ANTI-MONEY LAUNDERING ANNUAL REPORT, 2017

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

法務部調查局一〇六年洗錢防制工作年報

The Investigation Bureau, Ministry of Justice
Anti-Money Laundering Annual Report,2017

PREFACE

Since the establishment of the Anti-Money Laundering Office, Executive Yuan, the public and private sectors have jointly carried out national money laundering and terrorist financing risk assessment. At the beginning of this year (2018), we finally completed the initial assessment of risks and threats faced by Taiwan, 8 crimes, including drug trafficking, fraud, corruption, securities crimes, tax crimes, smuggling, third-party money laundering, and organized crime, are listed as "very high-risk threats" of Taiwan. After several national risk assessment procedures, Taiwan's first "national money laundering and terrorist financing risk assessment report" was completed and published on May 2, 2018. It shows Taiwan's active response to the mutual evaluation of the Asia/Pacific Group on Money Laundering (APG) and demonstrates Taiwan's ability in meeting international standard requirements.

In 2017, international geopolitical winds were surging, and the situation in East Asia was fluctuating. Certain Taiwanese transported oil products to North Korean vessels and were suspected of violating the sanctions against North Korean resolved by United Nations (UN) Security Council. They were listed on the designation by the TF Review Committee of Taiwan, which was the first targeted financial sanctions rendered after the implementation of the "Counter-Terrorism Financing Act" (CTFA), fulfilling our obligations as a member of the international community. Faced with the rapid development of financial globalization and cross-border criminal activities, all countries are seeking cross-border co-operation to jointly fight crimes. The Anti-Money Laundering Division (AMLD) of the Investigation Bureau of the Ministry of Justice (MJIB), Taiwan's Financial Intelligence Unit (FIU), is dedicated to international co-operation and implementation of international standards. Memoranda of Understanding were signed with 5 FIUs, including the Saint Lucia, Hungary, the Holy See, Latvia, and Ghana, last year for a grand total of 44 countries. It demonstrates that Taiwan's commitment to anti-money laundering (AML) and countering the financing of terrorism (CFT) is widely recognized by the international community.

After the amendment of the "Money Laundering Control Act" (MLCA), the designated non-financial businesses and professions (DNFBPs) are obligated to file reports concerning AML/CFT; also, after the CTFA comes into effect, there are Taiwanese citizens and their offshore companies that were designated as targeted financial sanctions. The number of suspicious transactions report and report related to terrorist financing processed by the AMLD, MJIB has gone up significantly. With the consent of the Financial Supervisory Commission, the insurance industry has been adopting online filing system since October 1, 2017 to improve the reporting efficiency of the industry and to strengthen the efficiency of database construction and implementation, after the banking industry.

The evolution of informationization and digitalization of financial services is relentless. The FinTech issue regarding virtual currency, such as Bitcoin, is in the ascendant. How should law enforcement agencies deal with the increasing digital crime problem? Su, Wenjie, the special agent of the MJIB, gives advices in investigating funds involved in money laundering via virtual currency and the Bitcoin search and seizure faced by the front-line law enforcement officers.

The Financial Action Task Force (FATF) issued the "Private Sector Information Sharing" guidelines in November last year. The AMLD is authorised to translate it into Mandarin and has it included in this annual report for the reference of relevant authorities and 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.

Investigation Bureau, Ministry of Justice
Director General

Shawn C.h. Tsai

July 2018

Editorial Note

I. Purposes

The Recommendation 33 of the Financial Action Task Force (FATF) 40 Recommendations amended in February 2012 states; "Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT (anti-money laundering and countering the financing of terrorism) 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 domestic financial institutions and judicial agencies are summarized in this report.

II. Contents

(I) This Annual Report consists of the following five parts:

1. Background and Organization Structure
2. Work overview (including statistical chart and data)
3. Significant case studies
4. Project research: Funds Investigation Concerning the Virtual Currency with the Procedure of Searching and Seizing Bitcoin Wallets
5. Event Calendar of 2017

(II)The statistics and related information of this annual report is based on the data collected by the AMLD and cases prosecuted by the prosecutor offices for violating the MLCA (including deferred prosecutions and petitions for summary judgment).

III. Notes

(I)The year quoted in this Annual Report refer to the Western 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 prosecutions in Taiwan prosecutor offices and judgments at all levels of courts are based on the number of cases. The value of money is calculated in New Taiwan Dollar (NTD). 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) The newly amended MLCA came into effect on June 28, 2017. The relevant provisions of the Money Laundering Control Act cited in this annual report are revised as follows unless otherwise stated.

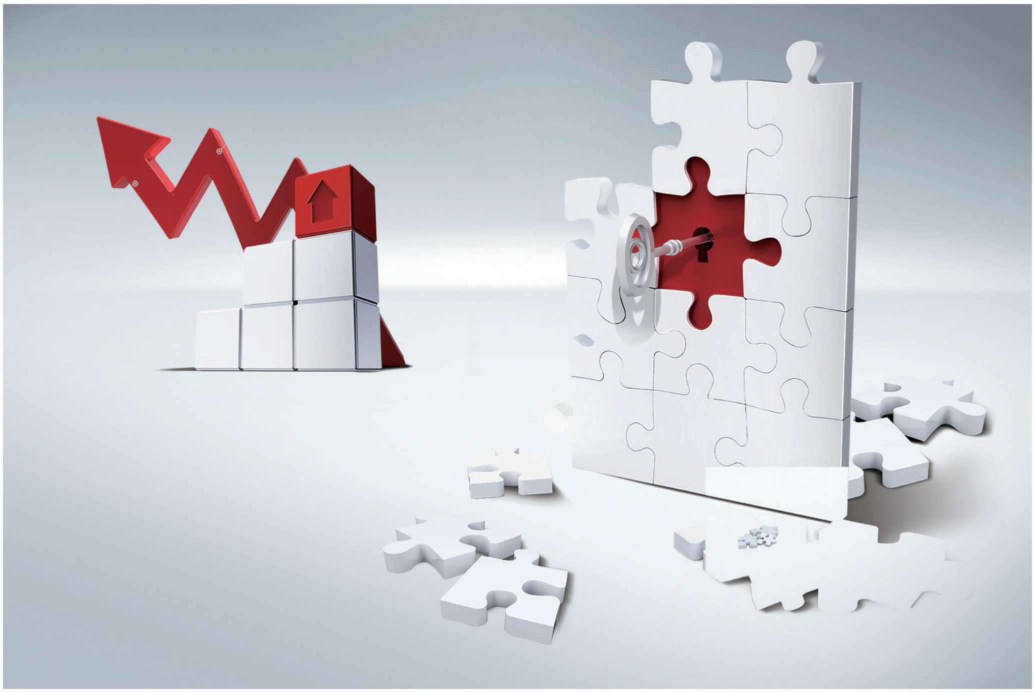
IV. This annual report has been rushed to print; therefore, please feel free to point out the mistakes and incompletions for our correction.

Table of Contents

CONTENTS

Part One:

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 financial institutions (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.

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 and 2016 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 suspicious transaction reports (STRs). Based on the definition in the related international organizations, an authority responsible for receiving and analyzing STRs is called "Financial Intelligence Unit" (FIU). In accordance with the MLCA and the "Key Points for the Establishment of the Money Laundering Prevention Center MJIB", the Investigation Bureau, Ministry of Justice (MJIB) was assigned by the Executive Yuan to receive STRs filed by FIs, and the Money Laundering

Prevention Center (MLPC) was established in 1997 to act as the Taiwan's FIU. In addition, the Legislative Yuan passed the "Organic Act for the MJIB" in 2007. It is clearly enacted in Article 2, Paragraph 7, which the MJIB is in charge of "the AML related matters." Pursuant to Article 3 of the same Act, the MLPC changed the name to the "Anti-Money Laundering Division" (AMLD) and kept on the same functions of Taiwan's FIU. Moreover, Article 7 of the CTFA promulgated in July 2016 stipulates that the MJIB shall receive reports related to TF. The AMLD currently has a Section of STR Analysis, a Section of AML/CFT Strategic Planning, and a Section of Tracing Illegal Funds Flow setup with 25 personnel assigned. Organization and workflow, as shown in Figures A and B.

According to Article 9 of the "Regulations of the MJIB" amended on October 17, 2008, the AMLD is responsible for the following matters:

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

FATF
GAFI

FINANCIAL ACTION TASK FORCE
GROUPE D'ACTION FINANCIÈRE

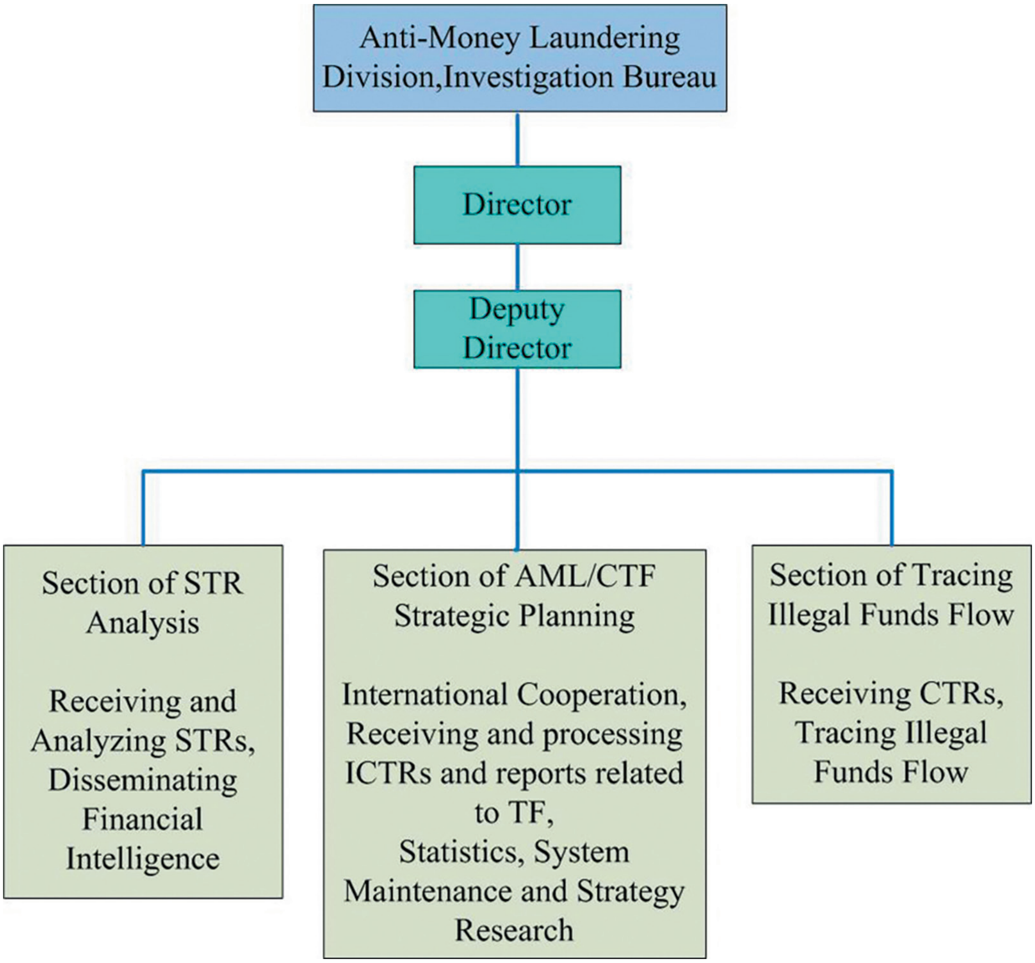
◎ FATF (Financial Action Task Force)

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 37 members (35 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 2 observers that can participate in the General Assembly and working group meetings fully.

Figure A: The AMLD Organizational Chart


Anti-Money Laundering Division,Investigation Bureau
Director
Deputy Director
Section of STR Analysis
Receiving and Analyzing STRs, Disseminating Financial Intelligence
Section of AML/CTF Strategic Planning
International Cooperation, Receiving and processing ICTRs and reports related to TF, Statistics, System Maintenance and Strategy Research
Section of Tracing Illegal Funds Flow
Receiving CTRs, Tracing Illegal Funds Flow

◎ 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: “Counties should establish a FIU with responsibility for acting as a national centre for the receipt and analysis of suspicious transaction reports and other information relevant related to money laundering, associated predicate offences preceding crimes, and terrorist financing, and for the dissemination of the results of that analysis.” Egmont Group, an international organization composed of FIUs of various countries, has the FIU is defined as: “a central, national agency responsible for receiving, (and as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information:

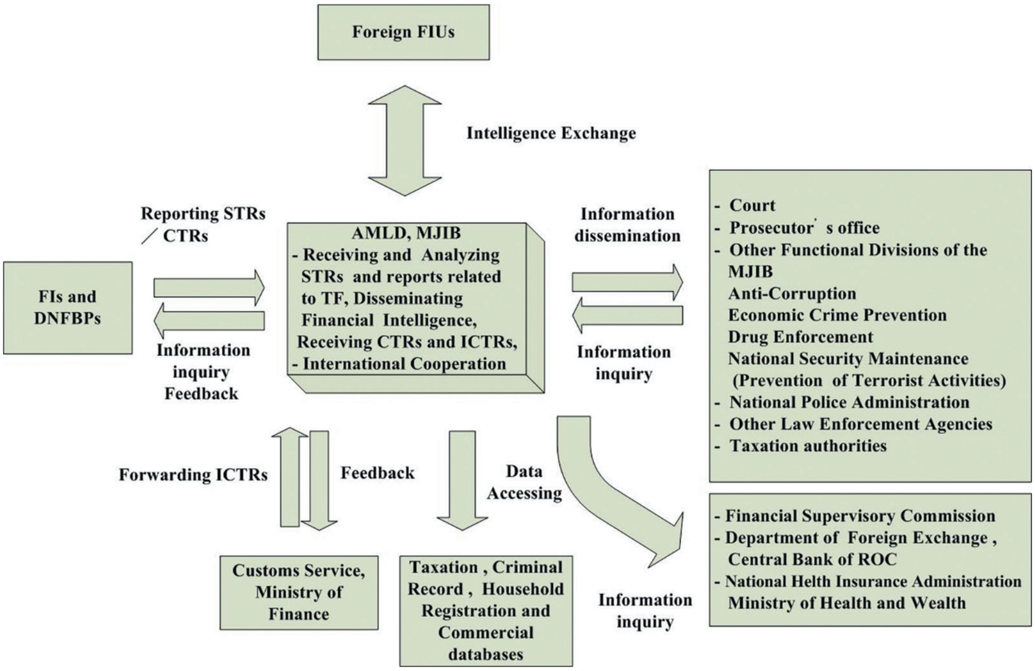
(i) concerning suspected proceeds of crime and potential TF, or

(ii) required by national legislation or regulation, in order to combat ML/TF”.

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: Workflow Chart of the AMLD


Foreign FIUs
Intelligence Exchange
Reporting STRs ／CTRs
FIs and DNFBPs
Information inquiry Feedback
AMLD, MJIB
- Receiving and Analyzing STRs and reports related to TF, Disseminating Financial Intelligence, Receiving CTRs and ICTRs,
- International Cooperation
Information dissemination
Information inquiry
- Court
- Prosecutor's office
- Other Functional Divisions of the MJIB
Anti-Corruption
Economic Crime Prevention
Drug Enforcement
National Security Maintenance (Prevention of Terrorist Activities)
- National Police Administration
- Other Law Enforcement Agencies
- Taxation authorities
Forwarding ICTRs
Feedback
Data Accessing
Customs Service, Ministry of Finance
Taxation , Criminal Record , Household Registration and Commercial databases
Information inquiry
- Financial Supervisory Commission
- Department of Foreign Exchange , Central Bank of ROC
- National Helth Insurance Administration Ministry of Health and Wealth

Part Two:

Work Overview

I. Strategy Research

A. Preparing for the 3rd Round APG Mutual Evaluation

Lunched in July 2017 under a proactive project, the special team led by Deputy Director General Lin is aimed at promoting preparatory works for the 3rd mutual evaluation (ME) of the APG. The AMLD as a hub organizes carefully and coordinates relevant Divisions of the Bureau, including: National Security Operation Division, Anti-Corruption, Economic Crime Prevention Division, Drug Enforcement Division, Information & Communication Security Division, and AMLD itself. A number of meetings were convened with full preparation. In addition, the special team sent representatives to participate in the meetings held by the Anti-Money Laundering Office, Executive Yuan, (hereinafter referred to as the “AML Office”), also provided professional opinions on the national AML/CFT risk assessment report and national technical compliance and effectiveness assessment reports for the reference of the AML Office.

◎ APG (Asia / Pacific Group on Money Laundering)

The APG established in 1997 focused on ensuring its members effectively implement the international standards set by the FATF against money laundering, terrorist financing, and proliferation financing related to weapons of mass destruction.

Taiwan had received 1st and 2nd round of APG mutual evaluation in 2001 and 2007. The evaluation report was approved at the APG Annual Meeting and gave a high degree of credibility to Taiwan’s AML mechanism. The MJIB acted as the FIU of Taiwan with highest performance evaluation received evidences its excellent performance.

At present, the APG has 41 member jurisdictions, 8 observers, and 31 international organization observers that are associate members of the FATF. Taiwan is a founding member of the APG and under the name of "Chinese Taipei;" also, Taiwan may participate in the conference activities of the FATF as a member of APG.

B. Compiling Strategic Analysis of Financial Intelligence

In the process of analyzing STRs, the AMLD may summarizes the emerging methods, transaction patterns and crime trends, the financial intelligence of the year will be compiled after the information is further gathered and have it disseminated to relevant competent authorities, FIs and DNFBPs. Also "The AMLD Collections of Cases" which is a compilation of sanitised cases is published occasionally for the reference of reporting entities and competent authorities. For example, the AMLD found that the number of Offshore Banking Unit (OBU) accounts with Taiwanese banks hold by Chinese or tax haven companies was extremely increasing in 2016. However, FIs faced the challenges to conduct the due diligence on their customers and the access to the information concerning beneficial owners may be hindered. Furthermore, the capacity of FIs to identify the very nature of transaction or business relationship of customers and to confirm the source of funds was impeded. These OBU accounts usually with low balances showed the pattern of frequent transfers of similar amounts both in and out. Taiwan's FIs therefore were exposed to excessive ML/TF risks.

The AMLD then held a Forum on AML/CFT for the Chief Compliance Officer of Financial Institutions in December 2016 for a briefing and discussion on the risk management of problems of these OBU accounts. Then, the AMLD, MJIB has submitted a complete written report "Circumvention of OBU CDD Measures for Unlawful Purpose" to analyze the current OBU business in Taiwan, vulnerabilities of OBU CDD (Customer Due Diligence) measures, risks of OBU's being misused, and regulation for OBU. This analysis report was disseminated to the Financial Supervisory Commission (FSC) and the Central Bank to facilitate the competent authorities in revising the "Rules Governing Offshore Banking Branches" in May (2017). The amended Rules, according to the FATF Recommendation 17, stipulates: "offshore banking branches shall re-perform CDD and review the level of risk on existing customers prior to the implementation of MLCA and CTFA before December 31, 2017." Also it authorizes offshore banking branches may rely on the assistance of intermediaries to perform CDD on customers in accordance with the Rules and MLCA or criteria no less stringent than the relevant regulations to ensure comprehensive compliance and ML/ TF risk management.

C. Processing Reports Related to the Designated Persons and Tracing Funds Flow of Cases

B Corporation, operated by Chen (Taiwanese), rented a Hong Kong-flagged tanker suspected of transferring oil to a North Korean vessel on the high seas in violation of the United Nations Security Council (hereinafter referred to as the UN Security Council) sanctions against North Korea. B Corporation was also the owner of "B No. 18" which had been designated by the UN Security Council since December 28, 2017. Upon receipt of the information, the AMLD immediately analyzed financial information of Chen and his vessels, and then had it submitted to the Ministry of Justice (MOJ) for consideration to refer to the TF Review Committee (hereinafter referred to as the Committee) for reference. The Committee decided to pose financial sanctions against Chen, B Corporation, C Corporation. Offshore companies "O Ltd." and "U Corporation" with Chen as the beneficial owner on January 12, 2018.

The AMLD continuously received reports related to Chen and the aforementioned companies as well as participated in the funds investigation. Moreover, Taiwan Kaohsiung District Prosecutors Office and the MJIB jointly investigated Chen's false declarations.

The AMLD also participated in the joint investigations or project meetings of the following cases: Taiwanese involved the cross-border telecom fraud in Dominican Republic; Ching ○ Shipbuilding Co., Ltd., suspected of defrauding banks.

D. Reception of International Guests

Mr. Dulcidio De La Guardia, the Minister of the Ministry of Economy and Finance of Panama, visited this Bureau on 3rd March 2017. Director General Tsai of MJIB presented a souvenir to the Minister. Both parties held a work meeting on the AML/CFT.

Director General Tsai presented a souvenir to Mr. Guardia.

Ms. LaTeisha Arielle Rachael Sandy, Deputy Director of the St. Vincent FIU, led a team to Taiwan for training. The AMLD conducted a workshop from 18th to 20th October 2017 to exchange opinions on FIU operations and practical experiences.

Director Lee presented a souvenir to Ms. Sandy.

E. Attending International Conferences and Training Courses

The AMLD keeps attending in the annual meetings and working group meetings as well as training courses of international organizations, including the FATF Training & Research Institute (TREIN) standards training, Egmont Group's Strategic Analysis Courses and APG Typologies Workshop, to grasp the emerging the trend and issues, and to improve our performance and international participation.

◎ Egmont Group

Recognizing the benefits inherent in the development of a FIU network, a group of FIUs met at the Egmont-Arenberg Palace in Brussels Belgium in 1995 and decided to found a group for the stimulation of international co-operation. Now known as the Egmont Group of FIUs. The organization provides a platform for the secure exchanges of expertise and financial intelligence to counter ML/TF.

Taiwan has become a member since the 6th annual meeting in June 1998 under the title "Anti-Money Laundering Division, Taiwan" (AMLD, Taiwan) and regularly participates in the annual and working group meetings. The Egmont Group currently is a united body of 155 FIUs. As of the end of 2017, the AMLD of MJIB signed a Memorandum of Understanding with 44 FIUs to facilitate information exchange and international co-operation in accordance with international AML/CFT standards.

20th Annual Meeting of the
Asia/Pacific Group on Money Laundering (APG)
15 - 21 July 2017, Colombo - Sri Lanka

Director Lee of the AMLD and representatives of competent authorities, Taiwan attended the 20th APG Annual Meeting in Colombo, Sri Lanka.

F. Holding a Workshop on Enforcing the MCLA/CTFA

Law enforcement officers play an important role in supporting international and national efforts to combat ML/FT. With the aim of enhancing the related investigation, the AMLD held a workshop to strengthen the understanding of the CTFA and the amended MLCA for the special agents MJIB by presentations and case examples, and introducing databases under the operation of the Division on April 20, 2017.

■ The head of the AMLD, Mr. Lee, delivered a speech at the “The Workshop on enforcing the MCLA/CTFA”

II. Processing the STRs

According to the 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.” After receiving, the STRs will be filed, screened, analyzed, and disseminated to other Divisions of MJIB or other competent authorities by the AMLD. This Bureau received 23,651 STRs in 2017 and the statistics and analysis were distributed by the reporting entities, dissemination, region, month, subjects’ age group, and amounts. Among them, 81.7% of STRs were filed by domestic banks; 35.3% of the suspicious transactions occurred in Taipei City; 51.1% of the subjects were distributed between 31 and 60 years old; and 21.8% of the transaction amount were below $500,000 (Please refer to Table 01 to Table 07 and Figure C to Figure E for detailed statistics and analysis).

A. Statistics of STRs

Table 01: Statistics of STRs

Reporting Entities	No. of Reports
Domestic Banks	19,329
Foreign Banks	30
Trust and Investment Corporations	0
Credit Cooperative Associations	700
Credit Departments of Farmers’ & Fishermen’s Associations	234
Postal Service which handles money transactions of deposit, transfer and withdrawal	2,303

Bills Finance Companies	0
Credit Card Companies	13
Insurance Companies	800
Securities Companies	115
Securities Investment Trust Enterprises	17
Securities Finance Enterprises	5
Securities Investment Consulting Enterprises	0
Centralized Securities Depository Enterprises	24
Futures Commission Merchants	9
DNFBPs	46
China’ s Banks	3
Electronic Payment and Electronic Stored Value Card Issuers	23
	Total: 23,651

Table 02: Statistics of STRs in the last 5 years

Year	2013	2014	2015	2016	2017
No. of Reports	6,266	6,890	9,656	13,972	23,651

B. Dissemination of STRs

Table 03: Statistics of STRs Disseminated by the AMLD

Process	No. of Reports
Disseminated to other Divisions of the MJIB	2,660
Disseminated to LEAs, administrative agencies, and courts or prosecutor offices	920
Stored in the AMLD database for reference	19,664
Under analysis	279
International co-operation	127
Domestic sharing of intelligence	1
	Total: 23,651

C. Distribution of STRs by Region

Table 04: Statistics of STRs by Region

Trading area	No. of Reports	Trading area	No. of Reports
Taipei City	8,341	Chiayi City	340
New Taipei City	3,874	Chiayi County	119
Keelung City	382	Tainan City	1,202
Yilan County	139	Kaohsiung City	1,976
Taoyuan City	1,969	Pingtung County	200
Hsinchu City	474	Hualien County	97
Hsinchu County	279	Taitung County	39
Miaoli County	199	Penghu County	26
Taichung City	2,849	Kinmen County	57
Changhua County	711	Lianjiang County	7
Nantou County	190	Others[1]	26
Yunlin County	155		
			Total: 23,651

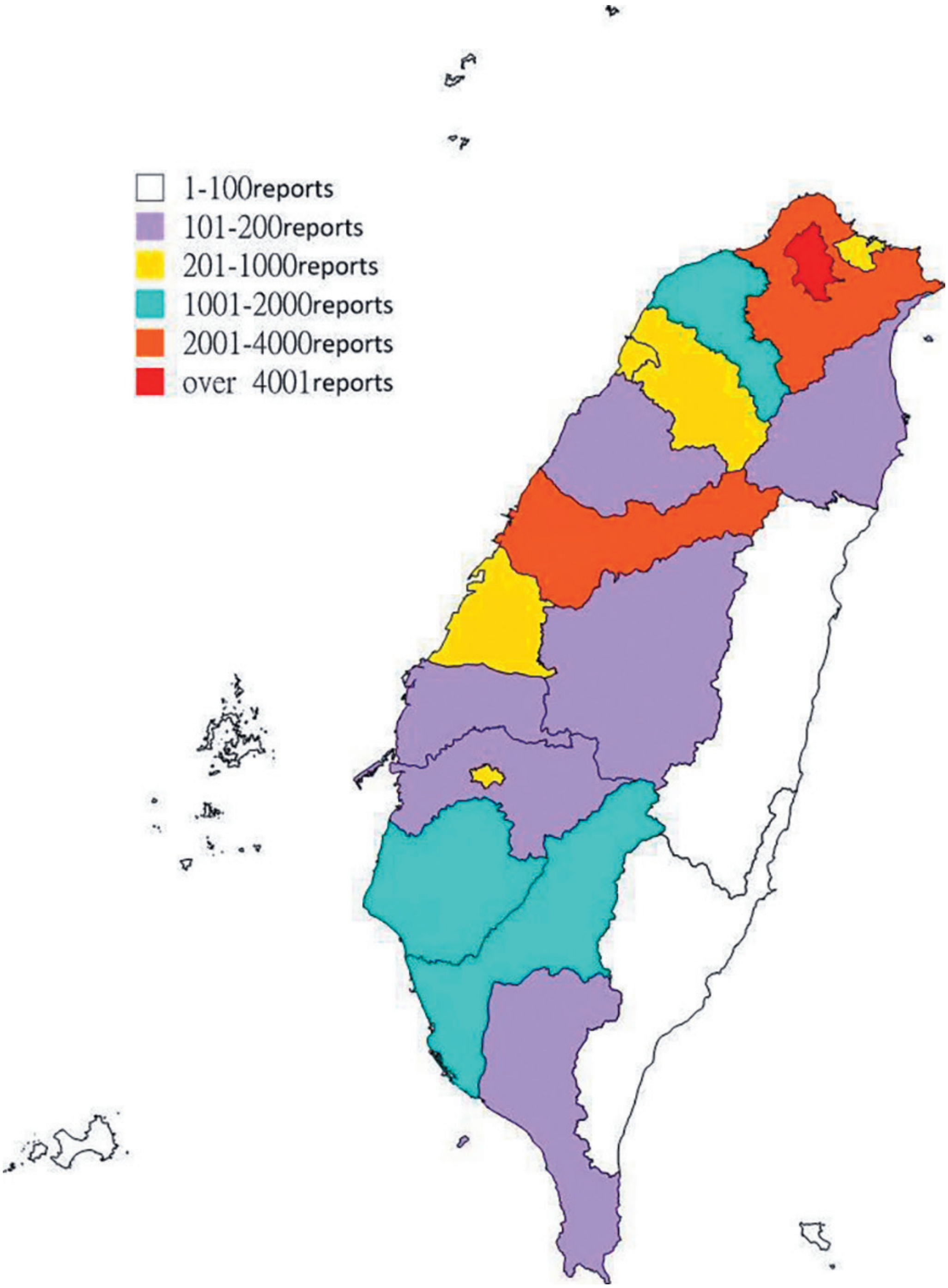
D. Distribution of STRs by Month

Table 05: Distribution of STRs by Month

Month	Jan.	Feb.	Mar.	Apr.	May	Jun.	July	Aug.	Sept.	Oct.	Nov.	Dec.
No. of Reports	1,369	1,184	1,663	1,295	1,511	2,038	1,852	2,348	2,483	1,935	3,001	2,972

[1] Refers to foreign countries, etc.

Figure C: Choropleth Map of STRs Distribution by Region

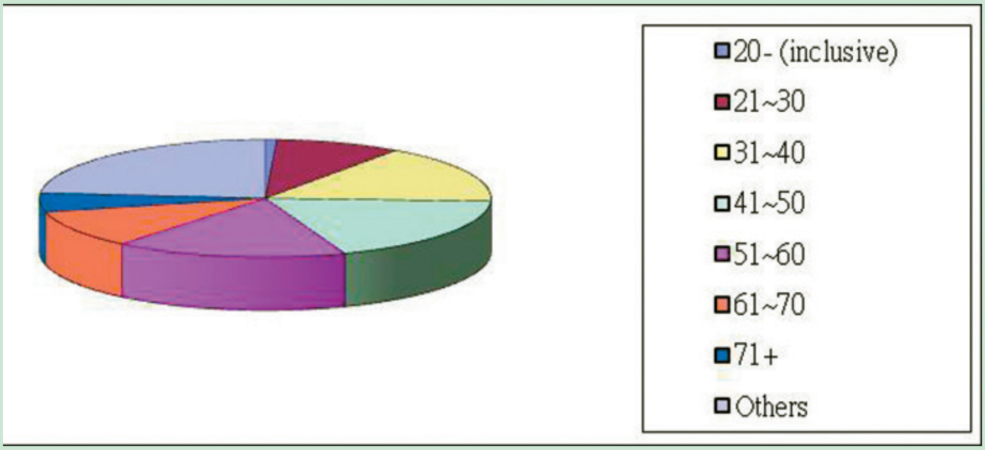


E. Distribution of STRs by Subjects' age group

Table 06: Distribution of STRs by Subjects' Age Group

Age groups	No. of persons
Under 20 (inclusive)	193
21~30	2,129
31~40	3,783
41~50	4,368
51~60	3,938
61~70	2,436
Over 71	1,235
Others[2]	5,569
	Total: 23,651

Figure D: Pie Chart of STRs Distribution by Subjects' Age Group



□ Under 20 (inclusive) 0.82%	□ 21~30 9.00%
□ 31~40 16.00%	□ 41~50 20.17%
□ 51~60 16.65%	□ 61~70 10.30%
□ Over 71 5.22%	□ Others 23.55%

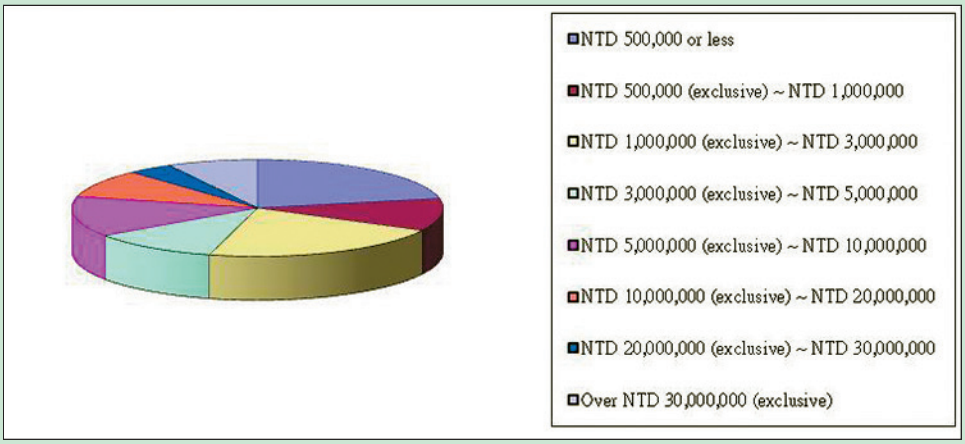
[2] Other: refers to companies, non-corporate groups, etc.

F. Distribution of STRs by Amount

Table 07: Distribution of STRs by Amount

Amounts	No. of Reports
$500,000 or less (inclusive)	5,164
$500,000 (exclusive) ~ $1 million	2,570
$1 million (exclusive)~ $3 million	5,081
$3 million (exclusive) ~ $5 million	2,628
$5 million (exclusive)~ $10 million	3,196
$10 million (exclusive) ~ $20 million	2,212
$20 million (exclusive)~ $30 million	930
Over $30 million (exclusive)	1,870
	Total: 23,651

Figure E: Pie Chart of STRs Distribution by Amount



□ $500,000 or less (inclusive) 21.83%
□ $500,000 (exclusive)~ $1 million 10.87%
□ $1 million (exclusive)~ $3 million 21.48%
□ $3 million (exclusive)~ $5 million 11.11%
□ $5 million (exclusive)~ $10 million 13.51%
□ $10 million (exclusive)~ $20 million 9.35%
□ $20 million (exclusive)~ $30 million 3.93%
□ Over $30 million (exclusive) 7.91%

III. 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). LEAs, judiciary and prosecutor offices are able to access to the CTRs database, after reports are received and filed. The MJIB received 3,543,807 CTRs in 2017 and the statistics and analysis were performed by the reporting entities and amount. 77.98% of CTRs were reported by domestic banks; 73.69% of CTRs were with an amount of $500,000 ~ $1 million. 59,382 transactions in the CTRs database had been accessed in 2017. (Please refer to Table 8 ~ Table 11 and Figure F for detailed statistics and analysis).

A. Statistics of CTRs

Table 08: Statistics of CTRs

Reporting entities	No. of Reports
Domestic Banks	2,763,529
Foreign Banks	16,240
China’ s Banks	1
Trust and Investment Corporations	0
Credit Cooperative Associations	146,835
Credit Departments of Farmers’ & Fishermen’s Associations	29,5670
Postal Service which handles money transactions of deposit, transfer and withdrawal	313,551
Insurance Companies	7,940
Jewelry Retail Businesses	32
Electronic Payment and Electronic Stored Value Card Issuers	9
Total: 3,543,807	

Table 09: Statistics of CTRs in the last 5 years

Year	2013	2014	2015	2016	2017
No. of Reports	3,995,726	4,107,745	3,934,708	3,712,685	3,543,807

B. Distribution of CTRs

Table 10: Distribution of CTRs by Amount

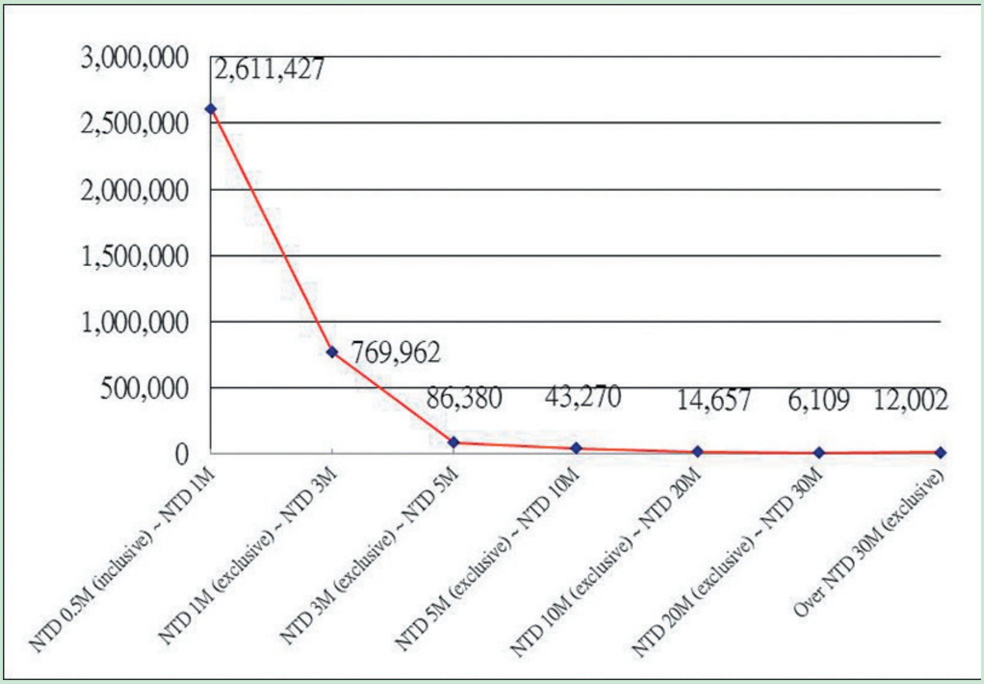
Amounts	No. of Reports
$500,000 (inclusive)~ $1 million	2,611,427
$1 million (exclusive)~ $3 million	769,962
$3 million (exclusive)~ $5 million	86,380
$5 million (exclusive)~ $10 million	43,270
$10 million (exclusive)~ $20 million	14,657
$20 million (exclusive)~ $30 million	6,109
Over $30 million (exclusive)	12,002
	Total: 3,543,807

C. Statistics of Accessing CTRs Database

Table 11: Statistics of Accessing CTRs Database in the last 5years

Year	2013	2014	2015	2016	2017
MJIB	28,205	61,092	36,040	21,413	32,402
Other LEAs	133	10,262	5,641	13,012	17,929
The Judiciary and prosecutor offices	16,010	16,635	8,987	5,186	9,051
Total transactions	55,368	88,464	50,668	39,611	59,382

Figure F: Line Graph of CTRs Distribution by Amount



□ $500,000 (inclusive) ~ $1 million	73.69%
□ $1 million (exclusive)~ $3 million	21.73%
□ $3 million (exclusive)~ $5 million	2.44%
□ $5 million (exclusive)~ $10 million	1.22%
□ $10 million (exclusive)~ $20 million	0.41%
□ $20 million (exclusive)~ $30 million	0.02%
□ Over $30 million (exclusive)	0.34%

IV. Receiving ICTRs

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

According to Article 12, Paragraph 1, of the MLCA: “Passengers or crew members entering or leaving the country along with the vehicle and carry the following items shall make declarations at Customs; the Customs should subsequently file a report to the MJIB. I. Cash in foreign currency or currencies issued by Hong Kong or Macau, and cash in NTD, totaling over an applicable designated threshold. II. Negotiable securities with a face value totaling over an applicable designated threshold. III. Gold with a value totaling over an applicable designated threshold. IV. Other items with a value totaling over an applicable designated threshold and might be used for the purpose of money laundering.”

In addition, according to Article 3 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 33,555 ICTRs were reported to the MJIB in 2017. In terms of the declared value, 81.41% of ICTRs were below $1 million. (Please refer to Table 12 to Table 15 and Figure G for detailed statistics and analysis)

A. Statistics of ICTRs

Table 12: Statistics of ICTRs

Inbound & Outbound	No. of Reports
Inbound	39,213
Outbound	5,952
Total	45,165

Table 13: Statistics of ICTRs in the last 5 years

Year	2013	2014	2015	2016	2017
No. of Reports	14,273	18,781	27,725	33,555	45,165

B. Distribution of ICTRs by Month

Table 14: Statistics of ICTRs by Month

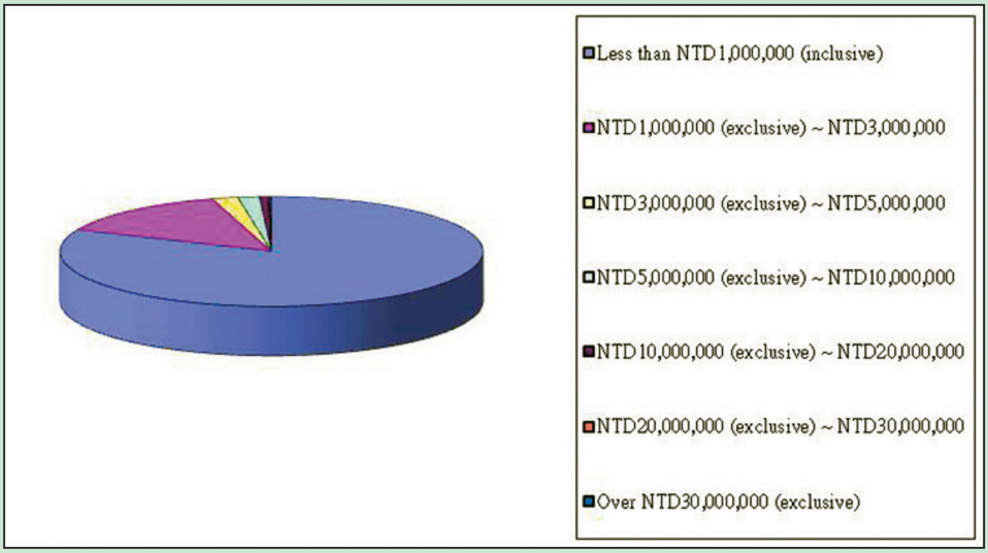
Month	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sept.	Oct.	Nov.	Dec.
No. of Reports	2,575	2,633	3,077	4,154	4,154	3,710	4,537	3,784	3,960	4,583	4,499	3,499

C. Distribution of ICTRs by Value

Table 15: Statistics of ICTRs by Value

Amounts	No. of Reports
$1 million or less (inclusive)	36,769
$1 million (exclusive)~ $3 million	6,350
$3 million (exclusive)~ $5 million	892
$5 million (exclusive)~ $10 million	740
$10 million (exclusive)~ $20 million	315
$20 million (exclusive)~ $30 million	48
Over $30 million (exclusive)	51
	Total: 45,165

Figure G: Pie Chart of ICTRs Distribution by Value



□ $1 million or less (inclusive)	81.41%
□ $1 million (exclusive) ~ $3 million	14.06%
□ $3 million (exclusive)~ $5 million	1.97%
□ $5 million (exclusive)~ $10 million	1.64%
□ $10 million (exclusive)~ $20 million	0.07%
□ $20 million (exclusive)~ $30 million	0.10%
□ Over $30 million (exclusive)	0.11%

V. Statistics of prosecution of ML Cases

Accessing to the Prosecution Document Database Search System maintained by the MOJ, the AMLD organized cases prosecuted for ML (including deferred prosecutions and summary judgments) under MLCA in 2017 according to predicate offences, the amounts, methods, channels of ML cases and so on, for analyzing the trend of crime.

41 cases had been prosecuted for ML and the amount of money laundered reaches $ 15,011,758,137 in 2017. (Please refer to Table 16 ~ Table 20 and Figure H for detailed statistics and analysis).

A. Predicate offences of ML Cases

Table 16: Predicate offenses of ML Cases

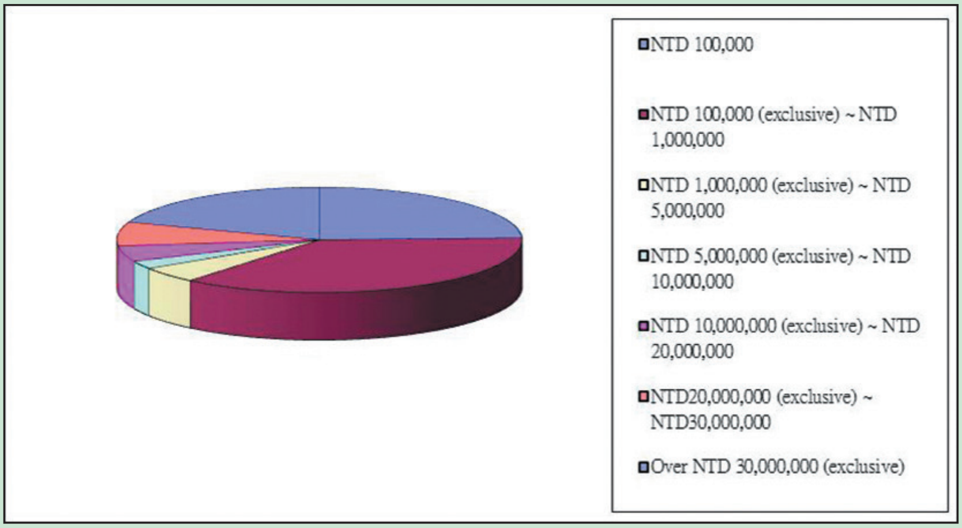
Offence Types	Predicate Offences	MJIB	Prosecutor Offices	National Police Agency	Special Investigation Division	Total
General Criminal Cases	Gambling	0	1	1	0	2
Subtotal		0	1	1	0	2
Drug crimes	Manufacturing, Transporting or Selling Narcotics	0	0	1	0	1
Subtotal		0	0	1	0	1
Economic Crimes	The Banking Act	1	1	3	0	5
	Fraudulence	1	0	29	0	30
	Fraudulence & Receiving Stolen Property	0	0	1	0	1
Subtotal		2	1	33	0	36
Corruption Crimes	Anti-Corruption Act	0	0	0	2	2
Subtotal		0	0	0	2	2
Total		2	2	35	2	41

B. The Amount of Money Laundered in Prosecution Cases

Table 17: The Amount of Money Laundered in Prosecution Cases

Amounts	Cases
$100,000 or less (inclusive)	10
$100,000 (exclusive)~ $1 million	15
$1 million (exclusive)~ $5 million	2
$5 million (exclusive)~ $10 million	1
$10 million (exclusive)~ $ 20 million	2
$20 million (exclusive)~ $30 million	3
Over $30 million (exclusive)	8
	Total: 41

Figure H: Pie Chart of the Amount of Money Laundered in Prosecution Cases



□ $100,000 or less (inclusive)	7.14%
□ $100,000 (exclusive) ~ $1 million	0%
□ $1 million (exclusive) ~ $5 million	10.71%
□ $5 million (exclusive) ~ $10 million	17.86%
□ $10 million (exclusive) ~ $ 20 million	3.57%
□ $ 20 million (exclusive)~ $30 million	0%
□ Over $30 million (exclusive)	60.71%

C. Channels and Methods of ML in Prosecution Cases

Table 18: Channels and Methods of ML in Prosecution Cases

Channels	Cases
Others	4
Banks	37
	Total: 41

Table 19: Methods of ML in Prosecution Cases

Methods	Cases
Dummy Accounts	27
Underground Banking	3
Others	4
Foreign Remittance	1
Friends' Accounts or Properties	4
Relatives' Accounts	2
Total	41
	Total: 41

D. Distribution of ML cases by Region

Table 20: Distribution of ML cases by Region

Region	Cases	Region	Cases
Hualien County	1	Changhua County	4
Kinmen County	1	Taichung City	10
Taoyuan City	12	Taipei City	8
Kaohsiung City	1	Taitung County	2
Hsinchu County	1	Tainan City	1
			Total: 41

VI. Publicity Outreach and Training

A. Publicity Outreach

All field offices of MJIB taking advantage of local activities and public occasions arrange outreaches to the public to increase their awareness of the importance of AML/CFT and their understanding of AML/CFT implementation.

Special agents of Kaohsiung City Field Office, MJIB at the “National Kaohsiung University of Science and Technology 2017 Employment and Internship Fair”

Special agents of Fuchien Field Office, MJIB at the " Wheat and Oyster Festival"

B. AML/CFT Capacity-Building Training

The FATF Recommendation 34 states: "The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist FIs and DNFBPs in applying national measures, and in particular, in detecting and reporting suspicious transaction." The AMLD coordinates training courses for FIs and DNFBPs to better understand the AML/CFT requirements, the compliance with the MLCA as well as the indicators of suspicious transactions in order to improve the quality and quantity of STRs by sharing sanitised cases and providing feedbacks on STRs. These courses also can be a communication channel to avoid ambiguity in understanding in implementation.

Table 21: Statistics of Publicity Outreach and Training

Types of FIs		Subtotal	
		No. of Seminars	No. of Participants
Bank	Domestic Banks (including Financial Holding Companies)	48	3,220
	Foreign Banks	4	118
	China’s Banks	2	50
Credit Cooperative Associations		4	310
Credit Department of Farmers’ and Fishermen’ s Associations		3	414
Securities Investment Trust Enterprises		2	76
Securities Companies		6	650
Futures Commission Merchants		0	0
Postal Service Institutions which also Handle the Money Transactions of Deposit, Transfer and Withdrawal		0	0
Insurance Companies		14	991
Bills Finance Companies		0	0
Others		3	322
Total		86	6,151

VII. International Co-operation

A. International Intelligence Exchange

The FATF Recommendations 40 states: “Countries should 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 authorised to use the most efficient means to co-operate; have clear and secure gateways, mechanisms or channels that will facilitate and allow for transmission and execution of requests; have clear processes for the priorities and timely execution of requests; and have clear process for safeguarding the information received. Where component authorities need bilateral or multilateral agreements or arrangements to co-operate, these should be negotiated and signed in a timely way, and with the widest range of foreign counterparts.”

Table 22: Statistics of International Intelligence Exchange in the last 5 years

Types	Year	2013	2014	2015	2016	2017
Requests from Overseas FIUs	Cases	41	32	51	50	55
	No. of Reports	113	89	152	169	161
Requests to Overseas FIUs	Cases	17	18	45	34	26
	No. of Reports	62	67	222	165	94
Spontaneous Exchanges from Overseas FIUs	Cases	17	33	32	25	53
	No. of Reports	39	58	44	44	100
Spontaneous Exchanges to Overseas FIUs	Cases	4	6	9	26	45
	No. of Reports	11	13	18	45	94
Questionnaires and Other Matters	Cases	0	0	0	0	0
	No. of Reports	100	85	201	262	354
Total	Cases	79	89	137	135	179
	No. of Reports	325	312	637	685	803

B. Concluding Agreements/MOUs with foreign FIUs

ML activities carried out by the criminals occur internationally. For the purposes of effectively combating ML/TF, and the proliferation of WMD, countries are required to reach consensus and closely work together. The AMLD of MJLB, the FIU of Taiwan shares related information with a number of foreign FIUs. Exchanging information benefits not only the operational work of FIUs but also the LEAs to track the proceeds of crimes. The AMLD signed an MOU concerning co-operation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing with St. Lucia, Hungary, the Holy See, Latvia, and Ghana in 2017. As of December 31, 2017, MOUs or agreements were signed with 44 FIUs.

Director Lee of the AMLD (second from the left) , witnessed by Ambassador Lee to the Holy See (in the middle), had an MOU signed with Tommaso Di Ruzza (second from the right), the Director of the Financial Information Authority of the Holy See.

C. Host an International Workshop

Ms. LaTeisha Arielle Rachael Sandy, Deputy Director of the FIU of St. Vincent, led financial investigators to visit Taiwan. The MJIB was commissioned by Ministry of Foreign Affairs to conduct a workshop from 18th to 20th October 2017. A briefing was given on the operation of the AMLD, including the receipt of STRs, CTRs and ICTRs, and the dissemination of the results of analysis. Other Divisions of the MJIB were also invited to share experiences of tracing funds that are proceeds of crimes and to introduce MJIB's efforts on international co-operation. Since these investigators from the St. Vincent were mostly former policemen with law enforcement experiences, the two parties also exchanged views on the co-operation of the FIU and LEAs.

Ms. LaTeisha Arielle Rachael Sandy (right one), Deputy Director of the FIU of St. Vincent led financial investigators to attend the workshop in Taiwan.

Part Three

Significant Case Studies

I. Detecting a Stock Manipulation Case

II. Detecting a Multinational Tax Avoidance Case

III. Detecting an Illegal Fundraising Scheme

IV. Detecting a Fraud and ML Case

V. Assisting to Trace the Funds of the Designated Person, Chen

I. Detecting a Stock Manipulation Case

A. Case Overview

(I) Disclosure of STRs

The AMLD received a STR from Bank A in December 2014: Shih on behalf of JA Company withdrew $24 million dollars in cash with the explanation for purchasing commercial real estate, however Shih was not employed by JA Company. During the same period, Chang, an employee of JA Company, had frequently made cash withdrawals.

(II) Suspect

Jiang, the owner of JA Company; Chang, the secretary of JA Company; Chen, the employee JA Company

(III) Methods

Ms. Jiang in charge of the business of JA Company which is listed on the stock market used the shares of JA Company at a price of $30 plus per share as collateral for loans from many banks since 2014.

Jiang instructed Cheng, Chen, and co-operated with a stock market speculator, Hsu, to increase the stock trading volume by using the securities accounts of 34 persons for the purpose of creating an artificial price for the shares of JA Company, profiting from the sale of stock shares, and avoiding collateral requested by banks. The securities accounts of Z Company, Chen, and the spouse of Shih were involved in the manipulation. From 1st May 2014 to 31st December 2015 (a total of 415 business days), repeated order transactions were made by Jiang's group in 405 business days. The total purchases and sales of Jiang's group accounted for 29.07% and 26.66% of the total stock trading volume of JA Company during the period, of which, the stock price of JA Company was increased by 128.98%. Jiang's group misled the stock price JA Company again in 2016. Jiang and others thus obtained illegal gains totaling $194 million dollars.

B Indicators

Large amount of cash transactions; concealment of beneficial owner of funds

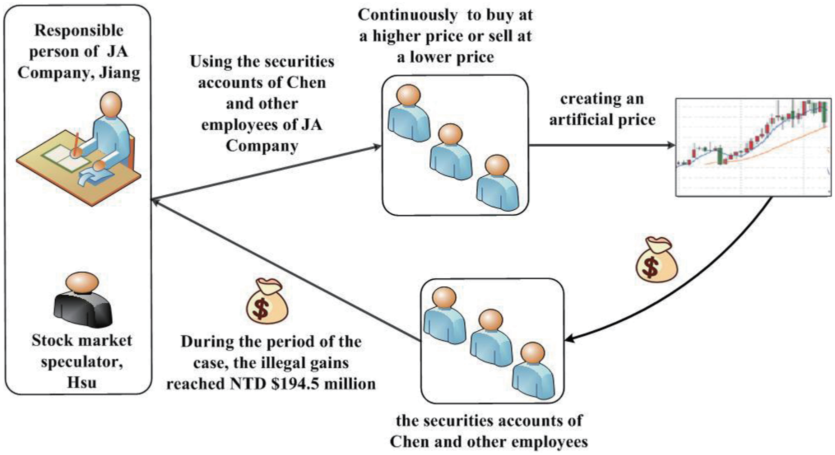
C. Indictment

Jiang and others were indicted on the charges of violating the Securities Exchange Act by the Taiwan Taipei District Prosecutors Office in September 2017.

D. Experience sharing

Upon detecting the unusual withdrawal and the change of trading pattern, Bank A filed a STR and continuously provide financial information on the JA Company's counterparties. The AMLD therefore traced the fund flows to identify securities accounts that may be used by Jiang to manipulate the JA Company's stock price, so that the law enforcement could carry out the investigation accordingly. In addition, other financial institutions also filed STRs related to the relevant parties after the media reports, which assist the subsequent investigation.

Illustration of Jiang Stock Manipulation Case


Responsible person of JA Company, Jiang
Stock market speculator, Hsu
Using the securities accounts of Chen and other employees of JA Company
Continuously to buy at a higher price or sell at a lower price
creating an artificial price
During the period of the case, the illegal gains reached NTD $194.5 million
the securities accounts of Chen and other employees

II. Detecting a Multinational Tax Avoidance Case

A. Case Overview

(I) Disclosure of STRs

Company B submitted a STR in August 2017: ZA Company acquired life insurance from Company B's Offshore Insurance Unit (OIU). The insured was the special assistant to the Chairman of ZA Company for an insurance coverage of US$383.4 million dollars and an insurance premium of US$399.9 million dollars. It is unusual for a company to acquire such a high insurance coverage for its staff.

(II) Taxpayer

Mrs. Hsu, the spouse of the Chairman of ZA Company

(III) Methods

Hsu, Taiwanese, is the Chairman of ZA Company which is registered in SEYCHELLES and Mrs. Hsu is the only shareholder. The actual business office of ZA Company is located in Tokyo, Japan with international trade as the main business operation. In early August of 2017, ZA Company acquired an OIU life insurance coverage of US$383.4 million for the special assistant Ms. Y, a Japanese citizen, and the insurance premium was entirely transferred from Bank C in Country X by Mrs. Hsu to the bank account of Company B in Taiwan.

According to the analysis of the AMLD, Ms. Y with dual citizenship of Taiwan and Japan is actually the first daughter of Hsu. Mrs. Hsu paid the insurance premium through an overseas financial institution with her own funds in the name of the offshore ZA Company to avoid paying gift tax by intentionally hiding the kinship with Ms. Y.

B. Indicators

Others: an unusual insurance policy

C. Gift duty

National Taxation Bureau assessed that Mrs. Hsu, the actual insurance premium payer, should be responsible for paying gift duty with the amount of $20.4 million dollars and then Mrs. Hsu paid completely.

D. Experience sharing

(I) The OIU business has been granted since 2015. According to the Offshore Banking Act, personal insurance business where the applicant is a natural person, a legal person, a government agency, or a financial institution outside the territory of the ROC and the insured is a natural person outside the territory of the ROC. Applicant and the insured however can still evade such restriction with an offshore paper company and dual citizenship in order to avoid paying tax or conceal illegal proceeds; therefore, insurance companies should perform CDD measures and carefully review the clients profile, transaction reasons, business activity, and the source of funds to prevent OIU products from being abused.

(II) This insurance policy was unusual. The insurance company should prudently verify the concerning documents and consider to file a STR to offer information for further analysis or investigation.

(Ⅲ) The offenses listed in Articles 41 and 42, and paragraphs 1 and 2 of Article 43 of the Tax Collection Act are included in “specified unlawful activity” according to the amended MLCA. In the future, financial institutions should pay more attention to transactions which may involve in potential tax evasion for effectively implementation.

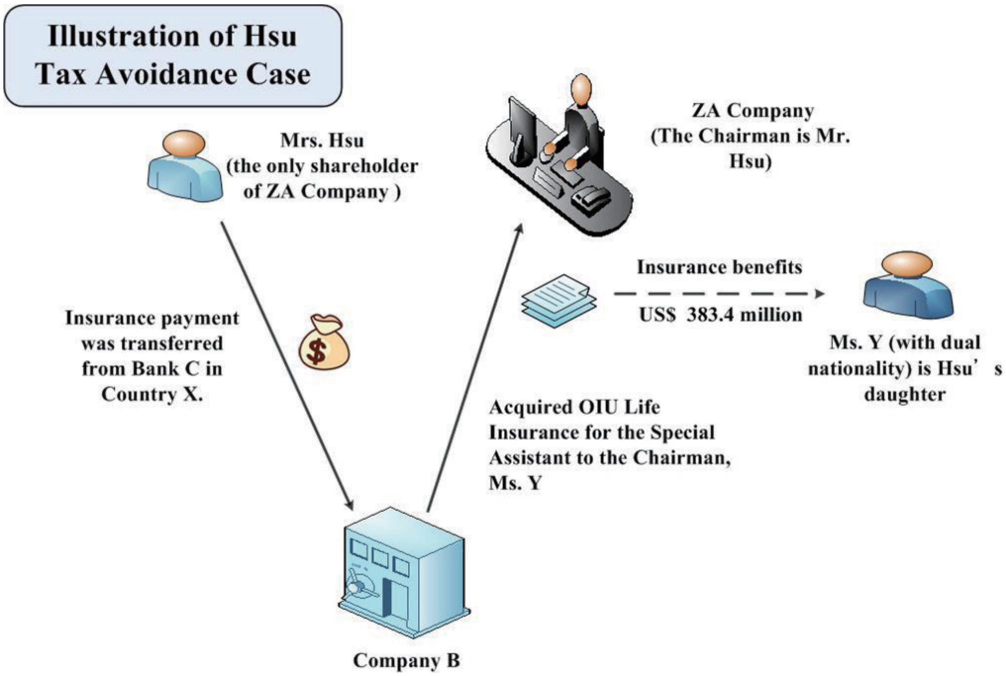


Illustration of Hsu
Tax Avoidance Case
Mrs. Hsu
(the only shareholder
of ZA Company)
ZA Company
(The Chairman is Mr.
Hsu)
Insurance benefits
US$ 383.4 million
Ms. Y (with dual
nationality) is Hsu' s
daughter
Insurance payment
was transferred
from Bank C in
Country X.
Acquired OIU Life
Insurance for the Special
Assistant to the Chairman,
Ms. Y
Company B

III. Detecting an Illegal Fundraising Scheme

A. Case Overview

(I) Disclosure of STRs

Bank C submitted a STR in March 2015: Hong, an employee of M Company, frequently made large cash withdrawals from the account of D Company with Bank C. The account maintained with the same balance every day and the transaction pattern was unusual. In addition, M Company's employees actively lobbied the public to participate in investments and the business model was suspicious.

(II) Suspect

Zhou, in charge of the operation of M Company; Wu and Chen, associates of Zhou.

(III) Methods

Together with Wu, Chen, and others, Zhou jointly organized "M Investment Holdings Co., Ltd." (M Company) to work with the affiliated companies D and E to sell unauthorized investment products such as stocks and shares of M Company, through a pyramid network as well as public activities, including public offering and tours by the guarantee of an unreasonable annual interest rate ranging from 14.34% to 220.8% in the name of "miscellaneous fee," "consulting fee," and "custody fee". M Company however is not allowed to run a business of a bank that to accept investment or deposits.

Moreover, Zhou deliberately paid 2 accomplices to have their names changed to the same name as the Chairman and a board director of the listed technology company X hence investors falsely believed that company X had been cooperating with M Company.

From August 2013 to December 2016, Zhou and his associates had accepted over $4.4 billion dollars for purchasing real property, luxury cars and paying bonus/interests to investors and commissions to employees.

After offices of M Company and residences of Zhou and his associates were searched on 13 December 2016, his associates were arrested; also their cars and cash with the amount of $6.4 million dollars were seized onsite. Then the court, according to the evidence collected, made an order to seize suspects' assets, including 359 bank accounts, 14,051 thousand shares of securities and 145 units of real properties, for a total value exceeding $1.8 billion dollars.

B. Indicators

(I) Frequent cash transactions with a large amount, and the deposit and withdrawal amount were equivalent and in a short interval

(II) The account with a high volume of activity and low balances

(III) Unreasonable wealth compared to the client profile

C. Indictment

Wu, Chen, and others were prosecuted for violations of the Banking Act, Securities Exchange Act, and Criminal Law by the Taiwan New Taipei City District Prosecutors Office in March 2017; however, Zhou was wanted for arrest.

D. Experience sharing

(I) Frequent cash withdrawal triggered an alert therefore Bank C scanned through relevant transactions and actively visited such high-risk client to collect information to evaluate whether the trading pattern concerning ML/TF and to file a STR.

(II) After the case was reported by the media, all financial institutions immediately reported relevant transactions, which was of considerable benefit to the follow-up investigation.

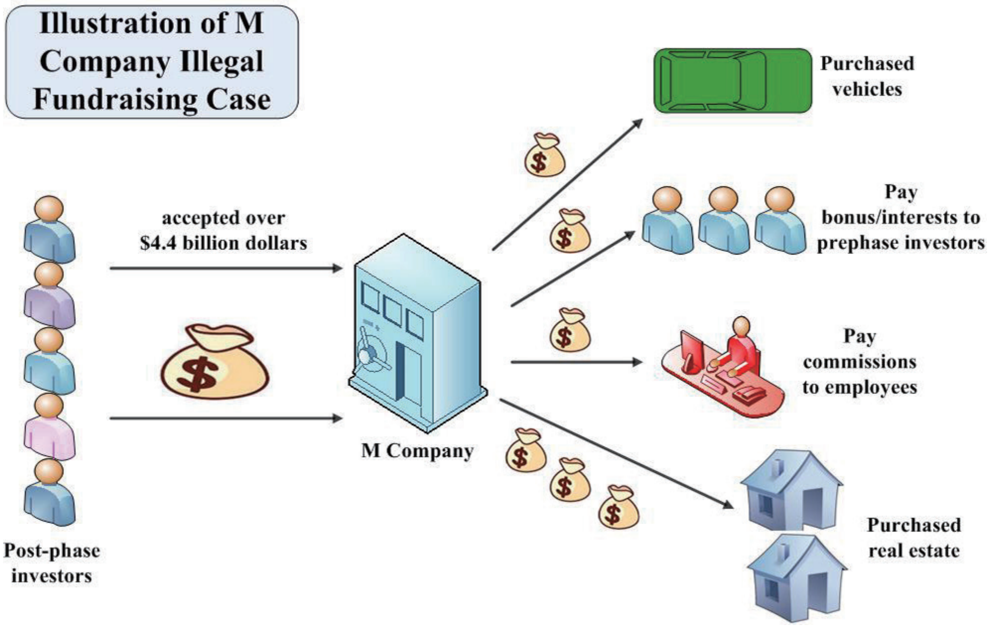


Illustration of M Company Illegal Fundraising Case
accepted over $4.4 billion dollars
Post-phase investors
M Company
Purchased vehicles
Pay bonus/interests to prephase investors
Pay commissions to employees
Purchased real estate

IV. Detecting a Fraud and ML Case

A. Case Overview

(I) Disclosure of STRs

After receiving a STR in August 2016, the AMLD found: funds were transferred frequently among the bank accounts of Li, Da Corporation, Fa Shipbuilding Company, and L3 offshore company. However it seemed that L3 offshore company does not operate. The pattern and amount of transactions were unreasonable compared to the nature of business of Fa Shipbuilding Company and to Li's profile.

(II) Suspect

Chen, Jian, Chen Jr. , Mrs. Chen, Li, and others

(Ⅲ) Methods

Chen is the president of Da Corporation, responsible for all decision-making within the group, including Fa Shipbuilding Company; Jian was the former CEO of Da Corporation. Chen Jr., son of Chen, is the Vice Chairman of Fa Shipbuilding Company and the registered responsible person of 5 offshore paper companies (AZ, OK, L3, HS, and QY). Mrs. Chen, the spouse of Chen, is the board director of Fa Shipbuilding Company. Li was the consultant of Fa Shipbuilding Company and was responsible for assisting Chen Two in managing the Corporation's finance.

Fa Shipbuilding Company won a multi-billion contract to build 6 minehunters for the X Ministry, Taiwan on 23 October 2014. The contract price is $34.9 billion dollars, however capital of Fa Shipbuilding Company was merely $530 million and the Corporation had other investments in Mainland China, the Corporation may not be considered creditworthy enough to get a syndicated loan due to scarcity of capital.

Since November 2014, Chen and others successfully increased the authorized capital of Fa Shipbuilding Company three times, from $530 million to NT$4 billion, by using false documents; therefore, a syndicate (including the lead Bank F for a total of 9 banks) approved a loan of $20.5 billion on 4th February 2016.

Afterwards, Chen and his family forged trading documents, such as procurement contracts, commercial invoices and payment applications, to demonstrate that Fa Shipbuilding Company purchased related equipment from offshore companies (AZ, OK, L3, HS, and QY) in order to apply for transitional loans and disbursement; also, Fa Shipbuilding Company applied to the lead Bank F for a drawdown of the syndicated loan.

Fa Shipbuilding Company had swindled transactional loans 5 times from 4 banks in 2015 for a total amount of USD $67.66 million; again, it swindled the material purchasing fund of "Credit line" for a total of US$58 million between March and May 2016 and the material purchasing fund of "construction account" for a total of USD $76.33 million from a syndicate during 2016.

B. Indicators

(I) New customer with large-scale transactions

(II) Unreasonable wealth compared to the client profile

(Ⅲ) Rapid offshore transfer after funds deposited

C. Indictment

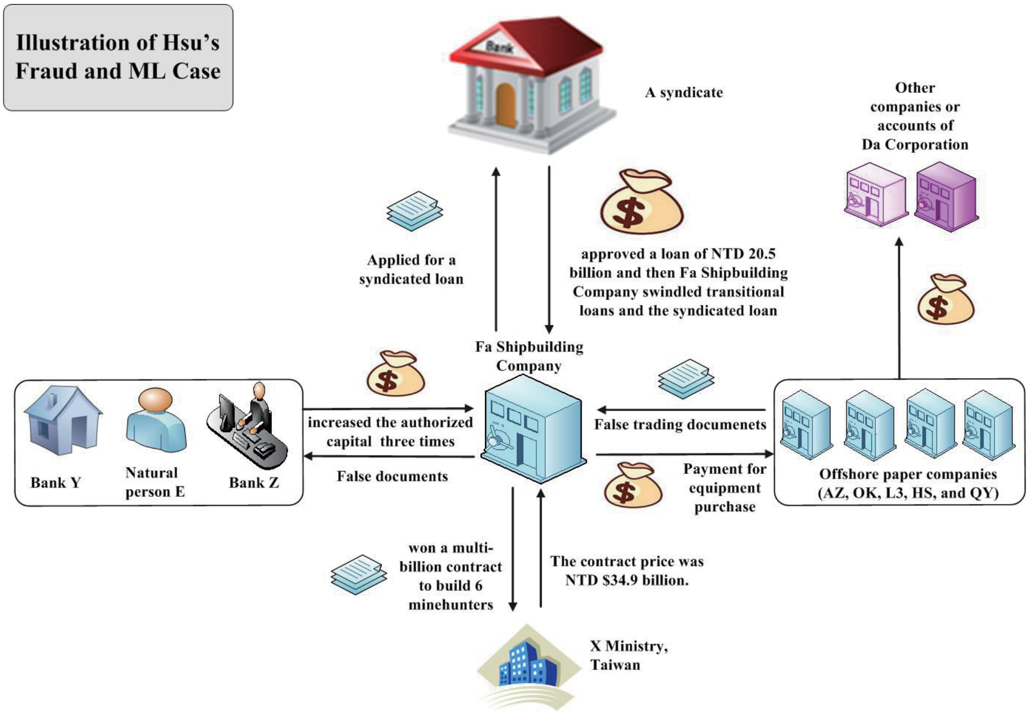
Chen and others were prosecuted for violating the Company Law, Business Entity Accounting Act, Criminal Law, and Anti-Money Laundering Act by the Taiwan Kaohsiung District Prosecutors Office in February 2018.

D. Experience sharing

(I) Offenders often initiated fake transactions through a dummy company or an offshore third party; also, transferred funds through an OBU account to conceal illegal gains. Since clients of OBU are mainly foreign legal persons or natural persons from tax havens, it may be a challenge to identify the beneficial owner of suspicious transactions through online banking. The business of OBU has been assessed to be a "very high vulnerability" of Taiwan according to the national ML/TF risk assessment. When the client refuses to provide or conceal information on the final beneficiaries of the account and the nature of business, or FIs are unable to identify the reasonableness of the transactions after enhancing the CDD and AML/CFT related measures, FIs should report it voluntarily.

(II) In regard of the credit, loan, and post-loan management of legal persons, FIs should identify the final beneficiaries of funds and unusual transactions by collecting the information on client profile, including nature of its business, ownership and control structure, proof of existence, location of operation, financial assets records, source of funds, business activity, business turnover, business relations, counterparties, the contract content and trading documents.

Illustration of Hsu's Fraud and ML Case


Bank
A syndicate
Other companies or accounts of Da Corporation
Applied for a syndicated loan
approved a loan of NTD 20.5 billion and then Fa Shipbuilding Company swindled transitional loans and the syndicated loan
Fa Shipbuilding Company
increased the authorized capital three times
False documents
Bank Y
Natural person E
Bank Z
False trading documenets
Payment for equipment purchase
Offshore paper companies (AZ, OK, L3, HS, and QY)
won a multi-billion contract to build 6 minehunters
The contract price was NTD $34.9 billion.
X Ministry, Taiwan

V. Assisting to Trace the Funds of the Designated Person, Chen

A. Case Overview

(I) Disclosure

On 29 December 2017, the media disclosed that a Hong Kong-flagged tanker rented by B Corporation was seized by the South Korean government for the oil transfer to a North Korean vessel on the high seas. B Corporation was owned by a Taiwanese businessman Chen. FIs therefore immediately filed STRs concerning Chen and offshore companies with Chen as the beneficial owner.

(II) Suspect

Chen

(III) Event Review

Because of violating the UN Security Council Resolution 2375 (2017), the foregoing Hong Kong-flagged tanker was seized and investigated by the South Korean government. The Ministry of Foreign Affairs of South Korea released the news on 29 December 2017.

FIs filed STRs concerning Chen and offshore companies with Chen as the beneficial owner since the news was reported. The AMLD found Chen holds 100% of the shares of 4 companies: B Corporation, C Corporation, O Ltd., U Corporation. Moreover, the UN Security Council Committee established pursuant to Resolution 1718 (2006) designated B No. 18 registered under the flag of Convenience owned by B Corporation pursuant to paragraph 6 of Resolution 2375 (2017) on 28 December 2017 and wished to recall the decision of the Security Council in paragraph 6 of Resolution 2371(2017) that members shall prohibit the entry into their ports of the designated vessel. Under the circumstances, Chen should be responsible for the violation of UN Security Council Resolution.

On 12 January 2018, the competent authority, the Ministry of Justice Taiwan invited representatives of relevant agencies to convene TF Review Committee (hereinafter referred to as the Committee) and the Committee announced to impose targeted financial sanctions against Chen, B Corporation, and Corporation. It was confirmed in the notice that Chen was the beneficial owner of O Ltd. and U Corporation; therefore, necessary measures should be taken against Chen and the four offshore companies in accordance with Article 7, Paragraph 1 of the CTFA. After the designation, all assets under the name of Chen and the four offshore companies should be frozen.

Afterwards, Taiwan Kaohsiung District Prosecutors Office and the MJIB jointly investigated Chen's false declarations.

B. Indicators

(I) Media coverage on accountholders activities;Identify assets of suspect

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

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

C. Experience sharing

(I) The 4 designated offshore companies holds different OBU accounts with many financial institutions. When filing their reports, FIs provided complete registration certificates, shareholders and directors' lists, which assists in clarifying the existence of offshore companies and the movement of funds.

(II) After the designation, FIs promptly complied with CTFA to report the property, property interests of the designated individual and legal persons, and the location of the property or property interests of the designated individual and legal persons. The AMLD received, analyzed STRs and disseminated intelligence to the Ministry of Justice and the relevant competent authorities for reference.

(III) This is the first case of targeted financial sanctions since the implementation of the CTFA announced in Taiwan. After the disclosure of the news, all FIs proactively filed STRs and kept in touch with the AMLD to continuously provide relevant information and documents that assists subsequent investigation and the tracing of funds flow.

Part Four:

Project Research

Project Research

Funds Investigation Concerning the Virtual Currency with the Procedure of Searching and Seizing Bitcoin Wallets

Su, Wenjie[1]

Summary

After the financial tsunami, the introduction of the blockchain has driven many economic demands. Bitcoin as the most mature virtual currency are indispensable. Anonymity and global liquidity of Bitcoin are also preferred. Bitcoin with the characteristics of fast payment and transactions is very different from the traditional or underground banking; also, Bitcoin can be a breakpoint of fund tracking; therefore, it has become a high risk factor in the field of AML that should not be underestimated. This article, based on the spirit of science and technology and empirical practice, explores the search and seizure procedures of virtual currency, such as Bitcoin, and discusses the difficulties and countermeasures encountered in the practice of investigating crimes domestically and internationally from a perspective of risk management in order to study and propose responsive measures and suggestions for the reference of the relevant domestic law enforcement agencies in investigation procedures.

Key words: Money Laundering, Seizure, Bitcoin, Virtual Currency, and Criminal Investigation

[1] Received a master's degree from the Graduate Institute of Science and Technology Law, School of Law, National Chiao Tung University. Currently serves at Taipei City Field Office, MJIB and was once a special agent of the AMLD, MJIB.

I. Background

Five years ago, the terms "Blockchain" and "Bitcoin" were unheard of. In recent years, with the high value and widespread use of Bitcoin, virtual currency has gradually entered the public arena. Related terms, such as, Bitcoin, mining[2], and miners are becoming familiar to the general public; also, related applications are rapidly gaining popularity. Therefore, proprietary terms, including Bitcoin, Initial Coin offering (ICO)[3], and blockchain technology are gradually being used in daily life. As Bitcoin has risen sharply, investors are keen to learn how to make a profit from investing in virtual currency, and advertisements for various virtual currency investments can easily be found on the Internet[4]. In these emerging areas of technology, issues of regulatory control, how to invest, trading platforms, and related exit mechanisms, for example, how to resolve investment disputes, whether the judicial system can offer a solution, various legal issues have emerged, impacting the current institution and regulations.

Such issues arising from emerging technologies, rules and regulations have not fully met the development of technology applications, however academic researches and commercial applications that explore virtual currency and blockchain technology are in full swing. The most initial and mature

[2] According to the "Bitcoin Energy Consumption Index" statistics, as of November 20, 2017, Bitcoin's total electricity consumption for mining in the last year had accumulated to 29.51 TWh, accounting for approximately 0.13% of the world's total electricity consumption. It is equivalent to 11.64% of Taiwan's annual electricity consumption. If the world's Bitcoin miners has their own country, its electricity consumption would be ranked in the 61st place in the world. In addition, according to statistics, the annual cost of mining globally is about US$1.5 billion, but the revenue is as high as US$7.2 billion.

[3] The concept of ICO-Initial Coin Offering, which means "virtual currency initial public offering," is derived from the IPO of the stock market, which means a financing activity that the enterprise or non-corporate organization issues coins with the support of blockchain technology to raise virtual currency from investors (Generally, Bitcoin and Ethereum). The difference is that IPO companies are issuing stocks to the public to raise funds for business development; however, ICO companies raise funds from the public for business development with the subject matter converted from securities to virtual currencies.

[4] Currently, Google, Twitter, and Facebook ban virtual currency-related advertising.

application of Bitcoin and blockchain particularly is to hide fund flows from tracking, a main advantage for illegal groups or individuals. A well-known case in the United States was "Silk Road," an online black market involving drug-dealing, firearms trafficking, pornography, and human trafficking. It was difficult to trace the use of Bitcoin payment transactions. At the time, such emerging payment instruments were not widespread; therefore, it had become the first choice for website payments. The website had been investigated and shut down by the Federal Bureau of Investigation (FBI); also, the 175,000 Bitcoins of the owner of "Silk Road" were seized, accounting for about 2% of the global Bitcoin stock at that time.

Tracing illegal proceeds has always been the focus of criminal investigation in Taiwan. Taiwan's laws and regulations have been in line with international standards in recent years. However, criminal cases of money laundering, illegal fund raising, or fraudulence involving virtual currency are still with blind spots due to the anonymity and liquidity of Bitcoin. It is often necessary to clarify the nature of transactions and the destination of funds through international cooperation (such as, Europol's European Cybercrime Center, EC3[5]) or corporates' informal mutual assistance. Additionally, law enforcement agencies still face challenges that to seize virtual currency at a crime scene, to persuade the suspect to cooperate and hand over the private key, and to prevent a third party from using the known private key to move the Bitcoin to other wallets before the law enforcement officials completing the seizure of the Bitcoin. Take Taiwan's largest Bitcoin fraud case detected by the MJIB in June 2018 for example, the multinational group illegally raised fund for more than $1.5 billion. Although a rehearsal had been carried out several times before the search and arrest, it remains a big challenge for law enforcement officials to effectively seize several hundreds of Bitcoins in a short time. Obviously, law enforcement agencies must deal with legal

[5] European Cybercrime Centre (EC3) was established in 2013 and located in the headquarters of Europol in Hague, the Netherlands. It coordinates international crime investigation and is also a technical consultant in the professional field of computer crime and virtual currency crime.

ambiguity and investigation predicament which have occurred in practice. Hence, this article focuses on introducing emerging issues of Bitcoin transactions based on blockchain; also, discusses the countermeasures for the law enforcement agencies while facing the virtual currency, including Bitcoin in the search and seizure site. Moreover, it provides suggestions on the seizure procedure and digital forensic tools. By Combining the actual practice of FBI, EC3, and the MJIB, it proposes effective practices for the reference of domestic relevant law enforcement agencies.

II. Risks of Virtual currency involving money laundering and other crimes

A. International organizations

Virtual currency has the characteristics of anonymity, liquidity, and immediacy of transactions. Coupled with its global influence, potential risks of ML/TF includes greater anonymity; may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source); may permit anonymous transfers, if sender and recipient are not adequately identified. The virtual currency system can be accessed via the Internet (including smart phone built-in application software) and can be used for cross-border payments and funds transfer. The system has no central server or service provider. For the implementation of AML/CTF, it involves regulation institutions and law enforcement agencies of several jurisdictions; however, there is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear6.

Financial Action Task Force (FATF) pointed out that "virtual currency is a complex issue that involves not only AML/CFT issues, but also other regulatory matters, including consumers protection, prudential safety, tax and soundness regulation, and network IT security standards." [7] As pointed out in the National Crime Agency's June 2015 report, "The use of virtual currencies to launder funds is currently mainly the perspective of cyber criminals and has not yet been adopted by the wider criminal community. We assess that this is, in part, due to a lack of familiarity with virtual currencies, and the

[6] Financial Action Task Force, "Guidance for a Risk-Based Approach Virtual Currencies," June 2015, No.13, pp.31-32.

[7] Robert W. Wood, "Bitcoin: Tax Evasion Currency," FORBES, 7 Aug. 2013. Also see http://www.forbes.com/sites/robertwood/2013/08/07/ bitcoin-tax-evasion-currency.

relative difficulty of exchanging them into hard currency without some degree of exposure to the regulated sector. However, if they embed themselves in the public consciousness and become more widely accepted as a payment method, law enforcement can expect to see a corresponding increase in their adoption by traditional (non-cyber) criminals, both as a vehicle to launder funds and as a means of payment for illicit goods and services." [8]

B. Europe and America

On September 30, 2015, Europol (EU law enforcement agency) released the "2015 Internet Organized Crime Threat Assessment (IOCTA)[9]," stating the viewpoint on the biggest cybercrime threat faced by the EU. The report mentions Bitcoin and virtual currency issues in different types of crime, including illegal financing and illegal activities related to this technology. According to statistics, Bitcoin is beginning to feature heavily in many EU law enforcement investigations, accounting for over 40% of all identified criminal-to-criminal payments, while PayPal[10] only accounts for 25%[11] of identified payments. The aforementioned data show that virtual currency has become an important trend in the development of the "criminal activity services" ecosystem. The "2015 Internet Organized Crime Threat Assessment (IOCTA)" report also pointed out: "Although there is no single common currency used by cybercriminals across the EU, it is apparent that Bitcoin may gradually be taking on that role. Bitcoin features as a common payment mechanism across almost all payment scenarios, a trend which can only be expected to increase." [12]

[8] National Crime Agency, "National Strategic Assessment of Serious and Organised Crime 2015," June 2015, p.22.

[9] The European Police Office, "The 2015 Internet Organised Crime Threat Assessment," Europol, 30 Sep. 2015, < https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015>.

[10] PayPal is the world's largest online cash flow system and is currently a subsidiary of eBay.

[11] Same Note 9, Page 46.

[12] Same Note 9, Page 47; "Although there is no single common currency used by cybercriminals across the EU, it is apparent that Bitcoin may gradually be taking on that role. Bitcoin features as a common payment mechanism across almost all payment scenarios, a trend which can only be expected to increase."

The Securities and Exchange Commission (SEC) of the United States stipulated in July 2017 that organizers of "Initial Coin Offerings" or "Token Sales" based on distributed ledger and blockchain technology should comply with federal securities regulations. In September 2017, the SEC further announced that Cyber Unit is created to investigate cyber-related misconduct. In the same month, it charged two ICOs enterprises with violating anti-fraud and registration provisions of the US Securities Exchange Act. The SEC announced in January 2018 that it is looking closely at public companies that suddenly change its names to blockchain-related or shift their business models to capitalise on the promise of distributed ledger and immediately offer securities to take advantages of blockchain hype.

C. Mainland China

On September 4, 2017, seven central regulators, including the People's Bank of China (PBOC), the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), the State Administration for Industry and Commerce (SAIC), the China Banking Regulatory Commission (CBRC), Securities and Regulatory Commission (CSRC), and China Insurance Regulatory Commission (CIRC), jointly issued the "Announcement on Preventing Financial Ricks from Initial Coin Offerings (ICO Rules)[13]." The ICO Rules clearly identified that ICOs engaging in public financing is illegal, which greatly shocked ICOs activities in China. The contents of the announcement are explained in six aspects: accurate understanding of the essence of ICOs, no organization or individual may engage in ICOs, imposing restrictions on the primary business of virtual currency trading platforms, prohibiting FIs and non-bank payment institutions from accepting any existing virtual currencies or providing relevant services, warning citizens about the risks of virtual commodities, and fully exercising the self-discipline of the industrial organization. Following the announcement,

[13] People's Bank of China, September 4, 2017, <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html>.

ICOs and related fundraising activities that were booming in the Chinese market came to an abrupt end. Several well-known trading platforms immediately suspended all ICOs services. In addition, platforms must liquidate and refund investors. At the same time, the Chinese government had intensively inspected the ICOs trading platforms. Fundraising through ICOs is completely banned, and the regulatory authorities could be described as acting vigorously.

According to the ICO Rules, ICOs that raise virtual currencies such as Bitcoin and Ethereum through the irregular sale and circulation of tokens are essentially engaging in public financing without official authorization, which is illegal. The ICO Rules warn that financial crimes, such as the illegal issuance of tokens or of securities, illegal fundraising, financial fraud, pyramid schemes, may be involved in ICOs. The various crimes mentioned therein are quite close to the press releases issued by the Financial Supervisory Commission of Taiwan (hereinafter referred to as the "FSC")[14]. The FSC stated in the press release on December 19, 2017: "If ICOs involves fundraising and the issuance of securities, it should comply with relevant provisions of the Securities Exchange Act; if issuers selling tokens through ICOs attract investors by misleading or false technology and/or achievements, for example unreasonable high rate of return, they may have committed a crime of fraud or illegal fundraising. It is obvious that the regulatory agencies in different jurisdictions have similar views on the financial crimes that may be involved in ICOs.

D. Japan

Unlike China, virtual currency regulations in Japan is much looser, which is worth of observation. So-called "Virtual Currency Act" (the Act), was approved by The House of Councilors (Sangiin) in 2016 and took effect in

[14] Financial Supervisory Commission, December 19, 2017, <https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201712190002&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News>.

May 2017. The Act defines virtual currency as “asset-like” value rather than a kind of commodity[15]. At the same time, Japan adopts a registration system that only companies registered with competent authorities are allowed to operate virtual currency exchange business and provide the service that trading virtual currency against Japanese yen or other national currencies. Moreover, Japan government amended the “Prevention of Transfer of Criminal Proceeds Act”, and virtual currency exchange operators are imposed AML obligations according to the amendment. The revised “Payment Services Act” includes new provisions concerning virtual currency.

In summary, Japan recognized the “asset-like” value of virtual currency and allowed it to be transferred and be used for payment and digital transactions. However, virtual currency exchange operators must register with the government and be audited and supervised.

In April 2017, the amended the “Payment Services Act” defines virtual currency as a legal payment tool in the Japanese market. In September of the same year, the “Financial Services Agency” (FSA) of Japanese government developed regulations and issued 11 virtual currency exchange business licenses after accepting and examining applications filed by companies. However, when the Japanese government promoted financial innovation, it also actively prevented money laundering and other crimes. The FSA established an inter-departmental team in October 2017 with a virtual currency supervision position created to supervise virtual currency transactions. According to the FSA regulations, virtual currency exchange operators must establish a safe and comprehensive computer system. Employees must complete pre-employment training, customer accounts should be quarantined, and customer identities must be checked to avoid hacking or being abused as a vehicle for money laundering.

Japan has opened up a portal of virtual currency exchange. Although it creates commercial interests, it also causes crimes to take place. The National

[15] Huang, Jingjing, “Japanese Love Bitcoin,” “Commercial Times,” January 4, 2018, <http://www.chinatimes.com/newspapers/20180107000393-260209>.

Police Agency, Japan recently published the first statistics on the virtual currency hacks and losses. 149 criminal cases concerning virtual currency occurred in 2017, resulting in a property loss of approximately 662.4 million Japanese yen. The police also found that 16 virtual currency exchange operators suffered losses due to illegal transactions of hackers. The most affected virtual currencies were Bitcoin, Ripple and Ethereum. There were 85 times attacks on Bitcoin, 55 times attacks on Ripple and 13 times attacks on Ethereum.

In addition, financial institutions' online banking services were hacked for 425 times and lost approximately 1,081 million yen according to the information released by the Japanese government. However, the number of aforementioned attacks were only one-fourth of that in 2014 and the amount of related criminal cases dropped to one third of that in 2015. Experts point out that this trend may mean criminal groups are shifting their targets to virtual currency investors who are more vulnerable than the business operators[16].

E. Other areas

The Reserve Bank of India (RBI) restricted the banking systems to do business with the enterprises or individuals engaging in virtual currency exchange and warned that there were still risks of consumer protection, market integrity, and money laundering on April 5, 2018. Also, banks must terminate virtual currency exchange services within 3 months; however, RBI has also established a trans-departmental unit to conduct research on legal cryptocurrencies, which is expected to be released at the end of June, 2018.

The South Korean Financial Services Commission (FSC) banned the ICOs in 2017, and announced that it begins a real-name registration mandatory for cryptocurrency traders from January 30, 2018 to prevent speculation and money laundering. Only the wallet accounts of the cryptocurrency traders

[16] Tsai, Peifang, "Virtual Currency Crime Day Over 100 Transactions in 2017," March 22, 2018, "UDN Paper," <https://udn.com/news/story/11316/3046692>.

which matches their real-name bank accounts can be used for withdrawals or deposits. At the same time, the South Korea government also prohibits minors and foreigners from setting up local cryptocurrency wallet accounts. In addition, the Ministry of Strategy and Finance, South Korea has begun to impose a 22% corporate income tax on the local cryptocurrency trading platforms since the end of March this year, and a 2.2% local income tax since the end of April 2018.

F. Taiwan regulations

In recent years, the increasing use of emerging cryptocurrencies or related derivatives as criminal vehicles has attracted the attention of domestic and international law enforcement agencies. In mid-June 2018, the MJIB also cracked a serious Bitcoin illegal fundraising case. Lin and others of the IRS Group were suspected of luring the public to make a profit by investing in Bitcoin. Such investors may purchase an investment package ranging from US$100 to US$7,000 to exchange for the equivalent "RM" (reserve money). RM has a fixed value increase of 0.35% per day; therefore, investors can recover up to 355% of principal and interest after one year. As Bitcoin is the investment target in the case, the MJIB and Taichung District Prosecutors Office jointly set up a task force to trace the funds and to confirm the flows of Bitcoin; also, to get specific evidence of illegal fund-raising, fraud and money laundering. On June 13, eight suspects including Lin were interrogated; their residence was searched; and other evidence, such as bank passbooks or investment documents were seized. In addition, 26 bank accounts of the suspects were frozen and 196 Bitcoins (market price of more than NT$40 million) were seized. The IRS Group have fleeced more than NT$1.5 billion in Mainland China and Taiwan from 2017. Lin and his associates, good at operating Bitcoin, attempted to create a breakpoint of funds flow and to conceal the proceeds of crimes by buying Bitcoin and then transferring it offshore. In order to successfully solve the case, the MJIB had the Bitcoin seizure tool studied and ready for use and the professional agents were at the search site to assist in seizing Bitcoin.

In addition, regarding the regulations and legal status of Bitcoin, it is not clear in most countries in the world, which is likely to cause controversy in the practice of seizure. Peng, who served as the president of the Central Bank of Taiwan (hereinafter referred to as the "Central Bank"), answered to the inquiry in the Legislative Yuan on November 23, 2013 that Bitcoin is not legal tender and is limited to be used in transactions between issuers and its' members. The game points currently issued by the video game manufacturers were similar to the payment application of Bitcoin; therefore, the Central Bank would have Bitcoin transactions treated as precious metal trading for management.[17] On November 27 of the same year, Peng once again announced in the Legislative Yuan that Taiwan's payment methods were mainly the currency issued by the Central Bank, according to the provisions of the "Central Bank Act"[18]. While he was about to retired from the position, he had pointed it out clearly that virtual currency involved money laundering, which was an issue to be taken seriously. Therefore, the Ministry of Justice invited the Central Bank, the Ministry of Economic Affairs, the FSC, the National Police Agency of the Ministry of the Interior, and the MJIB to jointly conduct research on the current regulations and practices in April 2018; also, to propose draft AML regulations concerning virtual currency before the end of this year[19].

[17] Tsai, Yizhen, "Bitcoin Money Laundering by Peng, Huainan: The Central Bank pays close attention to," "EtToday" January 24, 2016, < http://www.ettoday.net/news/20131120/298323.htm >.

[18] Lu, Guancheng, <Bitcoin Popularity, Peng, Huainan: Bubble>, Liberty Times, January 24, 2016, <http://news.ltn.com.tw/news/business/paper/734193>.

[19] Wang, Shengyu, "Peng, Huainan wrote to Chou, Taisan, the virtual currency included in the anti-money laundering norms," "UDN News," April 10, 2018, <https://udn.com/news/story/7321/3078861>.

III. Bitcoin and blockchain

Bitcoin is built on the application of blockchain. Blockchain means a "long chain of interconnection blocks." To understand the principle of blockchain, we must first understand two concepts, transactions and blocks. "Transaction" means a record in which all Bitcoins have been transferred at different Bitcoin addresses; each Bitcoin transfer is a transaction without any exception; "Block" is a type of cyberspace loading and "Block" is loaded with the records of all Bitcoin transactions. The relevance of the two is that the "transaction" is periodically caught and "loaded" into the block.

In short, a blockchain can be deemed as a worksheet in an Excel binder. Each Bitcoin transaction is recorded on a single row and each worksheet is a block. Blockchain has the data stored in a Flat File, which refers to a file containing a non-relative structure, usually in text format, such as a text file (".txt") format and the block is arranged in a structured manner in accordance with the transaction time; also, all the transactions recorded in the Bitcoin network are stored in the block. The difference between the blockchain and the worksheet in the Excel binder is that the former uses the link formed by the mathematical calculation principle to store the transaction in the block.

Each block has a header and the header will record the information of the block, including: (1) The hash value[20] of the previous block will point to the previous block so the two blocks will be linked intangibly; (2) Block Height: Bitcoin was first introduced on January 3, 2009, when the block height was 0 and the block height was increased along with the increase of each block starting from that day. The block height reached 524,670 on May 27, 2018[21];

[20] The hash value is derived from the hash function and the hash function, also known as the hash algorithm, is a method of creating a "digital fingerprint" from any kind of data. The message or data is compressed into a summary by hash function, which makes the data volume smaller and the data format fixed. The hash function scrambles the data and recreates a fingerprint called Hash values (Hash codes, Hash sums, or Hashes). The hash value is usually represented by a short string of random letters and numbers.

[21] This value is taken from the website "Bitcoin Block Explorer" at 23:58 on May 27, 2018, <https://blockchain.info/>.

(3) Timestamp: Time counted in the block, in the format YYYY-MM-DD HH:MM:SS (year - month-day hour: minute: second) with the use of the UTC (Coordinated Universal Time) time zone; (4) Merkle Root: record the hash value of all the root nodes of the transaction tree in each block through the Merkle Tree algorithm; (5) Nonce (random number) and Difficulty: Nonce is an arbitrary value in the cryptographic noun, usually only used once, the miner uses computer power to include Nonce in the hash function to see if the result meets the difficulty condition; also, a repeated calculation constitutes the so-called "mining." [22]

Blocks are linked backwards and each block points to the previous block in the chain. Technically, it points to the hash value stored in the Block Header of the previous block. The effect of such a link is to ensure that a block can be followed by multiple blocks and that all blocks after the block are not recalculated (Recalculation), cannot be changed; [23] therefore, the long chain in the block allows the blockchain having a far-reaching historical record that will never be changed. The so-called "forever invariance" is the key feature of the blockchain that is currently safe. Therefore, if any of the blocks is maliciously changed, the changed block will not be valid in the blockchain of the global bookkeeping.

Generally speaking, after the investigation by law enforcement agencies, only part of the real information can be obtained from Block Header. The relevant information includes: (1) Timestamp included in the UTC time zone, that is, the date and time that block is dug out by miners; (2) Block Height, which is unique in each block.

In addition to Block Header, each block also contains a list of transactions, which is usually based on the records of the miner's confirmed transactions. However, the miner must also abide by and not arbitrarily change

[22] Bitmain, the leader in ASIC mining, is one of the top ten customers contributing to TSMC's revenue. The company predicts that in 2018, crypto-currency will contribute 5% of TSMC's revenue.

[23] The so-called "recalculation" that can change the chain requires a huge value equal to the sum of all computer calculations nowadays.

the relevant rules. For example, the first transaction in the block must be the miner's mining reward; in addition, a series of transactions must occur after any of the series of transactions that have occurred. If Bitcoin is transmitted from address A to address B and address B to address C, then transaction A on which the series of transactions is based must be the first one to become effective.

In addition, law enforcement officers do not need to grammatically analyze the Flat Files of the blockchain, including block headers and transaction information, etc., which are carried out by developers of all major blockchains, such as Bitcoin wallets and block data query service provider "Blockchain.info." [24]

[24] It is a service provided by British merchant Qkos with the financial data, including the latest transaction data and the creation of new mining blocks available on its website.

IV. Blockchain address

Regarding the blockchain address, there is an important concept that needs to be clarified first. Bitcoin users can download Bitcoin software at any address. However, based on the selection of different Default Locations, the following differences will occur due to different operating systems:

A. Windows:

Old system storage path:

The path in Windows XP is "C:\Documents and Settings\<username>\Application data\Bitcoin".

New system storage path:

On later Windows operating systems (such as Windows Vista, Windows 7, Windows 8, and Windows 10), the path is changed to "C:\Users\<username>\Appdata\Roaming\Bitcoin;" the shortcut to open these files is to execute the syntax of "explorer %APPDATA %\Bitcoin" at the beginning in the Command Line.

B. Mac:

The path in the Mac OS X operating system is "~/Library/Application Support/Bitcoin/".

C. Linux:

The path to the mainstream Linux version is "~/.Bitcoin/".

D. Blockchain folders storage and space

The Bitcoin blockchain will be divided into several folders, each file size is generally about 134 MB, and the folder of the storage block will also store the Bitcoin blockchain in the same folder, including the Public Key and the Private Key[25] wallet file "Wallet.dat." As mentioned above, the default location of the Bitcoin can be changed. If the SSD[26] hard disk with a small capacity is initially stored in the computer (Drive C :\), the location of the blockchain folder can be changed to another hard drive with a larger capacity. Special attention should be paid to the fact that the blockchain contains a large number of folders, and the number of folders will be increased as the blockchain grows. Therefore, the need for hard disk space is extremely large; in fact, the file capacity had reached 70GB as early as in June 2016.

Some public websites provide free resources for the public to use, such as the aforementioned Bitcoin wallet and block data query service provider Blockchain.info[27] website also provides a frequently updated chart for use. The chart provided by the website shows the increased blockchain capacity space data, not a function, nor a complete flat file;[28] also, the new block continues to proliferate, as of May 2018, the average of each independent block is with file capacity increased from KB to 1MB.

Another highly rated public web resource, "WebBTC,"[29] provides a simple but highly practical and frequently updated blockchain summary. According to the data of the website, the total number of Bitcoin addresses in June 2016 was as high as 160 million. According to the process and record of the relevant address for Bitcoin transmission or receiving, there were more than 140 million Bitcoin transactions in total.

[25] Public-key cryptography, also known as Asymmetric cryptography, is an algorithm of cryptography that requires two keys, one is a public key and the other is a private key, when one is used for encryption, the other is used for decryption. Although the two keys are mathematically related, if you know one of them, you cannot calculate another one automatically; therefore, one of them can be published and known as "public key" and arbitrarily released; the undisclosed key is a "private key" that must be kept strictly by the user and never provided to anyone by any means.

[26] A solid-state drive or solid-state disk (SSD) is a computer storage device that uses flash memory as a permanent memory. It usually has a smaller capacity than a conventional hard disk.

[27] https://blockchain.info/charts/blocks-size.

[28] Europol EC3 (European Cybercrime Centre), "A Guide for Bitcoin Investigators", "… While we can see the increase is not exponential it is not completely flat either.…" version 1.09, March 2 2017, p.26.

[29] https://webbtc.com/.

In general, large Bitcoin transactions are mostly simple payment transactions, that is, using a multi-signature method to complete the transfer of Bitcoin to a certain address or directly to a public key. The transmission method accounts for about 5%, and only 0.02% of the Bitcoin address is the computer program syntax using OP_RETURN (data output operation), which stores non-financial data when some transmitters decide to keep it forever.[30]

[30] Same note 28, page 65.

V. Bitcoin wallet and seizure

When law enforcement agencies conduct Bitcoin-related investigations, they usually pursue two important goals: identifying and seizing the Bitcoin wallets used by suspects for criminal activities. Law enforcement officers need to recognize the important fact that Bitcoin is not stored in a Device, but is stored in a Wallet with a Private Key. The private key[31] is the key to have Bitcoin transferred.

To understand how to access and obtain the Bitcoin private key held by the suspect, one must first understand the mechanism[32] governing the private key. The private key can be controlled by: (1) a wallet stored in the device: also known as a "software wallet," a Bitcoin wallet stored in the suspect's computer, mobile phone, or other external storage device, including a Hot Wallet (HW) or USB disk device; (2) paper wallet: by paper wallet (usually using QR code records, some websites provide free printing programs) or directly handwritten on paper; (3) online wallet: manage the Bitcoin wallet through a third party, usually a virtual money exchanger or a service provider for online wallets. The description of each type of wallet is as follows:

A. Software wallet

There are many types of Bitcoin wallets available on the market currently; also, the most popular software wallets are Bitcoin Core and Electrum. These Bitcoin wallets are compatible with common desktop

[31] Bitcoin's private key can be imagined as randomly selecting a number from 1 to 2256; and for the need of stealth, many Bitcoin wallet accounts are used only once, that is, there are many accounts in the wallet, but many accounts are used only once. At present, most wallets are HD (Hierarchical Deterministic) wallets, that is, a seed generates a master private key and then a large number of sub-private keys and wallet accounts thereafter.

[32] A wallet is like a bank account. A private key is like an ATM card. If it is lost or damaged, a signature for transaction through the account is not possible. The Bitcoin of the account is still recorded on the ledger, but it cannot be accessed. In addition, a private key is an electronic record, which is easy to copy and back up. The copy is also equivalent to have the control power in hand.

operating systems (such as, Windows/Linux/Mac)[33] and provide a Graphical User Interface (GUI) for users to easily confirm Bitcoin account Balance, a list of recent transactions, and Bitcoin that can be transmitted or received.

The key difference between the software wallet Bitcoin Core (formerly known as "Bitcoin-QT") and other Bitcoin software wallets is whether it is necessary to download the complete blockchain in order to get the previous information. The Balance of Bitcoin Core software wallet is not an instant update. It needs to be updated after the complete blockchain download is successful, which usually takes several days. Most other software wallets are called "Lightweight Wallets." These light wallets only need to download the part related to the users instead of the entire blockchain. (Refer to "Table 1" below).

The software wallet is stored in a file named "Wallet.dat" and on a Local Drive. The Local Drive refers to the disk or tape drive connected to the user's computer. The files of these wallets contain unencrypted or encrypted private key. According to a foreign case study, it is necessary to log in to the suspect's computer on site in order to access and transfer Bitcoin to the wallet controlled by law enforcement agencies. However, most Bitcoin users, regardless of whether they hold the Bitcoin are legal or illegal, will encrypt the wallet used.

It can be expected that the capacity of the blockchain is huge and will continue to increase, and the Lightweight Wallet client does not need to download the entire blockchain, so the light wallet will become popular to the users and it is mainly used in mobile phones and other sophisticated devices that are with storage space, processing resources, and batteries. In short, as the capacity of the blockchain increases, the number of users for light wallets or online Bitcoin wallet services, such as Coinbase, Blockchain.info, Xapo or Circle, will gradually increase.

Scholars who have studied computer security mechanisms have also

[33] For complete Bitcoin wallet information of various platforms, please refer to the following URL: https://bitcoin.org/en/choose-your-wallet.

found that the operation of light wallet programs will request the relevant link, which will reveal the Bitcoin address, and then locate the wallet stored in a specific address. Currently, the tool service provider that provides relevant tracking data is Chainalysis; also, the service provided will also record the IP address, which can be used to trace the identity of the suspect.

Table 1. Comparison of main differences between Bitcoin clients

Functions	Miners	Full nodes	Light clients
Checking balance	○	○	○
Receiving or sending payments	○	○	○
Storage of full blockchain	○	○	
Validation of transactions	○	○	
Propagation of transactions	○		
Confirmation of transactions	○		

B. Mobile wallet

Famous mobile device wallets, such as Coinbase, Airbitz, Blockchain, Circle, Xapo, Bread, Copay, Blocktrail, etc. The mobile wallet can be used in any system. These wallets store the private key in the mobile device program. To access to the private key, the mobile phone needs to be unlocked. The wallet programs may also be encrypted by PIN code or fingerprint authentication, which is similar to the storage and management practices of the software wallet. The aforementioned private key access usually requires the cooperation of the suspect or uses some professional programs that can circumvent the security system.

In general, users tend to use a paper wallet, hardware wallet, or software wallet to store many Bitcoins, while placing few Bitcoins (one day transaction volume) in the mobile wallet, so if the law enforcement agency has found

Bitcoins in a mobile wallet while performing a search, it can be reasonably concluded that the suspect may store many Bitcoins elsewhere.

C. Web wallet

It is necessary to log in the user account or wallet account, password, and double authentication codes to access to the web wallet. Currently, the most widely used web wallet is Blockchain.info Most web wallet operators allow users to download wallets or export their private keys for Off-line storage.

D. Paper wallet

The paper wallet stores the private key in an off-line manner, and the private key needed for access to the Bitcoin is printed on a paper and isolated; also, such private key is usually accompanied by a public key and a QR code. Because paper wallet producers will provide public and private keys for Bitcoin offline, these public and private keys are usually manufactured and stored in an isolated network[34]. When the public keys and private keys of the paper wallet are recorded on a paper, the data on any computer can be deleted without the need of having a backup copy kept. It is conceivable that the paper wallet is free from Internet hacking or malicious attack, but the paper wallet still needs to be kept in a safe place to avoid being stolen or damaged.

Paper wallets are relatively inconvenient for users who are intensively trading through the Internet. Therefore, users use a paper wallet to store a considerable amount of Bitcoin. For law enforcement agencies, if a paper wallet is searched on the spot, any Bitcoin funds associated with the private key can be quickly transferred to and from the private wallet or web wallet using the private key. Since most wallets allow having private key imported, one can complete the operation by selecting the “File → import” command on the general computer.

[34] Air-gapped Computer, when governments, public utilities and enterprises want to protect sensitive information, an air-gap network will be created, mainly to store data in a computer that does not use the Internet permanently in order to protect data from hackers.

E. Universal wallet

"Universal wallet" refers to a form of software wallet, online wallet, paper wallet, or hardware wallet. It is possible to create a meaningful or orderly sentence of 10 to 15 words as a "seed"[35] to represent or drive the private key. The advantage of this type of wallet is that it allows users to easily back up or recover the private key.

Usually the universal wallet is also called the "brain wallet" because the "seed" can be stored, recorded, or printed by the computer, but also can be retained in the user's memory; however, some users cannot completely remember the "seed." Therefore, the "seed" is usually recorded in the computer or on paper. If the user can completely memorize or record the "seed" of the universal wallet, there is no need to worry about the inability to restore the wallet file or the hard disk damage problem. On the contrary, the user can also copy the new wallet from the "seed." Since the method can have the public key and private keys recovered from the wallet, the "seed" is also known as a "universal password." In other words, if cyber-attacker or law enforcement finds a "seed," one can know all the Bitcoin addresses in an instant.

In addition, the universal wallet may also be attacked: The length and uniqueness of a "Seed" is hard to guess, the wallet may still be exposed to the Internet world, while other users can crack the password by brute-forcing attack. The attacker downloads the blockchain's copy file and then obtains all Bitcoin addresses by PARSE - up to hundreds of millions of Bitcoin addresses, some of which are identified and retrieved, then confirms the address containing weak password by a cross-comparison method.[36] Once the password is resulted by comparison, the attacker can use the password to copy the private key and then steal the victim's Bitcoin.

[35] Or known as "recovery code."

[36] Same note 28, "… Addresses with non-zero balances could be identified and extracted and then cross-matched against addresses that can be generated by using weak passwords ('passw0rd,' 'Ford Perfect,' wordlists of popular songs, quotes, etc.)…," p.31.

F. Hardware wallet

A hardware wallet is a common way for a user to store a Bitcoin private key using a hardware device. The private key is securely stored in the wallet to prevent the private key from being transferred. The hardware wallet authentication transaction mode is as follows: (1) The hardware wallet receives the transaction from the computer with a pen drive (such as, USB); (2) the hardware wallet verifies the transaction; (3) the verified transaction record is transmitted back to the computer and then transferred to the Internet by broadcasting.

The aforementioned procedure does not leak the private key, so the procedure does not expose the private key to the Internet. To access and install the private key on the hardware wallet, one needs to connect to the hardware device. The hardware device can avoid malicious programs, KEYLOGGER threats, or the investigation of law enforcement agencies with the use of PIN code encryption or other types of authentication. It takes a long time to access to the hardware wallet by brute-forcing-attack; therefore, the cooperation of the suspect is needed to obtain the private key and funds in the hardware wallet.

The most well-known hardware wallet is TREZOR[37] and the manufacturer provides RECOVERY SEED (a notebook containing 12 to 24 blank initial values) for the user to record in order to back up the wallet.[38] As mentioned above, if the law enforcement agency obtains the seed content at the search site, the wallet can be recopied and then freeze the Bitcoin; therefore, when searching the site, the aforementioned notebook is an important subject

[37] The “Trezor” was developed in 2013 by the Czech company, SatoshiLabs (the company created the first Bitcoin mining pool), an open source wallet that used the BIP49 (Bitcoin Improvement Proposal) standard to generate private keys, even if the manufacturer went out of business, hardware wallet was lost or damaged, it did not affect the private key generated.

[38] In order to prevent the hardware wallet from being damaged and unreadable, there is also a setting of a recovery seed (a backup of the hardware wallet). The seed is 24 English letters. The initial setting is generated by the system random number. It needs to be manually recorded and can be used to recover the wallet private key and address.

matter of the search.

Another more special hardware wallet is BitLox. It is about the size of a credit card. According to the service it provides, the price ranges from US$200 to US$400, which is usually used to store a large amount of Bitcoin. BitLox allows users to create 50 invisible wallets. Only when the user enters the wallet number and the corresponding PIN code will the wallet be displayed.[39] Therefore, the law enforcement agency cannot know whether the suspect's wallet has been fully seized. In addition, the device works well on anonymous operating systems (such as "Tor and Tails") (using a USB cable to interface with the computer), and another incentive for BitLox to attract criminals is that the device was once sold on deep webs (such as "DEEPDOTWEB") at March, 2016; the site is the most popular online resource distribution center in the online black market.

[39] Taking Trezor as an example, the Pin code is set by the user to be more than 4 digits in order to prevent the hardware wallet from being lost and used by others. If the Pin code is entered incorrectly, it must wait for a while before entering the Pin code again. For each input error, the waiting time increases by an exponent of 2, for example, for 20 input errors, it is necessary to wait for 6 days before entering the Pin code again. For 30 input errors, it is going to be a wait of 17 years before the Pin code can be entered again.

VI. Bitcoin seizure procedure

A. Basic concept

If the law enforcement agency identifies the address of the Bitcoin held by the suspect in the blockchain, it must be recognized that it is impossible to perform Bitcoin seizure at the far end (unless the suspect places the Bitcoin on the network platform). If the seizure of the illegal Bitcoin in the suspect's residence is to be realized, the law enforcement officer must confirm:

(I) The Bitcoin wallet is stored in the suspect's associated hardware device and the password is confirmed because most of the wallets are encrypted.

(II) It is important to find the private key of the suspect so that it can be exported to other wallets.

(III) The "recovery seed" of the suspects is usually with 12 to 24 random letters and numbers.

It is not possible to seize Bitcoin by only copying and storing the wallet.dat file. For suspects or other third parties with private keys, it is still possible to move funds to other addresses. The key point is to export the private key or "recovery seed" to the wallet controlled by the law enforcement agency, so that the law enforcement officers can find out the associated public key, as well as the Bitcoin that has not been transferred or sold; also, transfer the Bitcoin funds in the wallet "completely" to the Bitcoin address held by law enforcement agencies.

In order to preserve the wallet, the wallet used by law enforcement agencies should have its own blockchain and can be fully audited by the blockchain community, so Bitcoin Core Wallet is a recommended option. The reason is that the wallet can be prepared before the search and seizure, and the law enforcement officer can use the file key or the drive key to transfer the Bitcoin immediately and without any delay.

Other than the aforementioned situation or the law enforcement agency's wallet address is unknown (i.e., not prepared in advance), but there is a need to immediately seize the Bitcoin, law enforcement officers may consider the second best option, that is, immediately establish a Bitcoin wallet on the spot. The fastest and relatively safe way to date is to use Bitadress.org, a website written purely in JavaScript. The website allows the user to compile the private key and the corresponding Bitcoin address by mouse or keyboard; also, the display mode is garbled. Furthermore, the site can only be viewed by a securely connected and certified computer, and the site has the ability to store and establish private keys and corresponding Bitcoin addresses offline, thus the seizure procedure is completed after transferring Bitcoin to the aforementioned Bitcoin address established by law enforcement agencies.

Other convenient options are that law enforcement agencies can request the exchange service provider to provide Bitcoin addresses, which is particularly useful when law enforcement agencies request immediate conversion of seized Bitcoins to other legal currencies (usually Euros or US dollars) since it helps law enforcement agencies save large expenses in establishing and maintaining the Bitcoin wallets.

B. Procedures of exporting / importing private keys

The private key may be printed on paper, in a mobile phone, in a wallet.dat file stored on the suspect’s computer, or in a drive key. In any of the aforementioned forms, the outgoing private key can be performed by a “dumpprivkey” command, and the private key displayed by the command is expressed in the form of WIP (Wallet Import Format). It is worth noting that the encrypted wallet still needs the suspect to provide a password so the law enforcement agency can export the private key. The private key itself will not be removed during the exporting process, but will be exported to the general note file. If the wallet does not contain a private key that can represent the Bitcoin address, the above operation will feed back an error message.

Once the private key is obtained, it must be immediately exported to the wallet of the law enforcement agency. Bitcoin can be completely controlled by law enforcement agencies and the operation method may vary depending on the type of wallet. Once the private key is successfully imported, it takes some time to synchronize the wallet with all the transaction records associated with the Bitcoin address, and finally the wallet will display the transaction balance.

After the private key is imported into the wallet and the balance is displayed, all Bitcoin should be completely transferred to the Bitcoin address represented by the law enforcement wallet; if the law enforcement agency can control the suspect's wallet and password, the Bitcoin can be transferred directly, and whether the private key is imported or exported is irrelevant.

The other simpler option to seize Bitcoin is to make a request to the platform trader. If the law enforcement agency identifies the suspect using a virtual currency account opened by any dealer, the dealer may be requested to freeze the virtual assets in the relevant account of the suspect. In addition to Bitcoin, virtual assets include Litecoin (LTC), Ethereum (ETC), Dash, or even Fiat. It is worth noting that although the suspect may retain some of the virtual assets in the account of the online trading platform, but the offender tends to store most of the virtual assets in their software wallets.

C. Remove the Bitcoin address of the wallet

Regardless of whether the seizure of the virtual currency going smoothly or not, the law enforcement officer should parse all the Bitcoin addresses in the suspect's wallet and use the relevant instructions (such as "Listaddressgroupings") to list all the Bitcoin addresses that have been spent or not spent. This is a very important step. Since the operation of the command does not require the user's password, and even in the encrypted wallet, law enforcement officers can perform further tracing, and can also use the free or commercial version of the funds to trace the software.

The remittance of the transaction list does not require a password. The remittance process can be performed in the trading field of the GUI interface of Bitcoin Core wallet. The result will be presented in the file (neat.csv) with date, amount, label, and transaction identifier.

D. Handling encrypted wallets

The encrypted wallet can still open the file and check the balance, the transaction list and the quantity of current Bitcoin addresses. However, the password is still required to export the private key and transfer funds. The possible ways to obtain the password are as follows:

(I) Promote suspect cooperation

Law enforcement officers need the password from the suspect, regardless of whether the suspect has offered it on a voluntary basis or as a result of legal restrictions. However, the investigator can still test and find the password within a certain period of time, and the wallet will not be locked or deleted due to the number of incorrect passwords.

(II) Use of information forensics

When open the Bitcoin query (in the Bitcoin Core wallet, in the Help→Debug Window Section command), the historical record of the query command can reveal the most recent executed commands, type “Up Cursor Key” to browse. Each command may reveal the behavior of the user back then.

Enter the “History” command on the Linux system to find out the user’s last command. Even if the password cannot be known immediately, there is still a chance to find the most recently used password. Even if the user makes some changes to the password, the relevant record will still be stored.

If possible, it is recommended to perform a Memory Dump before shutting down. There are a lot of tools available to retrieve the memory in use. One of the best known is the FTK Imager, which can retrieve the Random Access Memory (RAM) and image file of hard disk. The software tool uses a GUI interface or a simple command interface.

Use the relevant tools (such as “Volatility”) to retrieve the password of the relevant Bitcoin wallet after the memory dump. Another option is to use the “String” command to search the Text String in the memory and collect relevant information and have it compiled as “Brute-Forcing Attack” database. It is worth noting that all passwords are stored in RAM in an unencrypted format.

⑶ Brute-Forcing Attack

Law enforcement agencies can try to use related tools (such as “John the Ripper”) and other password-cracking software to crack the wallet password. There are some web coded[40] can be downloaded for password cracking, but the actual cracking of the encryption algorithm is not easy, especially if the code is not excellent in computing power per second in a general computer, which makes this method usually impractical. Therefore, before using the brute-forcing-attack, law enforcement agencies should have a certain knowledge or research on the password to be cracked.[41]

In addition, the effectiveness of this method varies according to the complexity of the password. Most Bitcoin users have a certain level of understanding on information security. The password is usually more than 10 characters. If the password is designed, never appeared in other computer programs or software services, and not stored in RAM, disk, or paper and record, it is difficult to obtain the password by brute-forcing-attack.

⑷ Use EC3 decryption platform

The EC3 Digital Forensic Laboratory under the European Interpol can assist in the investigation of member countries or third-party organizations. The laboratory not only provides analysis and restoration service after the digital data is extracted, but also provides a platform for decryption. The platform provides programs for decrypting Bitcoin wallets. Although there is very little success in cracking virtual currency wallets, the agency is willing to communicate with law enforcement agencies in various countries and provide services in cracking the password of the virtual currency wallets; at least the wallet or password related information can be provided.

[40] For example, https://github.com/gurnec/btcrecover.

[41] For example, the suspect’s date of birth, mobile phone number, identity card number, license plate number, and numbers or letter combinations that is easy to guess.

(V) Outsourcing vendor

The public sector can also turn to corporate and private sector for help. There are many online wallets on the Internet that provide relevant services that are powerful.[42] The provided services are also well-received in the Bitcoin community, but the service is not free of charge. In addition, the website that provides the service does not require uploading all wallet contents (such as, the Wallet.dat file) or the private key. On the contrary, it only requires uploading information that can help decryption, which greatly reduces the risk of the private key being stolen.

[42] For example, walletrecoveryservices.com.

VII. Suggestions

A. Develop a virtual currency search and seizure process

Because Bitcoin has a "decentralized architecture" and the "electromagnetic record storage" feature, law enforcement agencies cannot perform a freeze on a single responsible unit, and the private key is crucial to the Bitcoin wallet, which means "the private key and the wallet are co-existent." Therefore, law enforcement officers cannot initiate the search and seizure procedure in the traditional way. How to "transfer the control of the wallet" is even more crucial. Law enforcement agencies also need to develop rigorous pre-procedures to ensure the "uniqueness" of control transfer.

Since the hardware wallet has the advantages of "easy management" and "retention flexibility," law enforcement agencies can use it when performing search and seizure[43] (hereinafter referred to as "search and seizure"). The aforementioned "easy manage" is because the hardware wallet can ensure the access of the hardware wallet and its recovery code. The "retention flexibility" means that the sealed hardware wallet can be directly devolved to the prosecution. Suggestions are made to the case undertaker and the onsite executor before and after the search and seizure (including devolution and return) as follows:

(I) Case undertaker

1. Before the search and seizure:

(1) Set up a Bitcoin account for search and seizure

(2) Fill in the "Seized Property List" (see "Table 2"), "Bitcoin Search and Seizure Transfer Record" (see "Table 3"), and "Bitcoin Search and Seizure Transfer Amount Statement" (see "Table 4").

(3) Prepare the following items according to the number of search sites and send them to the officers at the search sites: The Bitcoin account

[43] It is necessary to initialize the hardware wallet, record the account Bitcoin Address, and seal it in a recording environment. Only the account number is needed for account transfer at the time of performing a search and seizure.

for the search and seizure of this case is stored in the write-protection USB /disc and the corresponding QRcode paper printed. The Bitcoin account for the search and seizure of this case is filled in the “Bitcoin Search and Seizure Transfer Record” with a printout prepared. Check and record the handling fee[44] and photographic equipment (full video recording when transferring Bitcoin) for confirming the account transfer within 20 minutes and photographic equipment.

2. After the search and seizure:

(1) Confirm the total credit amount again with the statement prepared

(2) Obtain and keep the sealed hardware wallet and recovery code envelope.

(II) Site executor

1. Before the search and seizure:[45]

(1) Collect the following from the case undertaker: Write-protection USB /disc (with Bitcoin account for the search and seizure); QRcode paper; number of copies (with the Bitcoin account for the search and seizure) of “Bitcoin Search and Seizure Transfer Record” (including the statement of amount transfer); and photographic equipment (full video recording when transferring Bitcoin).

(2) Download the Bitcoin Search and Seizure Manual.

2. Execution date:

(1) Search for Bitcoin wallets in devices, such as, computers/mobile phones.

(2) Transfer it to the law enforcement agency’s wallet address (full video recording when transferring Bitcoin) after obtaining the password.[46]

[44] Check it at https://bitcoinfees.earn.com to see that handling fee varied according to the time of confirmation. To save time and ensure that Bitcoin is not transferred by third parties, it is recommended to select the rate that can be confirmed within 20 minutes.

[45] It is recommended to prepare related equipment at each search site.

[46] The collection account number is the law enforcement agency’ account (Bitcoin address); also, the transfer amount is “Amount: Max.” Report to the field undertaker after confirming the completion of the transaction; also, immediately confirm it on the Internet (website: https://blockchain.info/, search keyword: transaction ID).

(3) Confirm that the account transfer is successful (photographed or printed on the spot) and report it to the undertaker.

(4) Fill in the “Seized Property List,” “Bitcoin Search and Seizure transfer Record,” and “Bitcoin Search and Seizure Transfer Amount Statement.”

(III) Devolution

1. Check the account currency amount and the printout before devolution.
2. The prosecution establishes a Bitcoin wallet so the seized Bitcoin will be transferred to the prosecution wallet by the judicial police at the time of devolution.

(IV) Return[47]

1. Open the hardware wallet envelope in a videoing environment with the party concerned.
2. Enter the Pin code and check the return address to complete the transfer.
3. Print the transfer certificate and ask the party concerned to sign the receipt.

[47] A direct return is with difficulty, that is, the searched person may claim that the Bitcoin in the wallet is damaged or does not match the amount of the seizure.

Table 2 “Seized Property List” of the MJIB

Investigation Bureau of the Ministry of Justice (full name) - “Seized Property List” template					
No.	Device	Currency	Unit	Owner/holder/ custodian	Remarks
○	○○○ Bitcoin stored in mobile phones	BTC	0.36	○○○	Refer to No. ○○ “Bitcoin Search and Seizure Transfer Record”
○	○○○ Bitcoin stored in a personal computer	BTC	1.58	○○○	Refer to No. ○○ “Bitcoin Search and Seizure Transfer Record”

Table 3 “Bitcoin Search and Seizure Transfer Record” of the MJIB

“Bitcoin Search and Seizure Transfer Record” of the Investigation Bureau of the Ministry of Justice
1. Transfer record number
2. (numbers of transactions) transaction(s) was/were made from ○○○ ’s Bitcoin Address
3. Transferred the searched and seized Bitcoin to the Bitcoin address (see below): ________________________
4. Total amount _____ BTC was transferred
5. Total handling fee (paid from the owner/holder/custodian account): _____ BTC
Owner/holder/custodian signature Signature of Devolver / Searcher & Seizer
Date: ___ (YY) ____ (MM) ____ (DD)

Table 4 “Bitcoin Search and Seizure Transfer Amount Statement”

No. _____ “Bitcoin Search and Seizure Transfer Amount Statement” of the MJIB
1. Last 5-digit of the transaction code _____, transfer amount _____ BTC, transfer fee _____ BTC, BlockChain No. _____, Time of BlockChain finality _____
2. Last 5-digit of the transaction code ______, transfer amount ______ BTC, transfer fee _____ BTC, BlockChain No. _____, Time of BlockChain finality _____
3. Last 5-digit of the transaction code ______, transfer amount ______ BTC, transfer fee _____ BTC, BlockChain No. _____, Time of BlockChain finality _____

4. Last 5-digit of the transaction code ______, transfer amount ______ BTC, transfer fee _____ BTC, BlockChain No. _____, Time of BlockChain finality _____

5. Last 5-digit of the transaction code ______, transfer amount ______ BTC, transfer fee _____ BTC, BlockChain No. _____, Time of BlockChain finality _____

6. Last 5-digit of the transaction code ______, transfer amount ______ BTC, transfer fee _____ BTC, BlockChain No. _____, Time of BlockChain finality _____

7. Last 5-digit of the transaction code ______, transfer amount ______ BTC, transfer fee _____ BTC, BlockChain No. _____, Time of BlockChain finality _____

8. Last 5-digit of the transaction code ______, transfer amount ______ BTC, transfer fee _____ BTC, BlockChain No. _____, Time of BlockChain finality _____

9. Last 5-digit of the transaction code ______, transfer amount ______ BTC, transfer fee _____ BTC, BlockChain No. _____, Time of BlockChain finality _____

In addition, law enforcement agencies may perform search and seizure on multiple sites at the same time. How to preserve digital evidence? How many wallets should the law enforcement agencies prepare and what is the cost? How the wallets to be managed onsite? How should the seized properties delivered to the local prosecutor’s office? What are the potential problems of return or cashing? The aforementioned questions are discussed separately as follows:

(I) Classification by site:

This program is “one site one wallet” and directly regards the hardware wallet as a seized property. Therefore, the law enforcement agency must prepare a hardware wallet in advance and bring it to the scene, then instruct the party concerned to have all the Bitcoin in the wallet transferred to the law enforcement agency’s wallet. After the transfer is completed, the hardware wallet is affixed with a seal and the signature of the party concerned is affixed on the list of seized property list; also, the party concerned can only visually identify the wallet account of the law enforcement agency on the sealed bag and cannot view the electromagnetic record in the wallet. In terms of custody, after confirming the completion of the transfer procedure, one or more wallets (depending on the number of Bitcoin at the search site) should be sent to the Loot

Library of Prosecutors Office.

At the time of the return, the sealed hardware wallet needs to be opened, and the law enforcement agency needs to identify the account to be returned is stored in hardware wallet or software wallet. If an immediate cashing is needed for any reason, the second sealing procedure is to be initiated after the cashing completed.

(II) Classification by case:

This solution adopts "one case one wallet." The advantage of this solution is reducing the number of wallets used in order to save money and time,[48] and it is not necessary to carry the wallet to the search site in order to avoid the risk of the wallet being lost or damaged in transit. Instead, ask the suspect to transfer the Bitcoin in the wallet held by the suspect to the designated wallet address. After the transfer is completed, the law enforcement agency will specify in the seized property list and request the party concerned to sign and confirm.

When it is returned after the case is closed, the seal of the hardware wallet is lifted. If an immediate cashing is needed for some reasons, the second sealing process is required after the cashing completed. In addition, the "one case one wallet" solution must be communicated to and coordinated with the prosecution for the transfer method, for example, transfer to the prosecution wallet again at the prosecutor's office or the prosecutor directly seizes the law enforcement agency's hardware wallet.

The above two solutions have their own advantages and disadvantages. In addition to the consideration of budgetary cost, the related issues worthy of discussion include: (1) If different types of virtual currency are to be seized, the initialization procedures of the hardware wallets are different, for example, Bitcoin and Ethereum should be stored in different hardware wallets. If a new site that should be searched is found suddenly and the number of existing hardware wallets is insufficient or the traveling distance is far away, it may

[48] Take the hardware wallet Trezor as an example, each unit price is about NT$4,500 and the wallet initialization takes 4 hours.

not be possible to carry out an effective seizure procedure. (2) Since the seal of the hardware wallet cannot be opened to confirm the stored electromagnetic record, the question is how to obtain the consent of the party concerned and complete the signature and confirmation. (3) If the prosecution does not agree that the hardware wallet attached by the judicial police administration is a formally seized property and cannot be kept in the Loot Library, are there other seizure methods available? (4) If a single suspect has several Bitcoin wallets that are scattered in different search locations, the return process will involve several hardware wallets, and the law enforcement agencies may have hard time to deal with the situation. If there is a problem of partial return or partial cashing to be dealt with, several hardware wallets will also increase the management difficulty. The introduction and differences of the two solutions are summarized as follows: (see “Table 5”)

Table 5 The introduction and differences of the two solutions comparison table

	Solution 1	Solution 2	Dispute / Supplementary Notes
Differentiation method	By the scene (One site one wallet)	By case (One case one wallet)	If different kinds of virtual currency are seized, the hardware wallet initialization procedure is different, for example, Bitcoin and Ethereum need to be stored in different hardware wallets.
Cost/time expenditure	Purchase the number of wallets based on the number of sites.	NT$4,500 / each 4 hours / initialization	Each Trezor is sold for about NT$4,000. The ordering time is 1 to 2 months. It takes 24 Polaroid photos for each initialization at a cost of about NT$480. Each hardware wallet initialization includes about 4 hours of video recording.

Implementation modalities	If the wallet is “required” to be brought to the scene, the party concerned transfers the BTC to the wallet of the law enforcement agency and documents it in the seized property catalog for the signature and confirmation of the party concerned (the party concerned cannot view the electromagnetic record in the wallet).	If the wallet is “not required” to be brought to the scene, the party concerned transfers the BTC to the wallet of the law enforcement agency and documents it in the seized property catalog for the signature and confirmation of the party concerned.	If a new site that should be searched is found suddenly, and the number of existing hardware wallets is insufficient or the traveling distance is far away, it may not be possible to carry out an effective seizure procedure; because the hardware wallet cannot be opened for confirmation, the question is how to obtain the consent of the party concerned and complete the signature and confirmation.
Search and seizure management	Keep multiple wallets according to the number of sites.	“One case one wallet” management	Centralized management or decentralized management, the former is with the risk of being lost.
Prosecutors identified	Deem as a seized property and deliver it to the prosecution discretionally.	The way it is devolved to the prosecution is to be confirmed.	If the prosecution does not agree that the hardware wallet attached by the judicial police administration is a formally seized property, are there other seizure methods available?
Return / cashing	Identify the original hardware wallet of the account that should be returned; lift the seal of such hardware wallet; transfer the Bitcoin for return or cashing; also, the second sealing process is needed.	After the seal of the hardware wallet is lifted; transfer the Bitcoin for return or cashing; also, the second sealing process is needed.	If the party concerned has multiple Bitcoin wallets that are scattered in different search locations, the return will also involve multiple hardware wallets. Multiple wallets will be difficult to handle for a partial return or cashing.

B. Joining international organizations to resort to cross-border cooperation

As mentioned earlier, Europol had pointed out in the relevant documents in 2015 that most crimes such as cybercrime or money laundering, fraud, and fund-raising scams were related to virtual currencies, such as Bitcoin, including illegal financing and illegal activities related to such technology. Among them, EC3 plays a vital role, and it maintains a good cooperative relationship with law enforcement agencies of various state members.

EC3 was founded in 2013 and it is a European Union cross-regional cybercrime expert group that assists law enforcement agencies in responding to cyber attacks, especially virtual currency-related money laundering crimes, such as Bitcoin. Several meetings were held by the organization at the European Interpol (EUROPOL) headquarters in Hague, the Netherlands to discuss the issue of cross-border crimes involving virtual currency. In addition to the gathering of law enforcement agencies from European countries, the US FBI, Fin CEN, and other institutions also attended the meetings; in the meetings, Bitfinex (Chief Executive: Jean-Louis Van der Velde, EC3's main technology consultant) that had served as the world's largest virtual currency trading platform operator, suggested the organization to establish a global law enforcement network to combat virtual currency-related crimes.

EC3 held the "4th Virtual Currencies Conference" on June 22 and 23, 2017 with the theme of "Continuous fighting against the abuse of virtual currency for criminal transactions and money laundering." It was participated by the law enforcement agencies of European countries and the United States, also, the private sectors, such as, Bitcoin.de, Bitfinex, Bitpanda, Bitonic, Bitstamp, Bitpay, Coinbase, Cubits, LocalBitcoins, Spectrocoin, and Xapo; however, only Japan and Singapore in Asia participated in the conference. It was discussed in the meeting that, given the increasingly global development of criminal activities, such as, virtual money laundering, it was imperative for law enforcement agencies to establish a global intelligence exchange network.

Taiwan’s IT industry is developed with the participation of sufficient information talents. In 2016, the ATM of Bank ○○ robbed by transnational criminal groups was solved, showing the professionalism of law enforcement personnel in the field of network security and information security forensics. A series of WannaCry ransom ware events occurred globally in 2017. Victims were blackmailed to pay Bitcoin as ransom. Taiwan was ranked in the third place as the digital disaster zone in the world. The capital tracking breakpoint was made possible due to the anonymity of Bitcoin and “computer crime has no boundaries, digital land must be protected.” Taiwan should actively seek to participate in the virtual currency cross-border crime intelligence exchange platform as mentioned above.

VIII. Conclusions

In terms of criminal investigation process, due to the decentralization of Bitcoin, it is impossible to freeze the suspect's illegal gains through only one designated agency. The only method of seizure is to "transfer the control of the wallet," in other word, transfer the balance of the suspect's Bitcoin wallet and the public key and private keys to the wallet of the law enforcement agency. In addition to Bitcoin, there are other crypto-currencies, such as, Ethernet, Litecoin, Bitcoin Cash, etc. The search and seizure process is subject to further integration by the law enforcement agencies, court, and prosecution.

In terms of cross-border cooperation, important international cybercrime units, such as, FBI and EC3 are committed to international intelligence exchange and technical assistance on virtual currency used for money-laundering-related crimes. Taking EC3 as an example, only a small number of Asian countries are participating; therefore, Taiwan may explore the feasibility of joining the law enforcement network and the intelligence exchange platform.

In addition, the responsibilities of the MJIB include money laundering prevention and international cooperation. The Anti-Money Laundering Division MJIB is also the financial intelligence unit of Taiwan. Transnational cooperation is an indispensable part for the effort of global money laundering prevention, while facing the diversification of virtual currency related crimes and the trend of globalization, the legal positioning of virtual currency in Taiwan is still unclear.[49] Before the virtual currency crimes are seriously deteriorated like in Japan, the relevant crime prevention strategies and criminal investigation procedures should be drafted at the earliest (the "search and seizure procedures for Bitcoin" in this article) to prevent accidents from occurring.

[49] Same as the previous note 16.

Literature references

Journals and Articles

Su, Wenjie, "An Empirical Study on the Emerging Money Laundering Crimes--Based on the Bitcoin's Virtual Currency study," Master Degree Thesis of National Chiao Tung University, 2016

Zang, Zhengyun, Tseng, Wanru, and Fang, Jialin, "A study on public fund-raising regulation trends from the blockchain financing," "The Taiwan Law Review," Vol. 273, February 2018

Chinese books

Du, Hongyi, "BLOCKCHAIN's Past and Present and Future - A Reading Note for BLOCKCHAIN," published by Taiwan-CA Inc., Taipei (3rd edition, August 1, 2016)

Foreign journals

Wood, Robert W., Bitcoin: Tax Evasion Currency, FORBES, August 7, 2013.

Other foreign literature references

Financial Action Task Force, "Guidance for a Risk-Based Approach Virtual Currencies," June 2015.

National Crime Agency, "National Strategic Assessment of Serious and Organized Crime 2015," June 2015.

The European Police Office, "The 2015 Internet Organized Crime Threat Assessment," Europol, September 30, 2015.

Part Five

Event Calendar of 2017

9 Jan. 2017	An MOU concerning co-operation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing was signed with the FIU of Saint Lucia.
18 Jan. 2017	Mr. Christopher Q. Pater, attache for Hong Kong, Homeland Security Investigation, Immigration, and Customs Enforcement, Department of Homeland Security visited the AMLD.
29 Jan.- 3 Feb. 2017	Delegates of the AMLD participated in the Egmont Group Heads of FIUs Intersessional and Working Group Meetings in Doha, Qatar.
31 Jan. 2017	An MOU concerning co-operation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing was signed with the FIU of Hungary.
3 Mar. 2017	Mr. Dulcidio De La Guardia, Minister of Economy and Finance of Panama, and Ambassador Alfredo Martiz visited the AMLD.
13 April 2017	Chief Executive of Greater China Region of HSBC led the President of Taiwan region, and associates to visit the AMLD.
20 April 2017	Hold a Workshop on Enforcing the MCLA/CTFA
11-12 May 2017	1. Head of the AMLD, a regional representative of Asia Pacific region of the Egmont Group, was invited to attend Egmont Committee intersessional meeting in Geneva, Switzerland. 2. Major General Huang, Director of the Planning Department of the Navy Command, Ministry of Defense led staffs to visit the AMLD and had a project meeting on fund tracing.

15 May 2017	An MOU concerning co-operation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing was signed with the FIU of the Holy See.
14 June 2017	The executive director of DBS Bank Singapore Headquarters, Group Chief Compliance Officer, visited the AMLD.
18-23 June 2017	Delegates of the AMLD attended the 3rd Plenary and Working Group Meetings for FATF-XXVIII in Valencia, Spain.
2-9 July 2017	Delegates of the AMLD attended the 24th Egmont Group Plenary Meetings in Macao.
17-21 July 2017	Delegates of the AMLD attended the 20th APG annual meeting and technical assistance forum in Colombo, Sri Lanka.
24-28/July 2017	The delegate of the AMLD participated in the FATF TREIN standards training course in Busan, South Korea.
8 Sep. 2017	A chief prosecutor of Taiwan Taichung District Prosecutors Office led staffs to visit the AMLD.
20 Sep. 2017	A chief prosecutor of the Taiwan Taichung District Prosecutors Office and a prosecutor came to visit the Director General of the MJIB and express their gratitude to the AMLD for tracing the fund flow of a cross-border telecom fraud case.
26-28 Sep. 2017	The delegate of the AMLD attended the 4th ARIN-AP annual meeting in Tokyo, Japan.
2 Oct. 2017	An MOU concerning co-operation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing was signed with the FIU of Latvia.

6 Oct. 2017	Chairman of the Asia Pacific Financial Systems Vulnerabilities Committee of HSBC visited the AMLD.
18-20 Oct. 2017	Deputy Director of the St. Vincent FIU led financial investigators to visit the AMLD and to attend a workshop.
22-28 Oct. 2017	The delegate of the AMLD attended the Egmont Group's Strategic Analysis course in Kuala Lumpur, Malaysia.
29 Oct.-3 Nov. 2017	Delegates of the AMLD attended the 1st Plenary and working group meetings for FATF-XXIX in Buenos Aires, Argentine.
30 Oct. 2017	A chief prosecutor of Taiwan High Court Prosecutors Office visited the AMLD and discussed the fund tracing of cross-border telecom fraud cases.
8 Nov. 2017	The AMLD held a workshop on AML/CFT for financial industry.
13-16 Nov. 2017	Delegates of the AMLD attended the APG Typologies Workshop hosted by FATF-TREIN and APG in Busan, South Korea.
26 Nov. – 1 Dec. 2017	Delegate of the AMLD attended the international financial investigation course, Hong Kong.
26-31 Dec. 2017	The AMLD received and analyzed STRs related to B Group suspected of transferring oil to the vessel of North Korea and traced funds of the group.
27 Dec. 2017	An MOU concerning co-operation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing was signed with the FIU of Ghana.

ANTI-MONEY LAUNDERING
ANNUAL REPORT, 2017

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

Issuer: Lin, Ling-Lan

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: August 2018

GPN：1010701314

ISBN：978-986-05-6652-9 (PDF)

ANTI-MONEY LAUNDERING
ANNUAL REPORT, 2017

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

ISBN 9789860547450
9 789860 547450
GPN 1010602494