

ANTI-MONEY LAUNDERING ANNUAL REPORT, 2016



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

法務部調查局一〇五年洗錢防制工作年報

The Investigation Bureau, Ministry of Justice

Anti-Money Laundering Annual Report, 2016



PREFACE

“It was the best of times, it was the worst of times.” Digital technology and globalization bring new opportunities for financial and economic development, but also impact government supervision and legal regulation at the same time. The interaction of financial technology innovation and regional economic infusion causes serious problems of transnational crimes, including drug crime, organized crime, weapons and human trafficking, money laundering, terrorist activities, and the proliferation of weapons of mass destruction (WMD). The situation is far beyond the capacity of a single country or regional alliance to deal with.

Looking back at 2016, the financial authority of Taiwan had proposed a project of promoting the development of Fintech, and continued to strengthen the legal system and capability of the financial industry in Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT). In the meantime, a string of high-profile cases, such as depositing counterfeit currency, ATM hacking, an overseas branch’s violation of the US regulation, and the stock acquisition of an Over-the-Counter (OTC) company, made a tremendous impact on financial institutions. Furthermore, domestic investigations of illegal fund-raising and telecommunications fraud faced challenges of multiple jurisdictions and cross-border financial services. All of the above-mentioned events highlighted the importance of financial supervision and the compliance with international standards, the enhancement of risk management, and the upgrade of AML/CFT awareness of public and private sectors in order to identify and detect suspicious transactions.

The enactment of the Terrorist Financing Suppression Act and the amendment of Money Laundering Control Act (hereinafter referred to as “MLCA”) in Taiwan were finalized by the Legislative Yuan in the second half of last year. It effectively strengthens the capability of the government to prevent and deter terrorism financing activities, safeguard national security, combat specific crimes, improve the financial system, and profound the legal basis of a transparent fund flow. Moreover, the Anti-Money Laundering Office of the Executive Yuan starts to operate this year (2017). It demonstrates political commitment and priority in implementing international standard

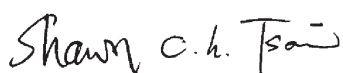
of AML/CFT. MJIB, as Taiwan's financial intelligence unit (FIU), should enhance performance, strengthen international participation and intelligence cooperation, grasp the trend and focus on the development of emerging issues, and seek for international convergence.

In last October, MJIB and FinTRACA (Financial Transaction and Reports Analysis Center of Afghanistan) signed a Memorandum of Understanding (MOU) concerning cooperation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing. The MOU established a basis for bilateral financial intelligence cooperation between Afghanistan and Taiwan. MJIB has an MOU signed with 42 countries so far. The AMLD had held the "Seminar on AML/CFT for Financial Industry," "Forum on AML/CFT for the Chief Compliance Officer of Financial Institutions" and other workshops to provide a platform for the communication between the financial institutions and the competent authorities.

The Financial Action Task Force (FATF) published the "Guidance: Criminalising Terrorist Financing (Recommendation 5)" in last October. MJIB is authorized to translate it into Chinese. Mr. Wen-Chieh Su, a special agent of MJIB, presents his research on virtual currency from aspects of technology, legal system, and policy. Guidelines and the essay are included in this Annual Report for the reference of the competent authorities and private sector.

Any comments or suggestions would be greatly appreciated.

Investigation Bureau, Ministry of Justice
Director General



September 2017

Editorial Note

I. Purposes

The Recommendation 33 of the 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 systems. This should include statistics on the STRs received and disseminated; on ML/TF cases investigated, prosecuted and convicted; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.” Therefore, this Annual Report, 2016 integrates the statistics and analysis of the annual data regarding AML/CFT performed by the Taiwan domestic financial institutions (FIs), law enforcement agencies, judicial authorities, and other competent authorities.

II. Contents

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

1. Introduction on the Organization of the AMLD;
2. Work Overview (including statistical information and charts);
3. Significant Case Studies;
4. Project research: “A New Strategy of Combating Crime: Perfecting the Financial Intelligence System against the Emerging Way of Money Laundering by Implementing Bitcoin.”
5. The Major Events of the AMLD.

(II) The statistics and related information of the 2016 Annual Report are based on the data collected by the AMLD and cases prosecuted by the Taiwan district prosecutor offices for violating the MLCA

(including deferred prosecutions and petitions for summary judgment).

III. Notes

- (I) The years quoted in this 2016 Annual Report refer to the Western calendar. The numbers of Suspicious Transaction Reports (STRs), Currency Transaction Reports (CTRs), and International Currency and Securities Transportation Reports (ICTRs) are based on the numbers of reports. The prosecutions in Taiwan district 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 percentages referred to hereinafter are rounded off. The round-off may create slight differences between integers and decimals.
- (III) The newly amended MLCA came into effect on June 28, 2017. The relevant provisions of MLCA cited in this annual report refer to the clause prior to the amendment, unless otherwise provided.

IV. This 2016 Annual Report was compiled and printed in haste. We welcome your precious comments. Should you spot any errors or would like to make suggestions, please have no hesitation to contact us.

Table of Contents

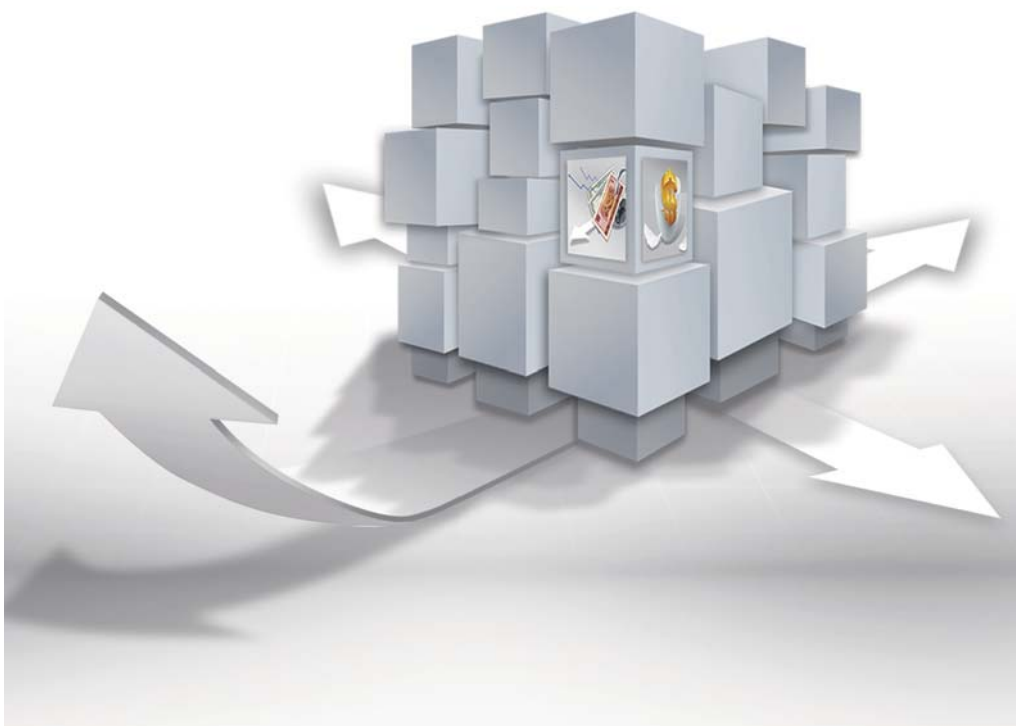
Preface	<i>II</i>
Editorial Note	<i>IV</i>
Part One: Introduction to the Organization of the AMLD	<i>1</i>
I. Legal Framework	<i>2</i>
II. Corporate Effectiveness	<i>7</i>
Part Two: Work Overview	<i>9</i>
I. Strategic Research on AML/CFT	<i>10</i>
A. Participation in The Terrorist Financing Suppression Act enactment.....	<i>10</i>
B. Participation in MLCA amendment.....	<i>12</i>
C. The Chairman of Egmont Group visiting Taiwan.....	<i>13</i>
D. Visiting the FIU of Vietnam.....	<i>14</i>
E. Participation in the “APG Third Round Mutual Evaluation Staff Meeting”	<i>15</i>
F. Holding the AML/CFT Seminars for Financial Institutions.....	<i>16</i>
II. Processing the STRs Filed by FIs	<i>18</i>
A. Statistics of STRs.....	<i>19</i>
B. Results of STRs Processed by the AMLD.....	<i>20</i>
C. Number of Reports on Strategic Financial Intelligence in Recent Years	<i>20</i>
D. Distribution of STRs by Region.....	<i>21</i>
E. Distribution of STRs by Month.....	<i>22</i>
F. The STRs Distribution by Subjects’ Age	<i>23</i>
G. STRs Distribution by Value	<i>24</i>
III. Receiving the CTRs Filed by FIs	<i>25</i>
A. Statistics of CTRs	<i>25</i>
B. Distribution of CTRs by Value.....	<i>26</i>
C. Statistics of Assisting Law Enforcement Agencies in Accessing CTRs Database.....	<i>27</i>

IV. Receiving the International Currency and Securities Transportation Reports (ICTRs) Forwarded by Taiwan Customs	28
A. Statistics of ICTRs Declared by the Passengers to Taiwan Customs ..	29
B. ICTRs Distribution by Month	29
C. ICTRs Distribution by Value	29
V. Statistics of Prosecuted Cases under the Money Laundering Control Act (MLCA)	31
A. Predicate Offence Types of the ML Cases	31
B. Prosecuted ML Cases Distribution by Value	32
C. ML Channels and Methods used in the Prosecuted ML Cases	33
D. Prosecuted ML Cases Distribution by Region	34
VI. Promoting Public Awareness and Training	35
A. Promoting Public Awareness of AML/CFT	35
B. AML Capacity Building Training	36
VII. International Cooperation	38
A. International Information Exchange	38
B. Concluding Agreements/MOUs with foreign FIUs	39
Part Three: Significant Case Studies	41
I. E-mail fraud	42
II. Violating Securities Exchange Act	45
III. Tax evasion	47
IV. Illegal Fund-raising	50
Part Four: Project research	53
A New Strategy of Combating Crime: Perfecting the Financial Intelligence System against the Emerging Way of Money Laundering by Implementing Bitcoin	54
Part Five: The Major Events of the AMLD	93

Table 01: Statistics of STRs Filed by FIs in 2016.....	19
Table 02: Statistics of STRs from 2012 to 2016	20
Table 03: Statistics of STRs Disseminated by MJIB in 2016	20
Table 04: Number of Strategic Analysis in Recent Years.....	20
Table 05: STRs Distribution by Region in 2016.....	21
Table 06: STRs Distribution by Month in 2016.....	22
Table 07: STRs Distribution by Subjects' Age in 2016.....	23
Table 08: STRs Distribution by Value in 2016	24
Table 09: Statistics of CTRs Filed by FIs in 2016	25
Table 10: Statistics of CTRs from 2012 to 2016.....	26
Table 11: CTRs Distribution by Value in 2016	26
Table 12: Statistics of Accessing CTRs Database from 2012 to 2016	27
Table 13: Statistics of Inbound and Outbound ICTRs in 2016	29
Table 14: Statistics of ICTRs from 2012 to 2016	29
Table 15: ICTRs Distribution by Month in 2016	29
Table 16: ICTRs Distribution by Value in 2016.....	29
Table 17: Statistics of the Predicate Offence Types of the ML Cases and the Competent Authorities Joined the Investigation in 2016	31
Table 18: Prosecuted ML Cases Distribution by ML Value in 2016	32
Table 19: Prosecuted ML Cases Distribution by ML Channels in 2016.....	33
Table 20: Prosecuted ML Cases Distribution by ML Methods in 2016	34
Table 21: Prosecuted ML Cases Distribution by Region in 2016	34
Table 22: Statistics of Seminars Carried out by the AMLAD and Participants in 2016	37
Table 23: Statistics of International Information Exchange from 2012 to 2016	38
Figure A: The AMLAD Organization Chart	7
Figure B: The Work SOP of the AMLAD.....	8
Figure C: Map of STRs Distribution by Region in 2016	22
Figure D: Pie Chart of STRs by Subjects' Age in 2016	23
Figure E: Pie Chart of STRs by Value in 2016	24
Figure F: Line Graph of CTRs by Value in 2016.....	27
Figure G: Pie Chart of ICTRs by Value in 2016	30
Figure H: Pie Chart of ML Value in the Prosecuted ML Cases in 2016.....	33

Part One:

Introduction to the Organization of the AMLD



- I. Legal Framework**
- II. Corporate Effectiveness**

I. Legal Framework

The lucrative proceeds and wealth originated from serious crimes make it possible for organized crime syndicates to infiltrate all levels of government agencies, legitimate businesses, Financial Institutes (FIs) and different parts of the society. The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances concluded in Vienna in 1988 (Vienna Convention) requires state parties to constitute laws to penalize Money Laundering (ML) associated with drug trafficking. In 1989's Summit of G7 in Paris, the leaders of the states recognized the threats exposed to banking system and to FIs, and contributed to the establishment of the Financial Action Task Force (FATF) to set out measures to combat ML. Sequentially, the FATF 40 Recommendations on AML were released in 1990 and amended in 1996 to require the predicate offences of ML should extend to other serious offences besides drug trafficking. Then in 2001, the FATF issued the 8 Special Recommendations on countering terrorist financing (CTF). In 2004, the FATF further strengthened the agreed international standards on AML/CFT (the 40+9 Recommendations). In February 2012, the FATF completed a thorough review of its standards and published the revised FATF Recommendations as "International Standards on Countering Money Laundering and the Financing of Terrorism & Proliferation".

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, the MLCA underwent amendments in 2003, 2006, 2007, 2008, and 2009 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 transactions, AML legislations

around the world require all FIs to file suspicious transaction reports (STRs).

Taiwan has a similar reporting mechanism provided in Article 8 of the MLCA. Based on the definition in the related international organizations, an authority responsible for receiving and analyzing STRs is called “Financial Intelligence Unit” (FIU). In 1997, in accordance with the MLCA, 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 the same year to act as the Taiwan’s FIU.

In addition, pursuant to Subparagraph 7, Article 2 of the Organic Act of MJIB passed by the Legislative Yuan on November 30, 2007 and put into practice on December 19 in the same year upon presidential decree, MJIB is in charge of “ML prevention related matters”. Pursuant to Article 3 of the same Act, the MLPC changed the name to the “Anti-Money Laundering Division” (AMLDD) and kept on the same functions of Taiwan’s FIU. The AMLDD currently has 25 staff members. Please refer to Figures A and B regarding the AMLDD’s organizational structure, mandates and SOP of work. Its budget allocated for 2016 was NTD 2,100,000 plus.

Pursuant to Article 9 of the Regulations for Department Affairs of Investigation Bureau, Ministry of Justice, which was amended on October 17, 2008, the functions of the AMLDD are as follows:

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 currency transaction reports (CTRs) filed by FIs and receiving and processing cross-border transportation of cash and bearer negotiable instruments reports (ICTRs) forwarded by the customs;
4. Assisting other domestic law enforcement partner agencies in matching the AMLDD database for investigating ML cases and coordinating/contacting with respect to ML prevention operation;
5. Liaison, planning, coordination and implementation of information

- exchange, personnel training and cooperation in investigating ML cases with foreign counterparts;
6. Compilation and publication of Annual Report on AML work and the management of relevant data and information; and
 7. Other AML related matters.



© FATF (Financial Action Task Force , FATF)

FATF is a policy-maker for AML/CFT. The members of FATF and FATF-style regional bodies (FSRBs) members, ie. Asia-Pacific Group on Money Laundering (APG), conduct self-assessment and mutual evaluations to ensure the technical compliance and the effectiveness of implementation of the AML/CFT international standards. Currently, the FATF has 37 member countries (35 jurisdictions and 2 organizations, the Gulf Cooperation Council and the European Commission) and 9 associate members (FSRBs).

© Financial Intelligence Unit (FIU)

According 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 terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)." According to Recommendation 29: "Countries should establish a Financial Intelligence Unit that serves

as a national center for the receipt and analysis of to handle and analyze 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 information with the analysis results of that analysis distributed.” The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly. Egmont Group that is an international organization organized in accordance with the Financial Intelligence Unit of each country has the Financial Intelligence Unit defined as: “Responsible for handling (or proposing a request with consent) and analyzing the following disclosed financial information, and forwarding it to the national central unit of the competent authorities:

- (i) Suspicious criminal property, or
- (ii) Anti-money laundering information enacted according to the national law and regulations;

According to Paragraph 1, Article 8 of the MLCA: “For the transactions suspected of violating Article 11, financial institutions should confirm the identity of the customer and retain the transaction records; also, should report it to MJIB.” According to Article 7 and Article 10 of the MLCA: “Financial institutions should report or declare a cash transaction exceeding a certain amount (NT\$500,000, currently) and passengers or transportation service personnel carrying a certain amount of foreign currency and marketable securities (equivalent to US\$10,000, currently) entering and departing the country to MJIB; therefore, MJIB is the Financial Intelligence Unit of Taiwan.”

II. Corporate Effectiveness

Figure A: The AMLD Organizational Chart

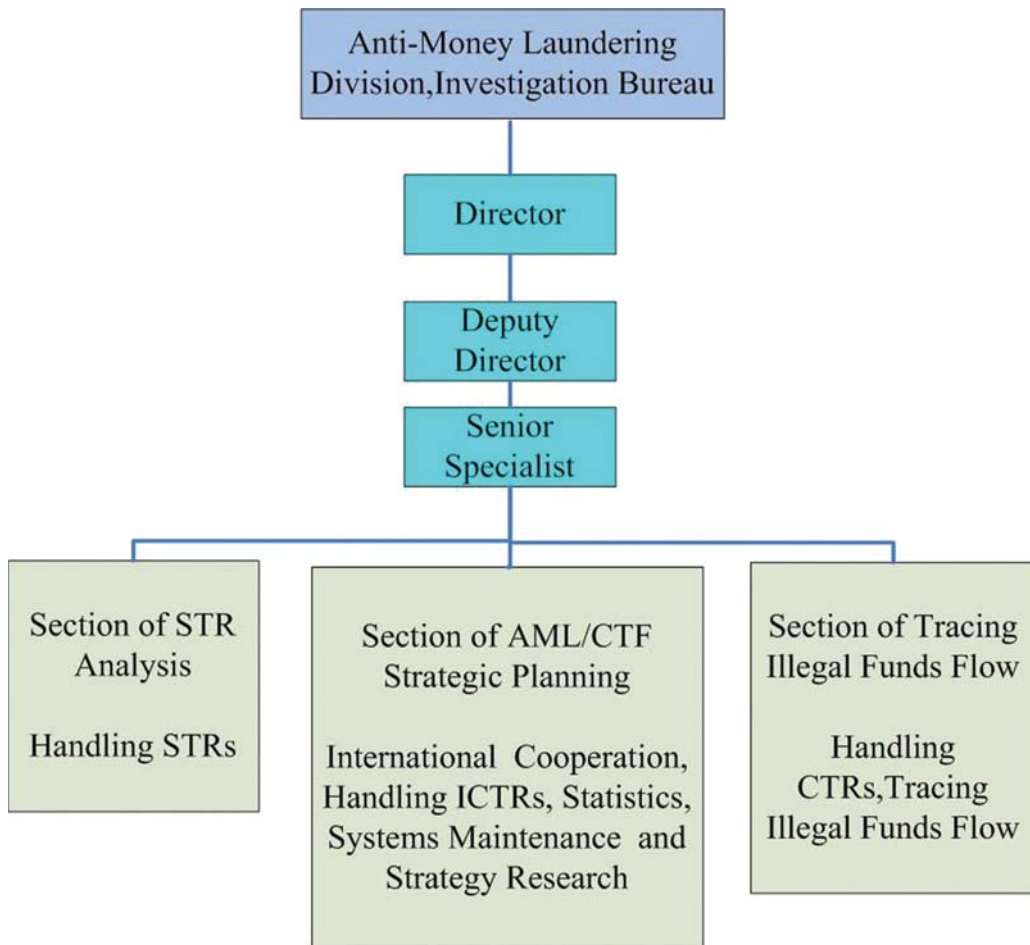
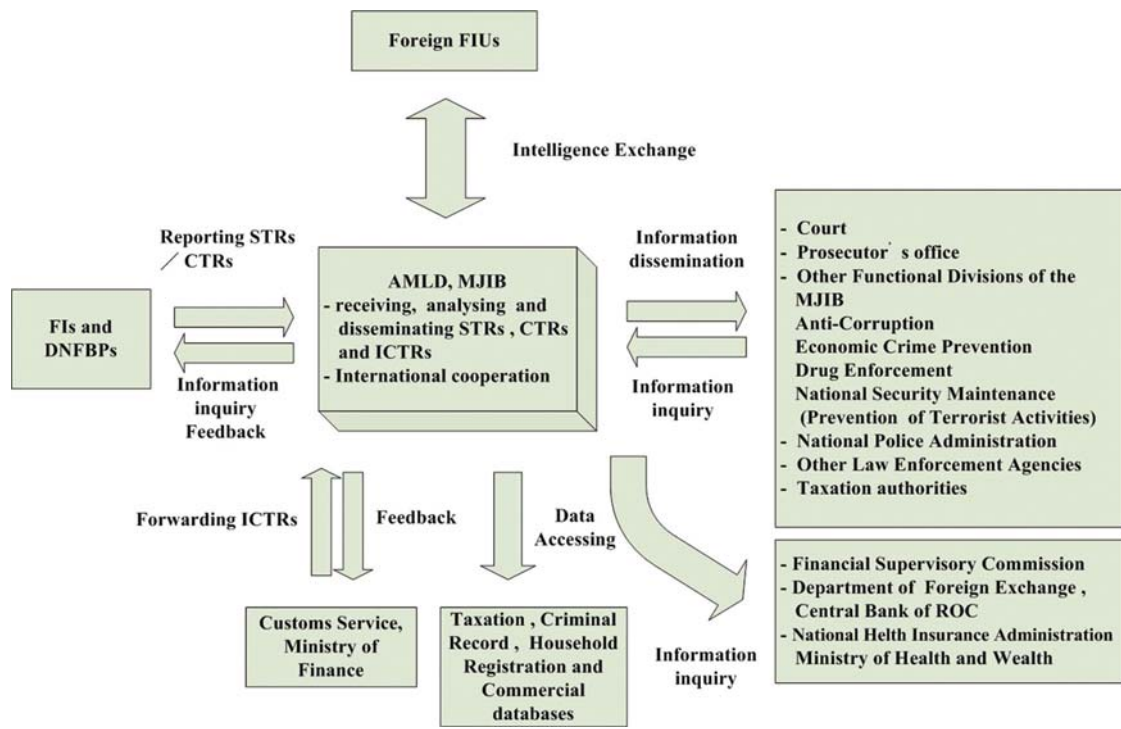


Figure B: The Work SOP of the AMLD



Part Two:

Work Overview



- I. Strategy Research on AML/CFT**
- II. Processing the STRs Filed by FIs**
- III. Receiving the CTRs Filed by FIs**
- IV. Processing the International Currency and Securities Transportation Reports (ICTRs) Forwarded by Taiwan Customs**
- V. The Statistics of Prosecuted Cases under the Money Laundering Control Act (MLCA)**
- VI. Promoting Public Awareness and Training**
- VII. International Cooperation**

I. Strategic Research on AML/CFT

A. Participation in The Terrorist Financing Suppression Act enactment

Terrorism is emerging aggressively in recent years. Extremists like the Islamic State of Iraq and the Levant (ISIL) and other terrorist organizations organized to launch terrorist attacks around the world and to promote their faith and show their power. In view of the fact that terrorism has posed a major threat, terrorism, terrorist organizations and their members, and terrorism financing should be internationally criminalized to curb the spread of terrorism and weapons. Countries complying with United Nations Security Council Resolutions (UNSCRs) have imposed targeted financial sanctions (FTS) against specific individuals and entities involved in terrorism financing and arms proliferation. In order to safeguard national security, align with international standards, and strengthen international cooperation in the field of CFT, Taiwan by referring to the spirit of the “International Convention for the Suppression” and the contents of the FATF 40 Recommendations formulated the “The Terrorist Financing Suppression Act.” The Law was passed by the Legislative Yuan on July 12, 2016 and was promulgated by the President on July 27, 2016. MJIB had actively participated in the review meetings throughout the review period of the draft; also, had assisted in the development of the relevant sub-laws, such as the “Regulations Governing Financial Institutions’ Reporting on the Property, Property Interests and Location of the Property and Property Interests of the Designated Individual, Legal Person or Entity.”

According to FATF 40 Recommendations, jurisdictions must freeze funds or assets without hesitation to ensure no fund or asset could be directly or indirectly used by the subject to sanctions. According to the MLCA of Taiwan, the Ministry of Justice (MOJ) will base on the duty or the report of

MJIB and with the resolution of the CFT Review Board (hereinafter referred to as the “Review Board”) to designate individuals, legal persons, or entities to be included in the TFS list and the subjects to such sanctions are not territorial. For the individuals, legal persons, or entities subject to the TFS resolved and published by the Review Board, financial institutions must not have their banking accounts, currency, or other payment instruments used for the purpose of withdrawals, remittances, account transfers, payments, deliveries or transfers; and must not have their assets or property interests used for the purpose of transfer, alteration, disposition, utilization, or others that may have their quantity, quality, value, and location changed; also, must not collect or provide assets or property interests on their behalf, otherwise, the offenders will be fined for an amount more than NT\$200,000 but less than NT\$1,000,000 by the central competent authorities.



© APG (Asia/ Pacific Group on Money Laundering)

The APG was established in 1997 and aimed to assist the Member States to accept and fulfill the international standards of AML/CFT, and anti-proliferation of weapons enacted by the FATF.

Taiwan had accepted APG mutual evaluation twice in 2001 and 2007, respectively. The mutual evaluation report was approved in the APG annual meeting with high regards on the AML mechanism of Taiwan. MJIB acted as the Financial Intelligence Unit of Taiwan with highest performance evaluation received evidences its excellent performance.

APG currently has 41 Member States, 8 Observer States, and 28 international observer organizations; also, it is an associate member of the FATF. Taiwan is one of the founding Member States of the APG under the name of “Chinese Taipei.” Taiwan may participate in the organizational activities of the FATF as a member of APG.

B. Participation in MLCA amendment

The current MLCA of Taiwan is the first AML law in Asia. Patterns and channels of ML are changing daily along with the development of science and technology. Every jurisdiction is devoted to improving transparency about fund flows and prosecution of ML offences. According to the recent judicial statistics of Taiwan, a significant increase in fraud, illegal fund-raising, and other economic crimes was seriously affecting Taiwan's financial regulation. In order to effectively prevent ML, enhance measures of AML, and promote international cooperation, Taiwan had amended the Act in accordance with the FATF 40 Recommendations and guidelines of the Basel Committee on Banking Supervision (BCBS) and FATF. The amendment was resolved by the Legislative Yuan on December 9, 2016, promulgated by the President on December 28, 2016, and implemented on June 28, 2017.

MJIB has participated in the coordination meetings, public hearings and draft review meetings continuously to promote the process throughout the period of the amendment. The Designated Non-Financial Business and Professions (DNFBP), including Jewelry retail businesses, lawyers, accountants, land administration agent and real estate agencies, notaries, trust and company service providers, are subject to the newly revised MLCA. Financial institutions must have designated personnel to be responsible for AML operation, must establish internal control procedure, and must implement regular on-the-job training. For the “Politically Exposed Persons” (PEPs), including customers, beneficiaries, and their family members and close associates, financial institutions shall apply a risk-based approach to undertake customer due diligence (CDD) measures. The amendment also broadens the scope of specified unlawful activity, adjusts the definition the proceeds of specified unlawful activity, improves the procedure for AML, and complies with international standards.

C. The Chairman of Egmont Group visiting Taiwan

Sergio Espinosa, the Chairman of Egmont Group and head of the Peruvian Financial Intelligence Unit, and Jorge Yumi, Director of the International Affairs Office, visited Taiwan on June 14, 2016. Representatives of MJIB accompanied them to visit the AML relevant authorities, for instance Ministry of Justice, the Ministry of Foreign Affairs, and the Financial Supervisory Commission; also, visited other divisions of MJIB to strengthen mutual understanding and communication so as to enhance the participation of Taiwan in important international organizations.



- Sergio Espinosa (center), the Chairman of the Egmont Group and head of the Peruvian Financial Intelligence Unit, and Jorge Yumi (the 4th from the left), Director of the International Affairs Office, visited MJIB.

D. Visiting the FIU of Vietnam

The Director General Ching-Hsiang Tsai, MJIB, visited the banking Supervision Agency, State Bank of Vietnam (SBV) on November 15, 2016. The FIU of Vietnam is under the guidance of SBV; therefore, the Director General Tsai exchanged opinions with the Deputy Chief Supervisor Pham of the Banking Supervision Agency.



- The Director General Tsai of MJIB presented a souvenir to the Deputy Chief Supervisor Pham of the Banking Supervision Agency, SBV.

E. Participation in the “APG Third Round Mutual Evaluation Staff Meeting”



© (Egmont Group)

The Financial Intelligence Unit of each country convened at Egmont-Arenberg Palace in Brussels, Belgium on June 9, 1995 and decided to establish the Egmont Group as an important platform for intelligence exchange of law enforcement agencies around the world in order to prevent money laundering through joint effort, in particular, in the scope of intelligence exchange, training, and technology sharing.

Taiwan had become a member of Egmont Group in the 6th annual meeting in June 1998; it is currently named “the Anti-Money Laundering Division” (AMLD), Taiwan. The Egmont Group has 156 Member States (up to July 2017). The Member States are to exchange intelligence through a secure network. The AMLD, MJIB regularly attends the annual meetings and working group meetings organized by the Egmont Group; also, initiates intelligence exchange and promotes signing the Agreement or MOU with the FIU of each country on AML/CFT in complying with the FATF recommendations and the purpose of Egmont Group. MJIB signed the Agreement or MOU with 39 countries as of the end of 2016.

Taiwan will receive the APG third round mutual evaluation in the second half of 2018. The MOJ for the purpose of promoting communications among government agencies had invited the competent authorities to attend the “third round mutual evaluation staff meeting” with the third meeting held in April 2016 in order to review the risks and threats of ML/FT faced by Taiwan through a comprehensive discussion with a consensus formed and corrective actions organized.

In view of the grand opening of the Anti-Money Laundering Office of the Executive Yuan (hereinafter referred to AML Office) on March 16, 2017, the overall work of ML prevention in Taiwan will be coordinated by the AML Office to promote cross-sector coordination and cooperation, to gather suggestions, and to promote the joint participation to substantiate the AML/CFT operation for preparing the APG third round mutual evaluation properly.

F. Holding the AML/CFT seminars for financial institutions

The AMLD held the “Seminar on AML/CFT for Financial Industry” on May 5, 2016 with around 180 practitioners in the banking, securities, futures, and insurance industries invited, as well as the prosecutor, Ms. Pei-Ling Tsai, of the MOJ, the representatives of the Banking Bureau of the Financial Supervisory Commission (hereinafter referred to as the “FSC”), the Securities and Futures Bureau, the Insurance Bureau, and the Financial Examination Bureau had attended the meeting and conducted a business briefing, hoping to form a consensus on the law and to assist the industry to prepare for responding to the changes in practice upon the implementation of the amendment .

The AMLD held the “Forum on AML/CFT for the Chief Compliance Officer of Financial Institutions” on December 6, 2016 continuously with the Director of the Banking Bureau, Insurance Bureau, and the Securities and Futures Bureau of the FSC, the Commissioner of the Bankers Association, and the units responsible for AML of domestic and foreign banks invited. The senior special agent of MJIB, Mr. Chia-Hsuan Liu, gave a presentation on the “Substantiating Regulations Compliance and Enhancing Mechanism Effectiveness.” In addition, the special agents of MJIB, Ms. Ling-Hsuan Huang and Mr. Wen-Chieh Su, gave a briefing on the risk management of the offshore banking unit (OBU) and the ML risk of the emerging virtual payment tools “Bitcoin” to exchange opinions and to jointly implement money laundering control.



■ The senior special agent of AMLD, Mr. Chia-Hsuan Liu, gave a briefing on the “Current International AML/CFT Policy and Objective.”



■ The Deputy Director General Lin of MJIB presided the “2016 Forum on AML/CFT for the Chief Compliance Officer of Financial Institutions.”

II. Processing the STRs Filed by FIs

The revised 20th Recommendation of the FATF 40 Recommendations states “If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorism financing, the suspected transaction should be reported promptly to the financial intelligence unit (FIU).” The requirement should be set out in law.

Pursuant to Paragraph 1 of Article 8 of the MLCA, any financial transaction suspected of committing money laundering, the financial institutions (FIs) shall ascertain the identity of the customer and keep the transaction record as evidence, and report the suspected financial transaction (STR) to MJIB. MJIB upon accepting the report will have the STRs filed, screened, and analyzed. If it is suspected of any criminal act or for the stability of financial order and national security, practical or Strategic Financial Intelligence should be composed and distributed to the responsible unit of MJIB or other competent authorities.

In 2016, MJIB received 13,972 STRs. The STRs were compiled statistically and analyzed by FIs, dissemination, region, month, subjects’ age, and value, of which, 90.2% of the reports were filed by domestic banks, 42.1% of STRs happened in Taipei City, 50.9% of the subjects were distributed between 31 and 60 years old, and 22.7% of the transaction amount was under NTD 500,000. (Please refer to Table 01 to Table 07 and Figure C to E for the statistics and analysis of STRs)

A. Statistics of STRs

Table 01: Statistics of STRs Filed by FIs in 2016

Reporting Entities	No. of Reports
Domestic banks	12,608
Foreign banks	28
Trust and investment company	0
Credit Cooperative Associations	70
Credit Department of Farmer & Fishermen Associations	20
Postal Service which handles money transactions of deposit, transfer and withdrawal	1,010
Negotiable Instrument Finance Companies	0
Credit card companies	10
Insurance companies	182
Securities firms	11
Securities investment trust enterprises	6
Securities finance business	2
Securities investment consulting business	0
Securities depository enterprises	19
Futures merchants	2
China banks	3
Electronic payment and electronic ticket institutions	1
Total: 13,972	

Table 02: Statistics of STRs from 2012 to 2016

Year	2012	2013	2014	2015	2016
No. of Reports	6,137	6,266	6,890	9,656	13,972

B. Results of STRs Processed by MJIB

Table 03: The Statistics of STRs Disseminated by MJIB in 2016

Process	No. of STRs filed
Disseminated to other functional divisions of MJIB	1,537
Disseminated to police agency, prosecutor office, and other competent agencies	407
Stored in the AMLD database for reference	11,777
Under analysis	211
International cooperation	40
Others	0
Total: 13,972	

P.S.: The information in this Table was gathered on May 25, 2017.

C. Number of Strategic Analysis in Recent Years

Table 04: Number of Strategic Analysis in Recent Years

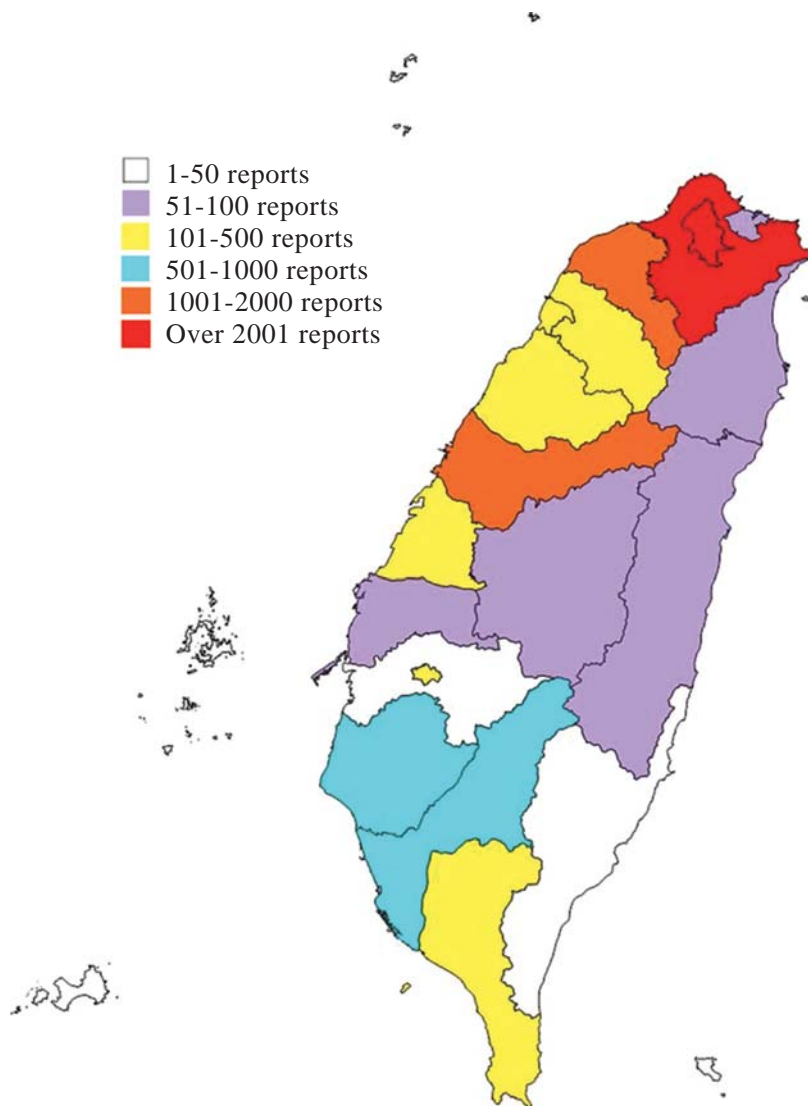
Year	2012	2013	2014	2015	2016
No. of Reports	1	1	1	1	1

D. Distribution of STRs by Region

Table 05: STRs Distribution by Region in 2016

Region	No. of Reports	Region	No. of Reports
Taipei City	5,882	Yunlin County	58
New Taipei City	2,468	Chiayi City	178
Keelung City	75	Chiayi County	34
Yilan County	52	Tainan City	546
Taoyuan City	1,121	Kaohsiung City	933
Hsinchu City	321	Pingtung County	144
Hsinchu County	159	Hualien County	53
Miaoli County	139	Taitung County	28
Taichung City	1,429	Penghu County	6
Changhua County	238	Kinmen County	34
Nantou County	72	Lianjiang County	1
			Total: 13,972

Figure C: Map of STRs Distribution by Region in 2016



E. Distribution of STRs by Month

Table 06: STRs Distribution by Month in 2016

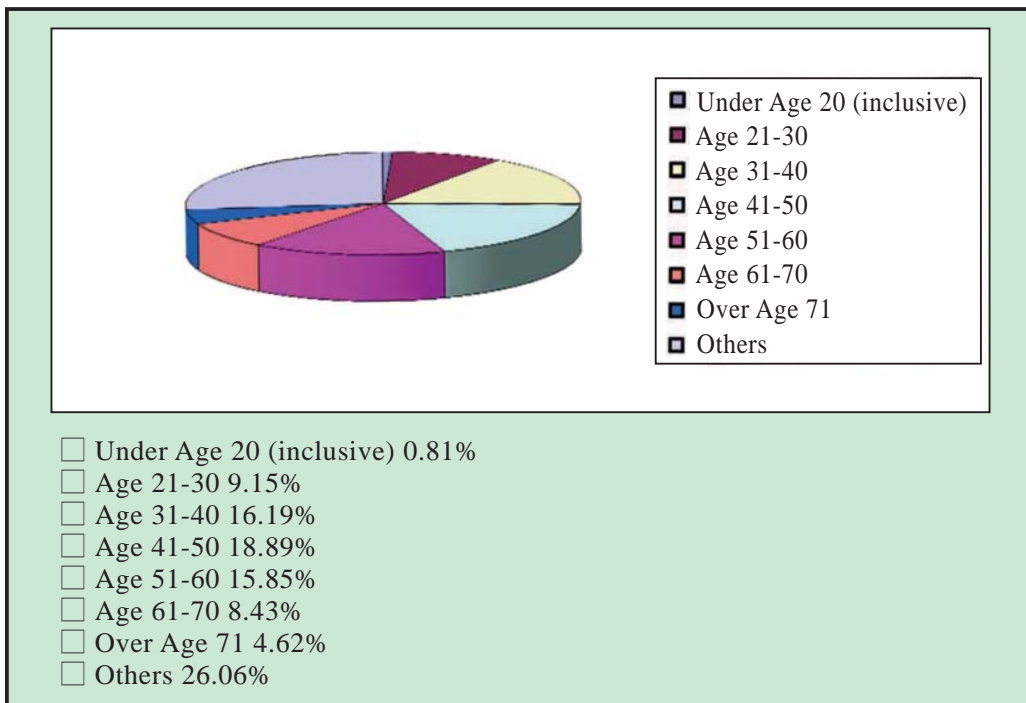
Month	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sep.	Oct.	Nov.	Dec.
No. of Reports	1,269	742	1,071	1,036	1,033	1,102	893	1,102	1,293	1,413	1,430	1,588

F. The STRs Distribution by Subjects' Age

Table 07: STRs Distribution by Subjects' Age in 2016

Age Group	No. of Persons
Under Age 20 (inclusive)	113
Age 21-30	1,279
Age 31-40	2,262
Age 41-50	2,639
Age 51-60	2,214
Age 61-70	1,178
Over Age 71	646
Others ¹	3,641
Total : 13,972	

Figure D: Pie Chart of STRs by Subjects' Age in 2016



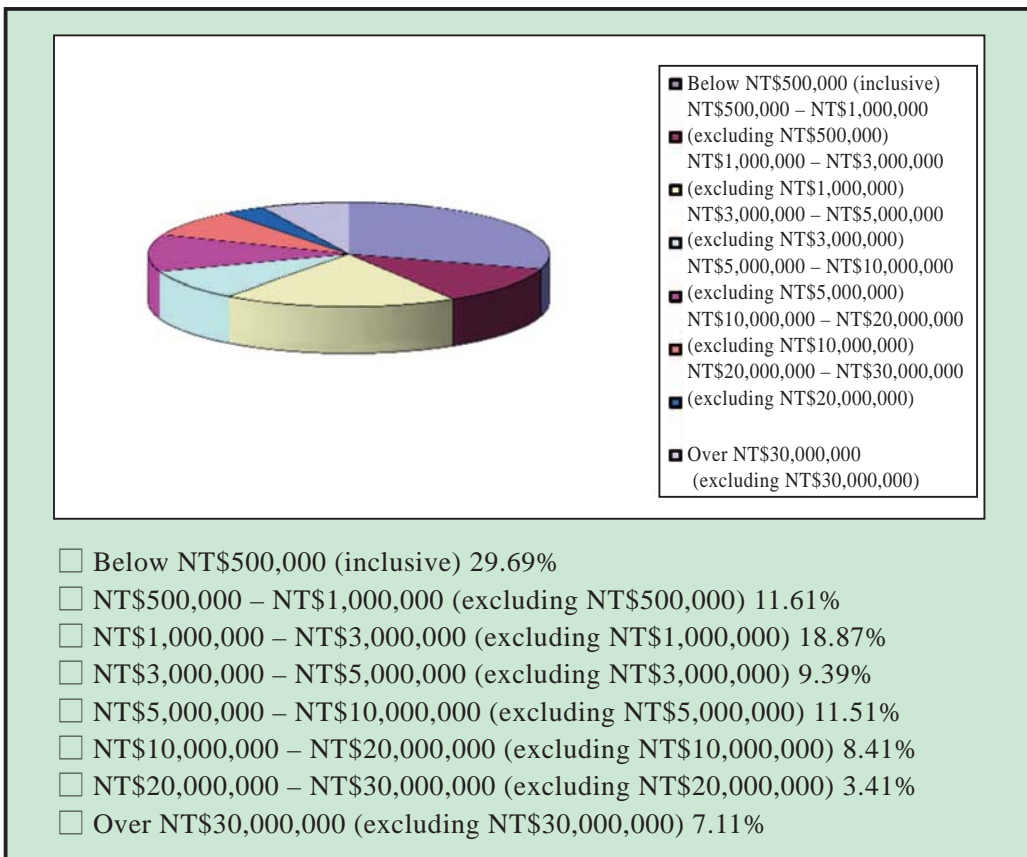
¹ Other: Refers to companies and unincorporated associations.

G. STRs Distribution by Value

Table 08: STRs Distribution by Value in 2016

Amount	No. of cases
Below NT\$500,000 (including NT\$500,000)	4,148
NT\$500,000 – NT\$1,000,000 (excluding NT\$500,000)	1,622
NT\$1,000,000 – NT\$3,000,000 (excluding NT\$1,000,000)	2,636
NT\$3,000,000 – NT\$5,000,000 (excluding NT\$3,000,000)	1,312
NT\$5,000,000 – NT\$10,000,000 (excluding NT\$5,000,000)	1,609
NT\$10,000,000 – NT\$20,000,000 (excluding NT\$10,000,000)	1,176
NT\$20,000,000 – NT\$30,000,000 (excluding NT\$20,000,000)	476
Over NT\$30,000,000 (excluding NT\$30,000,000)	993
Total: 13,972	

Figure E: Pie Chart of STRs by Value in 2016



III. Receiving the CTRs Filed by FIs

Pursuant to Article 7 of the MLCA, any currency transaction exceeding a certain amount of money (CTRs) reported by the FIs shall be filed for records by MJIB. Pursuant to Article 2 of the “Regulations Governing Cash Transaction Reports (CTR) and Suspicious Transaction Reports (STR) by Financial Institutions,” the term “a certain amount” shall mean NTD 500,000 (including the foreign currency equivalent thereof). In addition, according to the Operation Directions of MJIB (admitted with the MOJI 1000804273 Letter issued by the MOJ on July 14, 2011), the AMLD assists other Field Stations of MJIB, courts, prosecutor offices, and other law enforcement agencies to access CTRs database. In 2016, MJIB received 3,712,685 CTRs. According to the statistics and analysis by the FIs and reporting amount, around 77.7% of CTRs were filed by domestic FIs, 74.44% of the transaction amount was between NTD 500,000 and NTD 1,000,000. A total of 220,492 CTRs were processed in 2016 (Please refer to Tab 8 – Table 11 and Figure F for statistics and analysis in details).

A. Statistics of CTRs

Table 09: Statistics of CTRs Filed by FIs in 2016

Reporting Entities	No. of Reports
Domestic banks	2,884,788
Foreign banks	18,102
China banks	1
Credit Cooperative Associations	158,126
Credit Department of Farmers & Fishermen Associations	312,278
Postal Service which handles money transactions of deposit, transfer and withdrawal	330,287
Insurance companies	9,059
Other financial institutions	43
Jewelry retail businesses	1
Total: 3,712,685	

Table 10: Statistics of CTRs from 2012 to 2016

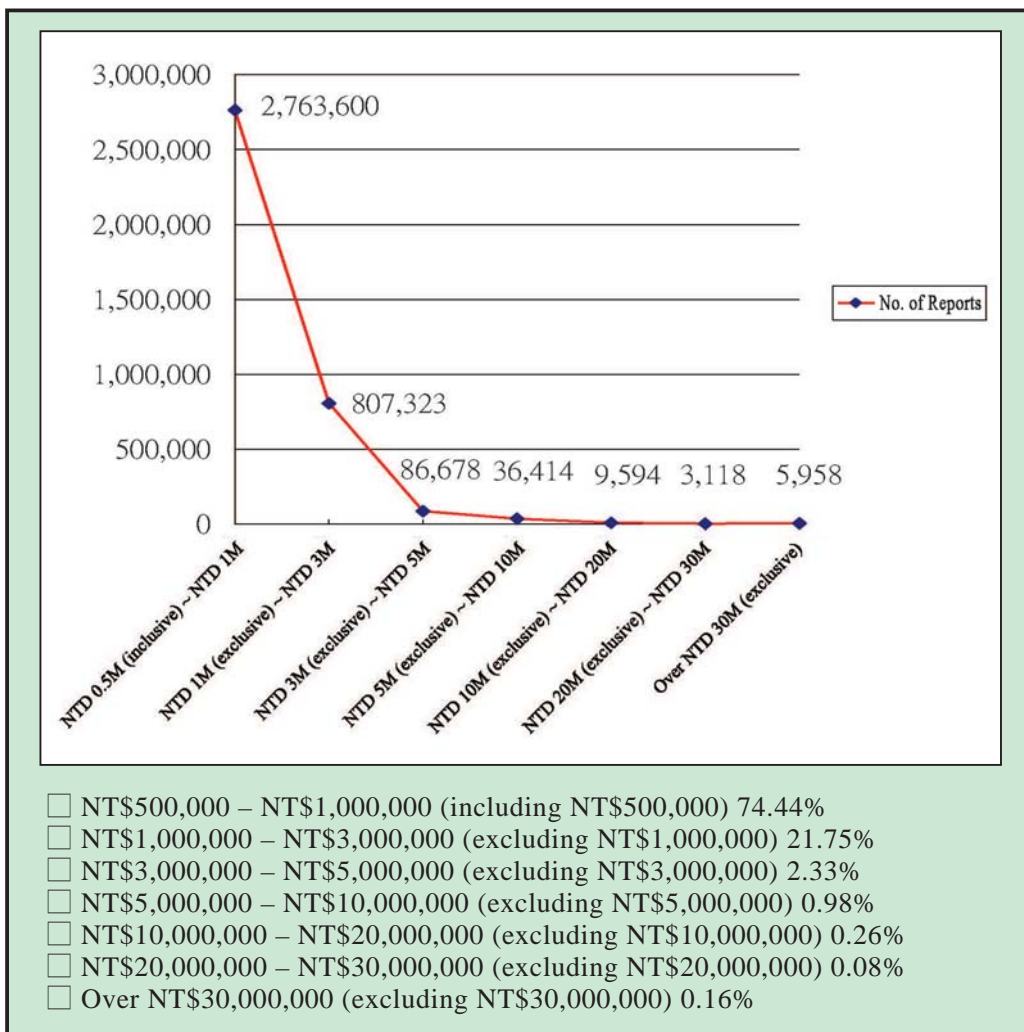
Year	2012	2013	2014	2015	2016
No. of Reports	3,726,585	3,995,726	4,107,745	3,934,708	3,712,685

B. Distribution of CTRs by Value

Table 11: CTRs Distribution by Value in 2016

Amount	No. of Reports
NT\$500,000 – NT\$1,000,000 (including NT\$500,000)	2,763,600
NT\$1,000,000 – NT\$3,000,000 (excluding NT\$1,000,000)	807,323
NT\$3,000,000 – NT\$5,000,000 (excluding NT\$3,000,000)	86,678
NT\$5,000,000 – NT\$10,000,000 (excluding NT\$5,000,000)	36,414
NT\$10,000,000 – NT\$20,000,000 (excluding NT\$10,000,000)	9,594
NT\$20,000,000 – NT\$30,000,000 (excluding NT\$20,000,000)	3,118
Over NT\$30,000,000 (excluding NT\$30,000,000)	5,958
Total: 3,712,685	

Figure F: Line Graph of CTRs by Value in 2016



C. Statistics of Assisting Law Enforcement Agencies in Accessing CTRs Database

Table 12: Statistics of Accessing CTRs Database from 2012 to 2016

Year	2012	2013	2014	2015	2016
MJIB	25,718	28,205	36,528	36,130	21,413
Other law enforcement agencies	138	133	10,262	5,641	13,012
prosecution and Judicial authority	729	16,010	17,110	8,897	5,186
Total	33,728	55,368	88,464	50,668	39,611

IV. Receiving the International Currency and Securities Transportation Reports (ICTRs) Forwarded by Taiwan Customs

The revised FATF Recommendation 32 states “Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system. Each State should ensure that the established reporting system or disclosure system can be applied to all entities cross-border transport either carried by passengers or through mail and cargo delivery; however, different systems should be applied for different transport pattern.”

Pursuant to paragraph 1 of Article 10 of the MLCA, “passengers or service crew on board who cross the border with the carrier and carry the following items shall make declarations to the Customs. The Customs shall report subsequently to the Investigation Bureau, Ministry of Justice: 1. Cash of foreign currency with total amount exceeding a certain amount; 2. Negotiable securities with face value exceeding a certain amount.” Pursuant to Article 4 of the “Regulations for the Declaration of Carrying Foreign Currencies or Securities by Cross-Border Passengers or Service Crew on Board of Transport and for the Interagency Report by the Customs,” the term “a certain amount” shall mean USD 10,000 or foreign currency with equivalent value. A total of 33,555 ICTRs cases were reported to MJIB in 2016. In terms of the declared value, around 78.43% of the ICTRs were under NTD 1,000,000 (Please refer to Table 12 to Table 15 and Figure G for the statistics and analysis of ICTRs).

A. Statistics of ICTRs Declared by the Passengers to Taiwan Customs

Table 13: Statistics of Inbound and Outbound ICTRs in 2016

Inbound & Outbound	No. of Reports
Inbound	3,621
Outbound	29,934
Total	33,555

Table 14: Statistics of ICTRs from 2012 to 2016

Year	2012	2013	2014	2015	2016
No. of Reports	8,726	14,273	18,781	27,725	33,555

B. ICTRs Distribution by Month

Table 15: ICTRs Distribution by Month in 2016

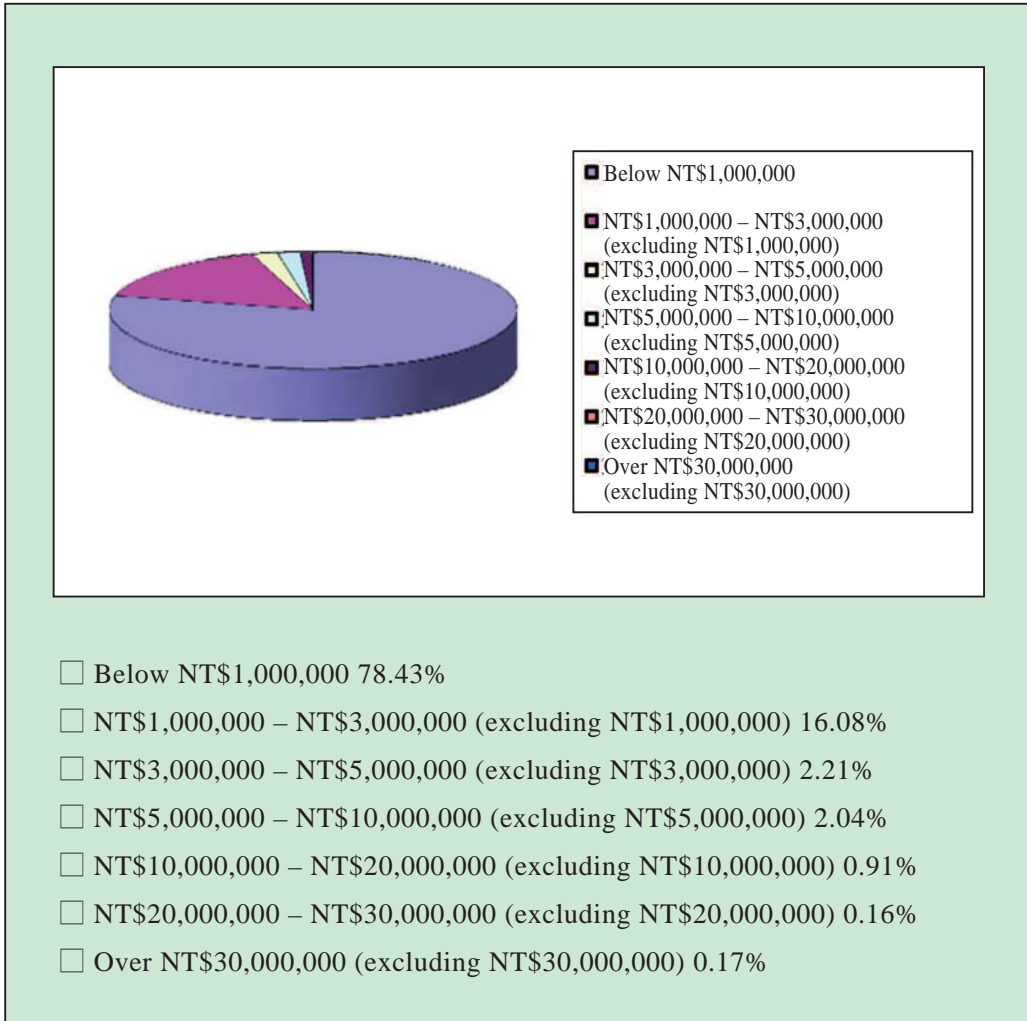
Month	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sep.	Oct.	Nov.	Dec.
No. of Cases	2,378	2,838	2,823	3,451	3,513	2,778	2,762	2,520	2,538	3,029	2,764	2,161

C. ICTRs Distribution by Value

Table 16: ICTRs Distribution by Value in 2016

Amounts	No. of Reports
Below NT\$1,000,000	26,318
NT\$1,000,000 – NT\$3,000,000 (excluding NT\$1,000,000)	5,394
NT\$3,000,000 – NT\$5,000,000 (excluding NT\$3,000,000)	742
NT\$5,000,000 – NT\$10,000,000 (excluding NT\$5,000,000)	686
NT\$10,000,000 – NT\$20,000,000 (excluding NT\$10,000,000)	304
NT\$20,000,000 – NT\$30,000,000 (excluding NT\$20,000,000)	55
Over NT\$30,000,000 (excluding NT\$30,000,000)	56
Total: 33,555	

Figure G: Pie Chart of ICTRs by Value in 2016



V. Statistics of Prosecuted Cases under the Money Laundering Control Act (MLCA)

Through accessing the Prosecution Document Database Enquiring System that is maintained by the MOJ, the AMLD had cases prosecuted by district prosecutor offices in 2016 under Paragraph 1 and 2 of Article 11 of the MLCA, including deferred prosecutions and petitions for summary judgments. The information retrieved included the types of predicate crime, charges, proceeds of crime, typologies of ML, and profiles of defendants. All the information should be analyzed in order to build the statistics regarding ML overview and trends in Taiwan in 2016. In 2016, there were 28 cases prosecuted under money laundering. A total of laundered money reaches NTD 15,011,758,137 from the cases (Please refer to Table 16 to Table 20 and Figure H for the statistics and analysis of the prosecuted cases).

A. Predicate Offence Types of the ML Cases

Table 17: Statistics of the Predicate Offence Types of the ML Cases and the Competent Authorities Joined the Investigation in 2016

Offence Types	Predicate Offences	MJIB	District Prosecutor Office	National Police Agency	Others	Total
General Criminal crime	Forged documents	1	0	0	0	1
	Organize crime, fraud	0	0	1	0	1
	Fraud	3	0	6	0	9
	The Smuggling Penalty Act	0	0	1	0	1
General Criminal crime - Total		4	0	8	0	12
Money laundering	Unauthorized disclosure	1	0	0	0	1
Unauthorized disclosure - Total		1	0	0	0	1

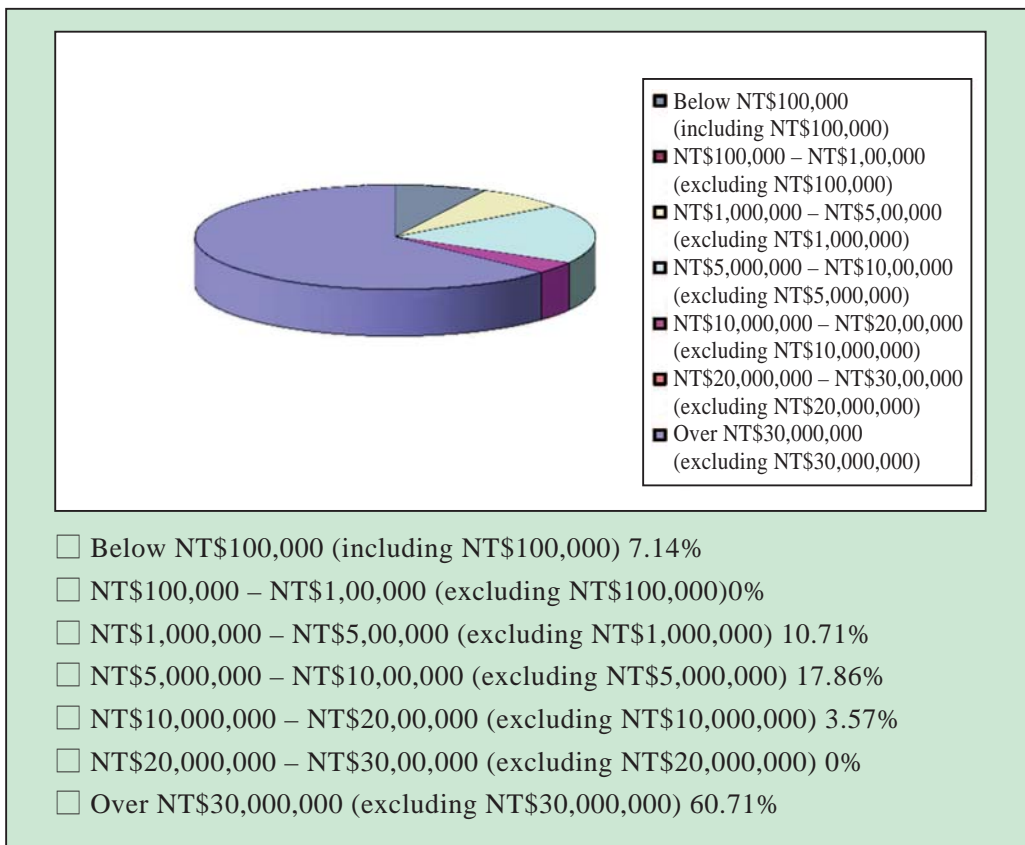
Economic crime	Securities Exchange Act	2	0	0	1	3
	Credit Cooperative Law	0	1	0	0	1
	Perfidy	1	0	0	0	1
	Banking Act	4	1	1	0	6
Economic crime - Subtotal		7	2	1	1	11
Corruption crime	Accepting bribes	1	0	0	0	1
	Accepting bribes for breaching duties	1	0	0	0	1
	Anti-Corruption Act	0	0	0	1	1
Corruption subtotal		3	0	0	1	4
Total		15	2	9	2	28

B. Prosecuted ML Cases Distribution by Value

Table 18: Prosecuted ML Cases Distribution by ML Value in 2016

Amount	Cases
Below NT\$100,000 (including NT\$100,000)	2
NT\$100,000 – NT\$1,00,000 (excluding NT\$100,000)	0
NT\$1,000,000 – NT\$5,00,000 (excluding NT\$1,000,000)	3
NT\$5,000,000 – NT\$10,00,000 (excluding NT\$5,000,000)	5
NT\$10,000,000 – NT\$20,00,000 (excluding NT\$10,000,000)	1
NT\$20,000,000 – NT\$30,00,000 (excluding NT\$20,000,000)	0
Over NT\$30,000,000 (excluding NT\$30,000,000)	17
Total: 28	

Figure H: Pie Chart of ML Value in the Prosecuted ML Cases in 2016



C. ML Channels and Methods used in the Prosecuted ML Cases

Table 19: Prosecuted ML Cases Distribution by ML Channels in 2016

Types of FIs	Cases
Real property	1
Creative banks	1
Banks	24
Others	2
Total: 28	

Table 20: Prosecuted ML Cases Distribution by ML Methods in 2016

Methods of ML	Cases
Dummy accounts	7
hawala	4
Remittance from abroad	6
Hidden by friends	2
Personally carry	2
Relatives' accounts	3
Purchasing real property	1
Purchasing precious metal and jewelry	1
Others	2
Total: 28	

D. Prosecuted ML Cases Distribution by Region

Table 21: Prosecuted ML Cases Distribution by Region in 2016

Region	Cases	Region	Cases
Taipei City	7	New Taipei City	5
Kaohsiung City	2	Taichung City	3
Taoyuan City	5	Tainan City	1
Hsinchu City	2	Penghu County	1
Miaoli County	1	Changhua County	1
Total: 28			

VI. Promoting Public Awareness and Training

A. Promoting Public Awareness of AML/CFT

Besides routinely promoting the public awareness campaigns of protecting government infrastructure and anti-corruption, AML/CFT as a vital part, of which are carried out year-round by the field offices of MJIB nationwide. By taking advantage of local activities and public occasions, the field agents introduce and explain directly and enthusiastically to the institutions and groups, schools, and private sectors for people to understand what the AML/CFT is and its related matters. With all these efforts, we firmly believe that the awareness will gradually be deep-rooted in Taiwanese people eventually.



■ Colleagues of Taipei City Field Office, MJIB at the “National Taiwan University of Science and Technology 2016 Employment and Internship Fair” in the AML task campaign



- Colleagues of New Taipei City Field Office, MJIB at the “2016 Ten Thousand People Power Walk and Fun Fair” in the AML task campaign

B. AML Capacity Building Training

The revised Recommendation 34 of the FATF states: “The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist FIs and DNFBP in applying national measures to combat money laundering and terrorism financing, and, in particular, in detecting and reporting suspicious transaction.” To help the staffs of FIs fully understand the requirements concerning AML/CFT, the indicators of suspicious transactions to improve the quality of filing STRs, the compliance with the MLCA, and media transmission protocols, the AMLD has been providing training programs with lectures and presentations. These programs, upon FIs’ requests, cover the topics of AML/CFT international standards, the MLCA reporting obligations of FIs, case studies and the emerging trends in

AML/CFT. The AMLD instructors have been sharing professional experience with the participants from FIs and discussing the pros and cons of the reported STRs. With case studies, the patterns of suspicious transactions that were connected with certain crimes, such as underground remittance, stock market manipulation, insider trading, business depletion by illicit means, fraud, and internet gambling, can thus be further understood and learned as lessons to detect and identify suspicious transactions more effectively in the future.

Table 22: Statistics of Seminars Carried out by the AMLD and Participants in 2016

Types of FIs		Subtotal	
		No. of Seminars	No. of Participants
Bank	Domestic Bank (including Holdings)	41	4,730
	Foreign Bank	7	405
	Mainland China Banks	0	0
Credit Department of Farmers and Fishermen Associations		2	230
Securities Investment Trust Business		1	55
Securities Firms		1	30
Futures Merchants		3	208
Postal Service which handle money transactions of deposit, transfer and withdrawal		4	258
Insurance Companies		22	1,178
Negotiable Instrument Finance Companies		0	0
Other Types		0	0
Total		81	7,094

VII. International Cooperation

A. International Information Exchange

The revised Recommendation 40 of the FATF 40 Recommendations states: “Countries should ensure that their competent authorities can rapidly, constructively, and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences, and terrorism financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation. Countries should authorize their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely manner with the widest range of foreign counterparts” and “Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritization and timely execution of requests, and for safeguarding the information received.”

Table 23: Statistics of International Information Exchange from 2012 to 2016

Matters	Year	2012	2013	2014	2015	2016
Requests from Overseas FIUs	Cases	36	41	32	51	50
	No. of Reports	95	113	89	152	169
Requests to Overseas FIUs	Cases	15	17	18	45	34
	No. of Reports	55	62	67	222	165
Spontaneous Exchanges from Overseas FIUs	Cases	15	17	33	32	25
	No. of Reports	27	39	58	44	44
Spontaneous Exchanges to Overseas FIUs	Cases	7	4	6	9	26
	No. of Reports	21	11	13	18	45
Questionnaires and Other Matters	Cases	0	0	0	0	0
	No. of Reports	77	100	85	201	262
Total	Cases	73	79	89	137	135
	No. of Reports	275	325	312	637	685

B. Concluding Agreements/MOUs with foreign FIUs

ML is usually a cross-boundary crime. In order to effectively combat cross- boundary crime of ML/TF, and the proliferation of WMD, it depends on the government of each country to form a consensus and to work together. MJIB is the FIU of Taiwan and strives to contribute in the effort of preventing international money laundering. Taiwan and the Islamic Republic of Afghanistan signed a MOU concerning cooperation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing on October 19, 2016, which helped lay the foundation for future exchange of information between the two countries



- MJIB and FinTRACA signed a MOU concerning cooperation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing.

Part Three

Significant Case Studies



- I. E-mail fraud**
- II. Violating Securities Exchange Act**
- III. Tax evasion**
- IV. Illegal Fund-raising**

I. E-mail fraud

A. Case Overview

(I) Disclosure of STRs

The AMLD received a STR from Bank A in January 2015: The OBU account of Company A was inactive for almost one year, but it suddenly was remitted US\$1,121,793.75 from Company B overseas; also, the receiving bank received a SWIFT message the following day informing that the transaction is suspected of fraud and requesting to have the said fund frozen and returned.

(II) Suspects

Chang, the responsible person of Company A, and Lin, the account broker

(III) Method

1. International fraud group's scheme:

An international fraud group forged the identity of Company B's Executive Director to inform Swiss Bank B by e-mail to transferred an amount of US\$859,939.75 and US\$1,121,793.75 from Company B's account to Company C and Company A. Swiss Bank B had followed such false notification by e-mail with two remittances arranged. On the following day, such international fraud group had repeated the same fraud scheme and forged the identity of Company B's Executive Director to notify Swiss Bank B by e-mail having US\$2,450,765.63 and US\$2,161,895.32 remitted from Company B's account to Company D's account in UK and Company E's account in Poland. Swiss Bank B still mistakenly believed that the payment notice was issued by Company B's Executive Director and with the two remittances processed on January 23, 2015. Company B was scammed for an amount of US\$6,594,394.45 (equivalent to NT\$209,945,736.15).

The intermediary Lin asked Chang if he was willing to provide his OBU account to help have funds transferred to Hong Kong and promised to have the balance amount after deducting the relevant fees paid for the use of the OBU account. Chang agreed to provide the OBU account of Company A for use. The aforesaid international fraud group had an amount of US\$1,121,793.75 that was scammed from Company B on January 22, 2015 remitted to the OBU account of Company A. Chang had an amount of US\$10,000 transferred to its dummy account in February 2015 and then transferred an amount of US\$1 million on the next day to Company A's foreign currency account with Bank D. Bank A's immediate informing the abnormal transactions and assistance had helped have the said amount of US\$1.01 million seized immediately.

2. The process of this case by other countries:

Company B was scammed by an international fraud group by causing Swiss Bank B mistakenly to have funds transferred out from Company B's account to the bank account of Company C in Mainland China, the bank account of Company D in UK, and the bank account of Company E in Poland, of which, the amount remitted to the United Kingdom and Mainland China had been fully recovered and returned to the Company B; however, the amount remitted to Poland was with only 73% of the money returned to Company B.

B. Detecting

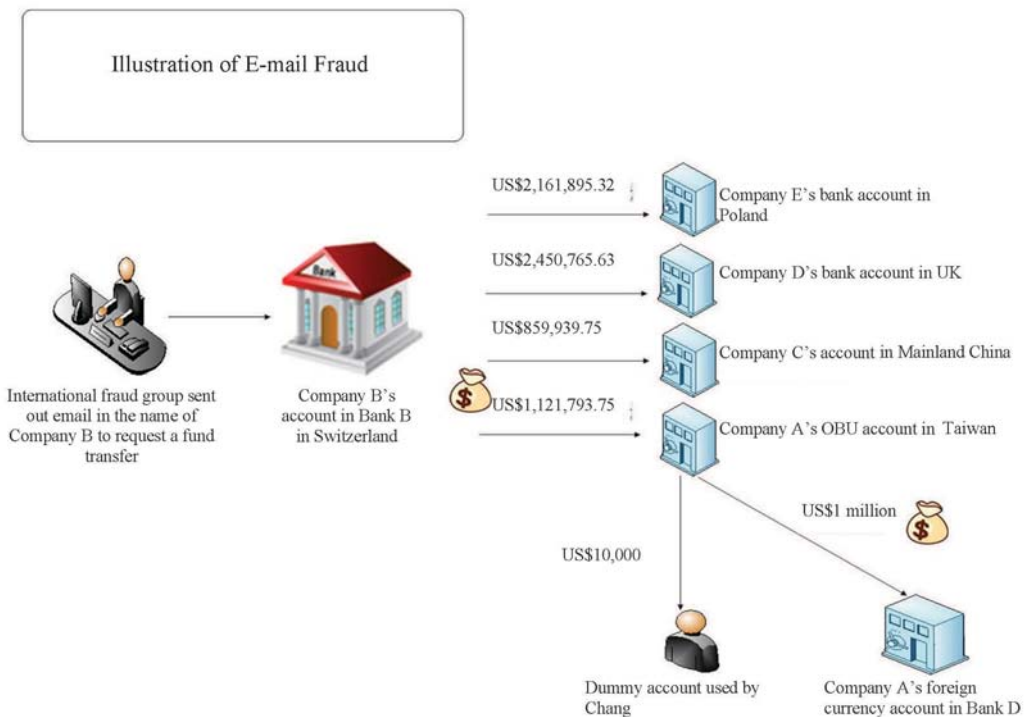
Customers have unusual deposits (such as, multiple promissory notes and checks deposited in the same account) that are not justified with their identity and income or are irrelevant with the nature of business operation.

C. Indictment

Taiwan Hsinchu District Court Prosecutor Office had Chang and others prosecuted in May 2016 for committing frauds and violating the MLCA.

D. Experience sharing

Bank A had noticed unusual changes in customers' trading habit; therefore, the suspicious transactions were reported to the AMLD, so that MJIB was able to grasp the capital flows at the beginning. International fraud groups utilize transnational fund transfer to conceal illegal benefits that has made the trail of funds hard to find. Bank A reports account transactions in a timely manner and works with law enforcement agencies to seize illegal income for the return of stolen money in the future and for significantly minimizing the loss of victims.



II. Violating Securities Exchange Act

A. Case Overview

(I) Disclosure of STRs

The AMLD received a STR from Bank B in March 2016: a large sum of cash was suddenly withdrawn from the account of Ms. Lin, indicating the funds were intended for investment. Lin was young and the transaction amount of the account was huge, not in line with the income and background of Lin that was suspected of ML.

(II) Suspects

Hsu, the responsible persons of Company B

(III) Method

Mr. Hsu was the responsible person of Company B that was an OTC company. Hsu, therefore, was in charge of the investing activities of Company B, including stock private placement, corporate bond issuance, mergers and acquisitions, and equity investment. However, when Company B issued the 4th and 5th secured convertible corporate bonds (hereinafter referred to as 4th and 5th convertible bonds), Hsu had made false statement in the prospectus and also participated in the inquiry to purchase and sale convertible bonds through dummy accounts, such as Ms. Lin's account. Hsu had acquired 5,984 units of 4th and 5th convertible bonds, of which, the dummy account of Lin was with 4,220 units of 5th convertible bonds, accounted for 84.4% of the total issued shares.

The convertible bonds issued by Company B were partially disassembled as “Convertible Bond Asset Swap Option (CBASO)” by X Commercial Bank. Hsu with his associates negotiated the undertaking and disassemble of CBASO before the issuance. Furthermore, Hsu arranged his associates to undertake CBASO through dummy accounts with extremely low royalties paid to gain substantial control of Company B's convertible bonds for reducing the cost of shareholding, manipulating stock price, and gaining huge spreads. When the stock price rose through manipulation, the dummy accounts were closed with a cash settlement in advance, or the

convertible bonds were converted to cash with illegal gains earned for a total profit of NT\$140,004,180.

B. Detecting

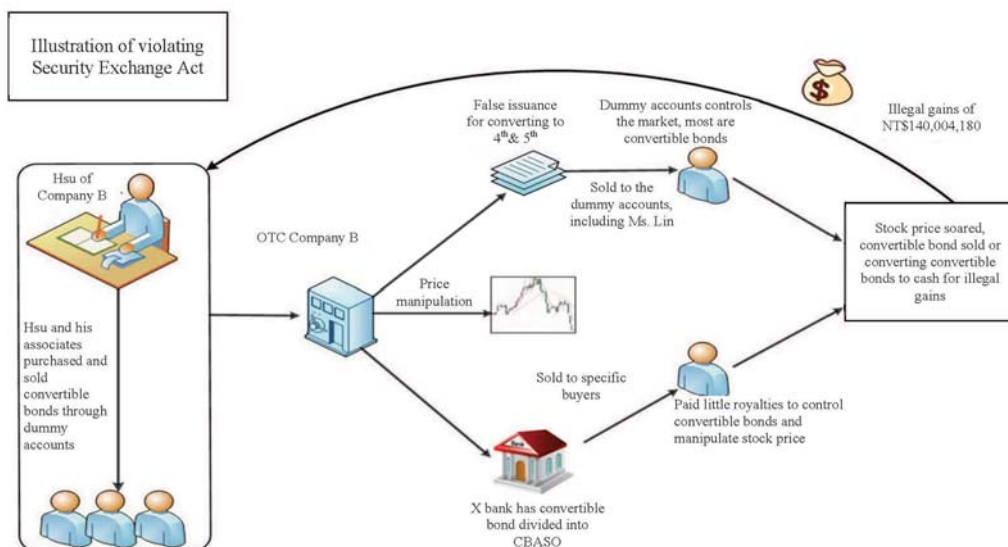
Each deposit and withdrawal amount of the account was equivalent and in a short interval of period; also, the huge amount of transaction was clearly not in line with the age or income of the client.

C. Indictment

Hsu was suspected of fraudulent issuance of convertible bonds and was indicted by the Taiwan New Taipei City District Court Prosecutor Office in January 2017 according to Article 171 Paragraph 1 Section 1 of the Securities Exchange Act with a penal servitude for a period of 7 years.

D. Experience sharing

Hsu used many accounts of others to engage in illegal transactions. The financial flow made between accounts was complicate. MJIB compared bank statements of many banks to produce a complete flow of funds. Each FI after such case being disclosed in the media had immediately reported STR that were helpful for the follow-up investigation and in understanding capital flows.



III. Tax Evasion

A. Case Overview

(I) Disclosure of STRs

The AMLD accepted a STR from Bank C in October 2014: The bank account of Company C had many notes for an amount less than NT\$500,000 deposited and cash withdrawals made since June 2014; also, the account had only a nominal balance that was suspected of avoiding the requirement of CTR. Although the bank had repeatedly asked this customer to make remittance or wire transfer instead, this customer continued the transaction mode of making cash withdrawals for an amount less than NT\$500,000.

(II) Suspects

The responsible person of Company C and Company E, Mr. Su.

(III) Method

Su served as the Director of a medical center of Hospital D. Hospital D and Su had an outsourcing contract signed in 1995 with an agreement reached making Su responsible for the operating profit and loss of the medical center. Since then, due to the continuous profitable operation of the medical center, a substantial increase in personal income of Su was seen. For the purpose of avoiding personal income high progressive tax rate, Su had incorporated dummy corporations of Company C and Company E in the name of others, then issued false medical supplies invoices from Company C and Company E to Hospital D. Hospital D then issued a check to pay for the goods to Company C and Company E that was actually the personal income of Su. Accumulated in the period from 2005 to 2014, the invoices issued by Company C and Company E to Hospital D for medical supplies amounted over NT\$90 million and NT\$200 million, respectively, for a grand total over NT\$300 million.

After reviewing the business tax information of Company C and

Company E in the period from 2007 to 2014, medical supplies were sold only to Hospital D without conducting any business operation with other hospitals. There was no relevant document for the purchase of medical equipment found; also, there was no inventory recorded to evidence the business operation. It was simply a paper company setup by Su and invoices were issued with false amount and description for writing off the earnings distributed from the medical center of Hospital D. Su had committed a crime of tax evasion for an amount more than NT\$100 million through Company C and Company E in the period from 2007 to 2014.

B. Detecting

The cash deposit and withdrawal of the same account in the same business day amounted to a certain amount, respectively, and the transaction was not in line with the status and income of the customer; also, it was irrelevant to the nature of business.

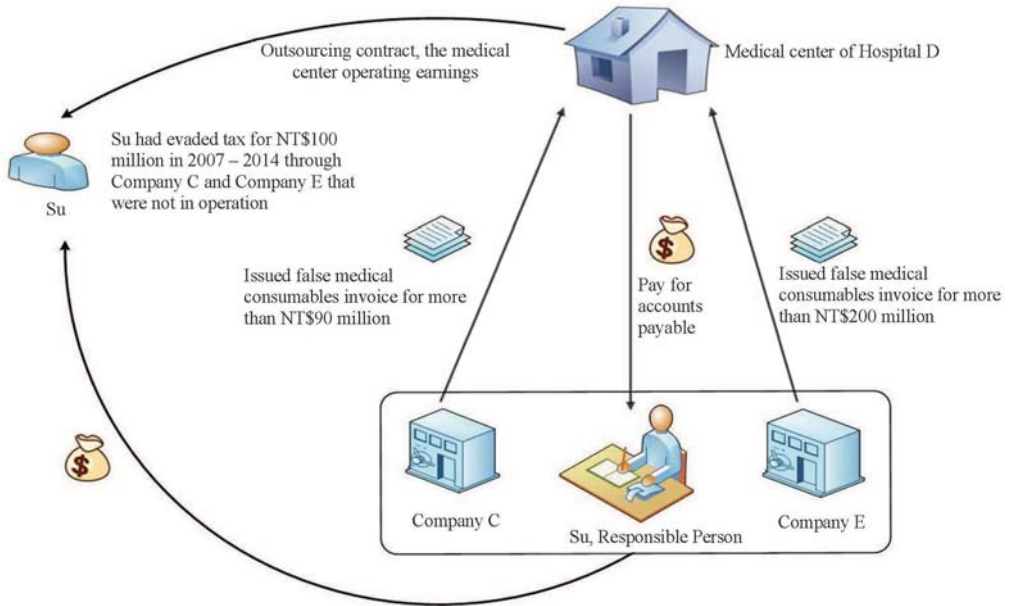
C. Punitive fines

National Taxation Bureau of the Central Area, Ministry of Finance had ruled for Su to pay tax for the period of 2008 to 2014 and a punitive fine for a grand total of more than NT\$70 million in June 2016.

D. Experience sharing

- (I) Su had incorporated paper companies to issue false invoices for significant tax evasion for many years. Bank C upon identifying the abnormal business operation of the paper companies took the initiative to have it reported for a disciplinary act to be rendered accordingly.
- (II) The newly amended MLCA has the offenses in Article 41, Article 42, and Article 43, Paragraph 1 and Paragraph 2 of the Tax Collection Act included in the scope of specified unlawful activity. FIs should pay more attention to the abnormal transactions suspected of tax evasion in the future.

Illustration of Tax Evasion



IV. Illegal Fund-raising

A. Case Overview

(I) Disclosure of STRs

The AMLD accepted a STR from Company D in April 2016: Chou arrived at Y Arcade several times to add cash value in hundreds of EasyCard or iPASS for an accumulated amount of several million, which seemed suspicious.

(II) Suspects

Mr. Tai, Mr. Wang, and Chou

(III) Method

A foreign Group M runs a business of virtual currency G (hereinafter referred to as “G coin”) on the platform of “M CLUB” website. Tai and Wang, as members of Group M, established Company E and Company D to recruit investors to become a member or an operator of the “M CLUB” website. Tai (foreigner) was in charge of the development of “M CLUB” website and downstream organization in Taiwan. Chou, the special assistant of Company G, assisted “M CLUB” website with contracting merchants and issuance of the “MeCard” and “MeCard Point” added-value, therefore investors may exchange it for physical items or services.

Investors paid in cash or by remittance to the account designated by Wang. The investment was completed after registering on the “M CLUB” website with the G coin electronic trading account setup. The website according to the investment package appropriated a certain amount of G coins to the investor’s account for the immediate use of the investor.

“M CLUB” website for ensuring the price of G coin to rise continuously and creating high return for investors’ doubled G coins after sale must continue to attract new investors. Investors who intended to redeem the investment amount would have to sell their G coins. Group M charged a service fee; also 5% the investment amount sold automatically converted to E-Credit. E-Credit could be applied to purchase the “MeCard” value of Company G. The amount in the electronic account

of the members could be transferred for exchanging psychical items, EasyCard, iPASS, gift certificates, and shopping electronic tickets or securities by deducting the “MeCard Point” from the online “MeCard Reader” of the merchants of Company D and Company G in order to attract investors to invest.

Tai, Wang, and Chou knew that their companies were not authorized by the competent authorities to operate a banking business; also, it was not supposed to collect money or funds from the majority or non-specific person by the means of borrowing money, accepting investment, making investor a shareholder or for any reason in exchange for unreasonable bonus, interest, dividend, or other remuneration. They had solicited a specific majority of people to invest in “M CLUB” by means of holding a briefing session or online advertising in the period from August 2012 to August 2016 with a total illegal fund over NT\$3 billion received.

Tai, Mr. Wang, and Chou for avoiding the inspection authorities’ investigating the flow of funds and for concealing and covering up the proceeds from a criminal act instructed Wang to have the illegal funds remitted to the financial account of others in the name of Company D, or to have the cash directly hidden at the premises of Company G. After a lawful search in August 2016, an amount over NT\$200 million was discovered at the premises of Company G and Company D. Financial accounts, real properties, and vehicles were seized in another criminal case.

B. Detecting

The cash deposit and withdrawal of the same account on the same business day amounted to a certain amount, respectively, and the transaction was not in line with the status and income of the customer; also, it was irrelevant to the nature of business. In addition, each deposit and withdrawal amount of the account was equivalent and in a short interval.

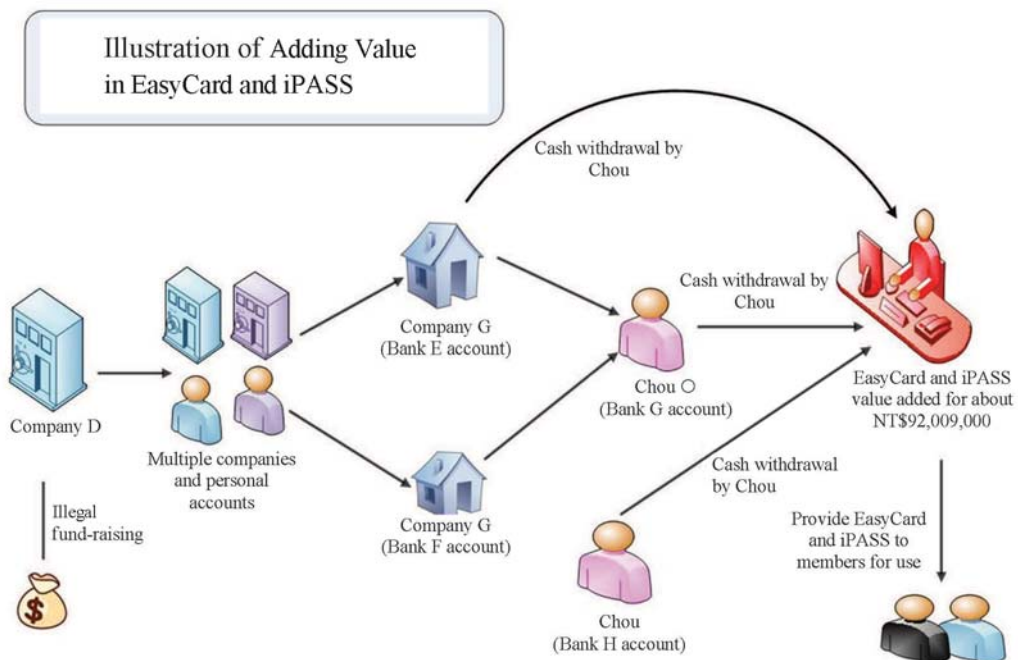
C. Indictment

The Taiwan Taichung District Court Prosecutor Office had Subject Tai and others prosecuted in November 2016 in accordance with the Banking

Act, Money Laundering Control Act, and Act Governing Issuance of Electronic Stored Value Cards.

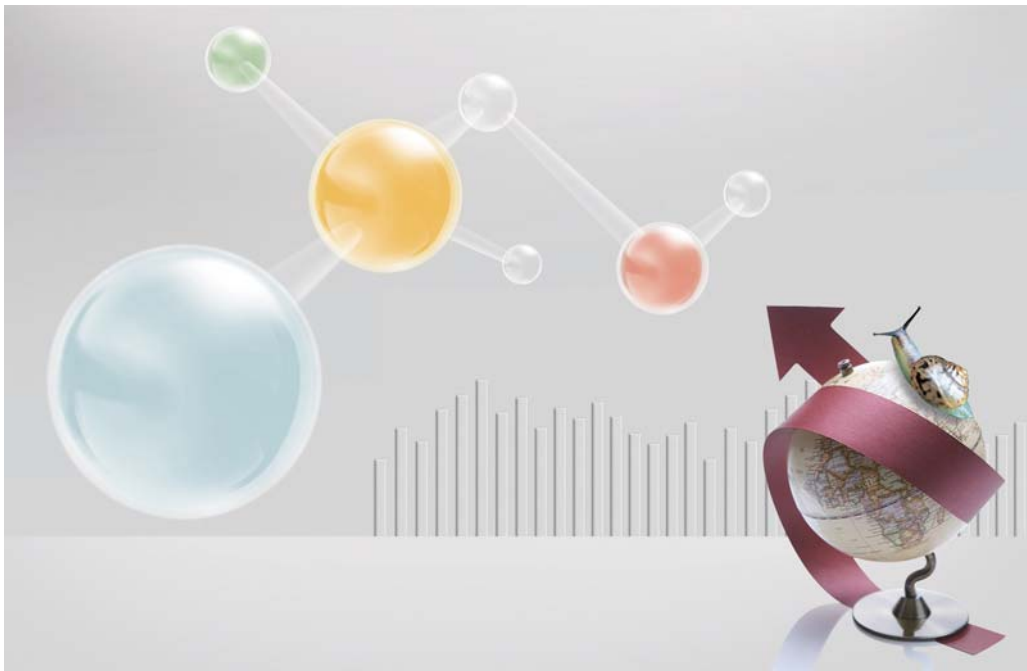
D. Experience sharing

- (I) Tai, Wang, and Chou continuously withdrawn large amount of cash for storing value in the EasyCard and iPASS. Such transaction mode (withdrawn large amount of cash) and fund use (stored large value) were not in line with the business operation and occupational background of the account holder and agent; therefore, the financial institutions reported such transactions suspected of money laundering.
- (II) Group M used the Internet platform to operate investment and redemption with a variety of incentives offered. Also, physical instruments, electronic tickets, and securities were provided as the subject of redemption to attract people to join. The investment structure was more complicate; however, the essence of such practice was no different from the traditional fund-raising with the guarantee of principal redemption and unreasonable high profits. Electronic tickets, electronic payment, and other virtual currency have become the new crime tools.



Part Four:

Project research



A New Strategy of Combating Crime: Perfecting the Financial Intelligence System against the Emerging Way of Money Laundering by Implementing Bitcoin

Wen-Chieh Su¹

Abstract

This study focuses on the empirical research of the trends concerning money laundering which is caused by “Bitcoin” that has been one of the innovative implements of Blockchain under the Fintech (Financial Technology) nowadays. Due to the reason that Bitcoin is not the fiat money in Taiwan, it has become one of the popular tools utilized for emerging financial or severe criminal crimes along with its characteristic features of anonymity, global-circulation, and low-processing fee. Bitcoin, as a crypto-currency with high potential risk of money laundering and terrorism financing, has already brought critical attention from governments and law enforcements internationally. Money Laundering Control Act,² conducting one of the specific laws countering significant economic crimes in Taiwan, lacks to include Bitcoin exchange platforms or companies into the designated “financial institutions” in its Article 5 which directly leads to the invalidation of Article 9 called “Currency Transaction Report (CTR)” and Article 10 called “Suspicious Transaction Report (STR)” that both work as gatekeepers to sniff impending economic crimes. Therefore, it is usually

¹ A special agent, MJIB Taipei City Field Office

² The relevant article referred to in this essay is from the amended “Money Laundering Control Act.”

too late for law enforcement to bring the criminals involving fraud, Ponzi scheme and money laundering, etc., to justice with the regulations such as offenses against the computer security of Criminal Code or The Banking Act, not to mention to trace the illegal proceeds and to return them to the victims. Facing the development of Bitcoin, we are never short of studies but systematic analysis in Taiwan, even the perspective of money laundering and Financial Intelligence Unit³ from the law enforcement which exactly this study endeavors to cut in. With the rough experience of manipulating Bitcoin commercially and personally, this study expects to make some suggestions through the systematic analysis in a way of empirical, international and integrate. The contribution of the study lies in, however, with the mentioned above, triggering our government to develop relative strategy or the law enforcement to perfect either the weapon against money laundering or the amending the criminal law dealing with virtual currency.

Keywords: Bitcoin, Anonymity, Blockchain, Money Laundering, Cybercrime

³ MJIB is the financial intelligence unit of Taiwan.

I. Background

The prevailing of “WanaCry” virus worldwide on May 12, 2017 had caused a severe “digital disaster” to more than 100 countries (including Taiwan) and regions. The offender requested the defender or the authorities to pay Bitcoin as ransom, otherwise the encrypted personal or sensitive data could not be restored. The government and law enforcement agencies of each country are all on high alert.

There was also Bitcoin related cases in Taiwan, such as, the kidnapping of Huang ○ Quin, a businessman in Hong Kong, that occurred in 2015, that shocked the people in Taiwan and Hong Kong. The kidnappers demanded to have ransom paid with Bitcoin that was a very un-traditional tactic. As Bitcoin is not the fiat money in Taiwan with the characteristic features of anonymity, paid ransom simply become untraceable. The kidnappers of Huang ○ Quin demanded a ransom of HK\$70 million to be paid in Bitcoin so that law enforcement officers could not track their virtual accounts or IP addresses. Another fraud with the use of Bitcoin took place in the second half of March 2016. A young couple who tricked nearly two thousand investors to invest in the high-earning Bitcoin in a short period of three weeks with an illegal gain more than NT\$50 million generated, that was indeed the first Bitcoin fund-raising crime committed in Taiwan.⁴ In early May of the same year, the Ministry of the Interior National Police Agency Criminal Investigation Bureau (hereinafter referred to as the “CIB”) Telecommunications Investigation Corps detected cross-strait Bitcoin money laundering center case. The syndicate adopted the entwined and complicated money-laundering operation to combine the e-bank USBKey⁵ and Bitcoin account for trade, through the

⁴ Junhao Chang and Peiju Pan, <Bitcoin fund-raising couple cheated NT\$50 million in 3 weeks,> “Apple Daily,” March 23, 2016, <<http://www.appledaily.com.tw/appledaily/article/headline/20160322/37121635/>>.

⁵ USBKey is a digital credential for the identification of customer identity on the network issued by commercial banks in Mainland China. Users when using Internet banking system must first confirm the customer’s identity through the USBKey encryption channel before initiating the network transactions.

pseudo-transformation of the Chinese identity card and dummy account money laundering, for a 5-layer money laundering, to protect the stolen money in the account from being frozen by the police and to have the funds successfully transferred and remitted to be withdrawn later by the withdrawer with the UnionPay card for an estimated transfer amount of NT\$50 million.⁶ In addition, around the world, many hackers steal millions of computer files, undermine the site or even threaten personal safety for obtaining Bitcoin as the ransom. The victims include general computer users, financial companies, and law enforcement agencies or departments. The victims were told to pay in Bitcoin and many ransoms were for an amount more than US\$20,000.⁷ The Bitcoin “Assassination Market” website had emerged in the United States. The former Federal Reserve Bank Chairman, Mr. Ben Bernanke, was blackmailed for more than 124 Bitcoins.⁸ Apparently, virtual currency is widely used in cybercrime or major crime with a severe threat imposed.

The uniqueness and novelty of virtual currency makes it difficult for regulators around the world to face and manage such payment instruments, and there are considerable differences in the policies adopted by countries. Some countries accept their commercial circulation while other countries have their use restricted harshly or completely. Mr. Huainan Peng, President of the Central Bank of Taiwan (hereinafter referred to as the “Central Bank”), on November 23, 2013, replied to the Legislative Yuan that the Bitcoin had no legal effect and could only be used for the transaction between the issuer and the members. The game points issued by the game developers are similar to the initial application of Bitcoin. For Bitcoin transactions, the Central Bank

⁶ Jianbang Liu, “Fraudulent Group’s New Tactics for Money Laundering and Redemption of Bitcoin,” “Central News Agency,” May 10, 2016, <<http://www.cna.com.tw/news/asoc/201605040264-1.aspx>>.

⁷ Translated by Lijing Wang, “Bitcoin Ransom is Preferred” <Udn e-News>, May 21, 2016, <http://paper.udn.com/udnpaper/PID0031/283392/web/#3L-6249299L>>

⁸ “‘Assassination market’: Bernanke tops ‘kill-list’ in crowd-sourced Bitcoin fundraiser for wannabe hitmen,” *RT News*, 24 May 2016, <www.rt.com/news/bitcoin-assassination-market-anarchist-983/>.

will have it regarded as precious metals transactions for management.⁹ Mr. Huainan Peng replied to the Legislative Yuan again on November 27 of the year that the currency issued by the Central Bank was the main transaction tool in Taiwan in accordance with the Money Laundering Control Act.¹⁰

The implementation of money laundering control in Taiwan in the past mainly relied on the transaction data provided by the financial institutions for tracing the flow of funds after a major crime had been committed in order to clarify the money laundering crime, which could only be considered as “counteracting or discovering the completed or undergoing major crime with the money laundering control” that did not reach the level of crime prevention.¹¹ In recent years, the number of Suspicious Transaction Reports (“STR”) and the quality of unfolding crimes have been increasing year by year through law enforcement agencies’ providing education and training and propaganda at the financial institution’s premise on a regular basis. However, the virtual currency (Bitcoin) is excluded from the money-laundering control norms of the financial institutions. How to achieve the same effect of money-laundering control effect, function, and purpose at the “outside the enclave” as the financial institutions? The importance of regulating the Bitcoin industry and the trade platform goes without saying; also, it is the focus and trend of the financial supervision and law implementation in Europe and the United States. This paper is prepared starting from the virtual currency – Bitcoin background analysis, discussing and summarizing several major events and derived issues, compiling the responsive strategies of major countries, analyzing the development and impact of Bitcoin in Taiwan, and proposing conclusions and recommendations. The paper, through a systematic analysis, is intended as a reference to the law enforcement agencies of Taiwan in response to the research and control of criminal trends, such as Bitcoin money laundering.

⁹ Yizhu Tsai, “Bitcoin Money Laundering - Huainan Peng: Central Bank Pay Close Attention,” “ETtoday News Cloud,” January 24, 2016, <<http://www.ettoday.net/news/20131120/298323.htm>>.

¹⁰ Kuancheng Lu, “Emerging Bitcoin – Huainan Peng: Bubble,” “Liberty Times,” January 24, 2016, <<http://news.ltn.com.tw/news/business/paper/734193>>.

¹¹ Zhijie Lin, “New Thinking on Anti-Money Laundering - On Financial Money Laundering Control, Financial Supervision and Investigation Authority” and “New Viewpoint of Prosecution,” Issue 3, January 2008, Page 271.

II. Money Laundering Control of Taiwan

(I) Operation of Financial Intelligence Unit

MJIB had the “Money Laundering Prevention Center” established in accordance with the “Directions for the Establishment of MJIB Money Laundering Center” approved by the Executive Yuan on April 23, 1997 to implement the FIU and the anti-money laundering related businesses. In addition, pursuant to Subparagraph 7, Article 2 of the Organic Act of MJIB passed by the Legislative Yuan on November 30 in the same year and put into practice on December 19 in the same year upon presidential decree, MJIB is in charge of “ML prevention related matters.” Pursuant to Article 3 of the same Act, the AMLD was established by MJIB. Article 7, Article 8, and Article 10 of the Money Laundering Control Act were amended in 1999 to clarify that MJIB should accept the declaration and notification of the Act.

In addition, pursuant to Article 9 of the “Regulations for Department Affairs of Investigation Bureau, Ministry of Justice” amended on October 17, 2008, Anti-Money Laundering Division are in charge of the following matters: Researching AML strategies and providing consultation in the formulation of relevant regulations; Receiving, analyzing, and processing STRs filed by FIs; Receiving and maintaining currency transaction reports (CTRs) filed by FIs and receiving and processing cross-border transportation of cash and bearer negotiable instruments reports (ICTRs) forwarded by the customs; Assisting other domestic law enforcement partner agencies in matching the AMLD database for investigating ML cases and coordinating/contacting with respect to ML prevention operation; Liaison, planning, coordination and implementation of information exchange, personnel training and cooperation in investigating ML cases with foreign counterparts; Compilation and publication of Annual Report on AML work and the management of relevant data and information; and Other AML related matters.

(II) Latest revision of the “Money Laundering Control Act”

In order to improve the money laundering control system and come

in line with international norms, the Taiwan government has promoted the amendment of the “Money Laundering Control Act” since 2013. However, a punitive fine imposed on Mega Bank New York Branch in the United States in August 2016, once again caused people to pay great attention to money laundering and indirectly accelerate the amendment of the Money Laundering Control Act. The amendment to the “Money Laundering Control Act” was finally passed by the Legislative Yuan on December 9, 2016, promulgated on December 28 of the same year, and formally implemented on June 28, 2017. Such amendment is expected to activate and substantiate the money laundering control task of Taiwan in order to enhance the overall financial activities and credit rating.

The latest amendment to the Act is in response to international efforts in money laundering control, link to the international standards, strengthen the judicial practice to combat cross-border telecommunications fraud and human money laundering related law amendment, improve Taiwan’s money laundering defense line, and demonstrate Taiwan government’s determination in combating economic crime and money laundering. The focus of the law amendment includes:

1. The essential criteria of money laundering crimes are in line with international norms. After the amendments made to the Act, the money laundering of a dummy company or real property in the name of the dummy account or figure head are deemed as moneylaundering crimes.
2. The current threshold of major crimes is changed from a penal servitude for a definite period of more than five years to a penal servitude for a definite period of more than six months. In addition, the specific scope of crime for money laundering is relaxed; also, the threshold of crime income is deleted.
3. The establishment of a transparent financial flow, a comprehensive customer review, transaction record preservation, and reporting obligations, of which, customer review obligations must be risk-based; also, reviewing the “politically exposed persons (PEPs)”, including

clients, beneficiaries, their family members or closely related persons and the real beneficiaries, and including the financing leases and designated non-financial business and profession, including lawyers, CPAs, notaries, land administration agent and the real estate business, trust and corporate services, etc., at the same time, the competent authorities are authorized to perform an audit and for the performance of an audit, a provision is added to allow the central authority authorizing the local or other relevant authorities to act.

4. In terms of border financial flow control, the New Taiwan Dollar, gold, and other items that could be used for money laundering are included for supervision; also, the reporting obligations for freight and courier service access to the border are added to strengthen the financial flow track preservation and monitoring.

III. Introduction of Bitcoin

(I) Principle and operation of Bitcoin

Bitcoin is a new electronic encryption virtual currency (Crypto-currency) that was proposed by an individual under the pseudonym of “Zhong Ben Chong.” The Bitcoin issuance, transaction, and account management operating system was developed from the “peer-to-peer (P2P)”¹² and decentralized database platform; also, there were 50 Bitcoins created. Bitcoin is not issued by any agency, bank, or government; also, it is known as “peer-to-peer e-cash.” It was created by peers by the way of “Mining” with value added.¹³ As Bitcoin is with the characteristic features of anonymity and does not need going through a bank transaction, that is, without an intermediary, it retains the infrastructure so that strangers can trade with each other without the possibility of tracking the flow of money.¹⁴

Bitcoin was first introduced in 2009 when the financial crisis at the worst. The central bank of each country had printed a large number of banknotes to save the economy, resulting in global capital flood and the deflation of USD; therefore, Bitcoin became a safe haven for investors and wealthy. By the end of 2013, the exchange rate of Bitcoin to the USD was at the peak, that was, 1 Bitcoin for US\$1,150 (about NT\$33,675.16). In 2014, governments imposed trading restrictions on the Bitcoin. At the beginning of 2015, the value of Bitcoin fell dramatically and 1 Bitcoin was for less than US\$200 (about NT\$6,000); however, the value of Bitcoin went back up to US\$290 (about NT\$9,000) in October of the year. Currently, 1 Bitcoin can be exchanged for US\$2,045.58 (about NT\$61,426.88).¹⁵ According to the existing computer

¹² The “Peer-to-peer (P2P);” also known as point-to-point technology, is without a center server and it relies on the user group (peers) for the exchange of information on the Internet system. It is to reduce the previous network transmissions in order to reduce the risk of data loss.

¹³ United States Government Accountability Office, “Virtual Economies and Currencies” , May 2013, p.7.

¹⁴ Paul Vigna and Michael J. Casey, "Virtual Currency Revolution," Big Publishing Company, Taipei (2016), Page 12.

¹⁵ <Fig>, "MaiCoin," at 12:53 on May 21, 2017, <<https://www.maico.in.com/zh-TW/charts>.

data structure, the unit of Bitcoin can be divided into the 8th decimal point,¹⁶ if necessary, it can split further.¹⁷ One of the biggest differences between the virtual currency (including Bitcoin) and the legal currency is that there is no national or any institution guarantees provided; also, its value depends entirely on the market demand, which is susceptible to speculation in the capitalism market that is full of speculative atmosphere and may cause severe fluctuation in price in a short period of time.¹⁸

At the beginning of 2015, Coinbase¹⁹ became the first company in the United States to legally operate the Bitcoin trading service, which meant that Bitcoin could be traded legitimately according to the US regulations. The first Bitcoin ATM²⁰ in the world was officially introduced for service in Vancouver, Canada, on October 29, 2013. The Bitcoin holders can have Bitcoin exchanged for legal currency easily. But in terms of proportion, most countries have not yet recognized Bitcoin as a legal currency and there is no relevant norm available. As for Taiwan, BitoEx, a Bitcoin trading platform, worked with the convenience store, FamilyMart, in October 2015 to allow people to buy Bitcoin at FamilyMart.²¹ According to statistics, there are about 50,000 people using Bitcoin in Taiwan.²² At present, the Central Bank has not banned such transactions and it considers that the “barter” transaction

¹⁶ The minimum unit of the Bitcoin is 0.00000001 Bitcoin, called 1 "satoshi." In addition, please refer to "The minimum unit of the Bitcoin?" "BitoEX," March 17, 2016, <<https://www.bitoex.com/help/1?locale=zh-tw#2>>.

¹⁷ Xingfang Yan, "King of the currency - Bitcoin," Dao-Tien Publishing Company, Taipei (2014), Page 106.

¹⁸ Rongjin Guo, "Legal Disputes on Internet Virtual Currency," "Analysis of Technological and Law," Tome 26, Vol. 10, October 2014, Page 23 - 31.

¹⁹ The Bitcoin trade and exchange company was established on June 20, 2012 in the United States, California.

²⁰ Charlie McCombie, "The 7 Uses of Bitcoin and the Best Way To Buy It," THE COINTELEGRAPH, 21 March 2016. Also see <http://cointelegraph.com/news/the-7-uses-of-bitcoin-and-the-best-way-to-buy-it>.

²¹ It cannot "directly" use Bitcoin to purchase goods at the convenience stores. Consumers will need to convert the Bitcoin in the Bitcoin Wallet converted to NT\$100 or NT\$200 cash coupon in order to shop at the convenience stores.

²² Mengxiu Tsai, Lide Wang, and Peijun Liao, "The world's first use of Bitcoin in Convenience Stores," "Apple Daily," March 26, 2016, <<http://www.appledaily.com.tw/appledaily/article/headline/20151118/36905617/>>.

of FamilyMart is without any concern of breaching law; however, a close observation will be implemented. In addition, the Central Bank indicated that such Bitcoin was not currency and it was not necessary to have it under control, but people needed to bear the risk. A fraudulent Bitcoin transaction violates the “Consumer Protection Act,” which should be handled by the Consumer Protection Foundation and the prosecution unit. A Bitcoin related money laundering violates the “Money Laundering Control Act,” which should be handled by the Financial Supervisory Commission (hereinafter referred to as the “FSC”) and the prosecution unit. The FSC indicates that banks may not trade and exchange Bitcoin currently and emphasizes that Bitcoin is not a legitimate payment tool in Taiwan.²³

(II) Bitcoin transaction type and payment mode

Bitcoin was originally obtained from mining. The system will have the “dug out” new Bitcoin distributed to the miners for them to have it recorded and attached to the Blockchain; also, the miners will receive a little more Bitcoin as a reward. According to the current mining speed, the system will reward “miners” 6 times in one hour with 25 Bitcoins given. Another way to obtain Bitcoin is to purchase it through the trading platform; on the contrary, the Bitcoin can be sold through the trading platform with the exchanged real currency deposited in the bank account.²⁴

From the viewpoint of the user regarding Bitcoin transaction, the user first has to install a Bitcoin Wallet on the computer and a Bitcoin Address and Private Key will be generated automatically that is similar to the password related to an email account. A Bitcoin transaction is concluded by having the payer directly paid the payee through the electronic device according to the recipient’ s address. The transaction data is transferred to a “Block.” The transaction that is confirmed preliminarily will be linked to the previous block

²³ Chris, "Financial Supervisory Commission, Mingzong Zeng: "Bitcoin is an illegal payment instrument in Taiwan," "INSIDE," April 9, 2016, <<http://www.inside.com.tw/2015/11/03/bitcoins>>.

²⁴ R. Joseph Cook, "Bitcoin: Technological Innovation or Emerging Threat?" 30 J. INFO. TECH. & PRIVACY L. 535, 539, 2014.

to get more confirmation. General transaction will be confirmed in six blocks in order to have the transaction risk controlled comprehensively.

(III) Legal Qualitative and Norm Vulnerability of Bitcoin

The history of quasi-money in the United States makes the legal status of most of the virtual currency in a state of un-identification.²⁵ American scholars talk about virtual currency as a “outside the enclave of federal law, state law, decrees, and regulations.” It seems that no one wants to solve the core legal issue of the virtual currency.²⁶ However, from the perspective of emerging science and technology issues, there are many uses of Bitcoin in Europe and the United States, making European and American government face up to the special problems arising from Biocoin. There is currently no major money-laundering crime arising from the use of virtual currency. However, there is doubt whether the current law of Taiwan is sufficient to deal with such situation when there is money laundering crime committed with the use of Bitcoin or other existing virtual currency. First of all, is Bitcoin or a virtual currency a “currency” as defined in Article 9 of the “Money Laundering Control Act?”

From the viewpoint of comparative law, the use of Bitcoin for money laundering is by using the illegal income (such as drug trafficking, fraud, etc.) to buy Bitcoins and then sell them to obtain the real money. Bitcoin is with the characteristic features of anonymity and hard to track; therefore, the use of such a pipeline will make money laundering difficult to detect. The United States District Court of Texas had made a ruling to directly recognize Bitcoin a currency in an electronic form, but Bitcoin could only be circulated in a place where its monetary nature was recognized. The German Ministry of Finance recognizes that Bitcoin can be used as a legitimate bookkeeping

²⁵ Edward Castronova, "Virtual Currency Economics," Yeh-Ren Culture Co., Ltd., Taipei (2015), Page 136.

²⁶ Sheppard Mullin, Making Sense of Virtual Dollars, Law of the Level (November 22, 2011); also see <http://www.lawofthelevel.com/2011/11/articles/virtual-currency/making-sense-of-virtual-dollars/>.

unit; also, it is also necessary to pay taxes on the use of Bitcoin.²⁷ Singapore is the first country in Asia to regulate the taxation of Bitcoin and recognizes the legal status of Bitcoin with the hope of attracting foreign investors to come.

Bitcoin is a virtual currency generated from peer-to-peer Internet technology and Principle of cryptography. Any person holding an electronic device can acquire and use it in a certain way or consideration. Although there are countries (such as, Germany) recognizing Bitcoin a legal currency with the need to pay income tax, according to the law of Taiwan, it is difficult to recognize Bitcoin with a monetary status. According to the current practice and recognition in Taiwan, the quantitative feature of virtual currency and treasure generated from Internet games are attributed to the electromagnetic record in Article 358 and Article 359 of the “Criminal Law” rather than a currency.²⁸ If a player obtains the visual currency or treasure of other players in the game by an inappropriate act (such as: malicious program), the offense will be prosecuted for an obstruction of computer act in accordance with Article 358 of the “Criminal Law” rather than a property crime in a fraud. Thus, there is room for discussion about the nature of Bitcoin or virtual currency.

In addition, the relevant laws and regulations of Taiwan are found with the following loopholes:

1. The domestic Bitcoin trading platform is not included in the financial institutions defined in Article 5 of the “Money Laundering Control Act;” therefore, it is not responsible for reporting to the CTRs public sector (MJIB). If the daily transaction of Bitcoin exceeds NT\$500,000, its status is essentially equivalent to the CTRs processed by the financial institutions, which need to declare while the former does not have to that is with the risk of money-laundering.

²⁷ Wenjia Wang, "Germany the first country recognizes the legality of Bitcoin," "cnYES," August 22, 2013, <<http://news.cnyes.com/Content/20130822/KH9PTM9P5DPY6.shtml>>.

²⁸ Please refer to the Supreme Court 2014, Tai.Sun.Tzi No. 3093 Verdict, High Court 2015 Sun.Yi.Tzi No. 1233 Verdict, Taoyuan District Court 2011 Shen.Sue.Tzi No. 1361 Verdict, and Taipei District Court 2009 Sue.Tzi No. 1000 Verdict.

2. If the Bitcoin is tied up to a credit card that is mainly with Bitcoin and other virtual currency paid and if the credit card issuing company is not in Taiwan,²⁹ it is not subject to the regulations of “credit card company” in Article 5 of the “Money Laundering Control Act.” If a criminal uses a credit card to purchase in foreign countries, the domestic regulatory authorities have no jurisdiction to investigate and review the consumption statements of the foreign credit card issuing banks.
3. According to the “Foreign Exchange Regulation Act” and “Regulations Governing Foreign Exchange Business of Banking Enterprises” of Taiwan, the inward and outward remittance of foreign exchange is subject to the restrictions of the aforementioned law. If an individual has NTD traded for Bitcoin through the Bitcoin trading platform and then has Bitcoin exchanged for foreign currency and deposited into foreign banks, such individual only needs to bear the low transaction fee of the trading platform and can obtain the equivalent value of foreign currency promptly and not subject to the relevant laws and regulations of Taiwan. From the technical point of view, the domestic industry has developed technologies to track the source of Bitcoin; therefore, Bitcoin transfer is not difficult to track; however, if it involves the issue of international jurisdiction, due to Taiwan’s international status and diplomatic difficulties, it is not easy to request an overseas investigation.³⁰

Furthermore, the prevailing WanaCry virus incidents worldwide highlight the threat of cybercrime or gross crimes with the use of Bitcoin and other virtual currencies. In regard of the difference between the nature of Bitcoin and the so-called “currency” (or “fiat money”), the nature of Bitcoin

²⁹ Currently, there are European companies, such as, WAVE CREST HOLDINGS LIMITED (UK), issued Bitcoin credit card, please refer to <http://jeremy5189.logdown.com/posts/427553-bitcoin-visa-debit-card>.

³⁰ James R. Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering: a handbook for law enforcement officers, auditors, and financial investigators*, p.70, CRC PRESS (1999).

payment, whether applicable to the seizure of general illegal income, and many other controversies, the seizure method and the amount determination of the investigation procedures in this report are as follows:

1. Seizure method: Bitcoin is a crypto-currency and a decentralized (i.e., no issuer) virtual currency that is different from the traditional currency that can be seized physically. However, under the precondition of controlling financial flow (that is, Bitcoin remains in Taiwan and used on the domestic network transactions or stored in the mobile virtual wallet); it could be seized in accordance with the existing digital evidence seizure method. In terms of the seizure procedure, the United States Federal Bureau of Investigation (FBI) had seized the illegal Bitcoin of the suspected individuals or organizations in accordance with the existing digital seizure procedures. In addition, it is also applicable to the auction procedures.
2. Amount determination: The United States has replaced Japan as the world's largest Bitcoin market.³¹ The federal court in the United States had the relevant judgments rendered on Bitcoin. In terms of amount determination method, the United States has adopted the current buying/selling price of international virtual currency transactions and foreign exchange market. The collecting (levying) price determination is same as the recognition timing of stock and other marketable securities.

³¹ Joseph Young, "How US Briefly Overtook Japan and Became Largest Bitcoin Exchange Market," THE COINTELEGRAPH, 18 May 2017, <<https://cointelegraph.com/news/how-us-briefly-overtook-japan-and-became-largest-bitcoin-exchange-market>>.

IV. Potential risk of virtual currency in money laundering and terrorism financing

After the Financial Crisis in 2007-2008, the virtual currency, virtual currency, such as Bitcoin, has emerged. It is important to understand the definition of virtual currency and how it is operated. Then, the government officials, law enforcement agencies, and the private sector will be able to analyze whether the virtual currency can be used as a new payment instrument and whether it has the risk of money laundering and terrorism financing. FATF also pointed out that the development of virtual currency is advancing with the times, as long as it is in circulation, regulators, law enforcement officers, and government departments need to face the incoming challenges.³² Virtual currency is a complex issue that involves not only the issue of money laundering prevention and countering terrorism financing, but also other regulatory issues, including consumer protection, social security, national taxation³³, sound regulatory systems, and network technology (IT) security. The National Crime Agency (UK) reported in June (2015) that although virtual currency was not commonly used in the criminal community, but with the community gradually accepted virtual currency as part of the payment tool, law enforcement agencies could expect virtual currency to be used increasingly by traditional criminals for money laundering or for the purchase of illegal goods and services.³⁴

Legitimate use of virtual currency has its positive significance, such as improving the efficiency of payment, reducing transaction, and increasing the convenience of international transactions; however, it may also help those

³² Financial Action Task Force, "Virtual Currencies- Key Definitions and Potential AML/ CFT Risks," June 2014, p.4.

³³ 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>.

³⁴ National Crime Agency, "National Strategic Assessment of Serious and Organized Crime 2015," June 2015, p.22.

who cannot get the legitimate bank pay service with an alternative payment tool. However, the key role of virtual currency may also involve money laundering, that is, the transfer of unlawful interests to legitimate assets of legitimate business, which has attracted the attention and concern of relevant scholars and countries. The United States enacted the first set of regulations in 2013.³⁵

Virtual currency with the feature characteristics of anonymity, liquidity, and real-time trading, coupled with its global influence, the current potential risks of money laundering and terrorism financing are as follows:³⁶

1. The transaction with high anonymity;
2. Customers cannot effectively identify and perform identity verification.
3. Funds can be traded anonymously (through a virtual trading platform that cannot confirm the source of funds to accept cash or third-party funding). If the transferee and the payee are not properly identified, an anonymous transfer will be arranged successfully. The virtual currency system can be accessed through the network (including embedded software in smartphones) and can be used for cross-border payments and fund transfer.
4. In the regulation of anti-money laundering and countering terrorism financing, a number of national regulators and law enforcement agencies are involved without the responsibility defined clearly.
5. Lack of a global central regulatory body.

The blockchain technology is the foundation of Bitcoin. The blockchain is an open and transparent transaction record method without a central management system available. Each endpoint of the blockchain can store transaction datas. After combining the data in each endpoint, a complete transaction record with a clear time is created. Since the data is shared in

³⁵ Clare Chambers-Jones, "Virtual Economies and Financial Crime: Money Laundering in Cyberspace," Cheltenham, U.K.: Elgar, 2012; Jeffrey Sparshott, "Web Money Gets Laundering Rule," Wall Street Journal, 21 March 2013. Also see <http://online.wsj.com/article/SB1000142412788732437320457834611351125202.html>.

³⁶ Financial Action Task Force, "Guidance for a Risk-Based Approach Virtual Currencies," June 2015, No. 13, pp.31-32.

thousands of endpoints, any incomplete data can be detected early and not written in the endpoints. One of the significant advantages is the “data irreversibility,” that is, the operator of any endpoint who intends to forge data will not be able to have data recorded without the confirmation of other endpoints. The traditional centralized management system, no matter how strictly protected, could be hacked. The blockchain makes the accounting book no longer needed and hackers have no place to start. Criminals can change one or two data, but cannot change the data in all endpoints. According to the history of Bitcoin, this technology can really prevent a hacker’s attack. However, from the viewpoint of crime detection, the Bitcoin encryption technology and anonymity, criminals may thrive. Since funds are not stored in a certain address, the account will not be directly attached or frozen by law enforcement agencies. It is much more complicated to check a transaction record on a blockchain than the traditional practice of preventing a subpoena to the financial institutions for supervision.³⁷

In addition, the European Police Office (EU Law Enforcement Agency) issued the “2015 Internet Organised Crime Threat Assessment Report” (IOCTA)³⁸ on September 30, 2015, which stated its viewpoint on the biggest cybercrime threats faced by the EU. The report highlights the issue of Bitcoin and virtual currency in a series of criminal situations, including the status of illegal financing and specific parts of the technology involved in the illegal activities. According to statistics, in the online payment between criminals, Bitcoin pay is accounted for up to 40% while PayPal³⁹ is only 25%.⁴⁰ As previously stated by this institution, these data indicated that virtual currency is an important trend in the development of the “criminal activity service”

³⁷ Marc Goodman, "Future Crime," Trojan Culture Publishing Company, Taipei (2016), Page 283.

³⁸ The European Police Office, "The 2015 Internet Organized Crime Threat Assessment," Europol, 30 Sep. 2015, <<https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015>>.

³⁹ PayPal is the world's largest online financial flow system and it is the subsidiary of ebay currently.

⁴⁰ Same as Note 39, Page 63.

ecosystem. The report also pointed out: “Although there is no common currency between cybercriminals throughout the EU, Bitcoin will gradually take on this role, which has a common payment mechanism that will make it available for all payment situations, and this trend will only intensify.”⁴¹

⁴¹ Same as Note 39, Page 63 ; "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."

V. Impact and Practice of Virtual Currency Circulation on Current Financial Intelligence Network

(I) International cases

1. Liberty Reserve hacked

Internet payment service provider “Liberty Reserve” is a website set up in Costa Rica, claiming to use: “the oldest, safest, and most popular payment process to serve as many as millions of users worldwide.” In 2011, “Liberty Reserve” was involved in the sales of thousands of stolen Australian bank accounts and American bank debit cards. In 2012, a group of hackers tried to blackmail Symantec, an anti-virus software company, and intended to ask for a transfer of US\$50,000 to “Liberty Reserve” account. Because “Liberty Reserve” did not require its users to provide any form of identity documents while opening an account on the website and deliberately ignored the possible criminal activities. The US federal prosecutors had the website closed in May 2013 due to its loose website security management and unable to detect most criminal activities. The website had more than 1 million users at the time.

2. “SILK ROAD” money laundering case

“Silk Road” is an online trading platform where users can use Bitcoin to trade drugs, illegal guns, and credit card data anonymously; also, to provide illegal services of pornography and hackers on the website with 8-15% service fee charged for each transaction and great profits accumulated. The site also uses a technology called “The Onion Route” (Tor)⁴² to make tracking more

⁴² Tor is used to prevent widespread traffic filtering and sniffing analysis on the Internet. Tor (The Onion Router) is communicating on the overlay network for anonymous external connections and anonymous hiding services. Tor was software developed by the American Navy Research Laboratory staff, Paul Syverson, and the computer scientists, G. Mike Reed and David Goldschlag, in the mid-1990s to protect American intelligence communications.

difficult. On October 2, 2013, the Federal Bureau of Investigation claimed that Ross William Ulbricht, the head of the “Silk Road” and known as “Dread Pirate Roberts” had been arrested in San Francisco. The federal government confiscated the illegal gains of 144,000 Bitcoins (also, a report indicated that Ross William Ulbricht had 600,000 Bitcoins with the remaining 489,000 Bitcoins missing) that was equivalent to US\$133 million. The website was closed by the US government, but an alternative website had appeared soon later. The day the website was closed; the Bitcoin price fell by 15%, but was recovered the next day.

In another case, the New York police had Charlie Shrem, age 24, the chief executive of BitInstant trading station and Robert M. Faiella, age 52, the agent of Bitcoin arrested on January 28, 2014. Robert was also a user of “Silk Road.” The two suspects planned to sell more than US\$1 Bitcoins to “Silk Road.”⁴³ Charlie Shrem helped Robert M. Faiella have cash converted to Bitcoin. Robert had operated underground Bitcoin transaction on “Silk Road” by the code of “BTCKing.” Charlie Shrem was prosecuted by Federal New York Southern District prosecutor office with a penal servitude for a definite period of two years⁴⁴ due to “facilitating unlicensed money transmission;” also, the case was closed with a plea.⁴⁵ In addition to money laundering, Charlie Shrem was also accused of concealing the suspicious trades of Robert M. Faiella and it was considered by the US Department of Justice a violation against the Bank Secrecy Act. It was reported that Charlie Shrem himself also purchased marijuana and other illegal drugs through the “Silk Road.” James J. Hunt, investigator of the Drug Enforcement Administration (hereinafter referred to as “DEA”) who was in charge of

⁴³ Matthew Kien-Meng Ly, "Coining Bitcoin's "legal-bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies," 27 HARV. J.L. & TECH. 587, 594, 608, 2014, p.603.

⁴⁴ U.S. v. Faiella, United States District Court, S.D. New York, No. 14-cr-243 (JSR), 19 Aug. 2014, 39 F.Supp.3d 544.

⁴⁵ Carlo Caraluzzo, "Charges Reduced: Charlie Shrem Agrees to Plea Deal," THE COINTELEGRAPH, 21 March 2016, < <http://cointelegraph.com/news/charges-reduced-charlie-shrem-agrees-to-plea-deal>>.

this case said: “The accusation issued today forces the law enforcement officers to trace suspects who sell illicit drugs all over the world. The two suspects are accused of deliberately selling drugs anonymously for significant illegal gains.” Currently, the operation of the Bitcoin trading station is ceased.

3. Bitcoins and anonymous Internet crime

The anonymous network is easy to operate, hard to track, cannot be monitored, anonymous use without any data retained on the user side; therefore, it could be misused by users, criminals, and hackers. Beginning in the second half of 2013, the use of Tor network features with third-party payment (Bitcoin) had gradually become a new type of computer kidnapping and other attacks mainstream. The well-known network security company “Trend Micro Technology Co., Ltd.” had malicious software “Mevade” disclosed on that August 19, 2013 and had the Tor components downloaded voluntarily to back up the connection with the “Command and Control Server (C&C server)” server. The user infected with malicious programs will contact the C&C server and hackers will control the hacked computer through the C&C.⁴⁶ On October 27, 2013, the Dutch police arrested four behind-the-scenes hackers who used the malicious program “TorRAT” to steal a Dutch user’s bank account, which connected to the C&C server through Tor and used alternative cryptographic services to avoid tracking and detection. At the end of 2013, if the “Cryptorbit” virus that was mutated from the encrypted virus “Ransomware” had attacked successfully, the user file would be encrypted and the victim to use would be requested to pay ransom at a specific page of the Tor browser before the encrypted file could be decrypted.⁴⁷ On May 26, 2014, McAfee, an internationally renowned company, found a site called Tox on an anonymous network that allowed users to log in and created

⁴⁶ G Data: Tor effectively blocks new zombie virus attacks>, "GDATA," October 1, 2012, <http://www.gdata.tw/index.php?option=com_content&view=article&id=385:2012-10-01&catid=44:2011-05-24-08-44-40&Itemid=157>.

⁴⁷ TREND LABS "Trend Micro Technology Co., Ltd." Global Technical Support and R&D Center, <Defeat Malware with Tor (The Onion Router) Anonymous Service (I),> <"Trend Micro Technology Co., Ltd." / Network Security Trends Blog," March 7, 2014, <http://blog.trendmicro.com.tw/?p=7255>>.

their own encrypted virus in three steps, allowing users to demand ransom from the victim through Bitcoin and Tor network. The Tox website charged only 30% of the ransom collected by the encrypted virus generator.⁴⁸

In order to avoid theft or eavesdropping in the process of data transmission, many anonymous networks like Tor networks are gradually being taken seriously. Many illegal websites or groups are also booming with such networks, such as, the aforementioned “Silk Road” money laundering case, which provides not only the sale of illegal drugs but also criminal transactions, such as, hitman contract and human trafficking. Also, third party payment technology, such as Bitcoin, is an online payment method that has been widely regarded by the world in recent years. This new (Bitcoin) and old (online payment) technology, through the C&C server and encrypted virus, successfully combined into a new type of crime and obtained crime proceeds. The judicial units cannot use the traditional communications surveillance method to obtain the C&C server in the Tor network and the actual address of the payment site; also, cannot find the true identity of the hacker through the traditional bank account to track the payment of the Bitcoin.

(II) Domestic cases

There is no Bitcoin related money laundering case in Taiwan, but Bitcoin related crime cases do catch the attention of the public. For example, the kidnapping of Huang ○ Quin, a businessman in Hong Kong, occurred in 2015 that shocked the people in Taiwan and Hong Kong. The kidnappers demanded to have a ransom paid in Bitcoin that was a very un-traditional tactic. The Taipei District Court had one case ruled in 2013 involving the suspects log-on Internet anonymously to download Tor browser software and log on to the Mt.Gox Bitcoin trading website to have an account opened with a considerable amount of US dollars remitted into such account and then log on to the “Silk

⁴⁸ Pierluigi Paganini, "McAfee discovered in the Deep Web a ransomware-construction kits that allow easy to build malware in just 3 steps, implementing an interesting model of sale," Security Affairs, 26 May 2015, < <http://securityaffairs.co/wordpress/37180/cyber-crime/tox-ransomware-builder.html>>.

Road” website to purchase Class II drugs and marijuana from Mexico and Italy with Bitcoin paid and then shipped back to the designated locations in Taiwan, which was in violation of the “Narcotics Hazard Prevention Act” (Taipei District Court 2013 Sue.Tzi No. 222 and No. 644 Ruling).

According to the law source retrieving system of Taiwan, there are not many money laundering cases being prosecuted; moreover, the prosecuted cases involving the use of virtual currency for money laundering is even lesser, in fact, there are also not many foreign cases available for query. However, input the keyword “virtual currency or Bitcoin” for the verdicts delivered by Taipei District Court in the law source retrieving system of the Judicial Yuan – there were 34 verdicts of 28 cases in 2002 to 2014, of which, 22 cases involved fraud, Banking Act, Infringement of Computer Usage, and “Narcotics Hazard Prevention Act”; also; the Supreme Court was with only one case involving virtual currency and drugs (2011 Tai.Sun.Tzi No. 4649 Ruling).

1. “Bitcoin” fund-raising crime - Krypto Bitcoin Mining Group offense

Krypto Bitcoin Mining Group in Hong Kong claimed to be able to invest in virtual currency “Bitcoin” was searched by the Hong Kong Police in 2014; however, its branch has continued to operate the scheme in Taiwan. Criminal Investigation Bureau Investigation Division III (hereinafter referred to the “Investigation Brigade III”) detected the couple Mr. Lu and Ms. Chen who led the illegal group in Taiwan and had arrested them with passbook, branded purses, and accounting books confiscated. Police said that the group had had at least 19 victims with one of the victims cheated for an amount of NT\$14 million and for a grand more than NT\$100 million.

The Criminal Investigation Bureau Investigation Division III had received several reports filed by victims in March 2015. The victims said that they were tempted and induced to setup a Bitcoin account with Krypto Bitcoin Mining Group by paying Bitcoin from Chen and Lu with an amount of NT\$1.62 million paid for 90 Bitcoin (1 Bitcoin for NT\$18,000, depending on the exchange rate of the day). Chen and Lu said that the Group had set

up a mine server in Iceland and would distribute 0.63 Bitcoin per day to each buyer's account (equivalent to NT\$11,000) and it would take only 4.5 months to earn back the principal. The Group invited well-known actors and actresses in Hong Kong to endorse the product and treated the victims to visit the headquarters in Hong Kong free of charge; also, claimed that all the Bitcoin purchased by the members could be traded at the "MY COIN Exchange;" therefore, many people were deceived. The police had the case forwarded to the prosecutors for investigation with a charge of fraud and breach of Banking Act.

2. "Bitcoins" fund-raising crime - social network investment crime

Beginning in early March 2016, a man nickname "Karen" promoted Bitcoin investment on the Internet with more than two thousand people to participate through the LINE. Therefore were once more than 20 groups in the LINE chat room. There were fund-raising groups formed in Mainland China by "WeChat." The suspect claimed that an investor would need to remit only 3 Bitcoins (about NT\$39,000) to the designated investment website and would receive a high return in the short term. There were more than two thousand investors participated in three weeks. The suspect had also set up the "Flower Wheel International Bitcoin Community" in Mainland China with funds raised by a "direct-sale" approach and a slogan of "earning 2.5 times of profit daily" to attract Taiwanese investors to remit Bitcoin and with NT\$50 million received in 3 weeks. The police had the crime in violation of Banking Act forwarded to the prosecutor for prosecution.⁴⁹

3. "Bitcoin" ransom case - Huang ○ Quin, a businessman in Hong Kong, kidnapping case

The kidnapping of Huang ○ Quin, a businessman in Hong Kong, occurred in 2015 that shocked the people in Taiwan and Hong Kong. The kidnappers demanded to have ransom paid with Bitcoin that was a very un-traditional tactic. As Bitcoin is not the fiat money in Taiwan with the characteristic features of anonymity, paid ransom simply become untraceable.

⁴⁹ Same as Note 5, Page 53.

According to the newspaper reported, the kidnappers of Huang ○ Quin demanded a ransom of HK\$70 million to be paid in Bitcoin because it would be untraceable and law enforcement officers said it would be “more difficult to trace than a dummy account.” The investigation team said that the kidnapping was planned meticulously and the crime could completely counter the police’s criminal investigation technology; also, the kidnappers asked for ransom to be paid in Bitcoin instead of the making telephone call for redemption to avoid being investigated.

4. “Bitcoin” fund-raising crimes - cross-strait underground money laundering center offense

In early May of 2016, the Ministry of the Interior National Police Agency Criminal Investigation Bureau Telecommunications Investigation Corps detected cross-strait Bitcoin money laundering center case. The syndicate adopted the entwined and complicate money-laundering operation to combine the e-bank USBKey and Bitcoin account for trade, through the pseudo-transformation of the Chinese identity card and dummy account money laundering, for a 5-layer money laundering, to protect the stolen money in the account from being frozen by the police and to have the funds successfully transferred and remitted to be withdrawn later by the withdrawer with the UnionPay card for an estimated transfer amount of NT\$50 million. The police had the case forwarded to the prosecution for investigation with a charge of violation against the Banking Act.

5. Other modes of crime

Currently, more and more Internet operators are optimistic about the Bitcoin trading market. The Internet platform is setup to provide Bitcoin account (wallet) combined with Taiwan’s bank account to conduct Bitcoin transactions, and uses the trading platform services through the overseas card issuing banks to apply for a Bitcoin credit card, that is, credit card spending paid in Bitcoin. In addition, Bitcoin remittance is a peer-to-peer transaction without any intermediate link, so the “Bitcoin transfer” between the Bitcoin Wallets eliminates the high handling fees required for general remittance and

the low transaction fee is more attractive than the general internet payment.⁵⁰ The trading platforms in Taiwan for the trade of Bitcoin or mutual transactions are free of any service fees.⁵¹

Therefore, the trading platform provides a “hidden” channel for those who are committed to committing a wrongful act or money laundering: The unlawful proceeds are remitted into the trading platform and then converted to Bitcoin and remitted to offshore dummy Bitcoin Wallet or equivalent value of commodity; or have the Bitcoin transferred to an Internet address, such as, “tumbler”⁵² and “tumbler” will have the same amount of Bitcoin transferred from another user to a new “clean” Address, but the program does not immediately convert all the amount of Bitcoin because the same amount may cause other people’s attention. The “tumbler” will make several transfers in a small amount and extend the interval between each transfer to avoid any suspicion. Under the circumstance, it is difficult for law enforcement officers to trace the financial flow.

⁵⁰ Marija Odineca, "Bitcoin Growth in 2016? Show Us Your Numbers!" THE COINTELEGRAPH, 1 Jan. 2016, <<http://cointelegraph.com/news/bitcoin-growth-in-2016-show-us-your-numbers>>.

⁵¹ "About Service Fees", BitoEX, 12 Jul. 201, <<https://www.bitoex.com/help/6?locale=zh-tw#44>>.

⁵² Legitimatization of Bitcoin is with the use of "mixers" (also known as "tumblers"), that is, mix the illegally obtained Bitcoin with the Bitcoin of others; however, the criminals will be able to get a clean address and the blockchain is unable to link it to those sites that are victimized. The "tumbler" can only be obtained through an anonymous Tor network, so it is difficult for law enforcement agencies to track its flow or find the offenders. Also refer to Lei Phone Website "Three steps of stealing Bitcoin: Duplicate password key, money laundering, and cash in." "Science and Technology News," December 21, 2013, <<http://technews.tw/2013/12/21/3steps-steal-bitcoin/>>.

VI. Learn from experience -International financial intelligence network strategy for the Bitcoin related money laundering

The attitude of some countries for the disposal of Bitcoin is as follows: The German government recognized the legal status and taxation of Bitcoin as a legitimate unit of bookkeeping on August 2013, becoming the first country in the world officially recognized the legal status of Bitcoin. Norway considered Bitcoin a commodity asset with the levy of capital gains tax in study. Denmark planned to include virtual currency in the legal norms. The French government announced Bitcoin illegal, but the national “Bitcoin Foundation” had been established few weeks later. Britain audited the taxation of Bitcoin or adjusted the value-added tax on January 21, 2014. Russia announced a full ban on Bitcoin on February 8, 2014. The Swiss Federal Government is currently assessing the impact of Bitcoin on the Swiss financial system and assessing whether the Bitcoin is to be identified as a foreign exchange in order to allow the institutional investors to conduct Bitcoin transactions under the existing law.

While facing the impact and influence of Bitcoin, Mainland China has gradually attached importance, because in addition to the vast domestic market for Bitcoin, many people gradually consider Bitcoin an emerging and hidden means for the transfer of funds to overseas, or buy large and high-speed mining Machine to have legal currency (RMB) converted to Bitcoin for remitting abroad.⁵³ The Vice President of the People’s Bank of China said on November 20, 2013 that China could not recognize the legitimacy of Bitcoin in the near future, but people had freedom to participate in Bitcoin

⁵³ Joel Valenzuela, "How to Move Money out of China: A Brief Guide," THE COINTELEGRAPH, 21 Mar. 2016, < <https://cointelegraph.com/news/how-to-move-money-out-of-china-a-brief-guide>>.

transactions on the Internet. On December 3, 2013, the People's Bank of China and the Ministry of Industry and Information Technology ("MITT"), China Banking Regulatory Commission ("CBRA"), China Insurance Regulatory Commission ("CIRC"), and China Securities Regulatory Commission ("CSRC") jointly issued the "Notice on the Prevention of the Risk of Bitcoin," which required the Bitcoin registration, Bitcoin electronic wallet, Bitcoin trading services institution's obligations in anti-money laundering, countering terrorism financing, and taking measures to identify customers and record identity information; also, requesting financial institutions and payment service providers to strengthen the monitoring and control measures against the Bitcoin service providers in order to prevent the relevant risks. In addition, request all branches of the People's Bank of China to study the ML risks associated with Bitcoin and take appropriate actions, including strengthening supervision actions and strengthening monitoring on suspicious transactions to offset risks.

The People's Bank of China had detailed the reasons why Bitcoin did not have currency attributes in the "China Financial Stability Report (2014)" as follows:

1. Bitcoin is without the support of national credit, without legality and not mandatory, so the circulation of Bitcoin is limited, unstable, and it is difficult to really play the role of circulation and payment means.
2. Bitcoin lacks the central adjustment mechanism, easily speculated, causing rapid price fluctuations, difficult to become the mean of currency and circulation. Currently, the merchandises paid with Bitcoin are mostly priced in the national currency.
3. Bitcoin scale is limited and it is difficult to adapt to the needs of economic development. If Bitcoin becomes the currency in circulation, it will lead to deflation and inhibit economic development.
4. Bitcoin is highly replaceable and it is difficult to act as a general equivalent value.

In addition, Hong Kong, in view of the global concern about virtual

goods such as “Bitcoin” and the associated risk of money laundering and terrorism financing in January 2014, reminded all accepting institutions to take prudent risk management in consideration of the latest developments in virtual currency. As indicated in Paragraphs 2 and 3 of the Hong Kong “Guidelines on Combating Money Laundering and Terrorism Financing,” anonymous virtual commodity transactions or anonymous holdings of virtual goods constitute a significantly higher risk of money laundering and terrorism financing, including the relevant risks arising from the potential or existing customers’ conducting virtual goods related activities through the accounts opened at the authorized institutions or other services. Therefore, the accepting institutions are required to ensure that they are particularly vigilant in relation to the risks in considering whether to establish or maintain a business relationship with the operator involved in the plan for virtual goods. In addition to other control measures, the accepting institutions should carefully consider whether the operators have established effective control measures in order to prevent the risk of money laundering involving virtual goods when assessing the relevant risk of money laundering and terrorism financing of such operators. The Hong Kong Monetary Authority expects the accepting institutions to continue to be vigilant in considering whether to establish or maintain business relationships with operators related to the virtual commodity program, including considering whether such operators have established effective control measures to prevent virtual goods from involving in the risk of money laundering and terrorism financing.

Macau and Taiwan hold a similar attitude towards the Bitcoin. The Monetary Authority of Macao has indicated that Bitcoin is a virtual commodity and is not a legal currency or financial instrument subject to the regulation of the Monetary Authority of Macao. However, the Monetary Authority of Macao reminds that the Bitcoin transaction involves the risk of money laundering and terrorism financing; therefore, participants are at their own risk. The Central Bank of Taiwan indicated on December 30, 2013 that Bitcoin was without legal effect and not a real currency; therefore, it should

not be regarded as currency. The Central Bank of Taiwan regards Bitcoin as highly speculative “virtual goods” with security risk; therefore, advises people to pay attention to the risks during the transaction and prohibits the use of Bitcoin in third-party payment transactions.

VII. Conclusions

In summary, how Taiwan's financial intelligence unit in response to the concern of money laundering triggered by Bitcoin and other virtual currencies will be concluded from the aspects of legal system, technology, and trend; also, it is for the reference of the domestic law enforcement agencies as indicated hereinafter.

(I) Legal system - clear specification

1. Reduce the risk of money laundering due to poor customer review of the Bitcoin trading platform in Taiwan

Taiwan's related industry for attracting customers ignores the review mechanism and is only controlled by mobile phone and/or identity card confirmation. However, the aforementioned documents can easily be forged or used for a dummy account. While the specifications are not yet cleared defined by the competent authorities of Taiwan, Bitcoin will be easily used as a crime tool for money laundering. Therefore, the country should designate the competent authorities to enact a customer review system for the use of Bitcoin trading platform, including identity verification, contact information, financial account verification, etc., in order to minimize the risk of money laundering on the trading platform.

In addition, include Bitcoin trading platform⁵⁴ in the "Money Laundering Control Act" in accordance with Article 5 Paragraph 2 of the "Money Laundering Control Act" and then Bitcoin trading platform will be subject to Article 9 and Article 10 of the "Money Laundering Control Act." There are non-bank and other institutions, such as, electronic ticket issuers and electronic payment agencies designated as financial institutions for management in accordance with Article 5 Paragraph 1 of the "Money

⁵⁴ There are not many Bitcoin trading platforms in Taiwan; however, the low transaction fee and the transaction free of taxation problem have attracted a large number of investors or players in China, Hong Kong, and Macao.

Laundrying Control Act,”⁵⁵ such as, the “Easy Card” issued by Taipei MRT. In the case of Article 10 of the “Money Laundrying Control Act,” if the operator finds that there is a large amount of suspicious funds remitted into the platform account for exchanging to Bitcoin, it should be reported to the competent authorities for records immediately.

2. Refer to FATF guidelines on virtual currency for future decision-making

The Asia/Pacific Group on Money Laundrying (APG) in 2007 had specifically pointed out at the APG 2nd Round Mutual Evaluation” that Taiwan’s “Money Laundrying Control Act” was with a number of legal deficiencies, such as: Unclear definition of money laundrying and property interests, limited money laundrying crime prevention and control function due to the precondition of money laundrying crime threshold, the limited range and high money laundrying crime threshold, lack of defined punitive clauses against terrorism financiers and terrorists, Designated Non-Financial Business or Profession (DNFBP), for example: lawyers, CPAs, notaries, real estate brokers, financing lease industry, and corporate service provider) not included in the anti-money laundrying system, and failing to meet the requirements of the aforementioned FATF anti-money laundrying / countering terrorism financing international standards. Although the relevant legislation on virtual currency was not included in the evaluation program, FATF explained in the “Virtual Currency - Key Definition and Potential Money Laundrying and Terrorism Financing Risks” that was published in June 2014 the risk of money laundrying and terrorism financing arising from Bitcoin and the recommendations to the country in formulating the relevant mechanism that could be regarded as a reference for the development of virtual currency and the prevention of money laundrying in Taiwan.

⁵⁵ Banking Bureau of the Financial Supervisory Commission, June 5, 2015 FSCBB.Bill.Tzi No. 201540002670 Letter interpretation: "According to Article 5, Paragraph 1, Section 18 of the 'Money Laundrying Control Act,' electronic ticket issuers and electronic payment agencies are designated as financial institutions in Article 5 Paragraph 1 of the 'Money Laundrying Control Act' and it shall enter into force immediately."

(II) Technical aspect - cross-border cooperation and data digitalization

1. Promote virtual currency cross-border and cross-agency cooperation

Because the development of a virtual currency has not been completely controlled by a single country or a single institution, the government for the purpose of supervision and management should promote cross-border cooperation, for example: the United States combined with 17 countries to expose the “Liberty Reserve” international money laundering crime. The Department of Culture and the Department of Commerce in Mainland China jointly announced the “Online Game Virtual Currency Transaction Management Notice.” European Criminal Police Organization in the “2015 Online Organized Crime Threat Assessment Report” strongly recommended that law enforcement agencies worked with the private sector and applied academic resources to “seize the opportunity to study emerging technology crime investigations.”⁵⁶ There are also scholars in Taiwan that believe that it is not possible for a single domestic agency to be the contact for the connection with the international norms in anti-money laundering and countering terrorism financing. The professional assistance in the identification and investigation process is necessary.⁵⁷ This concept should be applied to respond to the virtual currency related money laundering and terrorism financing.

2. Strengthening the data collection and research and data construction of law enforcement agencies

Since the virtual currency is without clear specification defined (such as, issuing vendors or trading platform to submit relevant statistical information, etc.), or due to its characteristics (such as, Bitcoin is difficult to track), or due to the difficulty of the statistical survey (such as, how many units of Bitcoin

⁵⁶ Same as Note 39, Page 63.

⁵⁷ Zhijie Lin, "Evaluation and Reflection of Mega Bank Case," "The Taiwan Law Review," Vol. 259, December 2016, Page 45.

is converted to NTD), so that the relevant data is extremely limited. It is necessary to strengthen data collection and to proceed with the construction of big data for exploring the risk of money laundering arising from virtual currency in order to prevent it from occurring and to prevent all possible criminal loopholes;⁵⁸ also, to minimize the possibility of Bitcoin becoming “invisible money laundering tool.”

(III) Trends - Monetary Diversification and Talent Specialization

1. Strengthening the awareness of the trend of currency diversification

There are 627 types of virtual currencies currently registered on the “Crypto Currency Market Capitalizations” website,⁵⁹ which initiates the exchange rate calculation between the virtual currency and the US Dollar. The overall scale of the virtual currency is more than US\$7.3 billion, of which, Bitcoin accounted for nearly 6.4 billion, representing 90% market share. In addition to Bitcoin, there are as many as 127 different types of Altcoin similar to Bitcoin principle and structure, such as: Litecoin, Namecoin, PP coin, Dogecoin, Ethereum, DAO, and so on. Virtual currency will become diversified in the future, so law enforcement agencies should include virtual currency and other financial and economic crime and information security courses⁶⁰ in the training courses for trainees in order to grasp the movement of financial technology and get familiar with the practice of criminal investigation.

⁵⁸ Such as, Taiwan's academic community applies "Social Network Analysis" (SNA) to analyze problem trends and data construction.

⁵⁹ "All Currencies" Crypto-Currency Market Capitalizations, Feb. 17 2016, < <https://coinmarketcap.com/currencies/views/all/>>.

⁶⁰ Foreign well-known universities, such as, New York University (NYU) and Duke University have set up the "virtual currency course" in response to the virtual currency trends. NYU has the course "The Law and Business of Bitcoin and Other Cryptocurrencies" and Duke University has the "Innovation, Disruption and Cryptoventures" course. All attach importance to the future impact and influence of virtual currency on the law and economy, worthy for the reference of our regional law enforcement agencies in grass-roots education.

2. Strengthening the training of professionals and budget integration

The responsible law enforcement agencies should base on the “resource sharing” mechanism to establish a virtual currency network money laundering control group, to arrange network crime prevention seminars, and to work with academy⁶¹ and private sector⁶² in Bitcoin tracking technology, and to have personnel participated in the courses or relevant seminars domestically or internationally in order to enrich their knowledge and skills; also, to accumulate the network anti-money laundering tracking and investigation energy. In addition, since the global circulation of virtual currency often involving international illegal assets recovery and mutual legal assistance, and in response to the particularity of our international status and the inconvenience of prosecution of money-laundering offenses, the “Money Laundering Prevention Fund” is established in Article 20 of the “Money Laundering Control Act” to supplement the funds needed for judicial interaction with other countries.⁶³ The idea is to have anti-money laundering and countering terrorism financing talents trained with the support of the integrated budget in a long run in order to accumulate cross-field energy and experience.

⁶¹ Such as, National Taiwan University "Financial Technology and Blockchain Research Center," Taiwan Academy of Banking and Finance, and other academic institutions or research units.

⁶² In fact, there is already the relevant tracking technology developed by Bitcoin operators. Also see Marco E. G. Maltese, "First 2016 Bitcoin Crisis at The Doors," THE COINTELEGRAPH, 17 Jan. 2016, < <http://cointelegraph.com/news/first-2016-bitcoin-crisis-at-the-doors> >.

⁶³ Peiling Tsai, "Analysis on the Money Laundering Control Act Amendment," "New Viewpoint of Prosecution," Vol 21, Page 57, January 2017.

References

Chinese Articles

Xingfang Yan, “King of the currency – Bitcoin,” Dao-Tien Publishing Company, Taipei (2014)

Edward Castronova, translated by Yuwen Huang and Lixue Lin, “Virtual Currency Economics,” Yeh-Ren Culture Co., Ltd., Taipei (2015)

Marc Goodman, translated by Junhong Linn, “Future Crime,” Trojan Culture Publishing Company, Taipei (2016)

Paul Vigna and Michael J. Casey, translated by Yiling Lin, “Virtual Currency Revolution,” Big Publishing Company, Taipei (2016)

Chinese Journal

Zhijie Lin, “New Thinking on Anti-Money Laundering - On Financial Money Laundering Control, Financial Supervision and Investigation Authority” and “New Viewpoint of Prosecution,” Issue 3, Page 271, January 2008

Rongjin Guo, “Legal Disputes on Internet Virtual Currency,” “Analysis of Technological and Law,” Tome 26, Vol. 10, Page 23 - 31, October 2014

Zhijie Lin, “Evaluation and Reflection of Mega Bank Case,” “The Taiwan Law Review,” Vol. 259, Page 45, December 2016

Pei-Ling Tsai, “Analysis on the Money Laundering Control Act Amendment,” “New Viewpoint of Prosecution,” Vol 21, Page 57, January 2017

Other Chinese Articles for reference

Supreme Court 2014, Tai.Sun.Tzi No. 3093 Verdict, High Court 2015 Sun. Yi.Tzi No. 1233 Verdict, Taoyuan District Court 2011 Shen.Sue.Tzi No. 1361 Verdict, and Taipei District Court 2009 Sue.Tzi No. 1000 Verdict
Banking Bureau of the Financial Supervisory Commission, June 5, 2015

FSCBB.Bill.Tzi No. 201540002670 Letter interpretation

Foreign articles

Chambers-Jones, Clare, “Virtual Economies and Financial Crime: Money Laundering in Cyberspace,” Cheltenham, U.K.: Elgar, 2012.

Foreign journals

Manning, John F., Separation of Powers as Ordinary Interpretation, 124 Harv. L. Rev. 1939 (2011).

Petersmann, Ernst-Ulrich, The Future of the WTO: From Authoritarian “Mercantilism” to Multilevel Governance for the Benefit of Citizens? 6 Asian J. WTO & Int’l Health L. & Pol’y 81 (2011).

Schmidt, Robert, Grateful to Be Employed, Borrowed Half to Death, Bloomberg Businessweek, June 20, 2011, at 35.

Cook, R. Joseph, Bitcoin: Technological Innovation or Emerging Threat? 30 J. INFO. TECH. & PRIVACY L. 535, 539, 2014.

Ly, Matthew Kien-Meng, Coining Bitcoin's "legal-bits": Examining The Regulatory Framework For Bitcoin And VirtualCurrencies,27 HARV. J.L. & TECH. 587, 594, 608, 2014.

Mullin, Sheppard, Making Sense of Virtual Dollars, Law of the Level, 22 November 2011.

Sparshott, Jeffrey, Web Money Gets Laundering Rule, Wall Street Journal, 21 March 2013.

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

Other Foreign Articles for reference

Financial Action Task Force, Virtual Currencies- Key Definitions and Potential AML/CFT Risks,” June 2014.

Financial Action Task Force, Guidance for a Risk-Based Approach Virtual Currencies, June 2015, No.13.

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, 30 September 2015.

United States Government Accountability Office, Virtual Economies and Currencies, May 2013.

U.S. v. Faiella, United States District Court, S.D. New York, No. 14-cr-243 (JSR), 39 F.Supp.3d 544, 19 August 2014

Part Five

The Major Events of the AMLD



The Major Events of the AMLD

DATE	EVENT
2016/1/30-2/7	The delegates of the AMLD attended the Egmont Group Working Group and Committee Meetings Program in Monte-Carlo, Principauté de Monaco. The chief director of the AMLD, Mr. Gilbert LEE, was elected to be a representative of Asia and Pacific region.
2016/2/6-2/14	The delegates of the AMLD attended the course of strategic analysis of the Egmont Group in Paris, France.
2016/2/12-2/21	The delegates of the AMLD participated in the 2nd Plenary Meeting of FATF-XXVII in Paris, France.
2016/5/5	The AMLD held a workshop on AML/CFT for Financial Industry.
2016/5/16-5/20	The delegates of the AMLD attended in the Intersessional Meetings of the Egmont group in Nadi, Fiji.
2016/5/23-5/27	The delegates of the AMLD participated in the APG Assessor Training course in Macau, China.
2016/6/14-6/18	Sergio Espinosa, the Chairman of Egmont Group and head of the Peruvian Financial Intelligence Unit, and Jorge Yumi, Director of the International Affairs Office of the Center, visited the AMLD and the AML relevant authorities.
2016/6/16	Mr. Martin Blair, International Liaison Officer of National Crime Agency of British Consulate-General Hong Kong visited the AMLD.
2016/6/17-6/25	The delegates of the AMLD participated in the 4th Plenary Meeting of FATF-XXVII in Busan, Korea.
2016/6/25-7/1	Mr. Gilbert LEE, as the representative of Asia and Pacific region, interviewed applicants for the chief of Egmont Group Secretariat in Toronto, Canada.

2016/9/4-9/10	The delegates of the AMLD attended the 18th APG Plenary and Working Group Meeting in San Diego, USA.
2016/10/11-10/23	The delegates of the AMLD attended Intersessional Meetings of the Egmont Group and the 2th Plenary Meeting of FATF-XXVIII in Paris, France.
2016/10/18	Representatives of Security and Integrity, the Hong Kong Jockey Club, visited the AMLD.
2016/10/19	AMLD and FinTRACA signed a MOU concerning cooperation in the exchange of financial intelligence related to money laundering, associated predicate offenses, and terrorism financing in Paris, France.
2016/10/23-10/28	The delegates of the AMLD attended the Information Exchange Working Group (IEWG) Meeting of the Egmont Group in Paris, France.
2016/10/25-10/28	The delegates of the AMLD attended the 3rd Plenary of the Asset Recovery Interagency Network Asia Pacific (ARIN-AP) in Tokyo, Japan.
2016/11/15	The Director General of MJIB, Mr. Ching-Hsiang Tsai, visited the banking Supervision Agency, State Bank of Vietnam (SBV).
2016/11/26-12/3	The delegates of the AMLD attended the APG Joint Typologies and Capacity Building Workshop, and made a presentation in Jeddah, Kingdom of Saudi Arabia.
2016/12/6	The AMLD held a Forum on AML/CFT for the Chief Compliance Officer of Financial Institutions.

ANTI-MONEY LAUNDERING ANNUAL REPORT, 2016

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

Issuer: Tsai, Ching-Hsiang

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: November 2016

GPN : 1010602494

ISBN : 978-986-05-4745-0 (PDF)



ANTI-MONEY LAUNDERING ANNUAL REPORT, 2016



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

