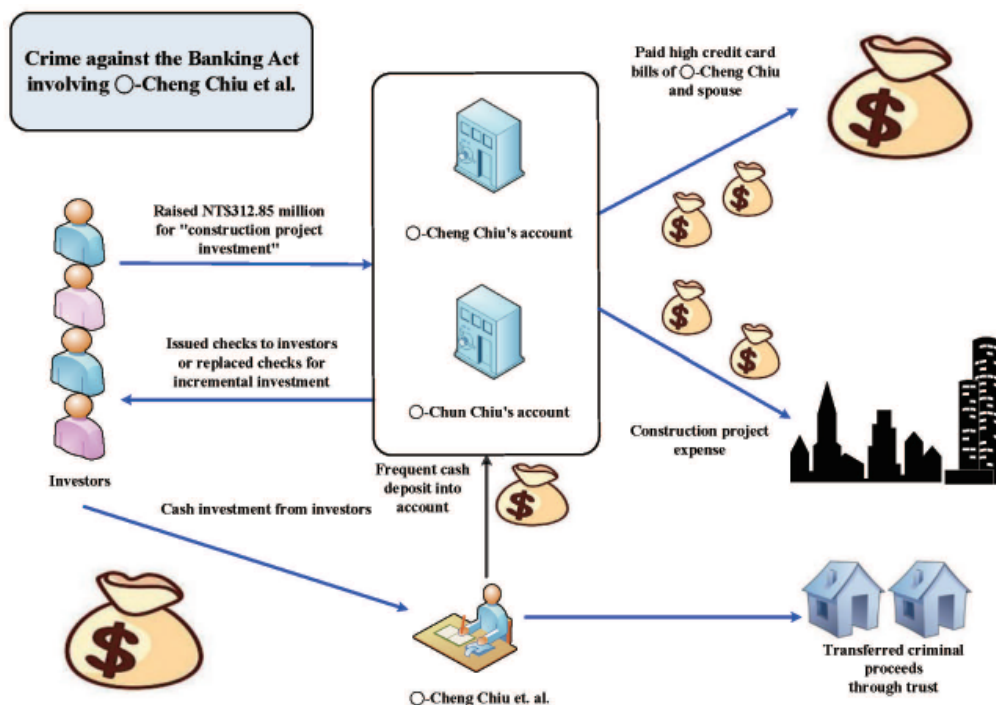
In May 2019, Taiwan Taoyuan District Prosecutors Office prosecuted O-Cheng Chiu for violations against Articles 29 and 29-1 of the Banking Act and for the crimes described in Paragraph 1, Article 125 of the Act.

## IV. Experience reference

(I) Bank K was vigilant of signs such as large cash deposit, frequent wire transfer, and check return involving its customers, and had been filing reports consistently to aid in the investigation of cash flow and illegal

fundraising. After the scam was exposed by the media, Bank K shared its intelligence immediately, which proved helpful to the trace of criminal proceeds afterwards.

(II) A construction company requires substantial capital during the construction period. Aside from banks and private lending, companies that are desperately short on liquidity may resolve to raise funds illegally from random subjects. Accounts used for such a scam are generally characterized by complex and unexplained source of fund, and each deposit is often followed shortly by withdrawal of similar amount, and therefore accumulate transactions above a certain amount or volume within a short period of time.



## Four. Violations Against the Criminal Code- Unredeemable Checks

### I. Case summary

#### (I) Source of intelligence

Following an analysis of financial intelligence in June 2016, AMLD found Taiwan nationals O-Chien Liao and O-Yang Chen having issued NT\$7.13 billion worth of checks in 2016 that were all returned on a later date. AMLD also found that only company phone number was specified as contact number for the accounts used, and an analysis report was prepared and sent to law enforcement agency for further investigation into the abnormality.

#### (II) Suspect

O-Liang Lin and O-Lai Ho et al.

#### (III) Involvement

O-Liang Lin and O-Lai Ho et al. had set up shell companies with the intent to defraud for gains by knowingly issuing checks that could not possibly be redeemed. The offenders first began their scheme by registering relatives O-Yang Lin and O-Wei Lin as persons-in-charge for shell companies, and then paid NT\$150,000 to NT\$600,000 for each third party they found who were willing to be registered as person-in-charge. With the help of professional bookkeepers O-Nu Cheng and O-Hsin Chang, the offenders founded 22 shell companies that conducted no business activity whatsoever, including Company Shen O, Company Chia O, Company Kuai O Enterprise, Company Po O, Company Hsin O Ta, Company Yi O, Company Shen O, Company Chueh O, Company Chuang O Enterprise, Company Hsien O Enterprise, Company San O Enterprise, Company San O Enterprise, Company Chia O, Company Kai O, Company Shan O Construction, Company Ho O, Company Te O, Company Yin O,

Company Po O Enterprise, Company San O Construction, Company Ting O, and Company Chia O. Persons-in-charge of the above shell companies then applied for bank accounts and passbooks for the respective companies, and requested for check books from each FI. All blank checks were stamped with the authorized seal of the respective shell company, and later sold by O-Liang Lin at NT\$2,800 per check to distributors including O-Lai Ho. O-Lai Ho subsequently resold the checks to buyers who, despite knowing that the checks could not possibly be redeemed, had the intention to defraud innocent third parties by presenting them for purchase, borrowing or debt repayment. It was not until the bearer presented the check for payment at a FI that the check was returned due to insufficient funds and the bearer realized having fallen victim to a scam.

The creation of 22 shell companies and sale of unredeemable checks yielded O-Liang Li et al. a total of NT\$11,441,600 in criminal proceeds. 3,172 checks with a total amount of NT\$5,014,925,754 were presented for payment and returned. The law enforcement department was able to seize NT\$3,561,520 of property placed under O-Liang Lin and associates.

## II. Signs of suspicious money laundering

Customer who issues checks above a certain amount on a cumulative basis is a sign of money laundering.

## III. Indictment

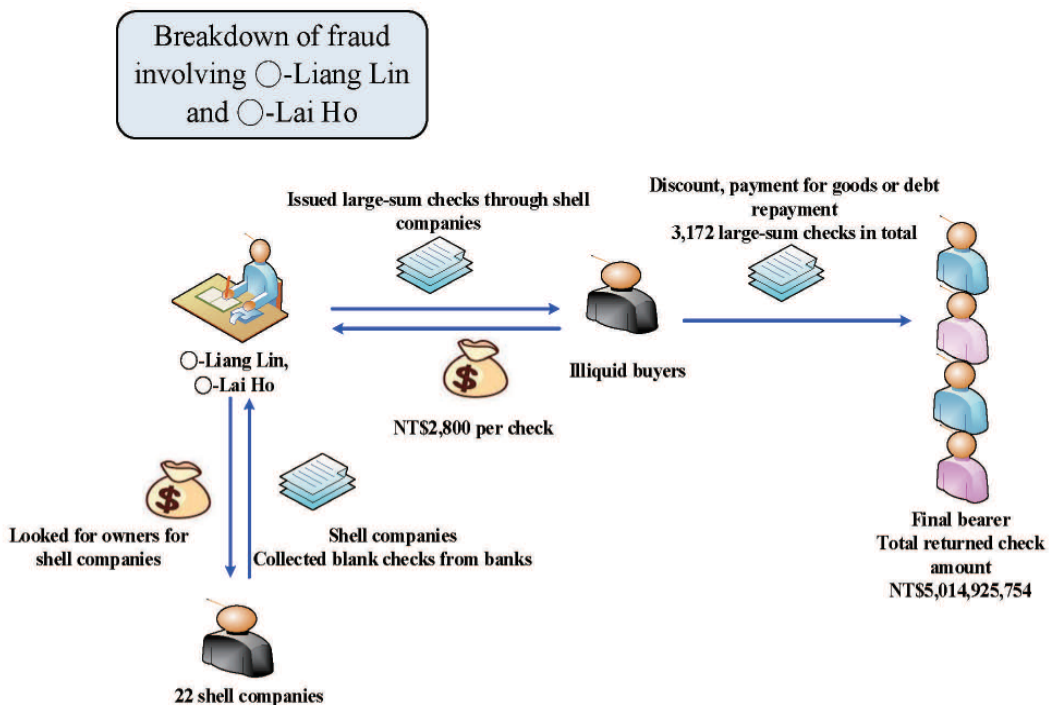
In August 2019, Taiwan New Taipei District Prosecutors Office prosecuted O-Liang Lin, O-Lai Ho, O-Chang Hsieh, O-Hsiung Tan and O-Kai Lu for fraud under the criminal code and for violations against The Company Act.

## IV. Experience reference

Bank accounts of the shell companies often had small, round-figure

deposits followed by cash withdrawals over automated equipment, and only a small balance is maintained. This pattern conforms with the sign - "deposits followed shortly by withdrawals of equivalent amount," and is unusual compared to the account activities of a normal business.

FIs shall gain insight into customers' business operations and conduct due diligence assessments when establishing banking relationship. Corporate customers seeking to apply for check accounts shall have trade counterparties and authenticity of underlying transactions checked thoroughly to avoid negotiable instruments being misused for illegal purpose.





## Part IV

### Project Research



**The International trends on counter proliferation financing and the current implementation of Taiwan- The case studies with the investigation on the Taiwanese citizen who becomes a financier for North Korea**



# **The International trends on counter proliferation financing and the current implementation of Taiwan- The case studies with the investigation on the Taiwanese citizen who becomes a financier for North Korea**

Kai Ting Ho<sup>5</sup>

## **Abstract**

With the fact that the Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT) and Countering the Proliferation Financing (CFP) issues have become crucial all over the world in recent years. The circumvent sanctions on the Weapon of Mass Destruction (WMD) and illicit procurement are also vital in the CFP issue. During 2018, one Taiwanese citizen and its related entities have been designated into the United Nations Security Council Resolution (UNSCR) 1718 sanction list due to the violation of proliferation financing with the Democratic People's Republic of Korea ("DPRK" or "North Korea"). Despite of the fact that Taiwan is not a member of the United Nations, Taiwan still voluntarily follows and implements the relevant UNSCRs as members of the international community. Besides, Taiwan is located in the Asia-Pacific trading hub, providing the conveniences of the shipping transportations and trade business. The geography also exposes the possibility that the shell or front companies and intermediaries may deceive and exploit the Taiwanese traders to conduct ship to ship transfers for North Korea, as well as continuously assisting with circumvention of the sanction nexus. Consequently, the CFP mechanism in Taiwan has become a key concern in the international community. In the same

---

<sup>5</sup> An investigator in the central region mobile team, Ministry of Justice Investigation Bureau.

vein, how to keep up to date with the obligation of UNSCRs, concerning CFP and the implementation of the duties stipulated in the Counter-Terrorism Financing (Taiwan) Act 2018 (CTFA), rely on the public-private cooperation. Only by enhancing the awareness on the UNSCRs and understanding the legal obligations can we successfully avoid being exploited by offenders taking advantage of our political status quo to finance North Korea or other designated entities as well as to develop WMD.

## I. The Introduction and the Background

During 2018, the Ministry of Justice (MOJ) had designated two Taiwanese citizens to the officially published sanction lists. Due to the fact that these two Taiwanese citizens involved in the illicit trade with North Korea in January and March 2018 respectively (MOJ, 2018). After the MOJ published the sanction list, the Financial Institutions (FIs) and Designated Non-Financial Business or Professions (DNFBPs) would immediately conduct Customer Due Diligence (CDD) on their customers, restrict the designated targets' financial resources and assets, and implement the reporting obligation as well. The duties were pursuant to the Money Laundering Control (Taiwan) Act 2018 (MLCA) and CTFA. The goal is to limit the usage of all financial resources of the targeted individuals and entities comprehensively. The CFTA has been promulgated for four years since 27th July 2016; however, owing to the fact that the content referring to the relevant UNSCRs is not close to Taiwanese daily lives, plus Taiwan is yet to be a member of the UN, Taiwanese citizens may be unfamiliar with international standards and the legal obligation of CTFA. Under this circumstance, Taiwanese people could possibly misunderstand and break the legal provisions. This article attempts to give an overview introduction of the CFP international standards, the domestic legal framework and case studies, with implied for the reference for the future CFP policy and practical operation.

## II. The International Standards of the CFP

According to the Charter VII of the UN, which authorized the power to the Security Council. Article 39 of the Charter VII, which has indicated that the Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken (UN, 2020). In other words, the Security Council can make relevant Resolutions and call for the member states to implement universal duties. To prevent an aggravation of the situation, the Security Council may take provisional measures, with recommendations or deciding the actions which can impose the economic sanctions. According to the Article 41 of the Charter VII, the economic sanctions including complete or partial interruption of economic relations and rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations (UN, 2020). Besides, under the economic sanctions were inadequate or have proved to be insufficient, it may take such action by air, sea, or land forces, blockade, and other operations by military actions, which was abided by the Article 42 of the Charter VII (UN, 2020).

In terms of the CFP issue, the UN has adopted a two-tiered approaches, which are “Global Approach” (Broad-Based Provisions) and “Country-Specific Approach”, which refer to North Korea and Iran (Erol & Spector, 2017; FATF, 2018). This article only focuses on the CFP on North Korea with the explanation on relevant UNSCRs and recommendations of the Financial Action Task Force.

### A. The UNSC and relevant resolutions (Beekarry, 2013; FATF, 2018; UN, 2020):

The global approach is pursuant under UNSCR 1540 (2004) and its successor resolutions. To call for the member states and Non-State Actors which means “for those organizations and individuals that have no affiliation with the government and are not guided or funded by the government (NSCR-NET, 2020)” shall prohibit from involving in the proliferation of financing activities. Also, to establish the adequate

scrutinization and control mechanism on those providing funds and services on facilitation of the WMD proliferation, such as financing, related to the export and trans-shipment of items are necessary (Erol & Spector, 2017; FATF, 2018).

Country-Specific Approach is pursuant under UNSCR 1718 (2006), 2231 (2015), and its successor resolutions which refer to the CFP on North Korea and Iran respectively. The apparent difference between Iran and North Korea on the CFP is that during 2015, the UNSC has terminated the UNSCR 1737 and its successor resolutions, with replace it by the UNSCR 2231 and maintain some Targeted Financial Sanctions on those designated individuals and entities. In contrast, with noting that North Korea continually conduct nuclear and missile program test, which provoked and violated the UNSCRs, therefore currently the UN still enhance the sanction power on North Korea.

Different from UNSCR 1540 (2004), which focused on the control measure on export and transit, the UNSCR 1718 (2006) was the UN to response North Korea's first nuclear test, and emphasis on economic and commercial sanction especially. The successor resolutions included 2087(2013), 2094(2013), 2270(2016), 2321(2016), 2356(2017), 2371(2017), 2375(2017) and 2397(2018). Sanctions can be approximately divided into two types:

i. Targeted Financial Sanctions (TFS)

According to the glossary in FATF methodology, the definition of TFS means “The term targeted financial sanctions means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities (FATF, 2013-2019, p187)”. The corresponded legal basis in Taiwan is Article 7 of CTFA.

ii. Other sanction measures (North Korea only)

- (i) The embargo on weapons, other weapons of mass destruction and other related materials;
- (ii) Travel ban;
- (iii) Interception and transportation inspection on the sea;

- (iv) Prohibition sanctions vessels from entering the ports and providing petroleum services on the sea;
- (v) Prohibit DPRK from supplying, selling or transferring coal, iron, iron ore, gold, titanium ore, vanadium ore, copper, nickel, silver, zinc, rare earth minerals, lead, lead ore, steel, other metals, food, agricultural products, machinery, electric equipment, earth and stone including magnesite and magnesia, wood, vessels, industrial machinery, transportation vehicles, seafood (including fish, crustaceans, mollusks, and other aquatic invertebrates in all forms), textiles, statue and helicopters;
- (vi) Prohibit North Koreans from going abroad to work;
- (vii) Prohibit members from supplying, selling or transferring luxury goods. In terms of the luxury goods, based on the UNSCR 2094 (2013), 2270(2016), 2321(2016) Annex, which refer to jewelry, transportation, luxury watches, items of lead crystal, recreational sports equipment, rugs and tapestries (valued greater than NTD15,000), and the tableware of porcelain or bone china (valued greater than NTD3,000). Details are given below:

Jewelry	Jewelry with pearls; ; Gems; Precious and semi-precious stones (including diamonds, sapphires, rubies, and emeralds); Jewelry of precious metal or of metal clad with precious metal.
Transportation items	Yachts; Luxury automobiles (and motor vehicles): automobiles and other motor vehicles to transport people (other than public transport), including station wagons; Racing cars; Aquatic recreational vehicles (such as personal watercraft); Snowmobiles (valued greater than \$2,000 USD)
Luxury watches	wrist, pocket, and other with a case of precious metal or of metal clad with precious metal
Items of lead crystal	
Recreational sports equipment	
Rugs and tapestries (valued greater than \$500 USD)	
Tableware of porcelain or bone china (valued greater than \$100 USD)	

- (viii) Prohibit members from supplying, selling or transferring aviation fuel, jet fuel, rocket fuel, condensates and natural gas liquids;
- (ix) The prohibition from financial transactions or provide financial services with North Korea and relating to the opening of branches, subsidiaries, joint ventures and opening of the account;
- (x) Prohibit the use and transfer of cash, and related to banks and money or value transfer service institutions;
- (xi) Prohibit to grant export credit or provide insurance services;
- (xii) Partial restrictions on the supply, sale or transfer of crude oil;
- (xiii) Partial restrictions on specialized education or training, scientific and technological cooperation.

## B. Financial Action Task Force (FATF)

In 1989, at the 15th Economic Summit in Paris, France, the Group of Seven (G7) recognized the threat of money laundering to the financial system and proposed the establishment of FATF to trace money laundering in drug crimes (Beekarry, 2013). Therefore, in 1990, the FATF formulated forty recommendations in order to build an international consensus on combating drug money laundering, which primarily focused on the prevention of money laundering among FIs in order to control the illegal financial flow (Beekarry, 2013). In addition, due to the 911 terrorist attack in the United States happened in 2001, the G7 convened a meeting in Washington, D.C., and the FATF successively added nine special recommendations, mainly related to CFT (Beekarry, 2013). In February 2012, the FATF consolidated the original forty AML Recommendations and Nine Special Recommendations for CFT. Furthermore, to add the Risk-Based Approach (RBA) as supervision method, in the meanwhile, the issue of CFP was also added and consolidated into new forty Recommendations (that is, forty Recommendations and eleven Immediate Outcome used in the 4th round of FATF and the 3rd round of APG mutual evaluation after November 2013). The methodology of the Mutual Evaluation

(ME) included "Technical Compliance Assessment" and "Effectiveness Assessment". "Technical Compliance Assessment" mainly scrutinizes whether the laws and regulations, legal frameworks, the powers and the procedures of the competent authority and procedures of assessed member states comply with the new forty Recommendations as well as to understand the member's AML and CFT mechanism (FATF, 2013-2019). "Effectiveness Assessment" is to evaluate the effectiveness of the implementation of FATF Recommendations by member states, and to identify the country's expected results in achieving a complete AML and CFT effectiveness. At present, the FATF Methodology for forty Recommendations and eleven Immediate Outcome, covering six significant evaluated aspects: national policy coordination mechanism, international cooperation, supervision and preventive measures, legal person and legal arrangement, law enforcement agency practical issues, CFT and CFP (FATF, 2013-2019).

In terms of the PF-TFS, which regulated in Recommendation seven of the FATF Forty Recommendations and adopted the targeted specific country. With response to the UNSCR1718 (2006) and 2231(2015) and its successor resolutions, which also call for members to impose TFS on those individuals, legal persons, or entities related to North Korea and Iran. Moreover, related mechanisms such as to establish the competent authority for the designated matters; The mechanism on identification on the proliferators that offer supports for the sanction countries; Freeze and prohibit related assets or other financial transactions of designated persons and entities; Report and investigation after freezing; delisting procedures, etc (FATF, 2013-2019). As of the completion of this article (June 22, 2020), based on the UNSCR 1718 sanction list, among 75 designated individuals, only one individual is Taiwanese, others are North Korean (UN, 2018).

Since ML, TF and PF have caused the threat to the financial system, a global response is required. To achieve this goal, the FATF operated by nine regional FATF-Style Regional Bodies (FSRBs), covering the regions

of the Caribbean, Council of Europe Committee, Asia-Pacific, Eastern and Southern Africa, Latin America, Eurasian, West Africa, Middle East and North Africa, and Central Africa (FATF, 2020). Besides, through the mutual evaluation to urge member states to effectively fulfil the international standards on AML, CFT and CFP.

Taiwan as a founding member, which had joined the Asia/Pacific on Money Laundering Group (APG) in 1997. APG is one of the FSRBs mentioned above. Hence, Taiwan also needs to follow the FATF methodology, meanwhile participate in FATF conference activities as an APG member. Indeed, Taiwan had accepted the APG evaluation in 2001, 2007 and 2018. The third-round mutual evaluation report of Chinese Taipei in 2019 was adopted by the APG members, and achieved the best evaluation result, which is “regular follow-up”. According to the Chinese Taipei AML/CTF Mutual Evaluation Report published in October 2019, the PF-TFS, which was the Recommendation 7 got the Largely Compliant (LC) rating, and Immediate Outcome 11 got the Substantial level of Effectiveness (SE). The part of the mutual evaluation report of the summary of technical compliance, the key deficiencies also provides references for the Taiwan government for future amendments of related laws and regulations (APG, 2019).



### III. Taiwan Domestic CFP Legal Framework

#### A. The Counter-Terrorism Financing (Taiwan) Act 2018 (CTFA):

##### i. CTFA included both TF and PF TFS

Based on the spirit of the "International Convention for the Suppression of the Financing of Terrorism" and the Recommendations six and seven of the FATF methodology, all member states should follow the Security Council resolutions on the suppression of terrorist financing, terrorism and the proliferation of weapons of mass destruction. For those relevant resolutions which have designated sanction targets shall impose TFS to freeze their assets. The implementation of the TFS for TF and PF in Taiwan are regulated by the same law called the CTFA. The provisions of CFTA include sanctions designation, delisting announcement procedures, the restrictions on the designated targets' assets and economic resource, reporting obligations and other due process procedures.

##### ii. Sanctions are divided into "statutory sanctions" and "resolution sanctions"

The MOJ is the competent authority of the CTFA. The CFTA sanctions announcements are administrative and take effect upon the MOJ announces the designated list or delisting. If the sanctioned targets disagree with the announcements, they may bring the action by Article 12 of the CTFA as well as follow administrative remedial channels. According to Articles 4 and 5 of the CTFA, sanctions can be divided into two categories: "resolution sanctions" and "statutory sanctions." The difference is that the former relies on the MOJ to convene a cross-department coordination platform called Terrorist of Financing Review Committee (TFRC) to approve the TFS sanction or not; the latter is followed with the latest UNSCR sanction list.

(i) Resolution Sanctions : According to Paragraph 1, Article 4 of the CTFA, for those individuals, legal persons, or entities suspected

of committing terrorist activities, under the requirements of an international treaty or convention in connection with TF prevention requires, or to implement international cooperation, or followed with the United Nations resolutions are necessary for designated sanctions. The MOJ may convene the TFRC with the report of the Ministry of Justice Investigation Bureau (MJIB) or according to its authority. The Minister of Justice presides as the convener, and an ex officio member while the deputy directors of the National Security Bureau, Ministry of Interior, Ministry of Foreign Affairs, Ministry of National Defense, Ministry of Economic Affairs, Central Bank and Financial Supervisory Commission seat the other membership. The designated individuals, legal persons or entities decision made by the TFRC, only published by the MOJ could the sanction lists take effect. The Taiwanese Chen serves an example, which was designated by the TFRC and announced by the MOJ under Article 4 of the CTFA (MOJ, 2018). For those who were designated by TFRC must be delisted by the Committee as well.

- (ii) Statutory sanctions : According to Paragraph 1, Article 5 of the CTFA, for those designated by the relevant UNSCRs and successor resolution on TF and the prevention of proliferation of the WMD, the MOJ shall publish sanction list by the reports from the MJIB or under its authority. Any individual, legal person, or entity designated according to the UN resolutions may only be delisted by the delisting procedures of the UN Security Council, and then the MOJ can publish the delisting afterwards. The Taiwanese Tsang serves an example, which was imposed sanction based on Article 5 of the CTFA (MOJ, 2018).
- iii. The legal effect of the sanction
  - (i) According to Paragraph 1, Article 7 of the CTFA, the designated targets under Article 4 (Resolution Sanctions) and Article 5 (Statutory Sanctions) of the CTFA will be prohibited from any

financial transactions, transfer or alteration its financial and property interests, as well as prohibited third parties from funding the sanctioned targets, which had demonstrated in line with the FATF Methodology, Recommendation 7.2 (b). According to FATF Recommendation 7.2 (b),

“The freezing obligation should extend to: (i) all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; (ii) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and (iii) the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as (iv) funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.”

(FATF, 2013-2019, p36)

It has shown that the scope of freezing assets was extensive. Therefore, Paragraph 2, Article 7 of the CTFA, which was amended and passed on 7 November 2018, expressly the provision of the restriction also applies to cases where a third party keeps or manages property or property interests of the designated individual, legal person and entity by authorization, appointment or trust of such individual, legal person and entity or due to other causes.

- (ii) Moreover, regarding the standard of directly or indirectly holding funds or other assets, the legislative reasons for the amendment of CTFA had referenced to the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC) standard, which means the whole assets of the designated targets. The standard here adopted 50 per cent or more (called the 50 Percent Rule) directly or indirectly owned of the designated targets, in other words, which is within the scope of the prohibition of disposition of funds or other assets.

## B. The MLCA and relevant regulations (CFP only)

- i. For those countries or regions with high risks of ML or TF, shall take the Enhanced Due Diligence (EDD), reject transactions, or other measures.
  - (i) According to Paragraph 1, Article 11 of the MLCA, for those countries or regions with high risks of ML or TF, the supervisors can order FIs and DNFBPs to strengthen relevant measures for verification of the customer's identity during transactions (the Subparagraph 1); To limit or prohibit FIs and DNFBPs to make wire transfers or conduct other transactions with high-risk ML and TF countries or regions (the Subparagraph 2); To take other necessary preventive measures those are effective and proportionate to the risks (the Subparagraph 3). DPRK's was a high-risk jurisdiction, which announced by the FATF, due to the failure to address the significant deficiencies in its AML and CFT regime; thus, the FIs and DNFBPs can adopt EDD measures on the customer due diligence and financial transactions, reject transactions, or other measures under the Article 11 of the MLCA. However, with the successive launches of missiles and nuclear weapons tests by North Korea, which had seriously affected the international order, the Ministry of Economic Affairs (2017) had ordered a total ban on trade with North Korea since September 25, 2017, which was pursuant by the Article 5 of the Foreign Trade (Taiwan) Act.
  - (ii) In terms of “countries or regions with high risks of ML or TF”, according to Paragraph 2, Article 11 of the MLCA, there are three categories. Firstly, the countries or regions where major flaws are detected in its ML prevention and CTF efforts, according to announcements issued by international AML organizations. For example, the “blacklist” here means North Korea and Iran (published on 21 February 2020). Secondly, the countries or regions where the advice of international AML organizations is not followed or not thoroughly followed, according to announcements issued by international AML organizations. For example, the “grey list”

here means Albania, The Bahamas, Barbados, Botswana, Cambodia, Ghana, Iceland, Jamaica, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen, Zimbabwe (published on 21 February 2020). Thirdly, other countries or regions where high risks of ML and TF are confirmed by sufficient evidence. Information about countries or regions with high risks of ML or TF” is updated from time to time. For the latest information, please refer to the website of the Anti-Money Laundering Division (FIU) of the MJIB.

ii. File Suspicious Transaction Reports (STRs) related to ML and TF

According to Article 10 of the MLCA, FIs and DNFBPs shall report to the MJIB all suspicious transactions, including attempted transactions, which may involve any of the offences described in Articles 14 and 15. The previous legal basis is the provision for FIs and DNFBPs to file the STRs. Article 15 of the " Regulations Governing Anti-Money Laundering of Financial Institutions" announced on November 14, 2018, stipulated that the timeline for reporting suspicious transactions shall be amended regarding international practices and FATF standards. It is required that those who meet the monitoring types shall complete the review process as quickly as possible. Besides, where review has resulted in a determination that a transaction was suspected of involving ML or TF activity, the FI shall promptly file an STR to the MJIB after the responsible chief compliance officer had approved the report at the institution within two business days of said approval. The above regulations amended the reporting period from ten business days to two business days was to in compliance with the FATF's Recommendation twenty, which stipulates that if FIs suspect or reasonably suspect that the transaction funds are criminal proceeds or involve terrorism of financing should "immediately" report the STR to the FIU, here means AMLD of the MJIB. The amendment to the declaration period to two business days is more in line with those above "immediate" requirements. Concerning

the DNFBPs, according to the FATF's Recommendation 23.1 required DNFBPs to comply with the provisions of the FATF Recommendation twenty. Therefore, the DNFBPs also have obligations to file the STR.

iii. Reporting the designated targets' property or property interests

According to Paragraph 3, Article 7 of the CTFA, an institution, business or profession prescribed in Paragraphs 1 to 3 of Article 5 of the MLCA, which refer to the FIs, enterprises handling financial leasing, virtual currency platform or transaction and DNFBPs shall immediately report any of the following circumstances discovered due to business relations to the MJIB. The one is withholding or managing property or property interests of a designated individual, legal person or entity. The other is the places where property or property interests of a designated individual, legal person or entity are located. On November 14, 2018, the revised announcement of the "Regulations Governing Reporting on the Properties or Property Interests and Locations of Designated Sanctioned Individuals or Entities by Financial Institutions ", Subparagraph 1, Paragraph 1, Article 3 of this Regulation, the reporting period from initially ten business days change into two business days, which following the date of the appointed chief compliance officer approval and then promptly file the report to the MJIB.

## IV. The PF Case Studies and Analysis

### A. Case Studies :

#### i. Chen Shih-Hsien Domestic PF-TFS Case (Chen Case)

On 12, January 2018 the competent authority, MOJ, convened the TFRC in the first time to discuss the fact that whether Chen and his associates were in violation of UNSCRs and finally to reach the decision (Ministry of Justice, 2018). The TFRC had designated Chen, Billion Bunker Group Co., (BBGC) registered at the Republic of the Marshall Islands; and Bunker Taiwan Group Cooperation (BTGC) registered at the British Virgin Islands (BVI) with a total one individual and two entities for the fact that conducting the ship to ship transfer of oil to North Korea. In addition, other two foreign legal entities, Oceanic Enterprise Co. Ltd. and UMC Corporation Peru S.A.C, which owned by Chen also were included in the sanctions list within the scope of the sanction. In order to completely block the money flow of the target, the MOJ had published the sanction and broadcasting through the media; the MOJ, the FSC and other relevant authorities also immediately strengthened the order to FIs and DNFBPs for name screening of their customers, imposing relevant restriction transactions, and reporting measures. According to official statistics (APG, 2019), after sanction announcement, the total number of related assets of the sanctioned subjects were frozen about 60 times, which reported from FIs, including deposits, stocks, and insurance premium. The value was estimated to be about NTD90 million (about 2.88 million US dollars). However, in 2019, Chen committed suicide and died (DeAeth, 2019). The MOJ (2019) finally published the TFRC de-listing approval of Chen's TFS measure on 25 November 2019.

#### ii. Tsang Yun-Yuan PF-TFS Case (UN TFS Case)

The Security Council updated its announcement on the sanctions

list of UNSCR 1718 and its successor resolutions on March 30, 2018, Taiwan time. The list of newly sanctioned individuals and legal persons includes Taiwanese Tsang and his 100% controlled foreign companies called Pro-Gain Group Corporation registered in Samoa, and Kingly Won International Co., LTD registered in the Marshall Islands. With the fact that Tsang suspected assisted North Korea in selling coal and obtaining crude oil illegally, Tsang was designated into sanction list by the UNSC 1718. The MOJ soon after published the sanction list (MOJ, 2018). According to official statistics (APG, 2019), after publishing the sanction list, FIs had reported the frozen assets of the sanctioned targets in approximately 30 times, amounting to a total sum of NTD30 million (approximately USD 1.08 million).

## B. Analysis

In the wake of these two sanctions cases mentioned above, there was relevant literature to illustrate cases in international publications. For instance, the Chen case, which had illustrated by the Royal United Services Institute (RUSI) in 2018. The finding in the research, which had identified that the vessels involved in the CFP cases are common utilizing various nation of Flags of Convenience (Dall & Keatinge, 2018). Although the Flags of Convenience is conventional in the international shipping industries, it might be a red flag indicator if the operation of the vessel is frequently near North Korea. In addition, under the complex cooperation structures, it is often difficult to have a detailed identity verification process for third-party chartered vessels. Therefore, the RUSI also called for that the role of the public sectors, insurance institutions, banking sectors, and shipping companies in CFP also play an essential frontline (Dall & Keatinge, 2018)

To explore the Taiwanese involving in the North Korea WMD proliferation network, the previous Chen case and Tsang Case were not the first time that Taiwanese conduct illicit trades with North Korea.



However, these two cases were the only two sanction cases since the CTFA promulgated. The difference between these two cases was that the Taiwan government designated the former case through the TFRC. The latter case was based on the UNSCR 1718 and its successor resolutions. Also, with the UNSCR updated list, which also announced by the MOJ afterword.

According to the past incidents, the Taiwanese suspected of engaging in illegal trade with North Korea can be traced back to the case of Tsai Hsien-Tai and Tsai Yueh-Hsun Case (Father and Son Case) in 1990. Tsai and his son used their subsidiaries in the United States to assist North Korea in purchasing goods related to weapons of mass destruction, and participated in the delivery of goods to North Korea to support North Korea's ballistic missile program (Lin, 2013). Based on the Taiwanese court documents in June 2008, Alex Tsai was charged by the Taiwan Taipei District Prosecutors Office for the violation of Article 27 of Foreign Trade (Taiwan) Act 2019. With the violations of the export of SHTC to restricted regions and forgery documents, which show that Tsai utilized at least two front companies called Global Interface Company and the subsidiary called TransMerits Co., Ltd. to accomplish the illicit procurement for North Korea (The Judicial Yuan of the Republic of China, 2008). After the Taiwan verdict had been rendered, the U.S. government had placed Alex Tsai, Global Interface, and Trans Merits under the Executive Order (E.O.) 13382 in 2009. However, even though Alex Tsai was being penalized for his first and second offences on forgery shipping invoice and declarations, it did not discourage his behaviour from continuing the procurement on behalf of North Korea. Both Alex and Gary Tsai were arrested by the U.S. government on 1 May 2013 and were indicted for conspiring to violate U.S. law with WMD proliferation. During 2014 to 2015, both father and son admitted involvement in illicit WMD trade. Alex Tsai was sentenced to two years imprisonment, and Gary Tsai admitted forgery export and import document to facilitate illegal trade WMD transfer and had been sentenced to three years of probation (The U.S. Department of Justice, 2016).

Before the CFTA being promulgated in 2016, only two Acts which are Criminal (Taiwan) Code 2020 and the Subparagraph 1, Paragraph 1, Article 27 of the Foreign Trade (Taiwan) Act 2019 can penalize the forgery and the unfaith declaration of exporter and importers in Taiwan. The Tsai case was an example. Although during 1994, the Taiwan government, the Ministry of Economic Affairs, had announced the Regulations Governing Export and Import of SHTC, which took effect on 1995 as export and import control mechanism for those commodities such as dual-use goods, technology export and general military goods. For example, if the shipping destination was North Korea or Iran, the exporter should apply for an SHTC export license before exporting and only with the issued license can the export be processed. Nevertheless, under the global CFP strategy, the legal framework at that time was indeed insufficient to respond to the international CFP strategy. Taken this point, the Taiwanese government promulgated the CTFA on July 27, 2016, and took the FATF Recommendations five to seven into consideration to enacting CTF and CFP related mechanisms, in order to be in line with international standards, and fulfil international responsibilities for global security.

## V. The PF Typologies And Methods

A. FATF (2018) had published the “Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction” , the summaries are as follows (FATF, 2018).

- i. Based on the UNSCR 1718 and its successor resolutions, the scope of the freeze including Funds, Financial Assets and Economic Resources. Besides, the designated list also extends from individuals, legal persons or entities to vessels.
- ii. There are four categories, which may involve in the DPRK proliferation of financing activities.

- (i) “Customers and transactions associated with countries subject to sanctions;
- (ii) Instruments that could particularly be used to finance prohibited transactions, such as certain trade financing products and services;
- (iii) Customers involved with and/or transactions related to items, materials, equipment, goods and technology prohibited by UNSCRs;
- (iv) Reasonableness of invoiced goods against market value, inconsistency or discrepancies in trade-related documentation” .

(FATF, 2018, P13)

iii. According to the 2008 FATF Typologies report on PF, which had compiled relevant PF elements with a total of twenty typologies. Consider the length of the content, this article introduces only five common typologies as follows.

- (i) “Transaction involved person or entities in foreign country of proliferation concern.
- (ii) A freight forwarding firm is listed as the product’ s final destination.
- (iii) Transaction involves shipment of goods incompatible with the

technical level of the country to which it is being shipped.

- (iv) Customer activity does not match business profile, or end-user information does not match end-user's business profile.
- (v) Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-a-vis the shipping cost” .

(FATF, 2018, P32)

iv. Based on the findings of the UN panel expert report and other academic researchers in the FATF guidance, there are eleven types of patterns. This article only lists the three common types as follows.

- (i) “Involvement of items controlled under WMD export control regimes or national control regimes.
- (ii) Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).
- (iii) Use of personal account to purchase industrial items” .

(FATF, 2018, P33-34)

#### B. The U.S. 2018 “*National Proliferation Financing Risk Assessment*” (NPFRA) report (U.S. Department of the Treasury, 2018)

The U.S. Treasury's Office of Terrorism Financing and Financial Crimes (TFFC) had consulted with eight central departments in 2018. There were Department of the Treasury (DOT), Department of Justice (DOJ), Department of Commerce (DOC), Department of Homeland Security (DHS), Department of State (DOS), Federal Functional Regulators (FFRs), National Defense University (NDU) and Office of the Director of National Intelligence (ODNI), with a total of thirty-one institutions and units to conduct PF risk assessment. This article only introduces the North Korea circumvent sanction methods as follows (U.S. Department of the Treasury, 2018).

- i. Utilize the complex multilayer networks to evade investigation :

The U.S. assessment report pointed out that entities involved in the PF programs included North Korea-owned enterprise, banks, intermediaries, brokers, agents, and even diplomats from third countries. These entities were good at using complex networks, for example, disguising North Korea funds through foreign shell companies. What is more, North Korea also established multiple overseas bank accounts and used overseas banking systems to transfer funds to suppliers for purchasing relevant weapon components. Most financial transactions occurred in foreign countries conducted by non-U.S. citizens. Due to the complicated structure of the transactions through U.S. banks, it was difficult for U.S. banks to identify the illegal sources of funds and obtain customer information.

- ii. Using the internal clearing of trade import and export transactions related to North Korea via the non-North Korean intermediary agencies to reduce the actual transfer record and create a tracing breakpoint

Recently, North Korea established non-North Korean trading companies through intermediaries as a hub for trading. Those companies purchased North Korea's natural resources and sold the related resources to the global market for funds. Some of the funds used to pay for import fee, the others used as clearance through the overseas banking accounts of the intermediaries and other North Korean entities. Therefore, intermediaries only need to track payments and orders on behalf of the North Korean customers and settle multiple accounts (including unknowing suppliers) internally; there was no need to conduct additional wire transfers between North Korea and other jurisdictions. In this way, the intermediary essentially acts as a "breakpoint", which allowed North Korea-owned entities to use foreign entities as a cover and continue to use the financial system in the global trade. It was also the reason that intermediary can earn higher commissions from the representative of the North Korean party.

- iii. Those front companies and shell companies trading with North Korea

are mostly established in some provinces in China

The front or shell companies used by North Korea were mostly in Mainland China or used Chinese banks to transfer illegal funds. According to the report, there were many companies, which had a close relationship with North Korea and are registered in Liaoning, Dalian, Dandong, Jinzhou, and Shenyang in Mainland China. At present, Liaoning province is a central banking hub, where North Korea mainly conducted funds transactions. The main business of those front or shell company were often related to import and export business, such as textiles, clothing, fisheries, seafood were the most common. Besides, these front or shell companies usually used the same address, the same manager or owner, phone number, and employees with no clear commercial purpose. The payment for products and services were also unrelated to their business scope. Indeed, the websites or other Internet information of front or shell companies may not maintain or update regularly.

C. During 2019, The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the U.S. Department of State and the U.S. Coast Guard had published "*Updated Guidance on Addressing North Korea's Illicit Shipping Practices*", the summaries as follows (OFAC et al., 2019).

- i. North Korea's common methods to circumvent sanction were to disguise the ship identity in order to carry out ship-to-ship transfers at sea or conceal the destination or origin of goods. Other common methods included turning off or manipulating the information of the Automatic Identification System (AIS), changing the ship's name or seven-digit vessel identification code of the International Maritime Organization number (IMO), forging certificate of origin and other related documents.
- ii. This report also recommended that all parties involved in the shipping industry and related commercial entities—including ship owners,

managers, operators, brokers, flag registries, oil companies, port operators, shipping companies, classification service providers, insurance companies, and financial institutions shall understand the North Korea circumvent sanction methods and to adopt the adequate measures in order to mitigate the PF risk.

**D. The UN Security Council, “*Report of the Panel of Experts Established Pursuant Resolution 1874 (2009)*” , S/2020/151- Latest circumvent sanction of North Korea (UNSC, 2020).**

- i. North Korea had continued to illegally import oil, luxury goods (including luxury cars, wine, robotic machinery, etc.), and conduct ship-to-ship transfers with foreign flags such as the Republic of Sierra Leone. Also, adopted obfuscated strategies, which included turning off the AIS, ship to ship transfer at night, or using a small ship without an IMO number for camouflage.
- ii. North Korea had continued to export coal and sand by shipping and illegally sold fishing rights to increase its income for the purpose of developing nuclear projects and related missile programs. The recent reports had indicated that North Korea no longer transfers coal to small-sized ships as it did in the past, instead, it transferred coal into tankers in order to increase the transferring amount of the illegal coal.
- iii. North Korea had continued to use international banks through third-party intermediaries and conduct cyber-attacks on global financial institutions to acquire virtual currencies or virtual assets illegally. According to the “Guidance on the North Korean Cyber Threat”, which was published in April 2020, by the U.S. Departments of State, the Treasury, the Homeland Security and the Federal Bureau of Investigation. The guidance had pointed out that the cyberattacks related to North Korea included 2014 Sony Picture Entertainment attack, 2016 Bangladesh Bank Heist, 2016 FAST Cash Campaign and 2017 WannaCry 2.0 ransomware (U.S. Department of State et al., 2020).

- iv. Based on the UNSCR 2397 (2017) requested all member states to dispatch North Korean citizens (including information technology workers abroad) earning income abroad before December 22, 2019. Therefore, the UN also calls for member states to dispatch North Korean citizens who worked overseas and to submit relevant reports if they found that those people earned their incomes so as to support North Korea's nuclear and missile programs. In addition, the UN also recommended that member states shall review all types of visas for North Koreans and prevent North Koreans who intend to earn income overseas from entering.
- v. In terms of the export of luxury goods, the panel of expert suggested the prohibition on resale to sanctioned jurisdictions (such as North Korea) should be included in the contract. Besides, the export control list should be unified for luxury goods, and a comprehensive review of the consignee should be taken into account with the risks of transshipments.

#### E. Taiwan domestic mechanism that to response North Korea sanction circumvention

With the fact of that PF is connected with maritime cargo transportation or shipping activities, the Taiwan "Financial Supervisory Commission of the Executive Yuan (FSC) had issued the insurance industry's best practice for AML and CFT on September 26, 2019. The guidance called "the Best Practical Practice on preventing the related insurance industries from involving in ML, TF and PF activities", provided different CDD measures in stages of solicitation, underwriting and claim settlement for "ship insurance" and "cargo transportation insurance" in order to avoid potential proliferators to exploit the insurer channel.

##### i. The stage of solicitation

This stage emphasize on customer due diligence, which focuses on the nature and the relationship of the business. For cargo transportation insurance, insurers can refer to documents such as commercial invoices



or letters of credit; for ship insurance, insurers shall check the vessels' registration nation or other registration documents. If the customer is a legal person, insurers must refer to reliable resources to identify the relevant substantial beneficiaries, etc. Issuers should refuse to establish relevant business relationships with the sanctioned targets.

ii. The stage of the underwriting

During the stage of the underwriting, it is necessary to understand whether the port of departure and the destination are located in countries or regions with high risks of ML or TF. The proper record-keeping for the consignee in cargo transportation insurance is essential. For ship insurance, it is crucial to scrutinize the identity of the ship. Currently, there are many relevant databases, such as the International Maritime Organization with the ship identification number, the Security Council with sanctions vessel list, the U.S. OFAC sanctions list, the Security Council port banned ship lists, the sanctions prohibited ship list of the Marine Port Bureau of the Ministry of Communications, which was in line with the Security Council Sanctions. Insurers can refer to the websites, such as "MarineTraffic" or "Equasis" for more information.

iii. The stage of the claim settlement

When dealing with the damage in cargo transportation insurance, it is necessary to note that whether the goods included SHTC; also, it is important to ensure that the manufacturer had submitted a license issued by the BOFT of the Ministry of Economic Affairs. In addition, when insurers deal with a ship insurance claim, it is necessary to check whether the AIS had an abnormal shutdown during the maritime shipping period. In addition, the issuers should examine the list of payees and keep the records during the stage of claim settlement.

## VI. Conclusion

As North Korea successively conducted a total of six nuclear tests in 2006, 2009, 2013, 2016 and 2017, resulting in international tensions and global security concerns. In recent years, the issue of CFP has captured international attention. Despite of the fact that Taiwan is not a member of the United Nations, Taiwan still voluntarily follows and implements the relevant UNSCRs as members of the international community. If relevant domestic public and private sectors can understand and grasp the latest CFP issues provided in this article, the risk of PF recurrence might be effectively avoided. This article aims to introduce and give an overview of CFP obligations to the readers, and help them implement CFP measures more smoothly.

## VII. Bibliography

### Books

Beekarry, N., 2013 *Combating money laundering and terrorism finance: past and current challenges*. Cheltenham: Edward Elgar Pub. Ltd.

### Newspapers

DEAETH, D., 2019. Taiwanese businessman guilty of N. Korea sanctions violations commits suicide. Taiwan News [online]. 22 June. [viewed 5 September 2020]. Available from: <https://www.taiwannews.com.tw/en/news/3729920>

LIN, CHANG- SHUEN., 2013. 違法出口北韓 蔡顯泰曾判拘役 [*Illegal export to North Korea, Tsai Hsien-Tai was sentenced to detention*] [online]. Taiwan News. [viewed 2 August 2020]. Available from: <https://www.taiwannews.com.tw/ch/news/2214543> (In Chinese).

### Legislation

Counter-Terrorism Financing (Taiwan) Act 2018 [online]. [viewed 5 September 2020]. Available from: <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0030047>

Criminal Code of the Republic of China 2020 [online]. [viewed 5 September 2020]. Available from: <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=C0000001>

Foreign Trade (Taiwan) Act 2019 [online]. [viewed 5 September 2020]. Available from: <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0090004>

Money Laundering Control (Taiwan) Act 2018 [online]. [viewed 5 September 2020]. Available from: <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380131>

### Cases

JUDICIAL YUAN OF THE REPUBLIC OF CHINA., 2008. 臺灣臺北地方法院 97 年簡字第 2747 號刑事判決 [*Taiwan Taipei District Court Summary Judgment, 2008, No. 2747*] [online]. Judicial Yuan Law and

Regulations Retrieving System. [viewed 2 August 2020]. Available from: [https://law.judicial.gov.tw/FJUD/Default\\_AD.aspx](https://law.judicial.gov.tw/FJUD/Default_AD.aspx) (In Chinese).

JUDICIAL YUAN OF THE REPUBLIC OF CHINA., 2019. 臺灣高雄地方法院 107 年簡字第 4289 號刑事簡易判決 [*Taiwan Kaohsiung District Court Summary Judgment, 2018, No. 4289*] [online]. Judicial Yuan Law and Regulations Retrieving System. [viewed 2 August 2020]. Available from: [https://law.judicial.gov.tw/FJUD/Default\\_AD.aspx](https://law.judicial.gov.tw/FJUD/Default_AD.aspx) (In Chinese).

### Governmental and Intergovernmental Organization Publications

APG., 2019. *Anti-money laundering and counter-terrorist financing measures – Chinese Taipei, Third Round Mutual Evaluation Report* [online]. Sydney: APG. [viewed 30 May 2020]. Available from: <http://www.apgml.org/includes/handlers/get-document.ashx?d=17b44799-0e1d-4701-90a1-79584101bb9e>

APG., 2020. *Home/ Members & Observers/ Members* [online]. Sydney: APG. [viewed 2 June 2020]. Available from: <http://www.apgml.org/members-and-observers/members/default.aspx>

DALL, E., & KEATINGE, T., 2018. *Underwriting Proliferation: Sanctions Evasion, Proliferation Finance and the Insurance Industry* [online]. London: Royal United Services Institute (RUSI). [viewed 2 September 2020]. Available from: [https://rusi.org/sites/default/files/20180710\\_underwriting\\_proliferation\\_web.pdf](https://rusi.org/sites/default/files/20180710_underwriting_proliferation_web.pdf)

EROL, E., & SPECTOR, L., 2017. *Countering North Korean Procurement Networks Trough Financial Measures: The Role of Southeast Asia* [online]. Monterey: James Martin Center for Nonproliferation Studies (CNS). [viewed 2 September 2020]. Available from: <http://www.jstor.org.ezproxy.lib.gla.ac.uk/stable/resrep17540.4>

FATF., 2013-2019. *Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems* [online]. Paris, France: FATF. [viewed 30 May 2020]. Available from: <http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html>

FATF., 2018. *Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction* [online]. Paris, France: FATF. [viewed 30 May 2020]. Available from: [www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html](http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html)

U.S. DEPARTMENT OF THE TREASURY., 2018. *The National Proliferation Financing Risk Assessment* [online]. Washington: The U.S. Department of the Treasury. [viewed 2 June 2020]. Available from: <https://www.hsdl.org/?abstract&did=820761>

### Internet Sources

ANTI-MONEY LAUNDERING OFFICE, EXECUTIVE YUAN., 2020. [viewed 2 June 2020]. Available from: <https://www.amlo.moj.gov.tw/1523/>

ANTI-MONEY LAUNDERING DIVISION, MJIB., 2020. [viewed 2 June 2020]. Available from: <https://www.mjib.gov.tw/mlpcen>

BANKING BUREAU, FSC., 2020. [viewed 2 June 2020]. Available from: <https://www.banking.gov.tw/en/index.jsp>

BUREAU OF FOREIGN TRADE, MOEA., 2020. [viewed 2 June 2020]. Available from: <https://www.trade.gov.tw/English/>

BUREAU OF FOREIGN TRADE, MINISTRY OF ECONOMIC AFFAIRS., 2017. Sensitive Commodities List for North Korea (Taiwan has ordered a total ban on trade with North Korea on September 25, 2017) [online]. Bureau of Foreign Trade. [viewed 8 September 2020]. Available from: <https://www.trade.gov.tw/English/Search2/List.aspx?query=north%20korea>

EQUASIS., 2020. [viewed 2 June 2020]. Available from: <https://www.equasis.org/EquasisWeb/public/HomePage>

INSURANCE BUREAU, FSC., 2020. [viewed 2 June 2020]. Available from: <https://www.ib.gov.tw/en/>

LAW AND REGULATIONS DATABAS OF THE REPUBLIC OF CHINA.,

2020. [viewed 2 June 2020]. Available from: <https://law.moj.gov.tw/Eng/index.aspx>
- LEGISLATIVE YUAN LEGAL SYSTEM, 2020. [viewed 2 June 2020]. Available from: <https://lis.ly.gov.tw/lglawc/lglawkm> (In Chinese).
- MARINE TRAFFIC., 2020. [viewed 2 June 2020]. Available from: <https://www.marinetraffic.com/en/ais/home/centerx:120.533/centery:24.291/zoom:13>
- MINISTRY OF JUSTICE., 2018. 法務部公告 [The official Announcement of the MOJ] [online]. Ministry of Justice. [viewed 2 August 2020]. Available from: <https://www.aml-cft.moj.gov.tw/media/166635/8112181258454.pdf?mediaDL=true> (In Chinese).
- MINISTRY OF JUSTICE., 2018. 因應聯合國安理會加強制裁北韓案 我國人張永源涉案部分已啟動目標性金融制裁措施 [*In response to the UNSC on the North Korea sanction, the Taiwanese government has initiated targeted financial sanctions to Tsang*] [online]. Ministry of Justice. [viewed 2 August 2020]. Available from: <https://www.moj.gov.tw/cp-21-101060-369f1-001.html> (In Chinese).
- MINISTRY OF JUSTICE., 2019. 法務部公告 [*The official Announcement of the MOJ*] [online]. Ministry of Justice. [viewed 2 August 2020]. Available from: <https://www.aml-cft.moj.gov.tw/624184/624196/624197/740831/post> (In Chinese).
- MINISTRY OF JUSTICE., 2020. [viewed 2 June 2020]. Available from: <https://www.moj.gov.tw/mp-095.html>
- NSCR-NET., 2020. Resources/Non-State Actors [online]. International Network for Economic, Social & Cultural Rights. [viewed 2 June 2020]. Available from: <https://www.escr-net.org/resources/non-state-actors>
- UNITED NATIONS., 2018. *Security Council 1718 Sanctions Committee Adds 22 Entries to Its Sanctions List, Designates 27 Vessels* [online]. New York: The UN. [viewed 27 August 2020]. Available from: <https://www.un.org/press/en/2018/sc13272.doc.htm>
- UNITED NATIONS., 2020. *Home/ Charter of the United Nations/ Chapter*

- VII* [online]. New York: The UN. [viewed 2 June 2020]. Available from: <https://www.un.org/zh/sections/un-charter/chapter-vii/index.html>
- UNITED NATIONS., 2020. *Home/ Sanctions/ 1718 Sanctions committee ( DPRK )* [online]. New York: The UN. [viewed 2 June 2020]. Available from: <https://www.un.org/securitycouncil/sanctions/1718>
- UNITED NATIONS., 2020. *Sanctions List Materials* [online]. United Nations Security Council. [viewed 31 August 2020]. Available from: <https://www.un.org/securitycouncil/sanctions/1718/materials>
- UNITED NATIONS SECURITY COUNCIL., 2020. *Report of the Panel of the Experts Established Pursuant to Resolution 1874 (2009), S/2020/151, March 2* [online]. New York: UNSC. [viewed 12 September 2020]. Available from: <https://www.undocs.org/S/2019/171>

## **Part V**

# **Strategic Analysis Report**



**Strategic analysis report on corruption crime**



## Strategic analysis report on corruption crime

### One. Preamble

AMLD received a total of 35,869 suspicious transaction reports (STR) in 2018; after applying value-added analysis, 4,339 of the STRs were produced into detailed analysis reports and distributed to competent authorities for 2,283 investigations<sup>6</sup>. Only 62 (2.7%) of the investigations were related to corruption and bribery<sup>7</sup> (See Figure I), meaning that the reporting entities had submitted low numbers of corruption and bribery related STR. To help reporting entities detect movement of corruption/bribery proceeds involving civil servants, the report analyzed major corruption cases that happened in the last 3 years and concluded on the common crime and money laundering patterns, how criminal proceeds were moved, and key reasons why cash flow remained undetected by FIs or DNFBPs. Recommendations were raised to provide useful reference for reporting entities in their case analysis and STR filing.

### Two. Research Methodology

This report takes into consideration the facts of crime and money laundering activities/cash flow in major corruption cases involving civil servants that MJIB and AAC had referred to prosecution between 2016 and 2018, and contains an assessment on the risk of FIs or DNFBPs being exploited for money laundering. The report also includes an analysis/summary of 207 STRs that AMLD had previously received on the abovementioned cases, and a list of suspicious signs for different types of corruption, which will provide useful reference to reporting entities for their case review.

---

<sup>6</sup> For detailed statistics, please refer to appendices of IO6 presented in the Mutual Evaluation Report of Chinese Taipei published in October 2019.

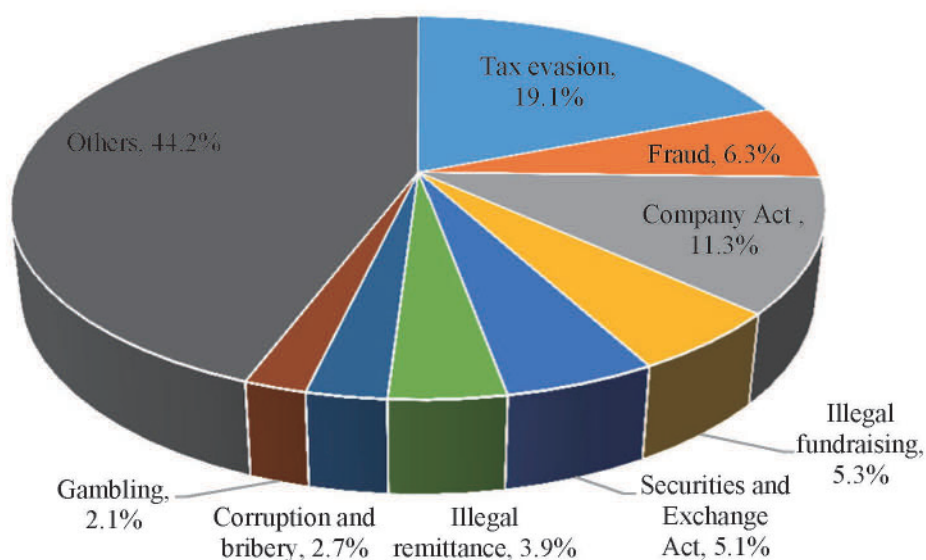
<sup>7</sup> Referred to as corruption case below.

## Three. Trend Overview

### I. Financial intelligence disseminated to competent authorities in 2018

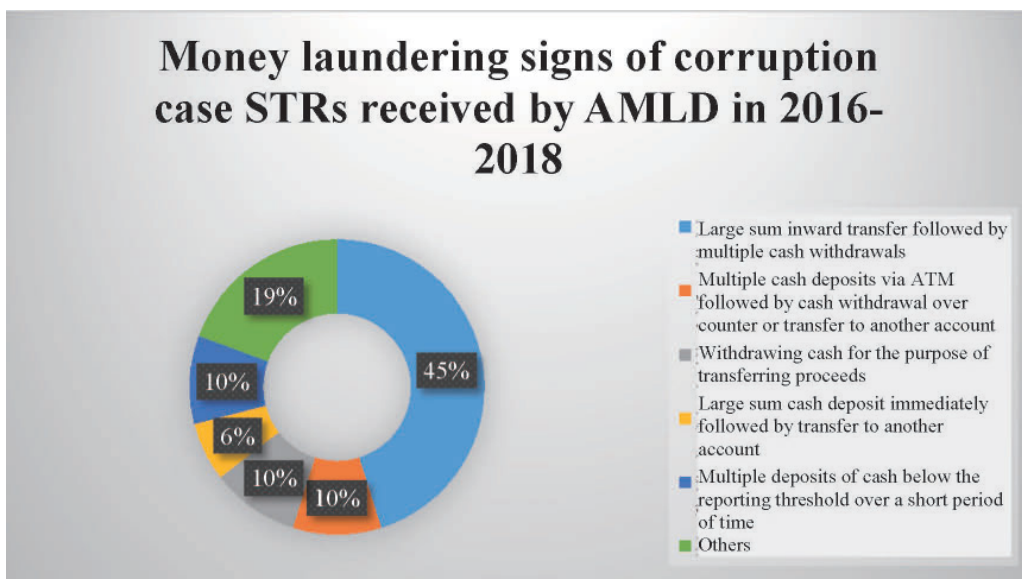
Based on an overview of crime analysis reports submitted by AMLD to the competent authorities in 2018 (see Figure I), the top 5 crimes, in descending level of significance, were: (1) tax evasion - 19.1%; (2) violation of the Company Act - 11.3%; (3) fraud - 6.3%; (4) illegal fundraising - 5.3%; and (5) violation of Securities and Exchange Act - 5.1%. Together, they accounted for 47.1% of all reports disseminated. Most of the cases involved direct transactions with FIs, which were characterized by transparent cash flow and more easily identifiable use of fund. Corruption cases, however, accounted for only 2.7% of total reports submitted in 2018, which was indicative of the difficulties involved in identifying corruption cases.

**Categories of cases raised  
by AMLD in 2018**



## II. Money laundering signs of corruption cases submitted in 2016-2018

Figure II is a summary of key money laundering signs in corruption case STRs received by AMLD, which MJIB and AAC had later referred to district prosecutors offices between 2016 and 2018. The most common signs of money laundering included: multiple withdrawals of cash, multiple cash deposits via ATM, and withdrawing cash for the purpose of transferring criminal proceeds. "Others" category included "purchasing vehicles with criminal proceeds under the name of another person," "depositing large amount of cash and immediately converting it into foreign currency or traveler's check," "transferring USD from an offshore account and shortly after remits USD to an overseas account of another company," "transferring multiple large sum proceeds from certain companies within a short period of time," and "regularly overpaying credit card bills."



<Figure II: Money laundering signs of corruption case STRs received by AMLD in 2016-2018>  
Source: AMLD

### III. Percentage of corruption cases referred to prosecution in 2016-2018 that AMLD had previously received STR for:

MJIB and AAC referred a total of 773 corruption cases<sup>8</sup> to prosecutors officers between 2016 and 2018, only 30 or 3.88% of which had STRs previously reported by FIs or DNFBPs. Many of the major corruption cases referred to prosecution within the period used small cash deposit, small cash withdrawal or in-person delivery of bribe to avoid detection by FIs. There were also several cases that exhibited suspicious account activities such as "large cash deposit/withdrawal," "substantial increase in property over short period of time," and "use of phantom account to conceal criminal proceeds," but due to the difficulties involved in identifying the beneficial owner, source of fund, and use of fund in a phantom account, detection of corruption crime is highly dependent upon the reporting entities being thorough with their KYC and customer due diligence.

## Four. Indicators for Suspicious Corruption and Bribery Offenses

The following is a list of suspicious criminal offenses, presented in different categories that MJIB and AAC had referred corruption cases and AMLD had received STRs for between January 1, 2016 and December 31, 2018.

### I. Violations against Government Procurement Act

Company A, an entity that was not eligible to bid for government project, submitted tender using Company B's name and credentials, and was awarded the tender.

Company B allowed Company A to submit tender using Company B's name and credentials, and placed account passbooks and common seals

<sup>8</sup> AAC referred a total of 347 corruption cases between 2016 and 2018, whereas MJIB referred a total of 426 corruption cases between 2016 and 2018.

under the custody of Company A.

Company A submitted tender using Company B's license to create the illusion of competitive bidders. Company A also prepared tender documents on Company B's behalf and supplied monetary capital to have cashier's check issued and placed as tender bond under Company B's name.

Company A and Company B jointly submitted tender using Company B's license and the tender was awarded to Company B. After acceptance of the project, Company B transferred the billings it received from Treasury to Company A in the form of a "credit note."

Company A and Company B jointly submitted tender using Company B's license. After being awarded the tender, Company B transferred the billings it received from the project owner to Company A net of 8% business tax.

Company A and Company B jointly submitted tender using Company B's license. After being awarded the tender, Company B retained 3.5% to 4% of subsequent billings and transferred the remainder to Company A's designated account.

A government agency tried to source the most advantageous tender by imposing specifications and restrictions in favor of a certain company.

Tenderers conspired among themselves not to compete with each other, but to take turns winning and to rig the tender price.

Tender documents submitted by different companies shared the same address, phone number, fax number, e-mail and contact person.

Although there were 3 or more tenderers, 2 of which were found to be ineligible after tender opening.

Checks that different tenderers had placed as bonds were in sequential numbers, and proceeds were refunded back to the same account.

## II. Offering or acceptance of bribes involving civil servants

### (I) Construction

Civil servants were found to have collected kickbacks from winners

of government procurement projects for 4% to 15% of the tender price. These bribes were paid when tender winners received their billings or final settlement after inspection.

Civil servants were found to have collected 5% of the tender price from winning tenderers as consideration/bribe for early project acceptance or early payment of billings and final settlement.

There were instances where, as soon as the first billing was paid into winning tenderer's account after inspection, the company assigned personnel to withdraw an agreed percentage of the sum as bribe and hand the cash over to a civil servant or a middleman in person.

Civil servants' accounts were deposited with checks issued from construction companies or other individuals or entities that benefited from the government procurement.

Civil servants responsible for government procurement received substantial transfers of money from overseas that were not commensurate with civil servants' status, occupation, or background.

Civil servants were found to have discussed or received bribes in secluded areas such as private dining rooms and private vehicles.

Accounting personnel of winning tenderer was found to have withdrawn cash from the company's account, delivered it as bribe, and accounted for the transaction as loan to shareholder and repayment from shareholder.

Civil servants were found to have changed tender rules from "lowest bid" to "open review" in favor of certain participants and collected kickbacks in the process.

Civil servants were found to have purposely lowered the project budget so that certain companies would meet the tender requirement, and collected consideration in the process.

Civil servants were found to have requested bribe from tender participants in the name of local activities such as "tour sponsorship," "religious worship" etc.

Civil servants were found to have helped businesses speed up land development review in return for consideration.

Civil servants were found to have covered for soil treatment service providers in back-filling using substandard soil, and collected benefits in return.

## (II) Tax-related offense

Tax officers were found to have covered for specific companies in issuing reciprocal/falsified invoices for purposes such as inflating revenues, window-dressing of financial statements, fictitious report of input tax, and tax evasion.

Tax officers were found to have helped specific companies make incorrect filing of "Business Sales and Tax Report (Form 401)" and "Zero-tax Rate Sales List" in an attempt to claim tax refund from National Taxation Bureau.

Tax officers were found to have conspired with members of criminal organization to set up shell companies and report fictitious exports for fraudulent claims of tax refund.

Tax officers were found to have used internal computers for making inquiries such as Form 401 filing of a particular company, whether the company was subject to purchase restriction or audit by the National Taxation Bureau etc. at the request of outsiders, and collected consideration for doing so.

## III. Property of unknown origin involving civil servants

Civil servants exhibited increase of cash asset over a short term that were not commensurate with their income, and were unable to provide complete, adequate and detailed explanation.

Civil servants or family members exhibited cash withdrawals of abnormal frequency and amount.

Civil servants or family members were found to have purchased foreign currencies or insurance products using cash of unknown origin.

Civil servants were found to have accepted properties of unknown origin using their own accounts and accounts of friends.

Civil servants were found to have deposited properties of unknown origin into personal accounts, and explained that they had arisen due to inheritance from elders who had the habit of keeping large stash of cash at home.

Spouse or children of a civil servant had significant increase of deposit in their accounts within a particular period, and the increase was not commensurate with the civil servant's income.

Civil servants were found to have deposited cash into accounts of different owners in multiple transactions for reasons such as gifting and mortgage payment.

Civil servants claimed to have accepted large sums of money for reasons such as part-time teaching, public speech, or income from share investment in an attempt to mask the corruptive origin of such income.

Civil servants were found to have accepted cash of unknown origin and placed it as down payment for home purchase immediately afterwards.

Civil servants or family members were found to have purchased real estate property through establishment of separate legal entity or alternative legal arrangement.

#### IV. Electoral corruption

Election candidates were found to have treated voters to paid overseas trips in exchange for exercising of voting rights.

Election candidates were found to have distributed complimentary meal vouchers to voters in exchange for exercising of voting rights.

Election candidates had attempted to bribe local voters by paying them to distribute campaign materials.

Election candidates had attempted to bribe local voters by offering allowance or fuel subsidy.

Election candidates were found to have delivered campaign budget



in cash to several chiefs of village, who used the money to secure voters' support.

## V. Corruption involving the police

Police officers were found to have helped local sex workers avoid raid in exchange for monthly bribe and festive cash.

Police officers were found to have covered for local gambling houses in exchange for share in the business.

Police officers were found to have covered for illegal moneylenders, and facilitated the transfer of real estate property from creditors who were unable to repay interests to friends of the police officer.

When making internal procurements, police officers were found to have leaked information such as number of participating tenderers and background of the review panel to specific companies in exchange for kickback.

Police officers were found to have concealed acts of crime for certain parties and asked for bribe in return.

## Five. Case Study

### I. Acceptance of bribe involving judge O-Pin Hu

#### (I) Case summary

The case involved O-Pin Hu (Hu) - a judge at Taiwan High Court Taichung Branch Court Civil Court Room; O-Chan Huang - Hu's domestic partner; O-Te Chiu - former Chairman of TH Hotel; O-Chu Chiu - O-Te Chiu's eldest daughter; O-Ling Huang - O-Te Chiu's eldest daughter-in-law; and O-Ling Kung - O-Te Chiu's second daughter-in-law. When assigned to review family dispute over the ownership of TH Hotel between October 2012 and August 2013, Hu exploited the opportunity and agreed to help O-Chu Chiu secure control in TH Hotel by purposely delaying the legal proceeding and forcing O-Ling Kung (the

plaintiff) to a settlement in exchange for bribe. O-Chu Chiu gave O-Pin Hu NT\$44,800 worth of exquisite glassware through O-Ling Huang in May 2013, and after the litigation was concluded, O-Pin Hu accepted another NT\$3 million of bribe from O-Chu Chiu through O-Ling Huang in August 2013 at Hu's residence.

(II) Signs of crime and money laundering:

1. Concealment of criminal proceeds using safe deposit box of another person:

After receiving the NT\$3-million bribe from O-Chu Chiu, Hu placed part of that cash inside the safe deposit box that O-Chan Huang, a domestic partner, had leased in the name of Huang's sister-in-law, in an attempt to conceal criminal proceeds.

2. Property of unknown origin:

The investigation found more than NT\$23 million of cash stashed inside the abovementioned safe, and one million dollars of cash at Hu's residence; the sum of which exceeded the amount of bribe that Hu had received. After checking Hu's every income source 3 years since the crime, the prosecutor was convinced of the presence of abnormal income, and Hu's reluctance to explain source of income constituted the offence - property of unknown origin.

3. Purchasing vehicle with criminal proceeds and transferring ownership to another person:

In an attempt to prevent seizure of the vehicle that Hu had purchased with criminal proceeds, Hu transferred ownership of the vehicle over to O-Chan Huang's father and instructed O-Chan Huang to withdraw NT\$1.77 million of cash from the abovementioned safe and have NT\$450,000, NT\$370,000 and NT\$12,000 deposited into the account of O-Chan Huang's father on three different days, which posed as payment for the vehicle purchase.

## II. Acceptance of bribe involving former Township Mayor O-Huang Li

## (I) Case summary:

The case involved O-Huang Li (Li) – former Mayor of OO Township, Pingtung County; O-Ho Tsai - Li's secretary who succeeded Li after service ended on December 25, 2014; and O-Lun Huang - the person-in-charge of Company L and Company Y. Li gained partial ownership and became a shareholder of Company Y after service ended. The township office hosted a public tender for the construction project - "Pingtung County OO Township OO Elementary School Student Footpath Safety and Environment Enhancement" on December 5, 2013, during which Li and O-Ho Tsai conspired to exploit their authority for bribe, and accepted NT\$2.33 million from O-Lun Huang, which approximated to 15% on the winning amount of tender for "OO Elementary School Student Footpath Phase I." Later in 2014 and 2015, O-Lun Huang made subsequent bribes of NT\$1.2 million to Li for project "OO Township Chenggung Road Phase I," NT\$3 million to O-Ho Tsai for projects "OO Township Chenggung Road Phase II," "OO Township Minzu Road Phase I," and "OO Station Landscaping," and NT\$100,000 to O-Ho Tsai for the supervision and design tender of "OO Station Landscaping." The bribe that O-Lun Huang had paid to O-Ho Tsai in June 2016 to win the "OO Station Landscaping" tender for Company Y was arranged by having Company M, owned by Huang's friend, purchase floor tiles and construction materials from third parties (Company A and Company B) and resell them to Company Y at a markup above 100%. The profit that Company M made on resale of materials was the source of the bribe paid to O-Ho Tsai<sup>9</sup>.

## (II) Signs of crime and money laundering:

### 1. Laundering of criminal proceeds through investment:

O-Ho Tsai's share of the bribe was partially handed over to friend for the purchase of local fruits that were subsequently sold to the Mainland; another NT\$1.3 million of the bribe was deposited into

<sup>9</sup> Pages 85-87, MJIB Anti-corruption Annual Report 2017, published October 2018.

the securities account opened at OO Commercial Bank OO Branch for share investment and to launder criminal proceeds through frequent trading activities.

2. Withdrawal of cash below the reporting threshold:

In order to secure win for tender, Company Y made arrangements with Li et al. to pay bribes at a fixed percentage on the winning amount of tender in cash. To avoid alerting FIs, Company Y would make several withdrawals of cash no more than NT\$500,000 per day months before the tender was awarded, and deliver the bribe in cash in one lump sum.

3. Inward transfer from another bank followed by immediate outward transfer via automated equipment:

Company M had collaborated with Company Y in the scheme to bribe O-Ho Tsai, and resold goods to Company Y at extreme high prices to source funds for the bribe. Account transaction history of Company M showed frequent deposits from Company Y within a small timeframe followed shortly by total withdrawal or outward transfer, leaving very small balance in the account. In addition, the sum of transactions far exceeded the share capital of Company M.

### III. Acceptance of bribe involving former Legislative Yuan Secretary-General O-Shan Lin

(I) Case summary:

The case involved O-Shan Lin (Lin) - former Secretary General of the Legislative Yuan; O-Wei Liu - spouse of Lin (no record of income from employment); O-Cheng Li - person-in-charge and General Manager of Company K; and O-Ni Hsiao - person-in-charge of Company K and O-Cheng Li's ex-wife. Between 2012 and January 2015, Lin intentionally exploited his role as Secretary General of Legislative Yuan and authority over administrative and procurement decisions for kickbacks and bribes. Lin leaked confidential details on

23 IT procurement tenders of the Legislative Yuan worth approximately NT\$200 million to O-Cheng Li of Company K in exchange for bribes calculated at 20% on the amount of winning tender, net of 5% business tax. Lin accepted a total of NT\$28 million in bribes from Company K on 8 occasions during the abovementioned period<sup>10</sup>.

(II) Signs of crime and money laundering:

1. Money laundering using phantom accounts:

In an attempt to hide and conceal criminal proceeds, Lin used his personal account and accounts of O-Wei Liu (spouse), O-Yang Lin (son), O-Yin Chen (subordinate) and Company T (idle entity with no business activity) to deposit and withdraw the bribes received, and occasionally deposited bribes into third party accounts to launder and conceal criminal proceeds under the cover of legitimate cash flows that regularly go into the accounts.

2. Property of unknown origin:

As per investigation of the prosecution: Lin was paid NT\$11,860,668 in salary from 2012 to January 2016, and had received NT\$233,043,440 of cash deposit or inward transfer into his active accounts and handed NT\$67,558,800 to subordinates for personal spending during this period,. Judging by the NT\$6,477,000 of unexplained cash uncovered at Lin's residence, Lin had received NT\$307,079,240 of suspicious income/property in cash; after eliminating double-counting and the NT\$28-million bribe mentioned above, Lin still had NT\$240,786,920 of cash that was not duly explained.

3. Delivery of bribe on Taiwan High Speed Rail:

Lin made arrangement with O-Cheng Li of Company K to deliver bribe on high speed rail for its fast speed, secrecy, and difficulty in tailing. They agreed in advance to take the same train and meet up in a specific car; O-Cheng Li then handed the NT\$7-million bribe

<sup>10</sup> Supreme Court criminal judgment No. 2018-Tai-Shang-2483.

to Lin before alighting at the next station. whereas Lin returned to the Secretariat Office immediately after receiving the cash. Lin then instructed O-Chuan Chen (a trusted individual) to meet up with O-Wei Liu at O Bank with the NT\$7-million cash, where O-Wei Liu deposited all of the cash into her personal account.

#### IV. Aiding of electronic gambling operators involving Chief O-Chang Li

##### (I) Case summary:

Chief O-Chang Li (Li) of Kaohsiung City Police Department O Precinct was formerly an officer of Administrative Section at Kaohsiung City Police Department between December 25, 2010 and January 28, 2013. Between March 2011 and the end of December 2012, Li accepted regular bribes from electronic gambling operators for a sum of NT\$11.14 million in exchange not to disrupt illegal gambling activities. Upon examining the bank accounts of Li, spouse and two children for new time deposits, cash deposits, credit card spending, insurance premium and foreign currency spending from March 2011 to January 2013 and the 3 years afterwards, the prosecution found NT\$11,117,164 of unexplained income after eliminating Li's salary and the amount of bribe received in the above period<sup>11</sup>.

##### (II) Signs of crime and money laundering:

###### 1. Deliver of bribe in cash and in person:

The electronic gambling operators mostly engaged a middleman to deliver bribes to officer's residence, or arranged to meet up at schools or officer's office. Each delivery was between NT\$30,000 to NT\$100,000.

###### 2. Unexplained significant increase of property during the period of bribery:

Chief Li was paid a total salary of NT\$6,704,564 between 2011

<sup>11</sup> High Court criminal judgment No. 2018-Shang-Su-383, Supreme Court criminal judgment No. 2018-Tai-Shang-3337.

and 2015; during this period, Li's account exhibited NT\$23,551,728 of questionable transaction including time deposit - NT\$12.5 million, cash from matured time deposit - NT\$300,000, cash deposit - NT\$2,758,013, credit card spending - NT\$2,366,429, insurance premium - NT\$2,747,076, and overseas study expense - NT\$2,880,210. After deducting salary income and the NT\$5.73-million bribe received during the period mentioned above, Li's household had properties of unknown origin totaling NT\$11,117,164.

### 3. Purchase of NTD and USD insurance policies using bribe:

Part of the bribes received by Chief Li was used to purchase life insurance products in regular installments as well as lump-sum payments. Li would also deposit cash into NTD account, purchase USD currency, and transfer balance to personal foreign currency account for purchase of USD-denominated insurance policy.

## V. Acceptance of bribe involving former Director General of Construction and Planning Agency O-Wen Yeh

### (I) Case summary:

The case involved O-Wen Yeh (Yeh) - former Director General of Construction and Planning Agency, Ministry of the Interior (CPAMI), between August 1, 2008 and June 1, 2013 who was subsequently appointed as Deputy Mayor of Taoyuan County (currently known as Taoyuan City) from July 15, 2013 to May 31, 2014, a civil servant with vested legal authority; O-Huei Tsai (Tsai) - former professor of National OO University; O-Hsiung Chao (Chao) - person-in-charge of Company Y; O-Hsiung Wei (Wei) - Vice President of Development Department at Company Y and Chao's nephew. In 2011, Yeh requested and accepted NT\$4 million in bribes from Chao while serving as Director General of CPAMI in exchange for helping Company Y plan its tender for public housing projects A7 and F. Furthermore, while serving as Deputy Mayor of Taoyuan County, Yeh exploited his position as convener of review

panel for B1 public housing project and requested NT\$26 million in bribes in exchange for disclosure of project details such as floor area ratio, building coverage ratio, basic unit count and map of auctioned land. This information was delivered through Wei to give Chao et al. an advantage to conduct preliminary assessment before it was made public. The actual amount of bribe received amounted to NT\$16 million<sup>12</sup>.

(II) Signs of crime and money laundering:

1. Multiple cash withdrawals and placement of cash inside vault:

To deliver the bribe, Chao instructed innocent accounting staff through assistant vice president or vice president of the company's treasury to make multiple small withdrawals of cash from Chao's account and place it inside vault. Treasury staff was instructed to withdraw cash from vault when it accumulated to the agreed sum of NT\$4 million; the cash was handed over to Chao wrapped in envelope, and subsequently passed on to Wei and to Tsai. Tsai visited Yeh the day after at the CPAMI office to deliver the cash in person. After collecting the NT\$4-million bribe, Yeh placed it at the CPAMI office and personal residence to be used for daily spending.

2. Delivery of cash in luggage case:

The NT\$16-million bribe that Yeh had received in cash on the B1 public housing project was loaded into a purple nylon luggage prepared by Tsai and delivered personally by Chao to Yeh at a specific restaurant in Taipei City at an agreed time. Details of the delivery was relayed through Tsai and Wei to Chao.

3. Placing properties of unknown origin in account of another person:

During investigation, the prosecution retrieved transaction details on bank accounts No. O from Bank A and No. O from Bank B that Yeh had borrowed from a friend named Chen, and found multiple cash deposits and abnormal transactions taking place between

<sup>12</sup> Supreme Court criminal judgment No. 2016-Tai-Shang-969, High Court criminal judgment No. 2015-Zhu-Shang-Su-5.



December 23, 2011 and May 30, 2014 (the day prosecutor began investigation on B1 public housing project), where Chen would pay for securities settlement due on Bank B account using available balances from Bank A account before collecting cash repayment from Yeh. Bank A and Bank B accounts had a total balance of NT\$33,175,678, which was a significant mismatch with Yeh's personal income in the above period.

## Six. Analysis of corruption crime nature and money laundering patterns

Below is a summary of common crime characteristics and money laundering patterns noticed in the major corruption cases presented above:

### I. Use of cash transaction to disrupt cash trail

Corruption is a crime of high secrecy conducted consensually in private between the briber and the bribed. To avoid leaving trail, the bribed party tends to favor cash delivery in person instead of involving FIs for the payment, transfer, or placement of criminal proceeds. Bribe takers who wish to deposit cash into a bank account would use the account of a trusted person or a phantom account to avoid drawing attention to the source of cash, and spread out cash deposit over multiple times and transactions to avoid arousing suspicion from bank staff.

### II. Concealment of cash in safe deposit box

As described above, bribes are mostly received in cash, and have to be kept inside a secure and hidden space. Safe deposit boxes offered by FIs deliver high level of security and secrecy, and therefore are often exploited for placement of criminal proceeds. Bribe takers who are particularly sensitive to public attention would rent safe deposit box from banks either in their own name or the name of family member or friend to stash criminal proceeds. In doing so, they avoid the risk of exposure or

seizure by law enforcement that would otherwise be present if cash was deposited/withdrawn over counter. For the above reasons, reporting entities shall adopt more rigorous practices in the identification of safe deposit box owners, while at the same time monitor abnormal use of safe deposit box to avoid the service being exploited for money laundering.

### III. Laundering of small bribes using automated deposit machine

Apart from simply placing criminal proceeds in safe, hidden places such as a safe deposit box, attempts may also be made to deposit bribes into bank accounts. In order to avoid AML measures of the financial system, bribe takers may choose to deposit cash without engaging a cashier face-to-face, which makes automated deposit machine a preferred way to place criminal proceeds. Using deposit machines, bribes can be deposited into different bank accounts in multiple small transactions without engaging a cashier, and thereby avoid the need for large cash report or enhanced customer due diligence. For the above reasons, reporting entities shall adopt rigorous practices to detect abnormal transactions using automated deposit machines; cash transactions that occur on a regular basis are of the utmost priority.

### IV. Concealing properties of unknown origin using phantom accounts

Civil servants are highly intelligent in general, therefore most corruption cases involving civil servants are committed at high level of complexity. Taiwan revised its Anti-Corruption Act on April 22, 2009 and introduced a new offence called "property of known origin" under Article 6-1 to provide the legal grounds to seize properties that are not commensurate with civil servant's income and that the source of which could not be reasonably explained. The offence applies not only to civil servants, but includes properties of spouse and underage children as well. Implications of this offence have been widely communicated to civil servants, and bribe takers are starting to hide illegal and unreported

properties/income under accounts other than those held by spouse and children, and thereby avoid any unusual increase in property that would attract attention or investigation.

## V. Laundering of criminal proceeds through investment

One of the common money laundering practices involves transferring criminal proceeds into phantom accounts that are within control. The funds may be invested into shares or transferred into personal NTD or foreign currency accounts for the purchase of insurance products; proceeds from policy termination or interests can be credited into specified accounts or converted into other investments to further mask the origin of investment.

## Seven. Related suggestions

From the above examples, it is apparent that most corruption and bribery cases were transacted in cash while some involved lump-sum cash deposit, use of phantom account for concealment, and attempts to launder criminal proceeds through investment there were virtually indifferent from financial crime. FIs may adopt the following practices to identify such activities:

### I. Establish rationality of customers' property and income based on customers' identity

Proper identification allows more accurate detection for abnormal and suspicious transactions. As seen in the above cases, many civil servants deposited large sums into personal accounts or phantom accounts that were under their control, and when the crime was uncovered, they were charged with possession of property of unknown origin for failing to provide reasonable explanation to the source of fund. Some of the cases presented also involved cash transactions exceeding the reporting threshold of NT\$500,000 per transaction that were not commensurate with the account holder's monthly/annual salary. For this reason, reporting entities shall pay particular attention on customers' transactions in relation to their job roles and their explanations to properties of unknown origin, after taking into

consideration their identity, job duties and transaction records.

## II. Identify abnormality of customers' transactions based on industry category

For corruption cases that involved government procurement, it was common for bribers and bribe takers to set kickbacks at a certain percentage of the winning tender amount, and have them paid from briber's company in the name of shareholder loan or financing, or in one large cash withdrawal from the company. Reporting entities may decide whether to file STRs by evaluating the rationality of customer's counterparty, frequency and amount of transaction etc. against usual business activities and collection/payment methods for the specific industry.

## III. Enhanced detection and monitoring of phantom accounts

From the cases above, it was apparent that bribe takers would use friends' accounts as phantom accounts for the acceptance, placement or laundering of criminal proceeds. It may be difficult for FIs to establish direct connection between phantom accounts and bribe takers due to their different background, occupation and area of activity. However, there are still clues to be found for money laundering activities that involve the use of phantom accounts. FIs may identify suspicious phantom accounts and analyze whether transactions taking place within a certain period match the account holder's wealth or income, and follow up with KYC procedures to determine if the account holder is aware of the transactions taking place within the account. For example, if an account exhibits frequent deposit of cash of unknown origin for settlement of share transactions but the account holder is unaware of the assets or amounts transacted, or refers the questions to someone else, then the FIs shall have reasons to believe that customer's account is being used as phantom account, and follow up with actions to investigate the source and destination of funds or establish identity of the actual user and purpose of such an account based on the identity of the proxy trader.

## IV. Establish facts of crime from signs

Based on analysis of the above cases, it is apparent that money laundering in major corruption crimes still fell largely within the 53 signs of money laundering or terrorism financing that have been provided to FIs as reference. Take the bribery case involving former Secretary-General Lin of the Legislative Yuan, for example, the money laundering method met several signs including: "Customer who frequently transferred funds between different accounts for a certain amount and above," and "Customer who made separate cash deposits and withdrawals in amounts below the reporting threshold within a period of time that accumulated to a certain amount or above." Reporting entities may configure their systems to detect certain signs and follow up with more thorough evaluation of customers' identity, occupation and transaction history to determine the rationality of the underlying transaction, and thereby improve the content of STRs submitted.

## Eight. Conclusion

Corruption and bribery are crimes of very high money laundering risk in Taiwan. Cash flows for this type of crime typically occur at higher level of secrecy and are therefore more difficult to identify compared to financial crimes. As a starting point, FIs may begin by establishing the identity, occupation and income of individuals characterized as civil servant, and trace cash flows large and small back to the source to determine the legitimacy of fund, and forward to evaluate whether distribution or placement of capital makes logical sense. By building an overview of customer's wealth and capital usage, FIs will be more efficient at detecting signs such as: abnormal deposit/withdrawal of cash to/from own account or account of others, distribution of criminal proceeds through phantom accounts, use of safe deposit boxes registered in another person's name, and investment with properties of unknown origin. These enhanced practices will further enforce the preventive measures currently in place, and reduce the risk of financial services being exploited by criminals for money laundering.

# Literature references

## I. Chinese materials

### (I) Chinese books:

MJIB Anti-corruption Annual Report 2016, published November 2017.

MJIB Anti-corruption Annual Report 2017, published October 2018.

MJIB Anti-corruption Annual Report 2018, published September 2019.

MJAAC 2016 Annual Report, published July 2017.

MJAAC 2017 Annual Report, published July 2018.

MJAAC 2018 Annual Report, published July 2019.

### (II) Court judgments:

Supreme Court judgment No. 2016-Tai-Shang-2478.

Supreme Court criminal judgment No. 2018-Tai-Shang-2483.

Supreme Court criminal judgment No. 2018-Tai-Shang-3337.

Supreme Court criminal judgment No. 2016-Tai-Shang-969.

Supreme Court criminal judgment No. 2018-Shang-Su-383.

Supreme Court criminal judgment No. 2015-Zhu-Shang-Su-5.

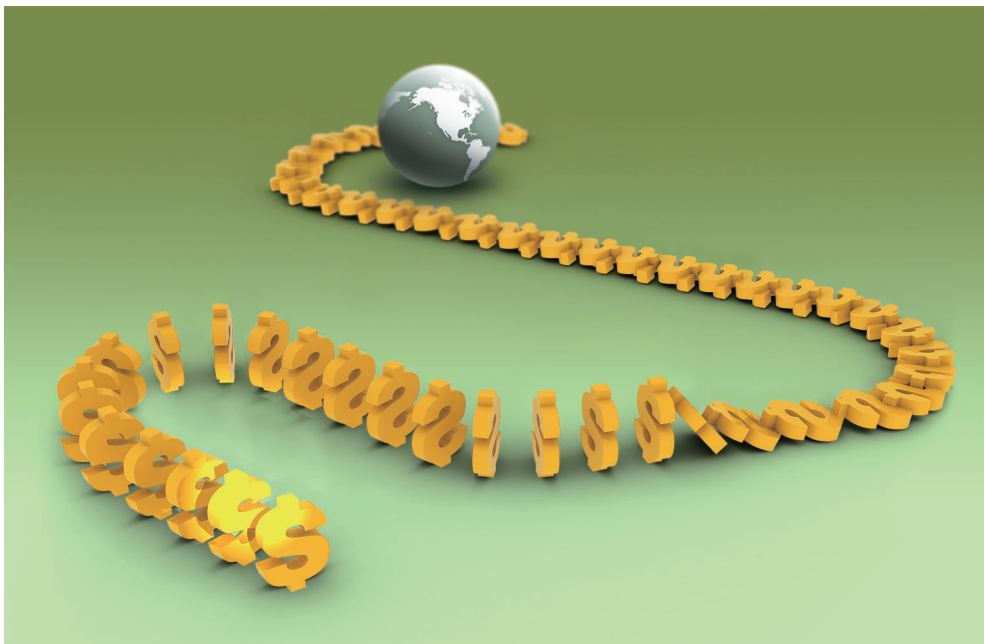
## II. English materials

APG (2019), Anti-money laundering and counter-terrorist financing measures-Chinese Taipei, Third Round Mutual Evaluation Report, APG, Sydney



## Part VI

# Event Calendar of 2019





2019/1/21	Convened "Money Laundering Border Control Coordination Meeting."
2019/1/28-2/1	Assigned staff to participate in Egmont task force meeting at Jakarta, Indonesia.
2019/2/26	Convened "2nd Money Laundering Border Control Coordination Meeting."
2019/3/14-3/15	Participated in the "Mutual Evaluation Face-to-face Simulation Meeting" organized by Anti-Money Laundering Office.
2019/3/18-3/21	Participated in APG's 3rd Mutual Evaluation face-to-face meeting.
2019/5/8-5/9	Participated in "Conference on Execution and Enforcement of International Sanction" organized by American Institute in Taiwan.
2019/5/10	Participated in "Conference on Execution and Enforcement of Policy and International Corporate Sanction" organized by American Institute in Taiwan.
2019/5/13-7/9	Assigned personnel to speak on AML and CTF at MJIB's field offices.
2019/5/24	Cooperated with Banking Bureau of Financial Supervisory Commission and Taiwan Financial Services Roundtable in organizing "Conference on Criminal Cash Flow Analysis and Abnormal Transaction Patterns."
2019/6/11	Participated in "2019 Conference on Money Laundering Control Act Practices" organized by Ministry of Justice.
2019/6/17-6/21	Assigned personnel to participate in FATF's 3rd Plenary Meeting and Work Group Meeting of the 30th year at Orlando, U.S.

2019/6/28-7/6	Assigned personnel to participate in Egmont Group's annual convention in Hague, The Netherlands.
2019/7/3	Signed "Cooperative Agreement on Exchange of Financial Intelligence Relating to Money Laundering, Laundering of Other Assets, Predicate Offences and Terrorism Financing" with Intendente de Verificación Especial de la Superintendencia de Bancos, the Republic of Guatemala, in Hague, The Netherlands.
2019/7/10-7/11	Participated in "2019 Conference on International Legal Assistance in Criminal Matters" organized by Ministry of Justice.
2019/8/18-8/23	Assigned personnel to participate in APG's 22nd Plenary Meeting and Work Group Meeting in Canberra, Australia.
2019/8/20	Signed "Collaborative Memorandum of Understanding on Sharing of Financial Intelligence Relating to Money Laundering, Predicate Offences and Terrorism Financing" with FIUs of Democratic Republic of Timor-Leste, Kingdom of Tonga, and Independent State of Papua New Guinea in Canberra, Australia.
2019/9/23-9/24	Assigned personnel to participate in the 6th annual meeting of "Asset Recovery Inter-Agency Network of Asia/ Pacific (ARIN-AP)" held in Ulaanbaatar, Mongolia.
2019/10/14	Signed "Collaborative Memorandum of Understanding on Sharing of Financial Intelligence Relating to Money Laundering, Predicate Offences and Terrorism Financing" with the Anti-money Laundering and Counter Terrorism Financing Center of Hashemite Kingdom of Jordan.
2019/11/6	Participated in the 2019 compliance forum on "Anti-money Laundering Case Studies" organized by Bankers Association.
2019/11/6-11/9	Assigned personnel to participate in the 2019 "No Money for Terror" Ministerial Conference on Counter-Terrorism Financing in Canberra, Australia.



# ANTI-MONEY LAUNDERING ANNUAL REPORT, 2019

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 2019

GPN : 4310901239

ISBN : 978-986-5443-37-5 (PDF)



**Anti-Money Laundering Annual Report, 2019**  
**Investigation Bureau, Ministry of Justice,**  
**Republic of China (Taiwan)**



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

ISBN : 978-986-5443-37-5



9 789865 443375

GPN : 4310901239