A Global Challenge of Taiwanese Banking Industry: Anti-Money Laundering and Combating the Financing of Terrorism – A Case Study of Mega International Commercial Bank

Student: Sun, Man-Jung

Advisor: Professor Jack Wu

December 2017
A Global Challenge of Taiwanese Banking Industry: Anti-Money Laundering and Combating the Financing of Terrorism – A Case Study of Mega International Commercial Bank

Student: Sun, Man-Jung
Advisor: Jack Wu

A Thesis Submitted to International MBA Program National Chengchi University in partial fulfillment of the Requirements for the degree of Master in Business Administration

December 2017
Acknowledgements

First and foremost, I would like to express my sincerest gratitude and appreciation to my thesis advisor, Professor Jack Wu, who has supported me throughout my thesis with his patience and knowledge. Without his guidance and encouragement, this thesis would not have been completed or written.

I would also like to express my gratitude and appreciation to the members of NCCU IMBA for their assistance and hospitality throughout all my studies at NCCU.

I would also like to thank my colleagues, Bessie, Lunna, and Mandy for their suggestions and mental support throughout the work.

Finally, I would like to express my special thanks to my parents for their support and encouragement to make this piece of work possible.

Sun, Man-Jung
Abstract

A Global Challenge of Taiwanese Banking Industry: Anti-Money Laundering and Combating the Financing of Terrorism – A Case Study of Mega International Commercial Bank

By

Sun, Man-Jung

Money laundering (ML) involves a wide range of predicate offenses, including drug trafficking, human smuggling, arms smuggling, gambling, fraud, tax evasion, etc. Additionally, money laundering activities had been associated with drug trafficking or organized crime in the past, but the terrorist attacks on September 11th, 2001 have highlighted the link between money laundering activities and terrorist financing (TF). Due to the over-banking phenomenon in Taiwan, banks focus more on business performance than compliance, resulting in the violation incident of Mega International Commercial Bank (Mega Bank) New York Branch with a huge penalty of US$180 million fined by the New York State Department of Financial Services (NYDFS) in August, 2016. The violation incident of Mega Bank New York Branch has reinforced the importance of compliance with international Anti-money laundering/Combating the financing of terrorism (AML/CFT) standards for risk mitigation. Taiwan will undergo the third round of the Asia/Pacific Group on Money Laundering (APG) mutual evaluations in 2018, it calls for not only government legislation but also raising public awareness of ML/TF crimes and involves the public cooperation with the government in the fight against ML/TF.

Keywords: Money Laundering, Financing of Terrorism, Mega International Commercial Bank, New York State Department of Financial Services, Panama Papers
TABLE OF CONTENTS

1. Introduction .......................................................................................................................... 1
  1.1. Background and Motivation for the Study ................................................................. 1
  1.2. Methodology of the Study ......................................................................................... 2
  1.3. Limitation of the Study ......................................................................................... 3
  1.4. Framework of the Study ......................................................................................... 3

2. Money Laundering and Terrorist Financing ................................................................. 6
  2.1. The Role of Banking System Involved in Money Laundering Activities ............... 6
  2.2. Overview and Background of Money Laundering ................................................ 7
  2.3. Money Laundering Cycle ....................................................................................... 8
  2.4. Methods and Typologies of Money Laundering Activities ..................................... 11
  2.5. Link Between Money Laundering and Terrorist Financing .................................... 16
  2.6. The Impacts of Money Laundering ...................................................................... 19
  2.7. Where the Money is Hidden ............................................................................... 22
  2.8. International Organizations on Money Laundering ........................................... 27
      2.8.1. United Nations Office on Drugs and Crime (UNODC) ................................. 27
      2.8.2. Financial Action Task Force (FATF) .............................................................. 28
      2.8.3. Asia/Pacific Group on Money Laundering (APG) ........................................ 31
      2.8.4. The Egmont Group of Financial Intelligence Units ..................................... 34
2.8.5. The Wolfsberg Group ........................................................................................................ 35

3. Anti-Money Laundering Legislation in Taiwan ................................................................... 36

4. Case Study of Mega International Commercial Bank .................................................... 42
   4.1. Overview of Mega International Commercial Bank ................................................. 42
   4.2. Violation Incident of Mega Bank New York Branch ................................................ 46
   4.3. Taiwanese Banking Industry Review .......................................................................... 51
   4.4. The Impacts of AML/CFT on the Operations of Mega Bank ...................................... 54
      4.4.1. Reform a Business Culture of Compliance and Internal Control ....................... 54
      4.4.2. Establish an Effective AML/CFT Program ......................................................... 56

5. Conclusion and Recommendation .................................................................................... 72

Reference ................................................................................................................................. 76
List of Figures and Tables

Figure 1: Framework Chart of the Study .......................................................................................... 5
Figure 2: Three Stages of Money Laundering ................................................................................. 10
Figure 3: A Simple Hawala Transaction Sample ............................................................................. 18
Figure 4: Global Sanctions Regimes 2016 ..................................................................................... 21
Figure 5: The 10 Most Popular Tax Havens in the Panama Papers .............................................. 23
Figure 6: Top 10 Countries with the Most Active Intermediaries in the Panama Papers .............. 26
Figure 7: How Mossack Fonseca & Co Helped its Clients Hide Their Wealth Offshore ............... 27
Figure 8: Timeline for Anti-Money Laundering Legislation in Taiwan ......................................... 41
Figure 9: Organization Chart of Mega International Commercial Bank ....................................... 43
Figure 10: Financial Statistics for Mega International Commercial Bank, 2014 ~ 2016 .............. 46
Figure 11: Deficiencies Directed by the New York State DFS Examination ................................... 51
Figure 12: Elements for Building a Business Culture of Compliance and Internal Control ......... 56
Figure 13: AML KYC Onboarding Lifecycle .................................................................................. 60
Figure 14: Elements for Establishing an Effective AML/CFT Program ....................................... 71

Table 1: Major U.S. Sanctions Violations Cases, 2009~2016 ..................................................... 22
Table 2: Financial Secrecy Index (FSI) – 2015 Results ................................................................. 25
Table 3: The FATF Recommendations ......................................................................................... 30
Table 4: APG Members List .......................................................................................................... 33
Table 5: Major Institutional Shareholders of Mega International Commercial Bank List ........... 44
Table 6: Taiwanese Banks Ranked Among the Top 500 Banks in the World in Terms of Tier One Capital .................................................................................................................... 45
Table 7: Number of Banking Institutions in Taiwan, as of the end of Sept., 2017.................53

Table 8: Major General Enforcement Actions of NYDFS for Violations of BSA/AML
    (Including Tax Evasion), 2013~2017 ...........................................................................74

Table 9: Number of Overseas Branches of Domestic Banks, as of the end of Sept., 2017.....75
1. Introduction

1.1. Background and Motivation for the Study

Mega International Commercial Bank (Mega Bank) New York Branch was fined by the New York State Department of Financial Services (NYDFS) at a penalty of US$180 million (NT$5.7 billion, in equivalent) for violations of the Bank Secrecy Act and Anti-Money Laundering (BSA/AML) on August 19, 2016 (Mega Financial Holding Co., Ltd. 2016), which has reinforced the significance of a vigorous Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regime. Additionally, the violation incident of Mega Bank New York Branch implied that Taiwanese banking industry has not yet well implemented the relevant regulations, reporting requirements, and compliance regimes of the BSA/AML, which not only undermined the brand image of Mega Bank itself but also deteriorated Taiwan’s international reputation (Ministry of Foreign Affairs, Republic of China (Taiwan), Taipei Liaison Office in the RSA).

Executive Yuan, Republic of China (Taiwan) mentions that Taiwan enacted the Money Laundering Control Act in 1996, which was the first dedicated law in Asia for the purpose of anti-money laundering and also became one of the founding members of the Asia/Pacific Group on Money Laundering (APG) in 1997. However, Taiwan’s efforts on combating money laundering became less effective over time since its subsequent amendments focused more on criminal prosecution than keeping up with international standards. Accordingly, Taiwan
received positive reviews in the APG mutual evaluations in 2001, but then was downgraded to a follow-up watch list in 2007. Fortunately, Taiwan was taken off from the APG 10-member watch list on July 20, 2017 with its ongoing efforts over the past few years on both Anti-Money Laundering (AML) legislation and counter-measures. Taiwan will undergo the third round of the APG mutual evaluations in the fourth quarter of 2018. Confronted with the challenge of the third round of the Asia/Pacific Group on Money Laundering (APG) mutual evaluations held in the fourth quarter of 2018, both public and private sectors need to speed up the legislation and enforcement associated with AML/CFT to meet international standards and earn a better reputation through the mutual evaluation process (張迺佳 2016).

1.2. Methodology of the Study

A case study is adopted as methodology of this thesis. This thesis will discuss the currently deficient AML/CFT regime of Taiwanese banking industry through the case study of violation incident of Mega Bank New York Branch. Moreover, this thesis will discuss the impacts of AML/CFT on the operations of Mega Bank as well as the entire banking industry in Taiwan in order to meet the international standards and pass the third round of APG mutual evaluations in the fourth quarter of 2018. According to the Financial Action Task Force (FATF) Mutual Evaluation Report in September 2016, the FATF assessed that Singapore has a strong framework for AML/CFT in terms of the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Singapore’s AML/CFT system through the on-site visit, which has made significant enhancements to its AML/CFT regime since its last FATF assessment in 2008 (Monetary Authority of Singapore (MAS); FATF and APG 2016). Therefore, this thesis will undertake the AML/CFT regime in Singapore – the Association of
Banks in Singapore (ABS) Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism which is in compliance with the MAS’ Notice and Guidelines – as a benchmark to discuss the counter-measures to combat money laundering and terrorist financing (ML/TF) in Mega Bank as well as the whole banking industry in Taiwan.

1.3. Limitation of the Study

In general, Taiwanese banks do not establish an effective and vigorous AML/CFT program with little experience and insufficient guidance from the authorities concerned since AML/CFT issues have been neglected for far long in the past and are relatively new in Taiwanese banking industry. For this reason, the discussion of this thesis is based on the experience and related AML/CFT regime in Singapore. Furthermore, the author also encounters some difficulties in gathering the AML/CFT regulations, regimes, and guidance of other foreign countries, such as the United States, which is supposed to be the country with the highest standards and best practice associated with AML/CFT. Additionally, it is difficult to gather an effective AML/CFT program from a certain bank, especially foreign-owned banks since they treat their AML/CFT policy as confidential.

1.4. Framework of the Study

This thesis is divided into five chapters. Chapter one provides an introduction to the background and motivation for the study, methodology of the study, and the framework of the study
respectively. Chapter two provides an overview of money laundering and terrorist financing, including the definition and cycle of money laundering, methods and typologies used in money laundering activities, the impact caused by money laundering, and the international organizations on money laundering, such as United Nations Office on Drugs and Crime (UNODC), Financial Action Task Force (FATF), Asia/Pacific Group on Money Laundering (APG), The Egmont Group of Financial Intelligence Units, and The Wolfsberg Group. Chapter three focuses on the governmental policy-making side, it looks at the legislation in association with AML/CFT in Taiwan. Chapter four focuses on the violation incident of Mega Bank New York Branch occurred in August, 2016 as a case study, which explains the role of banking industry involved in money laundering activities, discusses the deficient and inadequate AML/CFT program of Mega Bank, and explores the counter-measures to combat ML/TF based on the AML/CFT regime in Singapore and other international standards given that Taiwan is still at the beginning stage in AML/CFT field with insufficient regulations and guidelines provided by the authorities concerned. Chapter five provides the conclusion and policy recommendation to Mega Bank as well as the entire Taiwanese banking industry in the fight against ML/TF, particularly under the challenge of the third round of the APG mutual evaluations held in the fourth quarter of 2018.
Figure 1: Framework Chart of the Study
2. Money Laundering and Terrorist Financing

2.1. The Role of Banking System Involved in Money Laundering Activities

Jayasuriya (2003) states that money laundering is a process to disguise criminal activities in order to conceal the proceeds obtained from illicit origins to avoid detection. Furthermore, since the terrorist attacks happened on September 11th, 2001, which highlighted the link between money laundering activities and terrorist financing, terrorist financing has currently been treated as one of the most important predicate offenses, and thus, combating money laundering and terrorist financing becomes a national and international challenge of countries around the world (Jayasuriya 2003; Krieger and Meierrieks 2011; Rahman 2008).

Rahman (2008) mentions that the banking system tends to be one of the most important and common vehicles for money laundering due to its comparative advantages: convenience, accessibility, and security. As compared to other institutions, Association of Certified Anti-Money Laundering Specialists (ACAMS) states in 2016 that it is less risky for money launderers to be detected through banking institutions since there are hundreds of thousands of transactions every day in the entire banking system. Therefore, it is easier for criminals to conceal their proceeds from illicit origins comingled with other legitimate transactions in banking institutions, and even leave no trace by utilizing the banking system due to its difficulties in detection.
Nowadays, with the rise of online banking and Financial Technology (FinTech), there is an emerging trend to abuse the banking system to facilitate criminals’ illicit transactions without restriction by legal and border barriers or by government supervision. However, it makes the detection through banking system even more difficult since the criminals could undertake illegitimate transactions by using merely computers, mobile phones or other electronic devices without physical presence to mitigate the risk of detection with anonymity (Rahman 2008).

2.2. Overview and Background of Money Laundering

The term “Money Laundering” was derived from the US describing the Mafia’s attempt to “launder” illicit proceeds through cash-intensive washing salons in the 1930s, which controlled by criminal organizations (Schneider 2010). Jayasuriya (2003) relates money laundering to a process to make dirty money look clean, in order to disguise a wide range of criminal activities, such as drug trafficking, human smuggling, arms smuggling, gambling, fraud, tax evasion, etc. to conceal criminals’ illicit proceeds from illegitimate origins and evade investigation. According to the United Nations Office on Drugs and Crime (UNODC), there are two reasons why criminals have to launder money:

(1) The illegitimate origin of proceeds is evidence of their crime.

(2) The proceeds are vulnerable to be traced and has to be obscured.

Given that money laundering has negative impacts on state financial stability and economic development since it undermines a nation’s international reputation and also distorts the real supply and demand of an economy, countries all over the world have ratified and enacted anti-
money laundering legislation (Executive Yuan, Republic of China (Taiwan); ACAMS 2016). Terrorist attacks happened on September 11th, 2001 have highlighted the link between money laundering activities and terrorist financing whereas in the past money laundering activities had been associated with drug trafficking and organized crime. Moreover, in the aftermath of the September 11th attacks, terrorist financing has become one of the most important predicate offenses. In general, the methods and schemes used in terrorist financing and money laundering are basically the same, except that the proceeds of terrorist financing may be obtained from both illegitimate and legitimate origins. Furthermore, combating the financing of terrorism is currently one of the most important national and international tasks of countries worldwide since more and more emerging terrorist activities happened all over the world in recent years are undoubtedly harmful to world peace (Jayasuriya 2003; Krieger and Meierrieks 2011; Rahman 2008).

2.3. Money Laundering Cycle

Money laundering cycle takes basically three stages. These three stages are commonly referred to as placement, layering and integration. The following three stages can be accomplished in one combined transaction as well as in three separate transactions (Aluko 2012; ACAMS 2016; Mulig and Smith 2004; Rahman 2008):

(1) Stage One: Placement

At this stage, large amounts of illicit proceeds obtained from criminal activities are laundered into the financial system. Financial institutions, legally operated businesses, and casinos are all common vehicles for criminals to place their illicit proceeds into circulation of the financial
system. For example, criminals may make large repayment for bank loans or purchase foreign currencies in banking institutions by using their illegitimate funds to launder dirty money and make it appear legitimate. The purpose of placement stage is to comingle the illicit proceeds with other legitimate money in the entire financial system and convert their illegitimate funds into other assets to avoid detection and attention of regulatory agencies.

(2) Stage Two: Layering

At this stage, criminals intend to obscure the illegitimate origin of their criminal proceeds. Layering can be achieved through a series of financial transactions to obscure the trace and ownership of the proceeds. For example, criminals may use their illicit funds to invest in real estate, stocks, bonds, insurance products or other financial instruments, and even legitimate businesses by implementing multiple transfers and transactions to make the true source of illicit funds indistinct. With the help of nowadays technology, funds can be easily moved among accounts, banks, and countries via simple wire transfers or even e-banking. Additionally, utilizing shell companies is a common way to conceal the substantive beneficial owner and assets. The purpose of layering stage is to create a great deal of complicated financial transactions to make the detection and tracing of regulatory agencies more difficult with multiple transactions and facilitate criminals to hide the true source and ownership of the illegitimate funds.

(3) Stage Three: Integration

The money laundering process is completed at this stage. Criminals integrate the laundered money into legally operated businesses to create the perception of legitimacy. For example, criminals may use the funds to purchase luxury assets, such as real estate, jewelry, or high-value
automobiles to further launder their funds. The purpose of integration stage is to legalize the illicit proceeds from organized crime by investing the proceeds in legitimate businesses without compromising the true origins.

Figure 2: Three Stages of Money Laundering

Sources: Jayasuriya (2003); Mulig and Smith (2004); UNODC
2.4. Methods and Typologies of Money Laundering Activities

The Asia/Pacific Group on Money Laundering (APG) is devoted to detailed and relevant typologies research in order to well understand the phenomena of money laundering and terrorist financing in the Asia/Pacific region. The following examples taken from APG research are common methods, techniques, schemes and instruments used in money laundering and terrorist financing (APG; ACAMS 2016):

- **Corruption/Bribery**
  
  Criminal organizations may bribe the officials or compliance staff in banking institutions to facilitate money laundering by undermining AML/CFT measures, including possible influence of politically exposed persons (PEPs).

- **Currency Exchanges/Cash Conversion**
  
  Criminals may purchase traveler’s checks to transfer value to another jurisdiction or seek certain Money Services Business (MSB) with low reporting requirements to evade detection.

- **Cash Couriers/Currency Smuggling**
  
  The use of smuggling facilitates criminals to conceal the illegitimate movement of large amounts of cash across borders to avoid reporting requirements and detection.

- **Structuring/Smurfing**
  
  Criminals may break their illicit proceeds into small amounts below the reporting
threshold to undertake numerous transactions (deposits, withdrawals, transfers, etc.) by various people to evade reporting obligations and mitigate the risk of detection.

- **Use of Credit Cards/Checks/Promissory Notes**

  Criminals may use credit cards, checks, promissory notes, etc. to make their transactions and fund transfers look normal and facilitate their access to funds held in financial institutions. Especially, credit cards have a prepayment function, and thus criminals could prepay their credit cards to create a credit balance on their accounts and then request refunds for the purpose of layering and further conceal the original source of their funds.

- **Purchase of Portable Valuable Commodities**

  Criminals may purchase portable high-value commodities, such as gems, precious metals, etc. to conceal ownership or move value to another jurisdiction without detection and evade AML/CFT measures.

- **Purchase of Valuable Assets**

  Criminals may purchase high-value and negotiable assets, such as real estate, race horses, vehicles, etc. to take advantage of reduced reporting requirements to conceal the illicit origins of their criminal proceeds.

- **Commodity Exchanges/Barter**

  Criminals may directly exchange narcotic drugs for gold bullion - avoid the use of money or other financial instruments - to evade AML/CFT measures and detection by regulatory
• Use of Wire Transfers

Criminals may use wire transfers to move funds between financial institutions, accounts, and even countries to evade detection and confiscation.

• Underground Banking

Criminals may use Alternative Remittance Systems (ARSs) or Informal Value Transfer Systems (IVTSs), such as Hawala, Hundi, etc., which are based on trust and outside the formal banking system to move funds across borders without detection and official scrutiny.

• Trade-Based Money Laundering and Terrorist Financing

Criminals may use over-invoicing, under-invoicing, multiple invoicing, fictitious trades, etc. to transfer value between buyers and sellers, or use shell companies to reduce the transparency of their transactions.

• Gambling Activities

Businesses associated with gambling activities, such as casinos, horse racing, internet gambling, etc. are ones of the most cash-intensive businesses. Criminals may buy chips with criminal proceeds and then ask for repayment by a check drawn on the casino’s account to obscure the source of their criminal proceeds.
● Abuse of Non-Profit Organizations (NPOs)

It is common for criminals to utilize Non-Profit Organizations (NPOs) to raise funds for terrorism and hide the true origin and nature of funds by taking advantage of positive public reputations of NPOs.

● Investment in Capital Markets

Criminals may purchase stocks, bonds, or other financial instruments in capital markets by using criminal proceeds to obscure the source of funds.

● Comingling

It is essential for criminals to combine their illicit proceeds with legitimate funds in the financial and economic system to obscure the origin of proceeds. Criminals may comingle their proceeds into legitimate businesses to evade detection.

● Use of Shell Companies

Shell companies are companies established with neither significant operations nor assets, and their ownership structures can take multiple forms. Criminals may use shell companies to take advantage of their reduced transparency of ownership to further their money laundering and obscure criminal ownership.

● Use of Foreign Bank Accounts/Offshore Banking/Offshore Businesses

Criminals may use foreign bank accounts, offshore banking or offshore businesses to conceal ownership identity of ill-gotten funds and transfer funds to another jurisdiction to
avoid supervision by domestic authorities.

- **Use of Third Parties**

  Criminals may take advantage of third parties, such as trusts, family members or even nominees to obscure ownership identity of illegitimate funds.

- **Identity Fraud**

  Criminals may use identity fraud to obscure the true identity of persons controlling illicit funds and engaging in money laundering and terrorist financing activities.

- **Use of Gatekeepers**

  It is common for criminals to involve so called “gatekeepers,” such as lawyers, accountants, brokers, etc. in their money laundering activities. Criminals may bribe these professionals to provide them with specialized services to facilitate them to obscure identity of substantive beneficiaries and the origin of illegitimate funds.

- **New Payment Technologies**

  Criminals may take advantage of nowadays payment technologies to transfer funds among accounts, banks, and countries through e-banking or mobile phone-based remittance and payment system.
2.5. Link Between Money Laundering and Terrorist Financing

Rahman (2008) mentions that the terrorist attacks on September 11th, 2001 have highlighted the link between money laundering activities and terrorist financing while in the past money laundering activities had been associated with drug trafficking or organized crime. Accordingly, terrorist financing is currently treated as the most important challenge to all civilized countries given that the emerging terrorist attacks worldwide in recent years have been harmful to world peace (Jayasuriya 2003).

Freeman (2011) states that terrorism does need money to sustain their organizations for daily operations, purchase of weapons, recruiting new members, training, future terrorist attacks, and even pension funds for families of terrorists died from terror attacks. As a matter of fact, terrorists have four general sources to raise their funds, including state sponsorship, criminal activities, legitimate businesses, and charitable donations. The most distinct difference between money laundering activities and terrorist financing is the source of their funds. Money laundering activities generate funds from criminal activities, such as drug trafficking, human and arms smuggling, etc. while terrorist financing may obtain funds from illegitimate or legitimate sources, and even both (Rahman 2008). In addition to illegal fund-raising methods, such as smuggling, extortion, kidnapping for ransom, etc., terrorist organizations may also operate totally legal businesses like trading companies, investment companies, manufacturing companies, etc. for profit generating with their terrorism essence (Freeman 2011).
Rahman (2008) states that the purpose of traditional money laundering is to legitimize their criminal proceeds and conceal their illicit origins to facilitate their future use of funds whereas that of terrorist financing may be making use of their well legitimate funds for the purpose of illegitimate terrorism activities, operations, or attacks in the future. In terms of techniques, what money launders use to conceal their illicit origin of proceeds are similar to those used to obscure the sources of, as well as uses for, terrorist financing, such as wire transfers, smurfing, use of credit cards and underground banking systems, etc. Nonetheless, detecting terrorist financing is more difficult as compared to that of money laundering; only the ultimate use of funds for terrorism is illegitimate whereas the nature of funds may be well legitimate, which thoroughly reverses the traditional money laundering model and makes it difficult to apply AML measures to terrorist financing.

Furthermore, ACAMS (2016) states that charities and NPOs are vulnerable to be abused for terrorist financing due to their public trust. Evidence suggests that many charitable organizations are founded for the purpose of fund raising for terrorism with their seemingly normal operations. Terrorists may also take advantage of alternative remittance systems or informal value transfer systems (e.g. underground banking systems), such as Hawala, Hundi, etc., which are based on trust and outside the formal banking system to facilitate their fund transfers across jurisdictions with the anonymity feature and the lack of government scrutiny to evade detection. Additionally, it is suggested that the size of transactions involved in terrorist financing may be only small amounts below reporting threshold circulated via simple wire transfers among accounts of various persons, which also deepens the difficulties in detection and official scrutiny.
An effective way to combat terrorism is to disrupt their sources for fund raising, and thus terrorist organizations would be unsustainable with insufficient funds to support their daily operations and spending. Consequently, banking system is therefore obligated to establish and maintain an effective mechanism for identifying suspicious transactions associated with money laundering activities and terrorist financing to facilitate and further official scrutiny given that banking system is one of the most important and common vehicles for money laundering and terrorist financing due to its comparative advantages: convenience, accessibility, and security (ACAMS 2016; Rahman 2008).

Figure 3: A Simple Hawala Transaction Sample

Source: International Monetary Fund (IMF); KYC360
2.6. The Impacts of Money Laundering

The ultimate goal of money laundering is to comingle criminal proceeds into the financial system without restriction of borders and jurisdictions to legitimize their ill-gotten funds and obscure illicit origins. It is suggested that even well-developed global financial centers are vulnerable to money laundering activities as well due to their large volumes of transactions and various services provided. Accordingly, successive money laundering activities expose the global financial system to the circumstances of money laundering (ACAMS 2016). The International Monetary Fund (IMF) once estimated that the scale of money laundering lied between 2% to 5% of world GDP (Aluko 2012).

It is also common for money launderers to operate legitimate businesses as front companies to further comingling their criminal proceeds with legitimate funds to conceal their illicit origins. Moreover, these seemingly normal businesses controlled by criminal organizations have comparative advantage over other truly legitimate businesses, namely, they have plenty of illicit funds to support their businesses to compete with other competitors in the market by setting the prices of their products and services well below the market rates since their businesses are not established for profit maximizing but for the purpose of hiding their ill-gotten funds. Consequently, money laundering undermines state economic growth and financial stability since it distorts the real supply and demand of an economy, which further invalidates national economic policies with wrong decisions or mistakes as a result of the misleading macroeconomic statistics (ACAMS 2016; Aluko 2012).
On the other hand, ACAMS (2016) and Aluko (2012) mention that one of the predicate offenses of money laundering is tax evasion. Inevitably, money laundering also reduces government revenue and makes government tax collection even more difficult. As a result, raising the tax rates would often be the case to make up for the tax gap and government budget deficit, which is unfair to the honest taxpayers and would turn into a vicious circle resulting in economic instability as well. In the meanwhile, money laundering and terrorist financing also adversely affect the stability of financial institutions, and that is the reason why financial institutions are mandatory and responsible to establish and maintain an effective and adequate AML/CFT program. Once a country becomes recognized as a high-risk jurisdiction for money laundering, it will undoubtedly deteriorate a nation’s global reputation and result in dampening effect on foreign investments, and thus it diminishes global opportunities since its environment is not business-friendly—it involves extra scrutiny works with high costs—which will further damage national economic development.

Furthermore, ACAMS (2016) states that a high-risk or non-cooperative jurisdiction with critical deficiencies on its AML/CFT regimes would further expose the country to the risk of international sanctions. To combat money laundering and terrorist financing, some governmental bodies, such as the Office of Foreign Assets Control of the United States Department of Treasury (OFAC) or international organizations, such as the United Nations (UN), the European Union (EU), etc. may impose sanctions - both economic and trade sanctions - against foreign countries, entities, and individuals with high risk of money laundering and terrorist financing as counter-measures. OFAC imposes either targeted sanctions or comprehensive sanctions against foreign countries. Targeted sanctions prohibit transactions
with designated individuals, entities, and industries on the sanctions list whereas comprehensive sanctions prohibit all transactions with countries on the sanctions list. Consequently, the economic development of a country under international sanctions will be further deteriorated with no doubt since its cross-border economic activities are strictly limited or even fully prohibited. Therefore, a rigorous AML/CFT regime is essential to preventing a nation’s economy as well as its international reputation from the menace of money laundering and terrorist financing activities.

Figure 4: Global Sanctions Regimes 2016

Source: Council on Foreign Relations (CFR)
Table 1: Major U.S. Sanctions Violations Cases, 2009~2016

<table>
<thead>
<tr>
<th>Bank Name</th>
<th>Headquarters</th>
<th>Year</th>
<th>Fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>BNP Paribas</td>
<td>France</td>
<td>2014</td>
<td>US$8.9 Billion</td>
</tr>
<tr>
<td>Credit Agricole</td>
<td>France</td>
<td>2015</td>
<td>US$787 Million</td>
</tr>
<tr>
<td>Standard Chartered</td>
<td>UK</td>
<td>2012</td>
<td>US$667 Million</td>
</tr>
<tr>
<td>ING</td>
<td>Netherlands</td>
<td>2012</td>
<td>US$619 Million</td>
</tr>
<tr>
<td>Credit Suisse</td>
<td>Switzerland</td>
<td>2009</td>
<td>US$536 Million</td>
</tr>
<tr>
<td>ABN AMRO</td>
<td>Netherlands/UK</td>
<td>2010</td>
<td>US$500 Million</td>
</tr>
<tr>
<td>HSBC</td>
<td>UK</td>
<td>2012</td>
<td>US$375 Million</td>
</tr>
<tr>
<td>LLOYD’S</td>
<td>UK</td>
<td>2009</td>
<td>US$350 Million</td>
</tr>
<tr>
<td>Commerzbank</td>
<td>Germany</td>
<td>2015</td>
<td>US$342 Million</td>
</tr>
<tr>
<td>Bank of Tokyo - Mitsubishi</td>
<td>Japan</td>
<td>2014</td>
<td>US$315 Million</td>
</tr>
<tr>
<td>Barclays</td>
<td>UK</td>
<td>2010</td>
<td>US$298 Million</td>
</tr>
<tr>
<td>Deutsche Bank</td>
<td>Germany</td>
<td>2015</td>
<td>US$258 Million</td>
</tr>
<tr>
<td>Bank of Tokyo - Mitsubishi</td>
<td>Japan</td>
<td>2013</td>
<td>US$250 Million</td>
</tr>
<tr>
<td>Clearstream</td>
<td>Luxembourg</td>
<td>2014</td>
<td>US$152 Million</td>
</tr>
<tr>
<td>Royal Bank of Scotland</td>
<td>UK</td>
<td>2013</td>
<td>US$100 Million</td>
</tr>
</tbody>
</table>

Source: Council on Foreign Relations (CFR)

2.7. Where the Money is Hidden

The leak of the “Panama Papers” on April 3, 2016 revealed how politicians, public officials, criminals, and celebrities around the world have used secret offshore vehicles incorporated in tax havens worldwide by a Panama-based law firm Mossack Fonseca & Co – which helped the rich and powerful park their wealth in tax havens and offshore bank accounts or shell companies – over the past 40 years in an attempt for tax evasion, corruption, money laundering, sanctions.
evasion, hiding other activities, etc., which involved 11.5 million documents as well as more than 214,000 offshore entities, and some of the transactions involved in the documents could be traced back to the 1970s. The disclosure of the Panama Papers lifted the veil of secret money, involving top government officials, such as the Prime Minister of Iceland, the Former Prime Minister of Great Britain, the President of Argentina, high-level Chinese government officials, and the President of Russia (Mcgee 2016; O’Donovan, Wagner, and Zeume 2016; Trautman 2017). The ten most popular tax havens exposed in the Panama Papers revealed that almost one out of every two offshore legal entities were incorporated in the British Virgin Islands, followed by the second favorite jurisdiction – Panama – where Mossack Fonseca & Co is headquartered (International Consortium of Investigative Journalists (ICIJ); The Atlantic; Trautman 2017).

**Figure 5: The 10 Most Popular Tax Havens in the Panama Papers**

![Image showing the 10 most popular tax havens in the Panama Papers](image)

Source: Forbes; International Consortium of Investigative Journalists (ICIJ)
On the other hand, in 2015, the Financial Secrecy Index (FSI) published by the Tax Justice Network (TJN) named the most secretive jurisdictions around the world due to low taxes, tight secrecy laws, corporate transparency legislation, and lack of transparency of beneficial ownership (Newsweek U.S. Edition; SWI swissinfo.ch.). FSI is based on the weakness of financial regulation and the volume of transactions, which relies on a qualitative measure with a secrecy score and 15 secrecy indicators (SWI swissinfo.ch.; The Atlantic; World Economic Forum). Switzerland – which is the global leader in cross-border asset management with 28% of market share – has been ranked number one for financial secrecy for the third consecutive time, followed by Hong Kong, the United States, Singapore, and Cayman Islands, comprising the top five spots (SWI swissinfo.ch.; Tax Justice Network).

It is noted that if British Overseas Territories or crown dependencies, such as the Cayman Islands and Jersey were combined, the United Kingdom would occupy the top spot (SWI swissinfo.ch.; The Atlantic). Furthermore, it is also noted that the 2015 results of FSI do not align with the revelations in the Panama Papers. However, if the countries with the most active intermediaries disclosed in the Panama Papers are taken into consideration, the results will be somehow consistent since Mossack Fonseca & Co worked with intermediaries – including banks, law firms, accountants, etc. – in more than 100 countries worldwide, and their most active clients by number of offshore company incorporations were from Hong Kong, Switzerland, and the United Kingdom (ICIJ; The Atlantic). Meanwhile, many people were wondering why few Americans were named in the Panama Papers. In fact, U.S. states like Delaware and Nevada have recently become hubs for low taxes and corporate confidentiality, therefore, Americans don’t need to go to Panama since they have an onshore tax haven, which is as secretive as anywhere (The Atlantic; World Economic Forum).
Table 2: Financial Secrecy Index (FSI) – 2015 Results

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Jurisdiction</th>
<th>FSI Value</th>
<th>Secrecy Score</th>
<th>Global Scale Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Switzerland</td>
<td>1,466.1</td>
<td>73</td>
<td>5.625</td>
</tr>
<tr>
<td>2</td>
<td>Hong Kong</td>
<td>1,259.4</td>
<td>72</td>
<td>3.842</td>
</tr>
<tr>
<td>3</td>
<td>USA</td>
<td>1,254.8</td>
<td>60</td>
<td>19.603</td>
</tr>
<tr>
<td>4</td>
<td>Singapore</td>
<td>1,147.1</td>
<td>69</td>
<td>4.280</td>
</tr>
<tr>
<td>5</td>
<td>Cayman Islands</td>
<td>1,013.2</td>
<td>65</td>
<td>4.857</td>
</tr>
<tr>
<td>6</td>
<td>Luxembourg</td>
<td>817.0</td>
<td>55</td>
<td>11.630</td>
</tr>
<tr>
<td>7</td>
<td>Lebanon</td>
<td>760.2</td>
<td>79</td>
<td>0.377</td>
</tr>
<tr>
<td>8</td>
<td>Germany</td>
<td>701.9</td>
<td>56</td>
<td>6.026</td>
</tr>
<tr>
<td>9</td>
<td>Bahrain</td>
<td>471.4</td>
<td>74</td>
<td>0.164</td>
</tr>
<tr>
<td>10</td>
<td>United Arab Emirates (Dubai)</td>
<td>440.8</td>
<td>77</td>
<td>0.085</td>
</tr>
<tr>
<td>11</td>
<td>Macao</td>
<td>420.2</td>
<td>70</td>
<td>0.188</td>
</tr>
<tr>
<td>12</td>
<td>Japan</td>
<td>418.4</td>
<td>58</td>
<td>1.062</td>
</tr>
<tr>
<td>13</td>
<td>Panama</td>
<td>415.7</td>
<td>72</td>
<td>0.132</td>
</tr>
<tr>
<td>14</td>
<td>Marshall Islands</td>
<td>405.6</td>
<td>79</td>
<td>0.053</td>
</tr>
<tr>
<td>15</td>
<td>United Kingdom</td>
<td>380.2</td>
<td>41</td>
<td>17.394</td>
</tr>
<tr>
<td>16</td>
<td>Jersey</td>
<td>354.0</td>
<td>65</td>
<td>0.216</td>
</tr>
<tr>
<td>17</td>
<td>Guernsey</td>
<td>339.4</td>
<td>64</td>
<td>0.231</td>
</tr>
<tr>
<td>18</td>
<td>Malaysia (Labuan)</td>
<td>338.7</td>
<td>75</td>
<td>0.050</td>
</tr>
<tr>
<td>19</td>
<td>Turkey</td>
<td>320.9</td>
<td>64</td>
<td>0.182</td>
</tr>
<tr>
<td>20</td>
<td>China</td>
<td>312.2</td>
<td>54</td>
<td>0.743</td>
</tr>
<tr>
<td>21</td>
<td>British Virgin Islands</td>
<td>307.7</td>
<td>60</td>
<td>0.281</td>
</tr>
<tr>
<td>22</td>
<td>Barbados</td>
<td>298.3</td>
<td>78</td>
<td>0.024</td>
</tr>
<tr>
<td>23</td>
<td>Mauritius</td>
<td>297.0</td>
<td>72</td>
<td>0.049</td>
</tr>
<tr>
<td>24</td>
<td>Austria</td>
<td>295.3</td>
<td>54</td>
<td>0.692</td>
</tr>
<tr>
<td>25</td>
<td>Bahamas</td>
<td>273.1</td>
<td>79</td>
<td>0.017</td>
</tr>
</tbody>
</table>

Source: Tax Justice Network (TJN)
Figure 6: Top 10 Countries with the Most Active Intermediaries in the Panama Papers

Source: World Economic Forum; International Consortium of Investigative Journalists (ICIJ)
2.8. International Organizations on Money Laundering

2.8.1. United Nations Office on Drugs and Crime (UNODC)

United Nations Office on Drugs and Crime (UNODC) states that UNODC was set up in 1997 through a merger between the United Nations Drug Control Program and the Center for International Crime Prevention, which is a global leader in the counteraction against illicit drugs and international crime. UNODC is mandated to assist it members to fight against illicit drugs, crime and terrorism, and its work program is comprised of the following three pillars:

(1) To enhance the capability of its members in the fight against illicit drugs, crime and
terrorism through field-based technical cooperation projects.

(2) To increase knowledge and understanding of drugs and crime issues through research as well as analytical work and to augment the evidence base for policy and operational decisions.

(3) To assist its members to ratify as well as implement the relevant international treaties and develop domestic legislation on drugs, crime and terrorism, providing secretariat and substantive services to the treaty-based and governing bodies through normative work.

In addition to the three pillars of UNODC’s work program mentioned above, UNODC can also provide assistance in the following five areas associated with AML/CFT issues, including organized crime and trafficking, corruption, crime prevention and criminal justice reform, drug abuse prevention and health, and terrorism prevention.

2.8.2. Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) states that FATF was established in July 1989 by a G7 Summit in Paris, which is an independent inter-governmental body to examine and develop counter-measures for money laundering and terrorist financing. The FATF is mandated to set standards and promote effective implementation of legal, regulatory and operational measures in the fight against money laundering, terrorist financing, and other related threats to the integrity of the international financial system. Therefore, the FATF is a policy-making body, working to generate the necessary political will to bring about national legislative and regulatory reforms in these fields. The FATF has developed a series of Recommendations for combating money laundering and the terrorist financing, which are widely adopted all over the
world and recognized as the international AML/CFT standard. The FATF Recommendations were first issued in 1990, then revised in 1996, 2001, 2003 and 2012 respectively to ensure that they remain relevant and up-to-date, moreover, they are in an attempt to be of universal application. The FATF monitors its members’ progress in implementing necessary measures, reviews the techniques and counter-measures of money laundering and terrorist financing, and promotes the adoption and implementation of appropriate measures worldwide. The FATF works to identify national-level vulnerabilities with the objective to protect the global financial system against misuse by money laundering and terrorist financing in cooperation with other international stakeholders.
Table 3: The FATF Recommendations

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Assessing Risks &amp; Applying a Risk-</td>
<td>21</td>
<td>Tipping-Off and Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Based Approach</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>National Cooperation and</td>
<td>22</td>
<td>Designated Non-Financial Businesses</td>
</tr>
<tr>
<td></td>
<td>Coordination</td>
<td></td>
<td>and Professions (DNFBPs): Customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Due Diligence</td>
</tr>
<tr>
<td>3</td>
<td>Money Laundering Offence</td>
<td>23</td>
<td>DNFBPs: Other Measures</td>
</tr>
<tr>
<td>4</td>
<td>Confiscation and Provisional Measures</td>
<td>24</td>
<td>Transparency and Beneficial Ownership</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>of Legal Persons</td>
</tr>
<tr>
<td>5</td>
<td>Terrorist Financing Offence</td>
<td>25</td>
<td>Transparency and Beneficial Ownership</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>of Legal Arrangements</td>
</tr>
<tr>
<td>6</td>
<td>Targeted Financial Sanctions Related</td>
<td>26</td>
<td>Regulation and Supervision of Financial</td>
</tr>
<tr>
<td></td>
<td>to Terrorism &amp; Terrorist Financing</td>
<td></td>
<td>Institutions</td>
</tr>
<tr>
<td>7</td>
<td>Targeted Financial Sanctions Related</td>
<td>27</td>
<td>Powers of Supervisors</td>
</tr>
<tr>
<td></td>
<td>to Proliferation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Non-Profit Organizations</td>
<td>28</td>
<td>Regulation and Supervision of DNFBPs</td>
</tr>
<tr>
<td>9</td>
<td>Financial Institution Secrecy Laws</td>
<td>29</td>
<td>Financial Intelligence Units</td>
</tr>
<tr>
<td>10</td>
<td>Customer Due Diligence</td>
<td>30</td>
<td>Responsibilities of Law Enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and Investigative Authorities</td>
</tr>
<tr>
<td>11</td>
<td>Record Keeping</td>
<td>31</td>
<td>Powers of Law Enforcement and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Investigative Authorities</td>
</tr>
<tr>
<td>12</td>
<td>Politically Exposed Persons</td>
<td>32</td>
<td>Cash Couriers</td>
</tr>
<tr>
<td>13</td>
<td>Correspondent Banking</td>
<td>33</td>
<td>Statistics</td>
</tr>
<tr>
<td>14</td>
<td>Money or Value Transfer Services</td>
<td>34</td>
<td>Guidance and Feedback</td>
</tr>
<tr>
<td>15</td>
<td>New Technologies</td>
<td>35</td>
<td>Sanctions</td>
</tr>
<tr>
<td>16</td>
<td>Wire Transfers</td>
<td>36</td>
<td>International Instruments</td>
</tr>
<tr>
<td>17</td>
<td>Reliance on Third Parties</td>
<td>37</td>
<td>Mutual Legal Assistance</td>
</tr>
<tr>
<td>18</td>
<td>Internal Controls and Foreign</td>
<td>38</td>
<td>Mutual Legal Assistance: Freezing</td>
</tr>
<tr>
<td></td>
<td>Branches and Subsidiaries</td>
<td></td>
<td>and Confiscation</td>
</tr>
<tr>
<td>19</td>
<td>Higher-Risk Countries</td>
<td>39</td>
<td>Extradition</td>
</tr>
<tr>
<td>20</td>
<td>Reporting of Suspicious Transactions</td>
<td>40</td>
<td>Other Forms of International</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cooperation</td>
</tr>
</tbody>
</table>

Source: Financial Action Task Force (FATF)
2.8.3. Asia/Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG) states that APG is headquartered in in Sydney, Australia, which was established in 1997 in Bangkok, Thailand. The APG is an autonomous and cooperative global organization consisting of 41 members and a number of global and regional observers. APG members and observers are dedicated to the effective implementation and enforcement of internationally accepted AML/CFT standards, particularly the FATF Forty Recommendations. Additionally, the APG provides assistance to its members to better utilize resources to counter money laundering and terrorist financing through establishing national coordination mechanisms. The APG has the following five primary functions:

(1) Mutual Evaluations

The APG conducts mutual evaluations to determine its members’ compliance with global AML/CFT standards through a peer review system. APG mutual evaluations are comprised of a desk-based review of its members’ AML/CFT regimes and an on-site visit to its members by other APG members and the APG Secretariat. The APG has conducted two rounds of mutual evaluations since 1997, and the third round of mutual evaluations have been conducted since 2014 in accordance with the FATF’s revised 2012 standards and 2013 methodology, consisting of an assessment of the “technical” compliance of its members’ AML/CFT systems in compliance with the FATF Recommendations as well as the “effectiveness” of their AML/CFT regimes. Furthermore, Taiwan will undergo the third round of mutual evaluations in the fourth quarter of 2018.
(2) Technical Assistance and Training

The APG provides bi-lateral and donor-agency technical assistance and training in the Asia/Pacific region for the purpose of improving its members’ compliance with the international AML/CFT standards.

(3) Typologies Research

The APG has been devoted to research and analysis of typologies and methods of money laundering and terrorist financing in order to provide its members and the general public with the up-to-date and relevant trends, methods, risks and vulnerabilities of both financial and non-financial institutions to these criminal activities.

(4) Global Policy Development

The APG proactively takes part in the international network of FATF-style regional bodies (FSRBs) for participation and contribution of policy development in compliance with the global AML/CFT standards.

(5) Private Sector Engagement

The APG provides the private sectors with the up-to-date AML/CFT information and keep them posted on the global AML/CFT developments. Moreover, the APG also provides the private sectors with a forum to facilitate them to engage with the APG in the fight against money laundering and terrorist financing.
Table 4: APG Members List

<table>
<thead>
<tr>
<th>Afghanistan</th>
<th>Mongolia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Myanmar</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>Nauru</td>
</tr>
<tr>
<td>Bhutan, Kingdom of</td>
<td>Nepal</td>
</tr>
<tr>
<td>Brunei Darussalam</td>
<td>New Zealand</td>
</tr>
<tr>
<td>Cambodia</td>
<td>Niue</td>
</tr>
<tr>
<td>Canada</td>
<td>Pakistan</td>
</tr>
<tr>
<td>China, People's Republic of</td>
<td>Palau</td>
</tr>
<tr>
<td>Cook Islands</td>
<td>Papua New Guinea</td>
</tr>
<tr>
<td>Fiji</td>
<td>Philippines</td>
</tr>
<tr>
<td>Hong Kong, China</td>
<td>Samoa</td>
</tr>
<tr>
<td>India</td>
<td>Singapore</td>
</tr>
<tr>
<td>Indonesia</td>
<td>Solomon Islands</td>
</tr>
<tr>
<td>Japan</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>Korea, Republic of Korea (South Korea)</td>
<td>Chinese Taipei</td>
</tr>
<tr>
<td>Lao People's Democratic Republic</td>
<td>Timor-Leste</td>
</tr>
<tr>
<td>Macao, China</td>
<td>Tonga</td>
</tr>
<tr>
<td>Malaysia</td>
<td>United States of America</td>
</tr>
<tr>
<td>Maldives</td>
<td>Vanuatu</td>
</tr>
<tr>
<td>Marshall Islands, Republic of</td>
<td>Vietnam</td>
</tr>
</tbody>
</table>

Source: Asia/Pacific Group on Money Laundering (APG)
2.8.4. The Egmont Group of Financial Intelligence Units

The Egmont Group of Financial Intelligence Units states that The Egmont Group is a united body consisting of 154 Financial Intelligence Units (FIUs), which is mandated to provide a platform to securely exchange expertise as well as financial intelligence against money laundering and terrorist financing. This is especially relevant since FIUs are uniquely positioned to collaborate and support national and international efforts to combat money laundering and terrorist financing, which are a trusted gateway for sharing and exchanging financial information domestically and globally in line with international AML/CFT standards. In addition, the Egmont Group has made efforts to support its global partners and other stakeholders to well implement the resolutions and statements authorized by the United Nations Security Council, the G20 Finance Ministers, and the Financial Action Task Force (FATF). The Egmont Group could not only enhance its members’ work by improving their understanding of money laundering and terrorist financing risks among its stakeholders, but also be able to establish operational experience for considerations of policy making, including AML/CFT implementation as well as AML/CFT reforms. The Egmont Group facilitates and prompts sharing and exchanging financial intelligence around the world, which has been recognized as one of the most important counter-measures for the global efforts on combating money laundering and terrorist financing, and Financial Intelligence Units (FIUs) worldwide are obligated by global AML/CFT standards to share and exchange financial information as well as engage in global collaboration.
2.8.5. The Wolfsberg Group

The Wolfsberg Group states that The Wolfsberg Group was established in 2000 at the Château Wolfsberg in Switzerland, which is an association consisting of 13 international banks – including Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank, and UBS – in an attempt to develop frameworks and guidance for financial crime risk management, particularly in association with Know-Your-Customer (KYC) and AML/CFT policies. The Wolfsberg AML Principles for Private Banking were first published in 2000, then revised in 2002 and 2012 respectively to ensure that they remain up-to-date and relevant. Since the first set of AML Principles was issued, the Wolfsberg Group has published a wide range of documents, including Due Diligence Questionnaire for correspondent banks, the form of Principles, Guidance, Frequently Asked Questions (FAQs), Statements, etc. Materials issued by the Wolfsberg Group – such as Wolfsberg AML Questionnaire comprised of 27 questions, Statement on the Financing of Terrorism, AML Principles for Correspondent Banking, Guidance on a Risk Based Approach for Managing Money Laundering Risks, FAQs on Politically Exposed Persons (PEPs), Trade Finance Principles, Guidance on Anti-Bribery & Corruption Compliance Programs, etc. – are designed to provide financial institutions (FIs) with an industry perspective on effective management of financial crime risks in accordance with global AML/CFT standards.
3. Anti-Money Laundering Legislation in Taiwan

In response to the global trends for combating money laundering, Taiwan enacted the Money Laundering Control Act (MLCA) on October 23, 1996, which was the first dedicated law in Asia for the purpose of anti-money laundering, then revised in 2003, 2006, 2007, 2008, 2009, and 2016 respectively (Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice). However, Taiwan’s efforts on combating money laundering became less effective over time since its subsequent amendments focused more on criminal prosecution than keeping up with international standards. As a result, APG deemed Taiwan’s AML system non-compliant with FATF standards in 2007, then Taiwan was downgraded to a follow-up watch list in the subsequent audit in 2011. After the audit in 2011, Taiwan remained on the APG follow-up watch list since some of the issues in the banking and regulatory system were fixed or partially fixed at more of a form instead of substance level (Executive Yuan, Republic of China (Taiwan); TheNewsLens). Fortunately, Taiwan was taken off from the APG 10-member watch list on July 20, 2017 with its ongoing efforts in the fight against money laundering and terrorist financing – including legislation and counter-measures – over the past few years, which brought Taiwan into line with global standards (Executive Yuan, Republic of China (Taiwan); TheNewsLens).

Mega Bank New York Branch was fined by the New York State DFS Examination at a penalty of US$180 million (NT$5.7 billion, in equivalent) for violations of the BSA/AML on August 19, 2016 (Mega Financial Holding Co., Ltd. 2016), which has reinforced the significance of a vigorous AML/CFT regime. Additionally, the violation incident of Mega Bank New York Branch implied that Taiwanese banking industry has not yet well implemented the relevant
regulations, reporting requirements, and compliance regimes of the BSA/AML, which not only undermined the brand image of Mega Bank itself but also deteriorated Taiwan’s international reputation (Ministry of Foreign Affairs, Republic of China (Taiwan), Taipei Liaison Office in the RSA), which was caused by Taiwanese public sector’s insufficient legislation and surveillance. In light of the violation incident of Mega Bank New York Branch as well as to prepare for the third round of the APG mutual evaluations in the fourth quarter of 2018, Anti-Money Laundering Office (AML Office) was established under the Executive Yuan on March 16, 2017 to integrate Taiwan’s AML policies and directions staffed by experts from both public and private sectors. Moreover, the Anti-Money Laundering Division – part of the Ministry of Justice’s Investigation Bureau – is Taiwan’s financial intelligence unit (FIU), as required in the FATF 40 Recommendations serving as a national center for the receipt and analysis of suspicious activity reports (Focus Taiwan; International Financial Law Review (IFLR)).

Furthermore, International Financial Law Review (IFLR) mentions that the most significant amendments to the MLCA came into effect in Taiwan on June 28, 2017, which was approved by the Legislative Yuan on December 28, 2016 with a six-month period of preparation offered. The newly amended MLCA consists of the following new requirements and mechanisms:

(1) Expansion of the Definition of Money Laundering

The newly amended MLCA expands the definition of money laundering to include broader types of ML activities in compliance with the FATF 40 Recommendations and other international standards.
(2) Expansion of the Scope of Predicate Offenses

In line with the FATF 40 Recommendations, the newly amended MLCA was revised to include all predicate offenses punished by more than a six-month imprisonment under Taiwan Criminal Code and other criminal laws, which were not included in the old version of the MLCA.

(3) Adding the New Concept of Designated Non-Financial Businesses and Professions

The newly amended MLCA imposes the due diligence, record-keeping and reporting obligations not only on financial institutions (FIs) but also on designated non-financial businesses and professions (DNFBPs) – including jewelry retail businesses, attorneys, notaries, accountants, land administration/registration agents and real estate brokers – when providing certain services in accordance with the FATF 40 Recommendations. Additionally, the amendments were revised to include the financial leasing service provider in the scope of FIs.

(4) Introduction to the Concept of Politically Exposed Persons (PEPs)

The newly amended MLCA includes the concept of the PEPs as well as defined the scope of the PEPs to further monitor the ML activities of high-risk politicians. In addition, the “family members” and “close associates” of the PEPs are also subject to the same regulatory requirements as the PEPs.

(5) Customer Due Diligence (CDD)

In line with the newly amended MLCA, the FIs and DNFBPs are required to undertake CDD process – including identifying and verifying the identity of the customer as well as their substantive beneficial owners – when establishing a new business relationship with them and
report any transactions above the reporting threshold, which is currently NT$500,000
(US$16,666, in equivalent) in Taiwan.

(6) New Confiscation Scheme

The amendments permit Taiwanese customs to confiscate the cash, securities, gold, items
without the required declaration carried into/out of Taiwan exceeding certain thresholds, and
suspicious items used for ML activities or above certain thresholds. Cross-border delivery of
cash, securities, items via goods delivery, courier, and mailing service are also subject to the
same confiscation requirements. Additionally, the amendments permit the customs and the
court to confiscate such proceeds or instrumentalities without criminal conviction required.

(7) International Cooperation

In accordance with the newly amended MLCA, Taiwanese government may enter into treaties
or agreements with foreign governments, institutions or global organizations on the reciprocity
principle for the cooperation in the fight against ML activities. Moreover, the information
regarding declarations, reports or investigation results collected under the MLCA may be also
shared based on the reciprocity principle in response to request for assistance made by foreign
governments, institutions or global organizations.

In addition, Taiwan also enacted the Terrorism Financing and Prevention Law, which came into
effect on July 27, 2016 as part of its efforts in the fight against money laundering. The new law
imposes penalties for the financing of terrorist activities, organizations, and individuals as well
as emphasizes that those violations are classified as “serious crimes” under the MLCA (Executive Yuan, Republic of China (Taiwan); TheNewsLens). TheNewsLens states that combating money laundering and terrorist financing does not rely on government legislation only, it also calls for raising public awareness of ML/TF crimes and involves the public cooperation with the government in the fight against money laundering and terrorist financing.

In terms of the banking industry, The Bankers Association of the Republic of China also amended “Template of Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism of Banks” and established “Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program” in accordance with the “Money Laundering Control Act,” “Counter-Terrorism Financing Act,” and “Directions Governing Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Sector and Electronic Payment Institutions as well as Electronic Stored Value Card Issuers” to help Taiwanese banking industry to well develop an effective AML/CFT program to meet the international standards as well as to earn a better reputation through the APG mutual evaluations in the fourth quarter of 2018.
Figure 8: Timeline for Anti-Money Laundering Legislation in Taiwan

- 1996: Taiwan enacted the Money Laundering Control Act (MLCA), which was the first dedicated AML law in Asia.
- 2007: The APG deemed Taiwan’s AML system non-compliant with the FATF standards.
- 2011: Taiwan remained on the APG follow-up watch list.
- 2016: Taiwan enacted the Terrorism Financing and Prevention Law.
- The violation incident of Mega International Commercial Bank New York Branch occurred.
- 2017: Taiwan enacted the Terrorism Financing and Prevention Law.
- The most significant amendments to the MLCA came into effect.
- Taiwan was taken off from the APG 10-member watch list.

Sources: Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice; Executive Yuan, Republic of China (Taiwan); IFLR; Mega Financial Holding Co., Ltd.
4. Case Study of Mega International Commercial Bank

4.1. Overview of Mega International Commercial Bank

Mega International Commercial Bank Co., Ltd. (Mega Bank) states that Mega Bank is a merger between The International Commercial Bank of China (ICBC) and Chiao Tung Bank (CTB), effective in August, 2006. Both banks have their long histories in Taiwanese banking system. In order to enlarge the scale and scope of the businesses as well as increase the market share, ICBC and CTB formally merged into one bank under the name of Mega International Commercial Bank Co., Ltd. in August, 2006 for the purpose of synergy creation.

Mega International Commercial Bank is one of the fully-owned subsidiaries of Mega Financial Holdings Co., Ltd. As of December 31, 2016, Ministry of Finance, R.O.C., National Development Fund, Executive Yuan, R.O.C., Chunghwa Post Co., Ltd., and Bank of Taiwan Co., Ltd. hold 20.47 percent of the shares of Mega Financial Holdings Co., Ltd. In other words, Mega Bank is a private bank but state controlled. As of the end of 2016, Mega Bank had 108 domestic branches, and 22 branches, 5 sub-branches, and 5 representative offices abroad. Moreover, Mega Bank has fully-owned subsidiaries in Thailand and Canada as well, bringing the total number of overseas branches and offices amounted to 39 in total. Meanwhile, Mega Bank has 5,543 employees and an aggregate paid-in capital of NTS85.362 billion. It is believed that Mega Bank is an important banking institution in the international financial system (NYDFS 2016).
Figure 9: Organization Chart of Mega International Commercial Bank

Source: Mega International Commercial Bank
Table 5: Major Institutional Shareholders of Mega International Commercial Bank

<table>
<thead>
<tr>
<th>Name of the Institutional Shareholders</th>
<th>Top Shareholders (Percentage of Shares Ownership)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mega Financial Holding Co., Ltd.</td>
<td>Ministry of Finance, R.O.C. (8.40%)</td>
</tr>
<tr>
<td></td>
<td>National Development Fund, Executive Yuan, R.O.C. (6.11%)</td>
</tr>
<tr>
<td></td>
<td>Chunghwa Post Co., Ltd. (3.50%)</td>
</tr>
<tr>
<td></td>
<td>Fubon Life Insurance Co., Ltd. (3.47%)</td>
</tr>
<tr>
<td></td>
<td>Cathay Life Insurance Co., Ltd. (2.98%)</td>
</tr>
<tr>
<td></td>
<td>Bank of Taiwan Co., Ltd. (2.46%)</td>
</tr>
<tr>
<td></td>
<td>Nan Shan Life Insurance Co., Ltd. (1.80%)</td>
</tr>
<tr>
<td></td>
<td>China Life Insurance Co., Ltd. (1.69%)</td>
</tr>
<tr>
<td></td>
<td>Pou Chen Corporation (1.41%)</td>
</tr>
</tbody>
</table>

Source: Mega International Commercial Bank 2016 Annual Report

According to The Banker, issued July 2017, Mega Bank is ranked No. 164 among the top 500 banks in the world in terms of tier one capital, which is the second highest ranking among Taiwanese banks. In general, Mega Bank is a continuously profitable bank with a sound financial structure and stability. Net operating income/Net income (expressed in thousands of NT dollars) of Mega Bank from 2014 to 2016 were NT$50,680,532/NT$25,990,682, NT$49,815,491/NT$25,708,445, and NT$45,180,643/NT$19,009,961 respectively (Mega International Commercial Bank). The significant decrease in its net income in 2016 was attributed to the penalty payment in the amount of US$180 million (NT$5.7 billion, in equivalent) for the violation incident of its New York Branch.
Table 6: Taiwanese Banks Ranked Among the Top 500 Banks in the World in Terms of Tier One Capital

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Taiwan</th>
<th>World</th>
<th>Strength (Tier One Capital)</th>
<th>Size (Assets)</th>
<th>Rank (Taiwan)</th>
<th>Rank (World)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>US$m</td>
<td>US$m</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>155</td>
<td>155</td>
<td>8,249</td>
<td>109,007</td>
<td>2</td>
<td>150</td>
</tr>
<tr>
<td>2</td>
<td>164</td>
<td>164</td>
<td>7,722</td>
<td>92,043</td>
<td>4</td>
<td>182</td>
</tr>
<tr>
<td>3</td>
<td>196</td>
<td></td>
<td>6,087</td>
<td>147,623</td>
<td>1</td>
<td>129</td>
</tr>
<tr>
<td>4</td>
<td>210</td>
<td></td>
<td>5,497</td>
<td>97,165</td>
<td>3</td>
<td>174</td>
</tr>
<tr>
<td>5</td>
<td>214</td>
<td></td>
<td>5,432</td>
<td>76,905</td>
<td>8</td>
<td>216</td>
</tr>
<tr>
<td>6</td>
<td>225</td>
<td></td>
<td>5,005</td>
<td>77,728</td>
<td>6</td>
<td>207</td>
</tr>
<tr>
<td>7</td>
<td>233</td>
<td></td>
<td>4,881</td>
<td>64,949</td>
<td>9</td>
<td>238</td>
</tr>
<tr>
<td>8</td>
<td>239</td>
<td></td>
<td>4,710</td>
<td>77,028</td>
<td>7</td>
<td>215</td>
</tr>
<tr>
<td>9</td>
<td>250</td>
<td></td>
<td>4,232</td>
<td>57,870</td>
<td>11</td>
<td>257</td>
</tr>
<tr>
<td>10</td>
<td>258</td>
<td></td>
<td>4,104</td>
<td>82,716</td>
<td>5</td>
<td>194</td>
</tr>
<tr>
<td>11</td>
<td>262</td>
<td></td>
<td>3,956</td>
<td>50,960</td>
<td>12</td>
<td>275</td>
</tr>
<tr>
<td>12</td>
<td>272</td>
<td></td>
<td>3,825</td>
<td>62,048</td>
<td>10</td>
<td>247</td>
</tr>
<tr>
<td>13</td>
<td>279</td>
<td></td>
<td>3,731</td>
<td>46,855</td>
<td>13</td>
<td>302</td>
</tr>
<tr>
<td>14</td>
<td>286</td>
<td></td>
<td>3,609</td>
<td>46,592</td>
<td>14</td>
<td>304</td>
</tr>
<tr>
<td>15</td>
<td>366</td>
<td></td>
<td>2,587</td>
<td>46,377</td>
<td>15</td>
<td>305</td>
</tr>
<tr>
<td>16</td>
<td>465</td>
<td></td>
<td>1,902</td>
<td>26,826</td>
<td>16</td>
<td>447</td>
</tr>
</tbody>
</table>

Source: The Banker, Top 1000 World Banks 2017
Figure 10: Financial Statistics for Mega International Commercial Bank, 2014 ~ 2016

Source: Mega International Commercial Bank

4.2. Violation Incident of Mega Bank New York Branch

Mega Bank is licensed by the NYDFS to operate a foreign bank branch in New York State. At the time of violation incident of its New York Branch happened, Mega Bank held total assets of approximately US$103 billion, and assets held by its New York Branch were approximately US$9 billion. Mega Bank New York Branch has operated a correspondent banking business for many years (NYDFS 2016).
Mega Bank and its New York Branch signed a Consent Order with the NYDFS on August 19, 2016. The Consent Order concluded that Mega Bank and its New York Branch failed to maintain an effective and compliant anti-money laundering compliance program and failed to comply with regulations and reporting issues of the BSA/AML. Mega Bank was fined at a penalty of US$180 million (NT$5.7 billion, in equivalent) as a result of having an inadequate and deficient compliance program (Mega Financial Holding Co., Ltd. 2016). The New York State DFS Examination discovered numerous deficiencies in Mega Bank New York Branch's compliance function, which was extremely troubling and can be concluded into the following six aspects (NYDFS 2016):

(1) The New York Branch's Poor Internal Controls

(i) The compliance structure at Mega Bank New York Branch was significantly flawed given that the compliance and operational functions were comingled causing a conflict of interest arose from the dual conflicting responsibilities of certain compliance personnel with little familiarity with U.S. regulatory requirements. Similarly, its Chief Compliance Officer (CCO) had insufficient knowledge of U.S. BSA/AML and the Office of Foreign Assets Control of the United States Department of Treasury (OFAC) requirements.

(ii) New York Branch's transaction monitoring systems and policies were seriously deficient. Compliance personnel failed to periodically review surveillance monitoring filter criteria and thresholds. Moreover, plenty of documents relied upon in the transaction monitoring process remained un-translated from Chinese, preventing effective examination by the NYDFS. Additionally, its procedures provided little guidance associated with the reporting requirements for continuing suspicious activity, and it neither filed a Suspicious Activity Report (SAR) nor maintained necessary documentation to support decisions made by
compliance personnel during the investigation of alerts researched by compliance staff.

(iii) New York Branch's BSA/AML policies and procedures lacked consistency and unity of purpose. Also, New York Branch acts as a correspondent bank of other affiliates of Mega Bank, but it failed to conduct adequate reviews of these correspondent banking activities.

(2) Suspicious Activity Involving Mega Bank's Panama Branches

Mega Bank operates two branches in Panama, located in Panama City and the Colon Free Trade Zone (FTZ) respectively. Panama has been recognized as a high-risk jurisdiction for money laundering and is no longer subject to the Financial Action Task Force's monitoring process. Mega Bank New York Branch failed to treat transactions running between itself and Panama Branches with the highest level of due diligence and scrutiny, and its Head Office has been indifferent to the risks regarding such transactions indicative of possible money laundering and other suspicious activity, which indicated that both Mega Bank and its New York Branch lacked the understanding of the need for a vigorous compliance infrastructure.

(3) Failure to Conduct Adequate Customer Due Diligence

Mega Bank New York Branch neither followed established policies and procedures to undertake enhanced due diligence for high-risk customers nor conduct periodic reviews for medium and low-risk customers to identify any increase in the risk level of such customers. In addition, it failed to undertake adequate customer due diligence for its counterparties (e.g. foreign financial institutions) in correspondent banking business. Furthermore, a great number of customer files lacked adequate information on beneficial ownership, which seriously compromises its Know-Your-Customer (KYC) processes.
(4) Inadequate Risk Assessment Policies and Procedures

Mega Bank New York Branch's overall risk assessments were also found seriously flawed with insufficient methodology since its risk assessment for BSA/AML issues lacked a complete review for its customers, products, services, geographic locations served, etc. and not conducted on a yearly basis as recommended. Likewise, its risk assessment for OFAC concerns was found to be flawed for similar reasons.

(5) Lack of Diligent Oversight by the Head Office

Mega Bank New York Branch failed to forward its quarterly compliance meeting minutes to Head Office compliance, however, it substituted a meeting agenda for proper meeting minutes. Furthermore, its report on quarterly compliance meetings lacked sufficient information on the compliance environment and SARs filed during prior periods, preventing Head Office compliance from properly evaluating the compliance adequacy of its New York Branch. Similarly, plenty of documents remained untranslated from Chinese to English, which precluded effective examination by the NYDFS.

(6) Troubling and Dismissive Response to the DFS Examination

In Mega Bank’s response to the DFS examination report, it has refuted numerous examination findings. Mega Bank and its New York Branch declared that certain types of transactions do not constitute suspicious activity. Moreover, Mega Bank neither acted proactively to remedy its acute deficiencies as directed in the DFS examination report nor has taken sufficient steps to demonstrate its resolution to improve the quality of its compliance program.
According to the Consent Order, in addition to the US$180 million penalty paid within ten days of executing the Consent Order, Mega Bank shall engage a compliance consultant designated by the NYDFS to consult and oversee its New York branch for improving its compliance function. Also, Mega Bank shall retain an independent monitor designated by the NYDFS to monitor all the transactions for the past three years (Mega International Commercial Bank; NYDFS 2016). In the aftermath of the violation incident occurred, Mega Bank was also fined by the FSC in Taiwan at a penalty in the amount of NT$10 million (US$315,000, in equivalent), moreover, the FSC mandated the ouster of six executives of Mega Bank and banned it from establishing new oversea branches (TheNewsLens).
4.3. Taiwanese Banking Industry Review

Banking industry in Taiwan is extremely competitive since it is over-banking as a result of the deregulation of establishment of new banks in early 1990s. Reviewing the development of Taiwanese banking industry, it can be divided into the following three stages (Hung and Luo 2016; 邱莉婷 2011):
(1) Stage One: 1949 ~ 1960

In this initial period of Taiwanese banking system, the financing channels were gradually established.

(2) Stage Two: 1961 ~ 1989

In order to meet the needs of industrial development, the financial market - including stock market, bond market, and foreign exchange market - was also established in this period. Before the deregulation in 1991, banking industry in Taiwan was highly regulated and existed barriers to entry. Most of the banks were owned or controlled by government, few of them were privately-owned banks.

(3) Stage Three: 1990 ~ Present

In this period, in order to keep pace with the international trends of market liberalization and globalization, Taiwanese banking industry implemented a series of deregulations, including encouraging foreign banks to set up branches in Taiwan, allowing the establishment of new banks, allowing the privatization of public owned banks to enhance their competitiveness, and allowing the establishment of financial holding corporations to enlarge the scope of their businesses by providing a wider range of products, services, etc.

As of the end of September 2017, Taiwan has 38 domestic banks with 3,421 domestic branches. According to The Banker, issued July 2017, 16 Taiwanese banks are ranked among the top 500 banks in the world in terms of tier one capital (Financial Supervisory Commission, Banking
Bureau; The Banker 2017).

Table 7: Number of Banking Institutions in Taiwan, as of the end of Sept., 2017

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Head Office</td>
<td>Domestic Branches</td>
<td>Head Office</td>
</tr>
<tr>
<td>Central Bank of the Republic of China (Taiwan)</td>
<td>1</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Domestic Banks</td>
<td>38</td>
<td>3,421</td>
<td>38</td>
</tr>
<tr>
<td>Local Branches of Foreign Banks*</td>
<td>26</td>
<td>35</td>
<td>27</td>
</tr>
<tr>
<td>Local Branches of Mainland Chinese Banks*</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Credit Cooperatives</td>
<td>23</td>
<td>266</td>
<td>23</td>
</tr>
<tr>
<td>Credit Departments of Farmers' Association</td>
<td>283</td>
<td>820</td>
<td>283</td>
</tr>
<tr>
<td>Credit Departments of Fishermen's Association</td>
<td>28</td>
<td>44</td>
<td>28</td>
</tr>
<tr>
<td>Total</td>
<td>373</td>
<td>4,589</td>
<td>373</td>
</tr>
</tbody>
</table>

Source: Financial Supervisory Commission, Banking Bureau

* Total head office excludes foreign banks.
4.4. The Impacts of AML/CFT on the Operations of Mega Bank

4.4.1. Reform a Business Culture of Compliance and Internal Control

Mega Bank New York Branch was fined by the New York State DFS Examination at a penalty of US$180 million (NT$5.7 billion, in equivalent) for violations of the BSA/AML on August 19, 2016 (Mega Financial Holding Co., Ltd. 2016). With the boosting sales over the past few years, Mega Bank tended to put overemphasis on the business performance and was unaware of the importance of compliance and internal control, which made it unable to keep up with the trends to meet international standards associated with AML/CFT. As a result of the deficiencies, its New York Branch failed to identify and report a few questionable transactions involved in suspicious money laundering activities via remittance transactions, which led to the violation incident (Mega International Commercial Bank 2017). Global banking system has gradually recovered since the 2008 Financial Crisis, and thus Mega Bank as well as other Taiwanese banks have been in pursuit of outstanding performance at the expense of legal compliance. The violation incident of Mega Bank New York Branch has undoubtedly reinforced the magnitude importance and effect of a business culture of compliance and internal control while in the past few people treated that as a critical issue.

In the past, businesses tend to neglect their compliance department with insufficient staff since it is not a revenue-generating unit. With the emerging violation incidents and penalties occurred in recent years in the Taiwanese banking industry, evidence suggests that compliance function must be independent from other business functions, and banking institutions should allocate adequate resources and sufficient manpower to their compliance department even though it will
not bring in revenue. Furthermore, banking institutions should hire independent and dedicated compliance personnel to further their surveillance function and avoid the dual conflicting responsibilities for risk mitigation. Therefore, top management has to realize the magnitude of compliance as well as internal control and continuously emphasize the importance of compliance and internal control to their employees along with periodical employee training to enhance their understanding. Moreover, banking institutions should establish new KPI (Key Performance Indicators) criteria to avoid the contradiction that a business unit has high performance ranking but with serious compliance deficiencies (吳瓊佩 2014). In the aftermath of the violation incident of Mega Bank New York Branch, 2017 is the year of transformation and action for Mega Bank with no doubt. With top management’s emphasis, it is the first priority for Mega Bank to build up a work place under a business culture of compliance and internal control in order to reform its business culture from “performance-orientated” to “compliance-orientated” to regain its brand image and international reputation (Mega International Commercial Bank 2017; Mega International Commercial Bank).
4.4.2. Establish an Effective AML/CFT Program

Singapore has been deemed as a global financial center in Asia/Pacific region with the lowest domestic crime rates in the world, and it is also a member of both the FATF and APG. According to the fourth round FATF mutual evaluation report issued in September, 2016, the FATF assessed that Singapore has a strong framework for AML/CFT in terms of the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Singapore’s AML/CFT system through the on-site visit from 17 November 2015 to 3 December 2015, which has made significant enhancements to its AML/CFT regime since its last FATF assessment in
2008 (MAS; FATF and APG 2016). In terms of the banking institutions, above everything, all banks in Singapore are required to establish and implement their own AML/CFT policies in line with their ML/TF risks, size, nature and complexity of their business and operations both in Singapore and overseas. Moreover, banks shall communicate these to all of their employees to ensure that they well understand their AML/CFT policies and educate them how to implement these into their business (ABS 2015).

Therefore, this thesis will undertake the AML/CFT regime in Singapore – The Association of Banks in Singapore (ABS) Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism, which is in compliance with the Monetary Authority of Singapore (MAS) Notice and Guidelines – as a benchmark to discuss the counter-measures to combat ML/TF in Mega Bank as well as the whole banking industry in Taiwan in terms of building an effective AML/CFT program, including Know Your Customers (KYC), Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Sanctions Screening, Suspicious Activity Reporting (SAR), and Continuous Employee training.

**Know Your Customers (KYC)**

Alford (1993) states that The Basle Committee on Banking Supervision adopted a Statement of Principles regarding money laundering in 1988, which urged the banking sector to well establish a “Know-Your-Customer (KYC)” process for customer identification. It stated that the public confidence of the banking system would be undermined if any crime happened in association with negligence or direct involvement of the banking institutions, and thus bank
supervisors should be responsible to prevent the criminal use of the banking system. A sound KYC program is critical to protecting the soundness and integrity of the banking system, meanwhile, it also can keep the banks far away from criminals.

According to the Association of Banks in Singapore (ABS) Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism – in compliance with the Monetary Authority of Singapore (MAS) Notice and Guidelines – banking institutions should assess the risks of each customer to determine the true identity of its customers before establishing a new business relationship with each other under a certain customer acceptance policy in line with its risk preference and tolerance. KYC is a critical process for the banking institutions to well understand the background of their customers, including their customer’s products, services, location, ownership structure, etc. to identify the high risk customers associated with money laundering and terrorist financing in order to further cooperate with law enforcement authorities (Alford 1993; ABS 2015). Alford (1993) also mentions that a successive KYC regime will discourage the use of the banking system by criminals since banks require the evidence of the true identity of customers as well as their businesses, and thus criminals will exploit other vehicles with least requirements to facilitate their money laundering. In other words, the KYC process can ensure the safety of the banking system and protect it from criminal activities.

Before the violation incident of Mega Bank New York Branch, Taiwanese banking industry usually failed to well implement its KYC process due to the over-banking phenomenon, which exposed the banking system in Taiwan to the high risk of misuse by money launderers. In line
with the ABS Guidelines on AML/CFT, fully implementing the KYC process is a key to establish an effective AML/CFT program for the banking institutions. To establish an effective AML/CFT regime under the Risk-Based Approach (RBA) adopted by the FATF Forty Recommendations in 2012 (ABS 2015; FATF 2014), a sound KYC process initiates with the Customer Identification Program (CIP) involving collecting and verifying the information of the new customers, purpose of opening the account, source of funds, and verifying the related documents, followed by Customer Due Diligence (CDD) for low-risk customers and Enhanced Due Diligence (EDD) for higher-risk customers, which enables the banking system to well understand the true identity and risks of their customers for customer selection through risk assessment to protect the soundness and integrity of the whole banking system and prevent it from money laundering activities and terrorist financing (ABS 2015).
Figure 13: AML KYC Onboarding Lifecycle

According to the ABS Guidelines on AML/CFT, banking institutions should adopt the Risk-Based Approach (RBA) in line with the FATF Recommendations while conducting the risk assessment of their customers. The RBA refers to the process driving a dynamic framework to address risk. The RBA would guide the customer due diligence (CDD) assessment and highlight high-risk concerns when evaluating the money laundering and terrorist financing risk of a new customer. Banking institutions generally assess the money laundering and terrorist financing
risk of a customer and assign a risk rating (e.g. low, medium, and high) to their customers at the CDD stage. Once a customer is onboarding, banks should use an RBA to not only review their transactional behavior and activities but also update the customer’s risk assessment. The CDD assessment may differ from customer types - CDD in investment banking may differ from that in private banking - and a great deal of other factors. In accordance with RBA, jurisdictions may allow simplified CDD measures to be applied for lower-risk customers, such as government entities, listed companies, etc. The CDD process is not only limited to sanctions screening but also business assessment, negative information, and politically exposed persons (PEPs) screening. A sound CDD program should consist of the following seven elements (ACAMS 2016; MAS 2015; ABS 2015):

(1) Customer Identification

To avoid establishing business relationship with shell companies and mitigate the risk of abuse by money laundering and terrorist financing activities, it is essential for banks to understand the true identity of their customers, including the substantive beneficial owners, owner structure, and business types. In accordance with the FATF standards, banks should not only identify customers but also verify their identity. Additionally, banks should find out the source of funds and purpose of the account. The banking institutions have to update CDD information after a periodic review or a material trigger event, whichever is earlier to ensure that the customer’s information, data, documents, and risk assessment they previously maintained remain relevant and up-to-date.
(2) Profiles

Banks should create a transaction and activity profile for each of their customers. The profile should include sufficient information to facilitate future reviews between the anticipated and actual account activity to enable banks to identify suspicious activity based on comparing the actual activity to what the bank knows about the customer and nature of their business.

(3) Customer Acceptance

Banks should establish and implement their own customer acceptance policies and procedures to identify the types of customer with inherent or potential higher risks of money laundering and terrorist financing in line with the bank’s risk assessment. In addition, the bank’s customer acceptance policy should define circumstances under which the bank should not accept a new customer or should terminate a currently existing business relationship with the customer.

(4) Risk Rating

Banks should conduct risk assessment before establishing business relationship with a new customer with periodic review, or when a material trigger event occurs, whichever is earlier. A great deal of risk factors should be considered when determining risk (e.g. customer type, products and services, transaction type, and locations). Except for such a single factor constituting an illicit activity, no single factor alone should be used to determine risk. The banking institutions in Singapore are required to review their risk assessment at least once every two years or when a material trigger event occurs, whichever is earlier.
(5) Monitoring

Monitoring is one of the essential methods to effectively manage the bank’s money laundering and terrorist financing risk, and thus banks should have appropriate systems in place to detect suspicious transactions. Banking institutions should monitor the customer’s accounts and transactions in accordance with their risk level.

(6) Investigation

Banks should perform investigation and examination of unfamiliar customer or unusual account activity, which should be consistent with anticipated activity for each customer in line with their occupation or business type.

(7) Documentation

Banks should keep the record and document the findings as evidence to prove the actions they did perform. Banks should ensure that everything obtained at the CDD stage is documented. Both in Taiwan and Singapore, banking institutions are required to keep records of customer accounts for at least five years after termination of the business relationship or completion of such transactions, which is in accordance with the FATF 40 Recommendations (FATF 2012; ABS 2015; The Bankers Association of the Republic of China 2017).

There are no set standards to conduct the CDD process. Banking institutions have to know their customers and further understand the purpose of their accounts via customer identification followed by customer verification. Each bank should establish its own CDD regime in
accordance with its size, nature of business, risk preference or tolerance, etc. Furthermore, each bank should implement its own policies and procedures to control and mitigate the money laundering and terrorist financing risks arose from the deferred completion of customer verification, including (ABS 2015):

- Having limited financial services available to the customer.
- Limiting the amount of the transactions undertaken by the customer.
- Closely monitoring the customer’s transactions until completing the verification.

Once a bank is not able to complete customer verification at the CDD stage, the bank should terminate or not establish a business relationship with the customer, and determine whether it is necessary to file a SAR (Suspicious Activity Report). Certainly, the bank’s management must be kept posted on such occurrences.

**Enhanced Due Diligence (EDD)**

According to the ABS Guidelines on AML/CFT, banks should undertake the Enhanced Due Diligence (EDD) for high-risk customers identified at the CDD stage, which requires additional documents as well as more reviews to perform the further assessment. Such additional documents and reviews may also be triggered by other controls in the bank’s AML/CFT program, such as the occurrence of material trigger events or alerts from suspicious activities identified through transaction monitoring. In line with the international standards, banks should undertake the EDD process once a year or when a material trigger event occurs, whichever is earlier. The principle and procedure of the EDD assessment is not identical to a bank – EDD in
corporate banking may differ from that in retail banking – the EDD assessment usually differs from the business segments of the bank (ABS 2015). The EDD assessments should consist of the following risk factors (ACAMS 2016):

(1) Customer Risk Factors

- The business relationship is established under an unusual phenomenon, such as that the customer failed to explain the geographic distance between the bank and the customer.
- Non-resident customers, such as walk-in customers with different nationalities.
- Companies being used to be personal asset-holding vehicles.
- Companies can issue bearer shares with nominee shareholders.
- Cash-intensive businesses, such as restaurants, retail stores, parking lots, etc.
- The company’s ownership structure appears unusual or over complex as compared to the nature of its business.

(2) Country or Geographic Risk Factors

- Countries identified as high-risk jurisdictions or having inadequate AML/CFT regimes.
- Countries subject to sanctions imposed by the OFAC, EU, UN, etc.
- Countries identified as having a higher risk of drug trafficking, human/arms smuggling, corruption, fraud, financial crimes, or other criminal activities.
- Countries or geographic areas identified as funding/supporting the terrorist activities, or having designated terrorist organizations operating within the country.
- Countries sharing a common border and are known to have smuggling or illicit transactions.
• Geographic regions identified as having a higher risk of money laundering or financial crimes within the country.

(3) Product, Service, Transaction or Delivery Channel Risk Factors

• Private banking business.
• Cash based transactions with anonymity.
• Business relationships or transactions with non-face-to-face customers.
• Payment received from unknown or unrelated third parties.

In Taiwanese banking industry, banks are required to conduct the EDD program annually (The Bankers Association of the Republic of China 2017) whereas the CDD program is usually conducted every 2 to 5 years or when a material trigger event occurs, whichever is earlier. The rule may vary in different countries and banks. High-risk customers would expose the banking institutions to riskier circumstances of misuse by money laundering or terrorist financing activities, and thus high-risk customers and their transactions should be reviewed more strictly at account opening stage and more frequently during their business relationships with the bank as compared to low-risk customers for risk mitigation. Once if necessary, closely account and transaction monitoring should be taken to detect suspicious activities and transactions, if any, and report to supervisory authorities and law enforcement agency (ABS 2015).
Sanctions Screening

In accordance with the ABS Guidelines on AML/CFT, sanctions screening is essential for identifying and mitigating the money laundering and terrorist financing risks. Banking institutions should have an effective screening system in place with database covering the sanctions lists of UN, OFAC, EU, HM Treasury (i.e. The UK government’s economic and finance ministry), HKMA (Hong Kong Monetary Authority), MAS, etc. and the local sanctions lists to detect any individuals and entities who are sanctioned or suspected to get involved in money laundering or terrorist financing activities and document the results of screenings as well as assessments of potential matches. Banks should periodically review their database of sanctioned parties to ensure that they maintain up-to-date sanctions lists, set lower screening thresholds since a 100% match setting is not acceptable, and thus an assessment of potential matches is necessary. Before establishing a business relationship with a new customer, banks should conduct sanctions screening to ensure that the customer and their related parties are not sanctioned. If a bank has a positive hit against a sanctions list, it should halt all action on the account and assess whether it is required to freeze the funds or other assets of the sanctioned parties without delay and prior notice. Meanwhile, banks should also consider filing a SAR, reassessing the customer’s risk rating and whether to terminate the business relationship with the customer (ABS 2015; ACAMS 2016).

To mitigate the money laundering and terrorist financing risks and enhance sanction compliance, Mega Bank has conducted sanctions screening for all of local US-dollar transactions since August, 2017 given that it acts as the settlement bank of local US dollars in Taiwan, and these
US-dollar transactions would ultimately be settled in its New York Branch, which is in the US and subject to the surveillance of the US authorities concerned. Therefore, Mega Bank conducts day-to-day sanctions screening to check for the possibility of money laundering and terrorist financing and hits against sanctions lists to meet the international standards (Commercial Times).

**Suspicious Activity Reporting (SAR)**

In line with the ABS Guidelines on AML/CFT, a Suspicious Activity Report (SAR) is made when a bank knows or has reason to suspect that funds or wealth is directly or indirectly linked to criminal activities. Ongoing monitoring and review of customer’s accounts and transactions enables banks to identify suspicious activity, eliminate false positives and report promptly genuine suspicious transactions. Therefore, banks should have adequate and effective systems in place to undertake daily transaction monitoring and report suspicious activity. The system should be risk-based given that there are hundreds of thousands of transactions in the banking institutions every day. The determinant risk factors should contain customer’s firm’s size, location, frequency and size of transactions, nature of its business, types and geographic location of its customers, etc.

Banks should report suspicious activity to the appropriate law enforcement agency and supervisory authorities without notifying any parties involved in the transaction reported and under investigation. Banks are mandatory to file a SAR and timely submit to the relevant law
enforcement agency and supervisory authorities to ensure prompt disclosures where funds or wealth suspected to be the criminal proceeds remain in the account. Additionally, disclosure of such suspicious activity is not treated as a breach of “banking secrecy” against customers under the statutory protection for the filing bank as well as its employees.

Bank should consider filing a SAR if it receives any negative information about a customer regarding criminal activities. Filing a SAR not only facilitates investigation by the authorities but also urges the bank to take preventive measures against the customer. Once suspicion has been raised related to a business relationship or an account, in addition to filing a SAR, appropriate action should be taken to adequately mitigate the bank’s risk of misuse by criminal activities, including a review of the risk level of the customer, account, or even the business relationship itself. Appropriate action - such as cooperation with law enforcement agency and supervisory authorities - should be approved by the appropriate level of management to determine how to handle the business relationship with the customer, taking all relevant risk factors into account (ACAMS 2016; Bank for International Settlements (BIS) 2017; ABS 2015).

Continuous Employee Training

According to the ABS Guidelines on AML/CFT, a vigorous AML/CFT infrastructure should also include an effective AML/CFT training program. Banks are required to institute periodical training programs to educate their employees on AML/CFT issues. In addition to explaining the relevant AML/CFT laws and regulations, an effective AML/CFT training program should
also consist of the bank’s AML/CFT policies and procedures for risk mitigation as well as the common methods and typologies used for money laundering and terrorist financing. In addition, banks should train their employees to detect potential money laundering or terrorist financing activities as well as educate them about what to do if they encounter such transactions. A bank should adopt a training program in accordance with its size, nature of its business, etc. In addition, different business segments should adopt adequate training programs tailored to their job functions and responsibilities. In spite of seniority, all staff should be trained, including directors and management, and thus banks should provide appropriate training programs aimed at different levels. Periodical refresher training should be undertaken every one or two years for existing employees, and training for new employees should be undertaken as soon as possible to ensure that all staff is familiar with the bank’s AML/CFT policies and procedures with regular updates. Also, banks are required to maintain training records for internal and external auditing (ACAMS 2016; BIS 2017; ABS 2015).
Figure 14: Elements for Establishing an Effective AML/CFT Program

Sources: The Association of Banks in Singapore (ABS)
5. Conclusion and Recommendation

Taiwan is not a popular place for either international drug dealers and gun runners to launder their ill-gotten proceeds or terrorists to seek financing. Taiwan’s AML issues are more related to tax evasion since wealthy people in Taiwan usually move their funds offshore in an attempt to avoid taxes (TheNewsLens). AML/CFT management in Taiwanese banking industry has been passive and reluctant, focusing more of a form instead of substance level (TheNewsLens; 張迺佳 2016) since it brings in tons of compliance costs at the same time it is an obstacle to a bank’s business expansion given the over-banking problem in Taiwan. The violation incident of Mega Bank New York Branch has raised the awareness of both public and private sectors in association with AML/CFT. Moreover, Taiwan will undergo the third run of the APG mutual evaluations in the fourth quarter of 2018. If Taiwan is deemed as seriously deficient or non-compliant in AML/CFT infrastructure by international organizations, it will not only deteriorate the national reputation but also undermine the international trade since the cross-border fund transfers will be restricted and/or even rejected (張迺佳 2016).

Given that there are not enough AML/CFT professionals in the banking industry in Taiwan since few people treated it as a critical issue in the past, Taiwanese banking industry is supposed to hire external consultants with familiarity with local and international laws and regulatory requirements both in Taiwan and overseas to develop and oversee the bank’s compliance function. Furthermore, banks should hire well experienced compliance specialists from foreign-owned banks or those who were fined by the NYDFS previously since they must have made a lot of effort with a great progress in their compliance program in order to learn from their past
experience and further cultivate the bank’s own AML/CFT employees by continuous training. Above all, banks should establish an effective AML/CFT program with an appropriate global policy tailored to their ML/TF risks, size, nature and complexity of their business and operations both in Taiwan and overseas and set up an independent department to handle the AML/CFT issues of the bank with adequate and sufficient resources and employees. It is not possible for a bank with insufficient resources and employees to well implement the AML/CFT regime, which is also a common problem occurs in Taiwanese banking industry due to the cost saving since compliance will bring in no revenue but costs.

AML/CFT issues in Taiwan have been neglected for far too long to comply with the international standards. Therefore, the first step to combat ML/TF is to establish a culture of AML/CFT and educate the public by raising public awareness of AML/CFT and teaching them how to comply and cooperate with the government and financial institutions in the fight against ML/TF. Owning to the over-banking problem, Taiwanese banking industry is so competitive that banks tend to provide the most convenient services to their customers to maintain and attract more customers to keep profitable, and that is also one reason why Taiwanese banking industry is reluctant to well implement and comply with the AML/CFT regime since it is costly and harmful to their business expansion. A lesson learned from the US$180 million penalty, non-compliance with international AML/CFT standards is much more expensive given that it can be seen from Table 8, NYDFS fined international banking institutions at massive penalties every year in the past five years. Therefore, not having an effective AML/CFT program will expose the banks to the risk of being fined at huge penalties and further do harm to the bank’s brand image as well as the nation’s international reputation.
Table 8: Major General Enforcement Actions of NYDFS for Violations of BSA/AML (Including Tax Evasion), 2013~2017

<table>
<thead>
<tr>
<th>Bank Name</th>
<th>Headquarters</th>
<th>Year</th>
<th>Fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deutsche Bank AG and Deutsche Bank AG New York Branch</td>
<td>Germany</td>
<td>2017</td>
<td>US$425 Million</td>
</tr>
<tr>
<td>Commerzbank AG and Commerzbank AG New York Branch</td>
<td>Germany</td>
<td>2015</td>
<td>US$610 Million</td>
</tr>
<tr>
<td>Bank Leumi Le-Israel, B.M. and Bank Leumi USA</td>
<td>Israel</td>
<td>2014</td>
<td>US$130 Million</td>
</tr>
<tr>
<td>The Bank of Tokyo-Mitsubishi UFJ, Ltd. and The Bank of Tokyo-Mitsubishi UFJ, Ltd. New York Branch</td>
<td>Japan</td>
<td>2014</td>
<td>US$315 Million</td>
</tr>
<tr>
<td>Standard Chartered Bank and Standard Chartered Bank New York Branch</td>
<td>UK</td>
<td>2014</td>
<td>US$300 Million</td>
</tr>
<tr>
<td>Credit Suisse AG and Credit Suisse AG New York Representative Office</td>
<td>Switzerland</td>
<td>2014</td>
<td>US$715 Million</td>
</tr>
<tr>
<td>The Bank of Tokyo-Mitsubishi UFJ, Ltd. and The Bank of Tokyo-Mitsubishi UFJ, Ltd. New York Branch</td>
<td>Japan</td>
<td>2013</td>
<td>US$250 Million</td>
</tr>
</tbody>
</table>

Source: New York State Department of Financial Services (NYDFS)
Furthermore, with the emphasis of governments worldwide, not only the banks having overseas branches in the United States but also those with overseas branches in other foreign countries will face the challenge of being fined at huge penalties for not having an effective AML/CFT program since it involves international cooperation to win the fight against AML/CFT.

Table 9: Number of Overseas Branches of Domestic Banks, as of the end of Sept., 2017

<table>
<thead>
<tr>
<th>Countries</th>
<th>Institutions</th>
<th>Total</th>
<th>Branches</th>
<th>Representative Offices</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grand Total</td>
<td></td>
<td>478</td>
<td>144</td>
<td>42</td>
<td>292</td>
</tr>
<tr>
<td>Asian and Pacific area</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subtotal</td>
<td></td>
<td>402</td>
<td>109</td>
<td>41</td>
<td>252</td>
</tr>
<tr>
<td>Mainland China</td>
<td></td>
<td>76</td>
<td>29</td>
<td>3</td>
<td>44</td>
</tr>
<tr>
<td>Bahrain</td>
<td></td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td>42</td>
<td>7</td>
<td>-</td>
<td>35</td>
</tr>
<tr>
<td>Indonesia</td>
<td></td>
<td>14</td>
<td>-</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>India</td>
<td></td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td></td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>Cambodia</td>
<td></td>
<td>45</td>
<td>3</td>
<td>1</td>
<td>41</td>
</tr>
<tr>
<td>Hong Kong</td>
<td></td>
<td>71</td>
<td>20</td>
<td>3</td>
<td>48</td>
</tr>
<tr>
<td>Thailand</td>
<td></td>
<td>10</td>
<td>-</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Malaysia</td>
<td></td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Philippines</td>
<td></td>
<td>34</td>
<td>5</td>
<td>-</td>
<td>29</td>
</tr>
<tr>
<td>Vietnam</td>
<td></td>
<td>55</td>
<td>12</td>
<td>9</td>
<td>34</td>
</tr>
<tr>
<td>Singapore</td>
<td></td>
<td>12</td>
<td>12</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Lao PDR</td>
<td></td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Myanmar</td>
<td></td>
<td>13</td>
<td>1</td>
<td>12</td>
<td>-</td>
</tr>
<tr>
<td>Australia</td>
<td></td>
<td>12</td>
<td>11</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>Macau</td>
<td></td>
<td>3</td>
<td>3</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Korea</td>
<td></td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>European area</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subtotal</td>
<td></td>
<td>9</td>
<td>7</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td>Belgium</td>
<td></td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>French</td>
<td></td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>United Kingdom</td>
<td></td>
<td>6</td>
<td>5</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Netherlands</td>
<td></td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>North America area</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subtotal</td>
<td></td>
<td>64</td>
<td>25</td>
<td>1</td>
<td>38</td>
</tr>
<tr>
<td>Canada</td>
<td></td>
<td>9</td>
<td>2</td>
<td>-</td>
<td>7</td>
</tr>
<tr>
<td>U.S.A.</td>
<td></td>
<td>55</td>
<td>23</td>
<td>1</td>
<td>31</td>
</tr>
<tr>
<td>Center South America area</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subtotal</td>
<td></td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Panama</td>
<td></td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>African area</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subtotal</td>
<td></td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>South Africa</td>
<td></td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Source: Financial Supervisory Commission, Banking Bureau
Reference

English Reference:


Bank for International Settlements (2017), Sound Management of Risks Related to Money Laundering and Financing of Terrorism


FATF (2014), *Guidance for a Risk-Based Approach*, The Banking Sector, The Banking Sector

FATF and APG (2016), Anti-money laundering and counter-terrorist financing measures - Singapore, Fourth Round Mutual Evaluation Report


Krieger, Tim and Meierrieks, Daniel (2011), *Terrorist Financing and Money Laundering*, University of Freiburg


Mega Financial Holding Co., Ltd. (2016), Dodd-Frank Act Section 165(d), 2016 Resolution Plan, Part I: Public Section


Monetary Authority of Singapore (2015), Guidelines to MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism


New York State Department of Financial Services (2013), Consent Order to Bank of Tokyo Mitsubishi UFJ

New York State Department of Financial Services (2014), Consent Order to Bank Leumi

New York State Department of Financial Services (2014), Consent Order to Bank of Tokyo Mitsubishi UFJ

New York State Department of Financial Services (2014), Consent Order to BNP Paribas (BNPP)

New York State Department of Financial Services (2014), Consent Order to Credit Suisse AG

New York State Department of Financial Services (2014), Consent Order to Standard Chartered Bank, New York Branch

New York State Department of Financial Services (2015), Consent Order to Commerzbank
New York State Department of Financial Services (2016), Consent Order to Agricultural Bank of China Limited

New York State Department of Financial Services (2016), Consent Order to Intesa Sanpaolo S.p.A.

New York State Department of Financial Services (2016), Consent Order to Mega International Commercial Bank of Taiwan

New York State Department of Financial Services (2017), Consent Order to Deutsche Bank AG and Deutsche Bank AG New York Branch

O’Donovan, James, Wagner, Hannes F., and Zeume, Stefan (2016), *The Value of Offshore Secrets: Evidence from the Panama Papers*, INSEAD, Bocconi University, and University of Michigan

Rahman, Aspalella A. (2008), *An Analysis of the Malaysian Anti-Money Laundering Laws and Their Impact on Banking Institutions*, thesis for the degree of Doctor of Philosophy of Faculty of Law, The University of Western Australia


The Association of Banks in Singapore (2015), ABS Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism

The Banker (2017), Top 1000 World Banks 2017

The Bankers Association of the Republic of China (2017), Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program

The Bankers Association of the Republic of China (2017), Template of Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism of Banks

**Chinese Reference:**

吳瓊佩 (2014), 我國銀行法令遵循制度之研究，國立政治大學法學院法律科際整合研究所碩士學位論文。

邱莉婷 (2011), 我國金融服務業發展之回顧與展望，經濟研究第 11 期，pp. 171-197

張迺佳 (2016), 我國商業銀行洗錢防制與打擊資助恐怖主義法規範之問題與對策探討，國立政治大學法律學系碩士在職專班碩士學位論文。

**Reference Websites:**

Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice, Available at: https://www.mjib.gov.tw/EditPage/?PageID=3bf48af4-bfbe-41e3-9137-d908e16eb1cc

Asia/Pacific Group on Money Laundering (APG), Available at: http://www.apgml.org/about-us/page.aspx?p=91ce25cc-db8a-4249-9018-8bd1f6869162
http://www.apgml.org/about-us/page.aspx?p=ac38f87e-2341-43e6-84b2-4dbd6346f6c3

Chinatimes, Available at: http://www.chinatimes.com/newspapers/20160824000360-260102

Commercial Times, Available at: https://ctee.com.tw/News/ViewCateNews.aspx?newsid=155514&cateid=cjzc

Compliance Alert, Available at: http://www.calert.info/details.php?id=944
Council on Foreign Relations (CFR), Available at:
https://www.cfr.org/backgrounder/what-are-economic-sanctions

Executive Yuan, Republic of China (Taiwan), Available at:
http://english.ey.gov.tw/News_Hot Topic.aspx?n=5D67267C4F593FE7&sms=7F46BDB40CA63F10

Financial Action Task Force (FATF), Available at:
http://www.fatf-gafi.org/about/
http://www.fatf-gafi.org/about/whatwedo/

Financial Supervisory Commission, Banking Bureau, Available at:
https://www.banking.gov.tw/ch/home.jsp?id=157&parentpath=0,4&mcustomize=bstatistics_view.jsp&serno=201105120009

Focus Taiwan, Available at:

Forbes, Available at:

International Consortium of Investigative Journalists (ICIJ), Available at:
https://panamapapers.icij.org/graphs/
International Financial Law Review (IFLR), Available at:

International Monetary Fund (IMF), Available at:
KYC360, Available at:
https://kyc360.com/article/podcast-everyday-money-laundering/

Mega International Commercial Bank, Available at:
https://www.megabank.com.tw/other/event_01.asp?sno=810

Ministry of Foreign Affairs, Republic of China (Taiwan), Taipei Liaison Office in the RSA, Available at:

Monetary Authority of Singapore (MAS), Available at:

Newsweek U.S. Edition, Available at:

New York State Department of Financial Services (NYDFS), Available at:
http://www.dfs.ny.gov/about/eagen.htm

SWI swissinfo.ch., Available at:
https://www.swissinfo.ch/eng/secret-banking_switzerland-still-tops-financial-secrecy-index/41755204

Tax Justice Network (TJN), Available at:

The Atlantic, Available at:
The Egmont Group of Financial Intelligence Units, Available at: https://www.egmontgroup.org/en/content/about

The Wolfsberg Group, Available at: http://www.wolfsberg-principles.com/index.html

TheNewsLens, Available at: https://international.thenewslens.com/article/79235


World Economic Forum, Available at: https://www.weforum.org/agenda/2016/04/5-charts-on-the-panama-papers-leaks