# ANTI-MONEY LAUNDERING ANNUAL REPORT, 2001

The Investigation Bureau, Ministry of Justice
Republic of China

Address all inquires to:
Money Laundering Prevention Center, Investigation Bureau, Ministry of Justice
74 Chung-Hwa Rd., Hsin-Tien City
Taipei County, Taiwan 231
R.O.C.
E-Mail: mlpc@mjib.gov.tw

**Publication Data**

Anti-money laundering annual report. -- Taipei:
The Investigation Bureau, Ministry of Justice, R.O.C.,2001.

p.92 ; 26 x 19 cm.
ISBN 957-01-1160-7
1. Money laundering investigation-Taiwan (China) -annual report.
I. China. Ministry of Justice. Investigation Bureau.
HV8079.M64

---

Editor: Dan T.E.CHAN, Gilbert LEE
English revisor: Brian L. Kennedy
Printed in Taiwan, Republic of China

# Foreword

Crime and money laundering are really two sides of the same coin, and the relationship between them is extremely close. When criminals obtain illegal income, in order to escape detection by the authorities they have to make use of financial institutions (or other institutions) to conceal the income, so as to prevent the authorities from discovering its source. At the same time, when a criminal organization is raising the funds needed to commit a crime, in order to prevent the authorities from using the flow of funds to trace the identity of the persons who provided the funding, a variety of money laundering channels will be used to protect these persons by keeping their identity secret. In the case of the terrorist attacks which occurred in the USA on September 11th, 2001, in securing the funds for the operation the terrorist organization concerned had made use of various different foundations and legally-established companies in order to conceal the identity of the mastermind behind the operation.

Traditionally, when investigating a crime the judicial and police authorities have generally thought in terms of arresting the suspect and then either sending them for trial or closing the case. However, in the case of the September 11th terrorist attacks it was clear that this model was not applicable. Soon after the attacks occurred, the Financial Action Task Force (FATF) approved eight special recommendations with respect to tracing the funds used in terrorist activities, and the US Department of the Treasury convened a special meeting of the Egmont Group in Washington in late-October regarding the tracing of terrorist funds, with the aim of working together to detect these funds. It thus appears that using money laundering mechanisms to trace the masterminds behind criminal activity through the flow of funds has become an important weapon for the prevention of major crimes.

In line with the FATF's policy of performing mutual evaluation between members, an appraisal team from the Asia/Pacific Group on Money Laundering (APG), headed by the APG's Secretary General Mr. Rick McDonell, visited Taiwan over the period March 26 - 29, 2001 to conduct a mutual evaluation of Taiwan's money laundering prevention mechanism in terms of the legal system, supervision of financial institutions, and implementation. The results of the mutual evaluation were discussed at the APG's 5th Annual Meeting held in Kuala Lumpur in May 2001; it was agreed that money laundering prevention work in Taiwan had already reached international standards, whether in terms of

systems or actual implementation. Besides the achievements noted above in the area of international collaboration, the Investigation Bureau's performance in other areas of money laundering prevention work (including the revision of the Money-laundering Control Act and the provision of relevant strategic recommendations, helping the judicial and police authorities to investigate suspicious funds, and handling reports of suspected money laundering transactions received from financial institutions) over the past year has been very impressive.

Public opinion polls show that the general public as a whole supports the government's current efforts to eliminate money politics. Over the next year, therefore, the Investigation Bureau's money laundering prevention work will focus mainly on the three main elements in the campaign by the Ministry of Justice to eliminate money politics - uncovering criminal activity, combating corruption, and investigating bribery. It is hoped that the Bureau will continue to receive from all quarters the same support for its money laundering prevention work that it has received in the past, so that we can all work together to establish a clean government and a harmonious society.

Cherng - Maw YEH

Director General

Investigation Bureau

Ministry of Justice

May 2002

# Editor's Note

I. Objective of this Edition

This Annual Report compiles the anti-money laundering prevention work enforced throughout the whole year in 2001. In light of the analyzed information and statistics and studied crime-committing methods related to money-laundering, Money Laundering Prevention Center (MLPC) of The Investigation Bureau, Ministry of Justice (MJIB) was able to grasp the trend in the commission of crime for the year in question. As a result, appropriate responsive measures concerning anti-money laundering had been drafted in a timely manner. In addition, there are two articles by our colleagues and one special contribution by a pundit published in this Edition, all concerning the subject of money laundering.

II. Contents of this Edition

A. The text of this Annual Report contains seven interrelated parts.

1. Organization Overview
2. Overview of Job Performance
3. Case Study
4. Review of the Past and Outlook for the Future
5. Essays

Appendix

B. Compilation of this Annual Report is based on related information and statistics available at the MLPC and prosecuted money-laundering cases released by district prosecutor's offices.

III. Explanatory notes for this Edition

Where for each unit used in this edition, the year shall be the calendar year, suspicious activity reports (SAR's) shall be the number of cases filed, money-laundering cases arraigned by district prosecutor's offices shall be the number of cases prosecuted, and dollar amount shall be in the New Taiwan Dollars. Where special circumstances are involved, notes are explained in respective tables (figures).

IV. Publication of the Annual Report this year is a bit of a rash work and we are in no position to expect the publication to be perfect in such a circumstance. We therefore welcome your comments, if any, so that we may improve it in our next edition.

# Content

## Part Four:Review of the Past and Outlook for the Future

# Tables

# Figures

# Part One

# Organization Overview

By Article 8(1) of the Money Laundering Control Act (MLCA), for any transaction suspected to be money laundering, the financial institution concerned is required to report the case to the designated agency. In pursuance of Clause 3 of the same Article, "'The designated agency'' and 'the scope and procedure of reports handled' referred to in Clause 1 above shall be determined by the Ministry of Finance (MOF), after consultation with the Ministry of the Interior (MOI), the Ministry of Justice (MOJ) and the Central Bank of China (CBC)". Shortly after, on January 21st 1997, the Ministry of Finance convened a meeting of all concerned agencies, including the CBC, MOJ, MOI, Ministry of Transportation and Communications (MOTC), etc., to jointly discuss the MLCA authorizing the MOF to hold meetings with regard to draft of related matters. The meeting reached the following three conclusions:

1. The "certain amount" of currency transaction as referred to under Article 7 of the MLCA shall be over NT$1.5 million or its equivalent in foreign currency in cash receipts or payments, including the total amount transacted on the same business day, or exchange of notes.

2. With respect to the procedure of customer's status identification and the method and duration of keeping on file the transaction record as referred to under Article 7 of the MLCA, it specifies that the financial institution must confirm the ID or passport that the customer presents for identification and enter in its books the information of the customer's name, date of birth, address, account number, amount of transaction, and ID number. However, if the financial institution is certain of the identity of the customer presenting the transaction in person, the procedure of identity confirmation may be exempted. Should the transaction be done by an attorney in fact, the financial institution is required to confirm the identity of the attorney in fact and, if necessary, the customer also. The financial institution must keep the record of identity confirmation and transaction voucher on file for 5 years.

3. Article 8(1) of the MLCA specifies that the financial institution must confirm the customer identity and keep on file transaction voucher of suspicious activity reports (SAR's) and report same to the designated agency. By law, the 'designated agency' referred to are the Investigation Bureau of MOJ, or MJIB. As to the 'the scope and procedure of reports handled', the financial institution must fill out the standardized form of SAR's and file the completed form with the MJIB in accordance with established rules. Whereas the primary function of the designated agency is to process the SAR's filed by financial institutions by establishing databases from which to compile and analyze the information so collected. Should further action be required as a result of the analysis, all concerned regulatory agencies should automatically come to the assistance of the MJIB. Needless to say, the concerned regulatory agencies should offer their assistance in the form of manpower and funding.

In response to the needs of related operations required with the handling of SAR's filed by financial institutions following the enactment of the MLCA, the MJIB organized on January 29th,

1997 a preparatory office called the "Money Laundering Prevention Center" (MLPC) to integrate related business and administrative units and prepare to become operational. Apart from aggressive planning on personnel alignment, purchase of equipment and selection of office space, etc., the MLPC also devoted considerable energy to the drafting of the Guidelines for Establishment of MLPC for submission to the Executive Yuan via the Ministry of Justice.

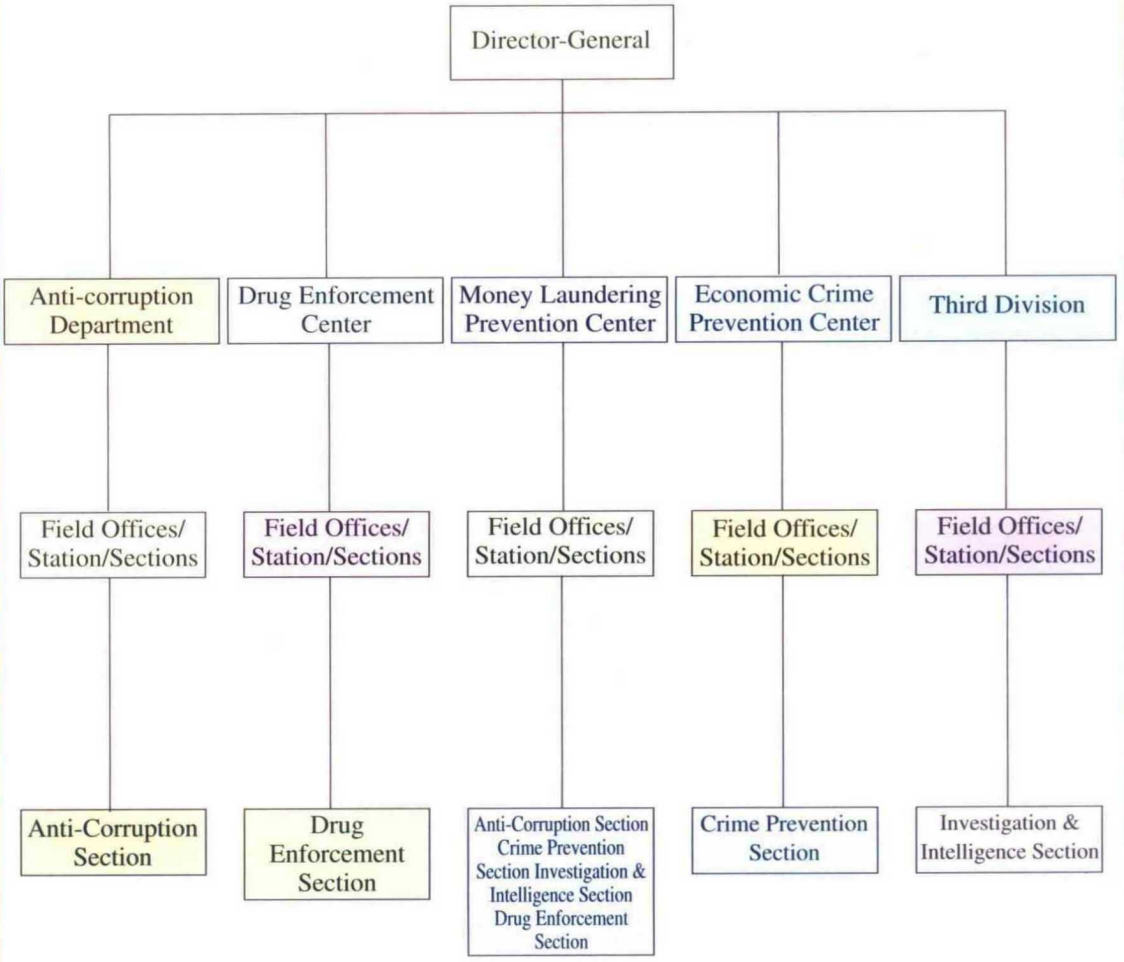
The aforementioned Guidelines were approved by the Executive Yuan on April 21, 1997 per letter re Tai-86-Fa-Tze-#155595, authorizing the MJIB to set up the mission-oriented MLPC under its supervision. Thus, the Money Laundering Prevention Center formally went into operation on April 23, 1997, the same day when the MLCA went into effect.

According to Article 2(1) of the MJIB's table of organization, the MJIB is responsible for "investigation and prevention of matters endangering national security and violating national interest", whereas Article 2(2) specifies that "the above-mentioned matters related to investigation and prevention shall be determined by the Executive Yuan." On October 30, 1998, the Executive Yuan approved per directive re Tai-87-Fa-Tze-#53381 to include "matters related to money laundering prevention" as one of the nine functions of the MJIB.

The function for the Center is as follows:

1. To study strategies for money laundering prevention.
2. Handling and processing of Suspicious Activity Reports (SAR's) by financial institutions concerning suspicious transactions that might be intended for money laundering.
3. Collection, analysis, disposal and use of money laundering information.
4. To provide assistance in investigation of money laundering cases conducted by domestic law enforcement agencies and coordination, as well as liaison concerning provisions set forth in the Money Laundering Control Act.
5. Information exchange, exchange of personnel training and joint investigation of money laundering cases with foreign counterpart agencies. The joint investigation involves contact, planning, coordination and implementation.
6. Establishment and compilation of databases concerning money-laundering intelligence.

## Interactive Relations Between the MLPC and Other Units, Including Field Offices, within the MJIB



# Part Two

# Overview of Task Performance

## A. Research anti-money laundering stractegies

To meet the ever-changing and often innovative forms of criminal conduct, it has become necessary to amend from time to time the related money laundering prevention mechanisms. In view of the domestic money-laundering situation, we prepared a theme report entitled "Prevention of Money Laundering Crime and Measures Needed in Counter Actions" and in August presented it before the Executive Yuan's 10th Project Meeting of Enforced Social Security for discussion. The report lists the weaknesses of the existing domestic MLCA. These include failure of a third reading of the amendment bill at the Legislative Yuan, immature attitude of law enforcement agencies toward investigation of ill-gained funds, the underground money remittance channel that has become a blind spot of the MLCA, improved concept of money laundering required of employees in financial institutions, imperfect internal auditing practice, investigation dislocation caused by fictitious accounts, and gradually emerging new money laundering channels through non-financial institutions. The article also cites measures needed in counter actions that includes: speedy completion of the legislative process by concerted joint efforts, intensification of training law enforcement and judicial police, upgrade of enforcement capability in investigation of ill-gained funds, intensified investigation in underground money remittance channels, stopping of the blind spots of the MLCA and fund outflow, full-scale indoctrination of the money laundering concept among employees in financial institutions and implementation of internal auditing over businesses that may lead to money laundering. The article further recommends establishment of a database covering registration of foreign currencies by incoming and outgoing travelers, so as to enable law enforcement agencies to use the information to discover cross-border money laundering of ill-gained funds. In addition, the article suggests the Department of Taxation of the MOF open up its files of income by wage earners to inquiries by law enforcement agencies in order to facilitate investigations of criminal cases.

Following the September 11 terrorist attacks in New York City, and in view of the international trend in forming alliances to counterattack terrorist activities, we have mapped out measures needed in counter actions, taking into consideration the current status on the home front as to stoppage of fund movement by terrorist groups. The measures needed in counter actions suggested are from viewpoints of the legal aspect and the aspect of mechanism employment as well. Briefly, they are:

### 1. From the legal aspect

a. The existing laws appear to be totally incapable of keeping terrorist activities under control. As such, it is likely that domestic and international crime syndicates may use the legal loopholes to target Taiwan as a site for terrorist activities, thus challenging seriously our national security,

social order and the financial system, not to mention the image of our country. Consequently, draft of an anti-terrorist act should be the basis of domestic anti-terrorist mechanism and therefore the legislative process must start as soon as possible. In addition, resolutions passed in the United Nations in 1999 to prevent financial assistance to terrorists and "strike back against terrorists" per resolution 1373 (see Appendix I) of September 28, 2001 in the Security Council are suggested for reference in the draft of an anti-terrorist act as a response to the UN resolutions.

b. Amendment needed for the regulations concerning freezing of assets:

Seizure of objects as specified under The Code of Criminal Procedure and Special Provisions of the Criminal Code mostly is limited to evidence and income derived from commission of the crime. In foreign countries, seizure of objects, similar to the provisional seizure under civil law in our country, is a conservative measure under public law, i.e., instantly freezing funds in a specific account and complete related properties. In our country, however, we have never cited such cases in rendered judgments. To facilitate international cooperation in the future and solidify anti-terrorist laws as well as fill the gap of our inadequate seizure provisions, it has become necessary that we need to establish our seizure law so that we may work together with foreign countries in this area.

c. Draft amendment to the MLCA remains in the legislative process at the Legislative Yuan

In an attempt to strengthen the legal system where the dirty money or "black gold" may be checked by law, the Executive Yuan proposed a draft amendment to the MPCA and forwarded the draft to the Legislative Yuan for legislation. The draft passed the review on May 2, 2001 by the joint meeting of the judicial committee and the finance committee. Despite the draft's expansion of the scope of major crimes, it nonetheless stresses the principle of world law when it comes to anti-terrorism. As to money laundering, it remains to be limited to income derived from trafficking of drugs when it comes to the scope of major crimes committed by offshore criminals. In other words, the draft appears to be insufficient with regard to income derived from crime commission. Albeit, there is no legal basis to punish those who have laundered money, generated directly or indirectly by terrorist activities overseas, to the shore of Taiwan. Further, what is considered to be a major breakthrough in the Executive Yuan's draft in the inclusion of the clause of "report of transactions involving huge sum of currency". The inclusion would shorten the process in collecting evidence in the investigation of terrorist group's assets. We would therefore urge the unanimous support of all legislators sitting in the joint committee. In addition, in order to make the anti-terrorism law and complementary acts more comprehensive, article 3 concerning the scope of major crimes in Executive Yuan's draft is suggested to be reviewed and amended so that the international anti-money-laundering trend against terrorist groups can be met.

## 2. From the aspect of mechanism employment

a. Failure to implement investigation of underground money remittance channels

The most swift and covert channel for money laundering by the terrorist group is the underground money remittance channel. It is difficult for anybody to track, as it leaves no trace of transaction. As such, it has been widely used by the organized crime syndicates. Here at home, with the frequent trade and economic transactions between the two sides of the Taiwan Strait, added by the control imposed on financial remittance by authorities on both sides of the government, prevalence of the underground money remittance system seems only natural, thereby creating an abnormal phenomenon in the courier business carrying huge sum of foreign currency in and out of Taiwan. Despite investigations by the judicial police, cases prosecuted have all been ended up with either violation of the Company Act or the Banking Law or both. In reality, there has never been any in-depth investigation into the source of funds to determine whether or not the transaction involves any major crime. As such, it is very difficult to effectively stop operation of the underground money remittance syndicates and the traffic of the courier business carrying huge sum of foreign currency. What could be effective would be an all-out and concerted investigation by all law enforcement agencies into the illegal transaction in addition to heavy penalties handed down by the court system to offenders, if convicted. Only in so doing, we can be assured of the distinction of the underground money remittance practice and use by the terrorist group to infiltrate into our financial system.

b. Necessity to establish an exclusive and interactive judicial business agency

To meet the gradually increasing demand for international cooperation against terrorism and after our accession to the World Trade Organization (WTO), it goes without saying that rapid increase in business involving legal affairs, international affairs and domestic affairs as well, is imminent. The situation dictates the MOJ to initiate setup of an exclusive business agency for international affairs. At home, the agency would promote interactive relations among judicial agencies by agreement and memorandum for mutual assistance. On the international front, the agency would, as assisted by all law enforcement agencies, aggressively promote mutual judicial assistance agreement with foreign countries and intensify international cooperation affairs.

c. Setup of financial intelligence database on anti-terrorism

The MJIB's MLPC shall, through the SAR's filed by domestic financial institutions and establishment of information exchange channels with foreign countries, become the domestic intelligence center to scrutinize fund movement by the terrorist groups. To meet the needs of investigating fund movement by terrorist groups and related organized crime syndicates in

future and establish an information exchange mechanism with the international intelligence community to facilitate future cooperation, it has become necessary to set up a financial intelligence database to do the job.

### 3. From the aspect of intensified enforcement measures

a. To strike down terrorism and trans-national crime commission, the paramount emphasis should be placed on mutual assistance within the judicial branch. By Article 14 of the MLCA, the government is invested in the authority to sign reciprocal agreement with foreign countries. In view of the predicament of our foreign relations with countries in the diplomatic world, however, transnational mutual assistance in the area of the judicial branch has never been effectively established. The Mutual Legal Assistance Agreement reached with the United States may serve as guidance for similar acts in the future. It is suggested that the MOJ may, in conjunction with other concerned ministries or councils, list names of countries that we may, on a priority basis, contact for signing of similar agreement. With planned promotion, we may be able to break through the current bottleneck existent in international cooperation so that we may be able to effectively strike down transnational and international crime commission.

b. Aggressive collection of the responsive measures and related laws and regulations that foreign countries have put into practice against financial activities by the terrorist groups

An integration of various agency personnel stationed overseas is desired. Under the integration program, all personnel stationed overseas are charged with the responsibility to collect information on the responsive measures and related laws and regulations that the host country has put into practice against financial activities by the terrorist groups. Information thus collected may be sent back home for reference by concerned agencies.

c. Rampant fictitious bank accounts in financial institutions have caused dislocation in investigation

The trend to use fictitious bank accounts for money laundering by organized crime groups has become a serious problem nowadays. It has rendered ineffective the government attempt to contain invasion by international terrorists, organized crime groups and professional money laundering syndicates. It seems the regulatory agency should step forward to develop its supervisory function while the financial institutions are advised to take the initiative to implement internal auditing, inclusive of intensified on-the-job training for new recruits and old-timers as well, not to mention the practice of confirmation of new account holder's identity, keeping on file transaction vouchers and filing the SAR's with the regulatory agency in pursuance of the provisions set forth in the MLCA.

## 4. Suggestions on Countermeasures

a. To set up banking account database to scrutinize terrorist financial activities

By coordination with the current investigation of the SAR's in connection with the September 11 attacks in New York, the MJIB's MLPC should set up a banking account database to scrutinize the financial activities by terrorist and related international organized crime groups. Meanwhile, improvement of the analysis capability of the SAR's involving transnational transactions is needed.

b. To intensify investigation of underground money remittance channels to stop money laundering by terrorist groups

The court system is advised to levy heavier penalties on those who engage in the underground money remittance business, if convicted, while the prosecuting and police agencies are advised to put in manpower and time in an all-out and concerted investigation into the source of funds to determine whether or not the transaction involves a major crime.

c. Aggressive collection of information on the responsive measures that foreign countries adopt to fight against the terrorist groups

Personnel of various agencies stationed overseas may act in concert to collect information on the responsive measures and related laws and regulations that the host country has put into practice against the terrorist groups. Information thus collected may be sent back home for reference by the MOJ and concerned agencies.

d. Speedy enactment of anti-terrorism law

Concerned agencies are advised to refer to the established anti-terrorism laws existent in foreign countries and the resolution passed in the United Nations to prevent financial assistance to terrorists and the Security Council's 1373 resolution as well. With those information on hand, the concerned agencies may draft an anti-terrorism bill for a priority processing at the Legislative Yuan so that we may put ourselves in the pace with foreign countries in anti-terrorism practice.

e. Addition of related laws of 'freezing' and 'confiscation' of property that terrorist owns

In our existing laws, there is no such clause as freeze of property. It is suggested that the MOJ take immediate action to study the feasibility of adding the provision of freeze of property in The Code of Criminal Procedure, the MLCA or regulations concerning organized crime prevention. Once the amendment is enacted, funds of violators may be confiscated and the law employed to strike down domestic terrorists and international organized crime groups may be

strengthened.

f. Aggressive promotion of signing reciprocal judicial agreement with foreign countries

It is recommended that responsible regulatory agencies take the initiative to aggressively promote signing of reciprocal judicial agreement and memorandum and the like with foreign countries. Once realized, our capability in joint operation with foreign countries fighting against transnational and international crime commission can be greatly enhanced.

g. Financial institutions are advised to implement money laundering-related businesses

The MLCA requires all financial institutions to confirm the identity of the customer when a certain amount of currency is transacted. In addition, the transaction voucher should be kept on file and, if the transaction is suspected of money laundering, the transaction should be reported to the designated regulatory agency. Therefore, it is the responsibility of the financial institution to strictly enforce internal auditing when it comes to money laundering prevention. At the same time, the financial institution should conduct regular on-the-job training course for new recruits and experienced employees as well, in order to enhance the concept of money laundering prevention and stop fictitious accounts used by terrorist groups or unlawful syndicates. In addition, all financial institutions are required to file the SAR's transacted with funds by suspicious terrorists and international organized crime syndicates. The MJIB's MLPC may use the information to analyze before further processing is carried out.

h. Enforcement of supervision over non-profit-making organizations

Non-profit-making organizations that are likely to become a channel for financial assistance from terrorist groups or international organized crime syndicates. The FATF launched the Special Eight Recommadations to strike down the finance of terrorist after September 11, 2001. In view of the fact that there are many responsible regulatory agencies that oversee the domestic non-profit-making organizations, including various foundations and civil bodies, each responsible regulatory agency is urged to exercise the right of supervision and examination to the fullest extent of the letter so as to stop infiltration of terrorist activities.

## B. Handling of SAR's

### 1. SAR's filed by financial institutions and the status of handling:

For the year in question, total SAR's handled and processed were 791 cases, 770 of which were filed by domestic and foreign banking institutions. The breakdown is as follows:

Domestic banks:703 cases
Foreign banks:67 cases
Credit Unions:5 cases
Farming & Fishing Credit Associations:6 cases
Securities Dealers:2 cases
Insurance Companies: 1 case
Directorate General of Postal Remittances & Savings Bank:6 cases
Other Financial Institutions: (Futures Dealer) 1 case
Total: 791 cases (see Table 2.1 & Figs. 2.1 & 2.1-1)

**Table 2.1 Statistics Showing Comparison of Number of SAR's Filed by Financial Institutions**

Unit: In cases

| Filed by \ Year | | | 1999 | 2000 | 2001 |
|---|---|---|---|---|---|
| Financial Institutions | Banks | Domestic | 265 | 459 | 703 |
| | | Foreign | 21 | 71 | 67 |
| | Credit Unions | | 12 | 10 | 5 |
| | Farming & Fishing Credit Unions | | 11 | 6 | 6 |
| | Securities Dealers | | 9 | 3 | 2 |
| | Insurance Companies | | 0 | 0 | 1 |
| | Postal Remittances & Savings Banks | | 12 | 4 | 6 |
| | Other Financial Institutions | | 1 | 0 | 1 |
| Total | | | 331 | 553 | 791 |

**Fig. 2.1 Analysis of SAR'S by Financial Institutions in 2001**

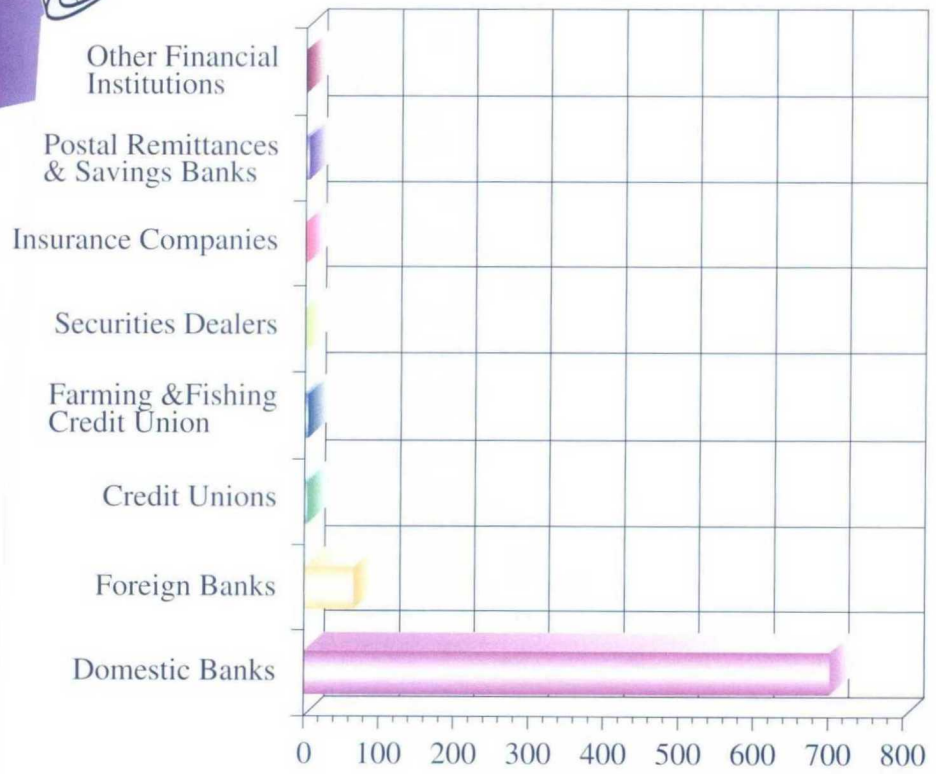
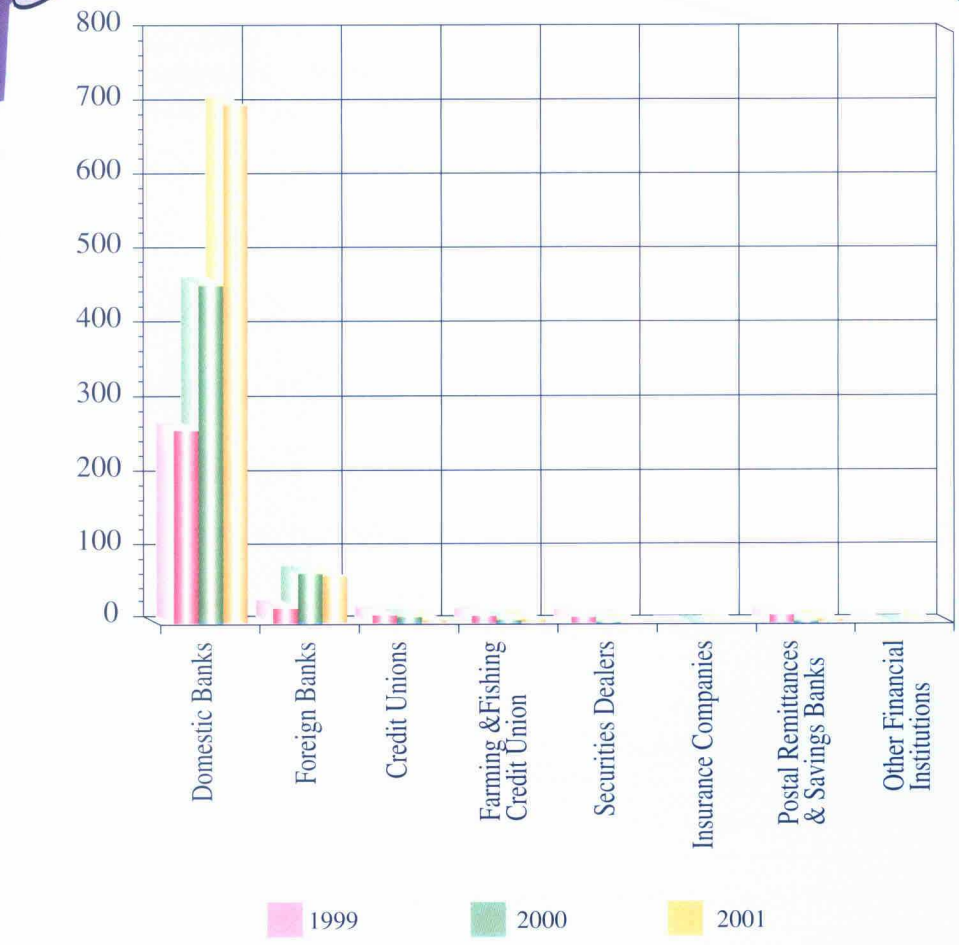


**Fig. 2.1-1 Comparative Chart of SAR's Filed by Financial Institutions**



Of the SAR's mentioned above, violators, after analysis and investigation, were respectively referred to concerned law enforcement agencies for action: 78 cases to the MJIB's field offices/stations; 196 cases to the police authority and other law enforcement agencies for reference and/or action. In addition, 501 cases were either suspended or closed after further investigation and filtration were conducted. By the year's end, there were 216 cases, including 200 cases carried over from the previous year, carried over requiring further analysis. For details, see Table 2.2 and Fig. 2.2).

## 2. Statistics and analysis of SAR's

On the basis of SAR's handled throughout the year in question, statistics were collected and analysis undertaken to include distribution of SAR transaction area, distribution of filed SAR's in each respective month, distribution of ages among offenders and the amount of transactions involved.

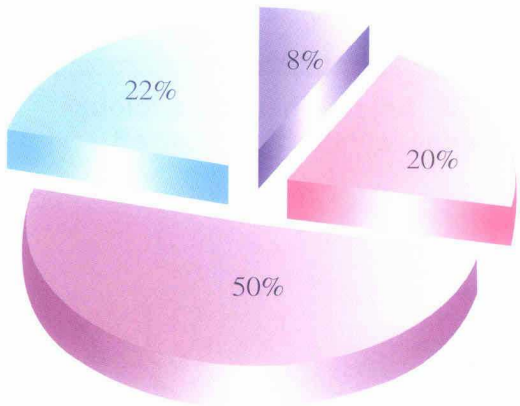
a. Distribution of transaction areas
Taipei City:260 cases
Kaohsiung City:49 cases
Keelung City:11 cases
Taipei County:143 cases
Taoyuan County:45 cases
Hsinchu County:11 cases
Hsinchu City:17 cases
Miaoli County:8 cases
Taichung County:38 cases

**Table 2.2 Statistics Showing Handling Status of SAR's in 2001**

Unit: In cases

| Handling Status | Number of Cases |
|---|---|
| Referred to MJIB's Investigative Units | 78 |
| Referred to Police & Other Law Enforcement Agencies | 196 |
| Cases Closed on File for Future Reference | 501 |
| Cases Under Analysis | 216 |

**Fig. 2.2 Handling Status of SAR's in 2001**




Referred to MJIB's Investigative Units

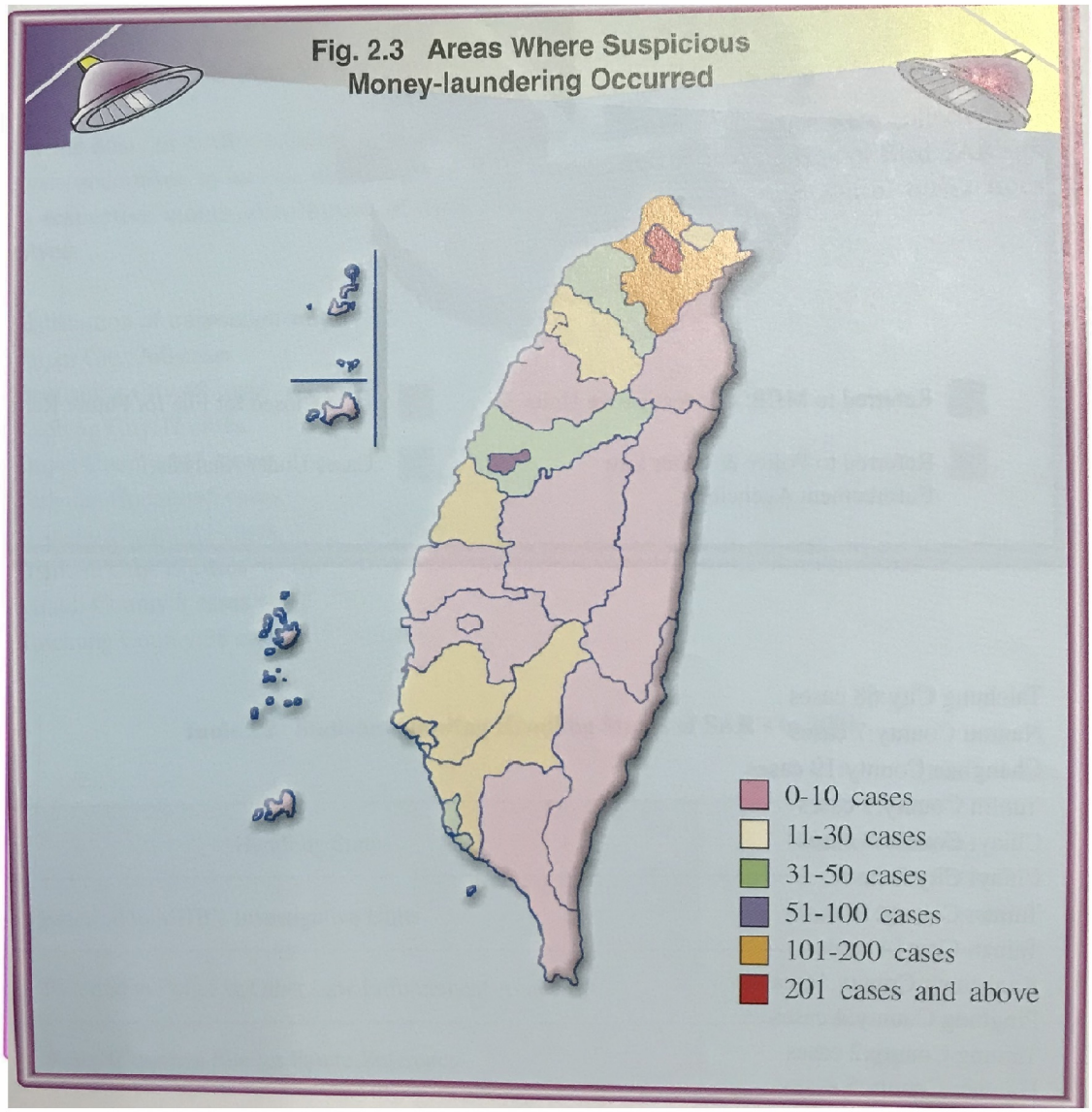
Case Closed for File for Future Refer

Referred to Police & Other Law Enforcement Agencies

Cases Under Analysis

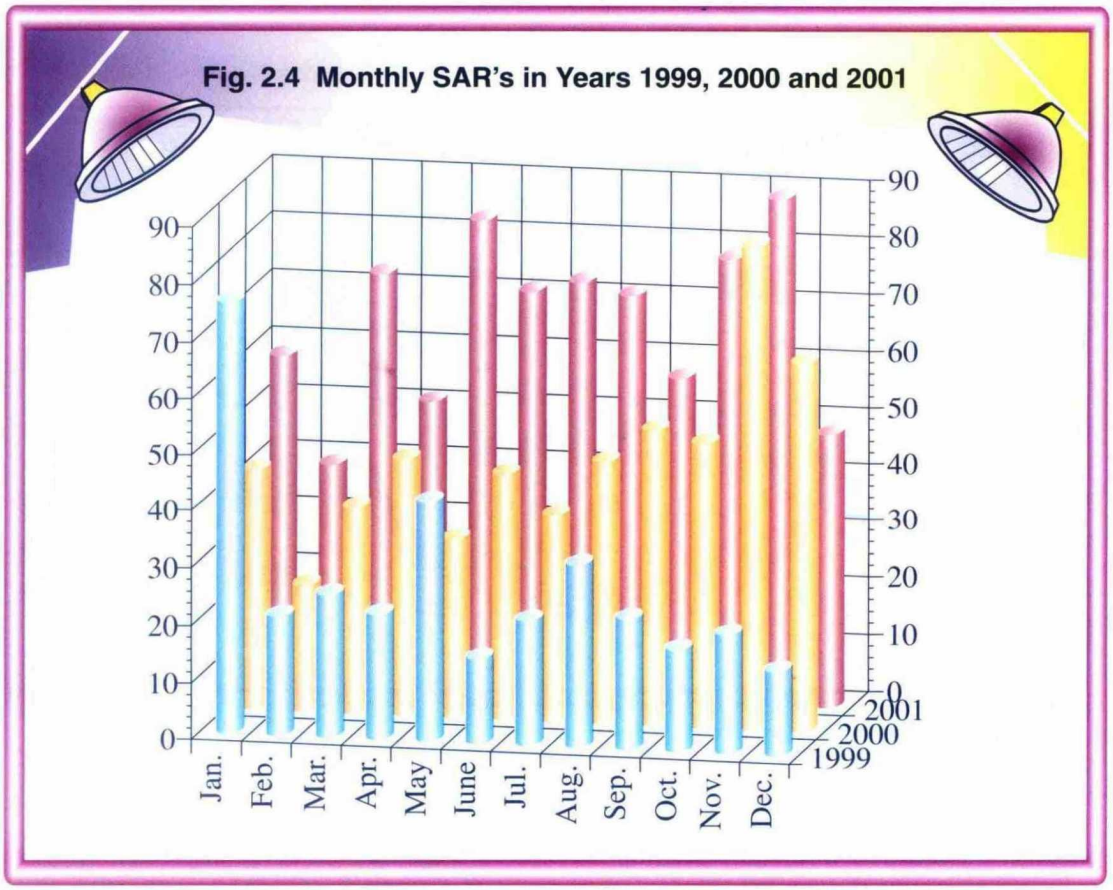
Taichung City:68 cases
Nantou County:7 cases
Changhua County:19 cases
Yunlin County:9 cases
Chiayi County:8 cases
Chiayi City:3 cases
Tainan County:16 cases
Tainan City:14 cases
Kaohsiung County:16 cases
Pingtung County:4 cases
Taitung County:2 cases
Hualien County:5 cases
Ilan County:10 cases
Penghu County:1 case

Kinmen County:2 cases
Lienchiang County:0 case
Total:791 cases



b. By the requirement of the Money Laundering Control Act, financial institutions report SAR's on a monthly basis. There were 58 cases in January, 39 cases in February, 73 cases in March, 51 cases in April, 83 cases in May, 71 cases in June, 73 cases in July, 71 cases in August, 57 cases in September, 78 cases in October, 89 cases in November and 48 cases in December. All in all, there were 791 cases of SAR's for the whole year in question. For comparison with the number of SAR's in 1999 and 2000, please refer to Fig. 2.4.

**Fig. 2.4 Monthly SAR's in Years 1999, 2000 and 2001**

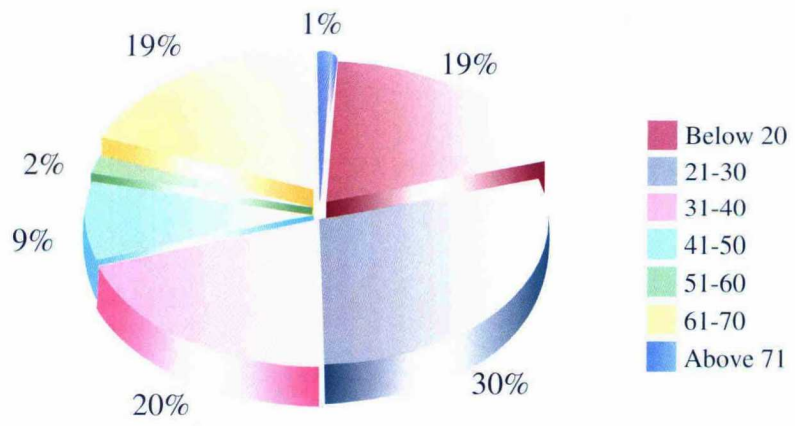


c. Distribution of age groups among offenders

From the statistics, it shows that the majority of offenders range in age from 31 to 40, followed by the age groups of 41 to 50 and 21 to 30. The three accounted for 69% overall. In addition, offenders, 71 and older, accounted for 19% of the total population, or a two-fold increase over the year before. The breakdown is shown below:

Under 20, inclusive: 6 persons
21 - 30: 154 persons
31 - 40: 233 persons
41 - 50: 161 persons
51 - 60: 71 persons
61 - 70: 17 persons
Over 71: 150 persons
Total: 791 persons (see Fig. 2.5 for details)

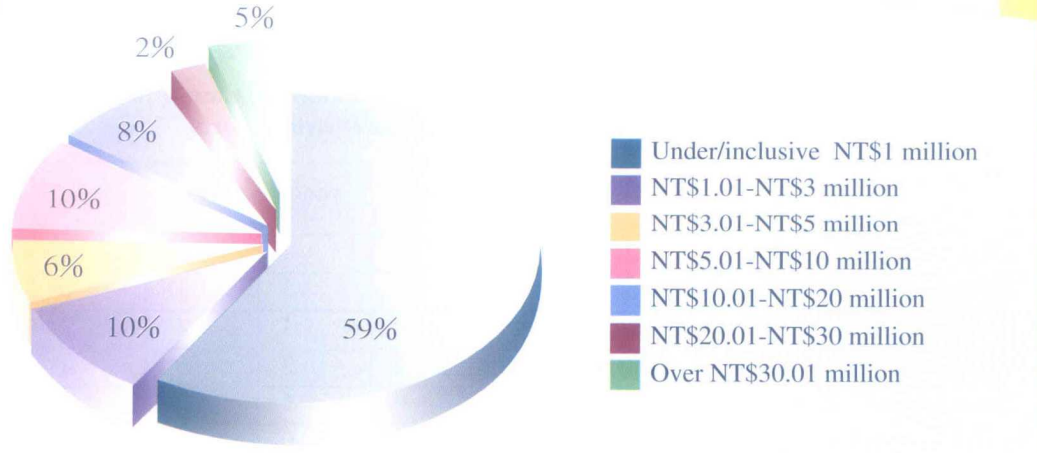
**Fig. 2.5 Suspicious Money-laundering Cases Conducted by Age Groups in 2001**



d. Statistics of transaction amount

Under/inclusive NT$1,000,000: 466 cases
NT$1,010,000 - NT$3,000,000: 80 cases
NT$3,010,000 - NT$5,000,000: 51 cases
NT$5,010,000 - NT$10,000,000: 77 cases
NT$10,010,000 - NT$20,000,000: 62 cases
NT$20,010,000 - NT$30,000,000: 18 cases
Over NT$30,000,000: 37 cases
Total: 791 cases
(See Fig. 2.6 for detail)

**Fig. 2.6 Dollar Amount of Suspicious Money-laundering Cases in 2001**



## C. Collection and analysis of money laundering information

### 1. Offending MLCA cases

According to the Ministry of Justice's inquiry system concerning cases of prosecution, cases prosecuted under Article 9 the MLCA since the act went into effect, quite a number of money laundering cases have been prosecuted by the prosecutor's office and convicted by the court. On the basis of the collected statistics, we, after analysis, present the following status report to show how the crime of money laundering had been conducted and where it had occurred in recent years:

a. The statistics regarding prosecuted money laundering cases released by each district prosecutor's office showed there were 2 cases in 1997, 4 cases in 1998 and 14 cases in 1999, 19 cases in 2000, 23 cases in 2001 or a total of 62 cases. The statistics shows that the trend has been on the increase each year with the passage of time. As to the distribution of the prosecuted cases, there were 13 cases by Taipei Prosecutor's Office, 11 cases by Panchiao Prosecutor's Office, 10 cases by Taichung Prosecutor's Office, 8 cases by Kaohsiung Prosecutor's Office, 6 cases by Tainan Prosecutor's Office, 2 cases by Yunlin Prosecutor's Office, 2 cases each by Shihlin, Pingtung and Hualien Prosecutor's Office, and 1 case each by Keelung, Ilan, Hsinchu, Nantou, and Kinmen Prosecutor's Office. (See Tables 3.1, 3.2 and Fig. 3.1 for details)

**Table 3.1 Statistics Showing Number of Money-laundering Cases Prosecuted by Prosecutor's Offices at Various District Courts**

Number of Cases

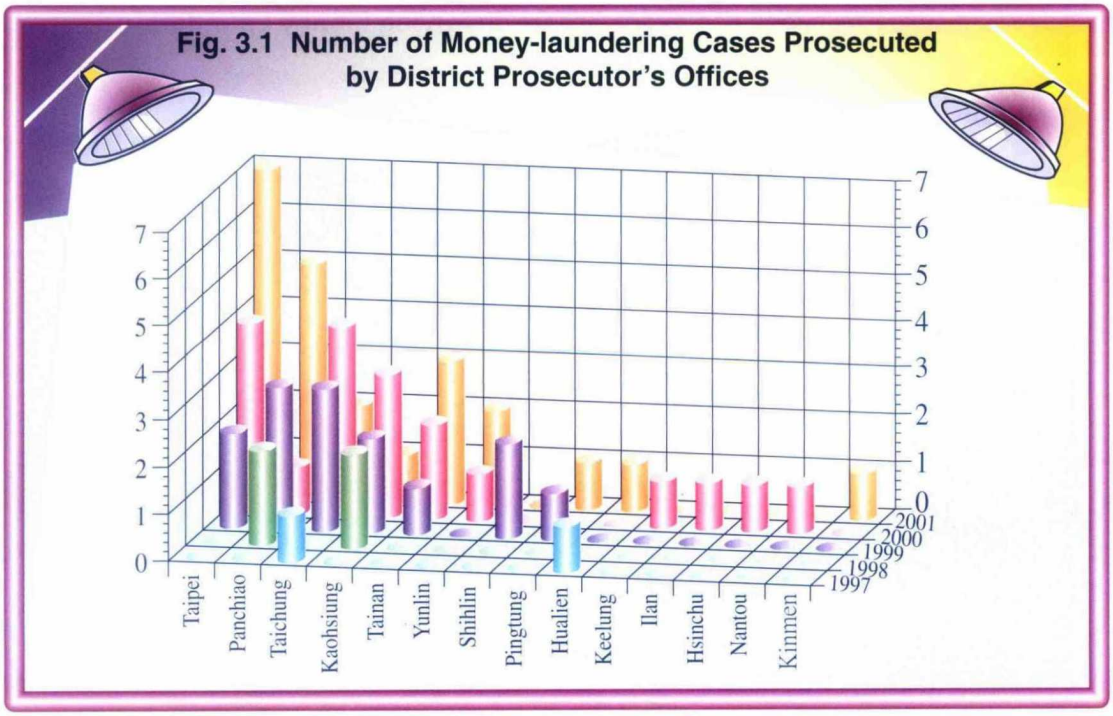
| Year / Name of Prosecutor's | 1997 | 1998 | 1999 | 2000 | 2001 | Total |
|---|---|---|---|---|---|---|
| Taipei District Prosecutor's Office | 0 | 0 | 2 | 4 | 7 | 13 |
| Panchiao District Prosecutor's Office | 0 | 2 | 3 | 1 | 5 | 11 |
| Taichung District Prosecutor's Office | 1 | 0 | 3 | 4 | 2 | 10 |
| Kaohsiung District Prosecutor's Office | 0 | 2 | 2 | 3 | 1 | 8 |
| Tainan District Prosecutor's Office | 0 | 0 | 1 | 2 | 3 | 6 |
| Yunlin District Prosecutor's Office | 0 | 0 | 0 | 1 | 2 | 3 |
| Shihlin District Prosecutor's Office | 0 | 0 | 2 | 0 | 0 | 2 |
| Pingtung District Prosecutor's Office | 0 | 0 | 1 | 0 | 1 | 2 |
| Hualien District Prosecutor's Office | 1 | 0 | 0 | 0 | 1 | 2 |
| Keelung District Prosecutor's Office | 0 | 0 | 0 | 1 | 0 | 1 |
| Ilan District Prosecutor's Office | 0 | 0 | 0 | 1 | 0 | 1 |
| Hsinchu District Prosecutor's Office | 0 | 0 | 0 | 1 | 0 | 1 |
| Nantou District Prosecutor's Office | 0 | 0 | 0 | 1 | 0 | 1 |
| Kinmen District Prosecutor's Office | 0 | 0 | 0 | 0 | 1 | 1 |
| Total | 2 | 4 | 14 | 19 | 23 | 62 |

**Table 3.2 Statistics Showing Types of Severe Crimes Involving Number of Money-laundering Cases Prosecuted by Prosecutor's Offices at Various District Courts**

Number of Cases

| Types of Crime / Name of Prosecutor's Offices | Economic Crime | Embezzlement | narcotic Drugs | Major Crime | Total |
|---|---|---|---|---|---|
| Taipei District Prosecutor's Office | 9 | 3 | 0 | 1 | 13 |
| Panchiao District Prosecutor's Office | 7 | 4 | 0 | 0 | 11 |
| Taichung District Prosecutor's Office | 5 | 1 | 2 | 2 | 10 |
| Kaohsiung District Prosecutor's Office | 4 | 3 | 1 | 0 | 8 |
| Tainan District Prosecutor's Office | 1 | 4 | 0 | 1 | 6 |
| Yunlin District Prosecutor's Office | 3 | 0 | 0 | 0 | 3 |
| Shihlin District Prosecutor's Office | 2 | 0 | 0 | 0 | 2 |
| Pingtung District Prosecutor's Office | 1 | 0 | 1 | 0 | 2 |
| Hualien District Prosecutor's Office | 1 | 1 | 0 | 0 | 2 |
| Keelung District Prosecutor's Office | 1 | 0 | 0 | 0 | 1 |
| Ilan District Prosecutor's Office | 0 | 0 | 0 | 1 | 1 |
| Hsinchu District Prosecutor's Office | 1 | 0 | 0 | 0 | 1 |
| Nantou District Prosecutor's Office | 0 | 1 | 0 | 0 | 1 |
| Kinmen District Prosecutor's Office | 0 | 1 | 0 | 0 | 1 |
| Total | 35 | 18 | 4 | 5 | 62 |

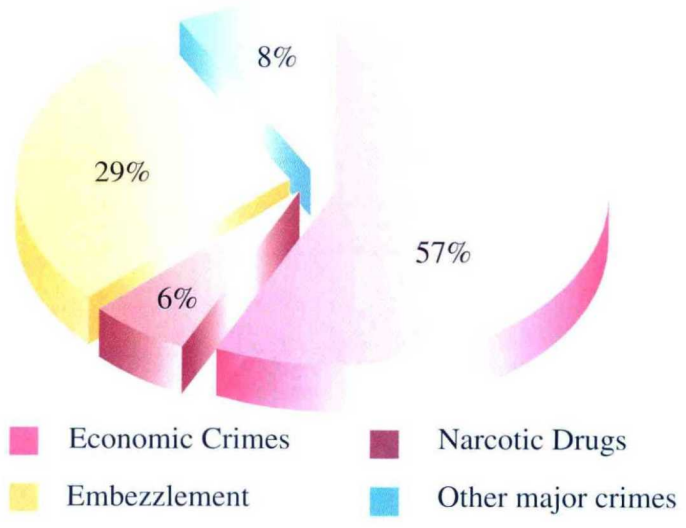
**Fig. 3.1 Number of Money-laundering Cases Prosecuted by District Prosecutor's Offices**



b. Types, names of offenses and mechanism of severe crimes prosecuted under MLCA

The object of money laundering crime is limited to the interest in the form of proceeds or property generated from the crime committed as described under Article 3 of the MLCA. The types of the crime can be defined as embezzlement, economic crime, crime of narcotic drugs and other major crimes. Economic crime ranked the top with 35 cases, accounting for 57%, followed by embezzlement with 18 cases, or 29%, other major crimes with 5 cases, or 8%, and crime of narcotic drugs with 4 cases, or 6%, and in that order (see Fig. 3.2). As to the names of offenses, there were 24 cases of habitual fraud, followed by 11 cases of what Article 4(1)(1), (3) and (4) of the Regulations Concerning Punishment for Corruption and Embezzlement calls crime, including embezzlement of public property, receipt of kickbacks through handling of public projects, or other corruption or acceptance of bribes in violation of professional ethics. As to other cases of crime, the distribution was fairly evenly spread. Cases referred to by police agencies were mostly economic crime while the majority of cases referred to by investigative agencies were embezzlement, followed by economic crime (see Table 3.3 and Fig. 3.3).

**Fig. 3.2 Types of Severe Crimes Involving Money Laundering**

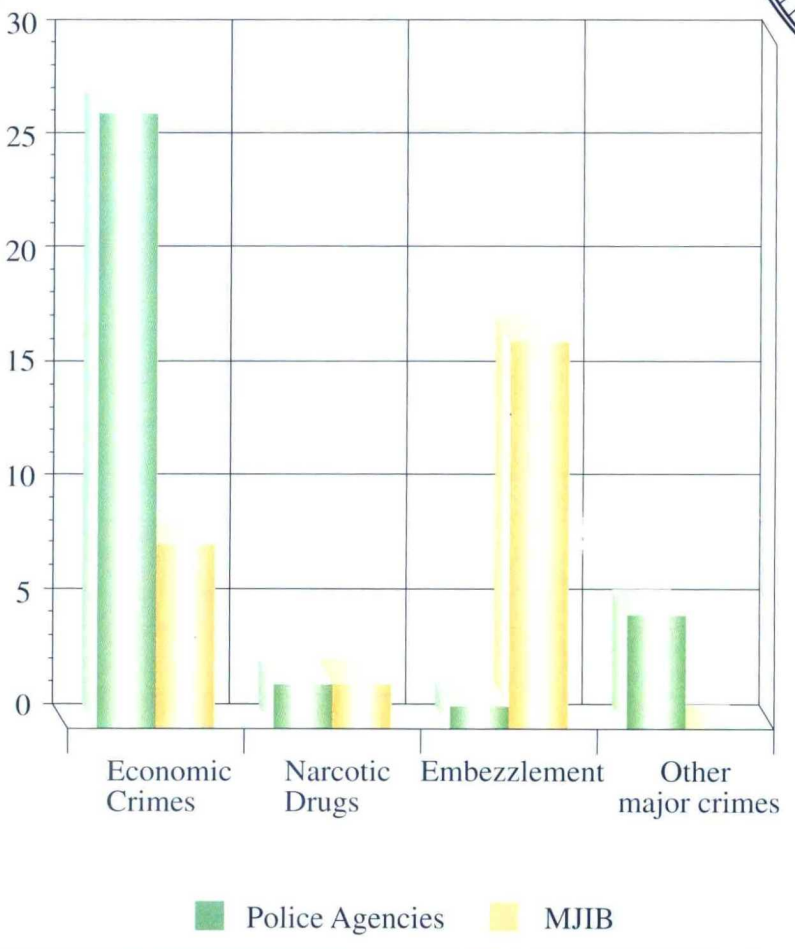


## Table 3.3 Statistics Showing Types of Money-laundering Cases Referred to Concerned Law Enforcement Agencies for Prosecution

Number of Cases

| Type of Crime \ Agency Referred / Year | | Police Agency | | | | | MJIB | | | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 86 | 87 | 88 | 89 | 90 | 86 | 87 | 88 | 89 | 90 | |
| Economic Crime | Habitual Fraud | 1 | 0 | 3 | 6 | 11 | 0 | 1 | 1 | 1 | 0 | 24 |
| | Violation of Securities Transaction Act by Manipulating Stocks | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 1 | 0 | 3 |
| | Professional Usury | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 3 |
| | Counterfeit of Securities | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 3 |
| | Counterfeit of National Currency | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 |
| | Sub-total | 1 | 1 | 3 | 8 | 14 | 0 | 1 | 4 | 3 | 0 | 35 |
| Embezzlement | Violation of Article 4 of the Regulations Concerning Punishment for Corruption and Embezzlement | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 2 | 5 | 2 | 11 |
| | Violation of Article 5 of the Regulations Concerning Punishment for Corruption and Embezzlement | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 2 | 2 | 5 |
| | Violation of Article 5 of the Regulations Concerning Punishment for Corruption and Embezzlement | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 2 |
| | Sub-total | 0 | 0 | 1 | 0 | 0 | 0 | 2 | 3 | 7 | 5 | 18 |
| Narcotic Drugs | Transportation & Trafficking of Grade A Narcotic Drug (heroin) | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| | Transportation & Trafficking of Grade B Narcotic Drug (amphetamine) | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 3 |
| | Sub-total | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 4 |
| Other major crimes | Robbery | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| | Murder After Robbery | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| | Kidnapping for Ransom | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 2 |
| | Violation of Regulations Concerning Sex with Children and Juvenile | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| | Sub-total | 0 | 0 | 1 | 1 | 3 | 0 | 0 | 0 | 0 | 0 | 5 |
| Total | | 1 | 1 | 6 | 9 | 18 | 1 | 3 | 8 | 10 | 5 | 62 |
| | | 35 | | | | | 27 | | | | | |

**Fig. 3.3 Type of Cases Referred to Law Enforcement**



According to the column that lists the suspicious money laundering acts in the information, it shows there were 47 cases, or the frequent used channel by domestic money laundering handlers, involving use of the banking institutions (a mono type or multiple varieties) to commit the crime of money laundering as described under Article 5 of the MLCA. Directorate General of Post Remittances & Savings Bank ranked the second with 20 cases, followed by securities dealers with 10 cases, credit unions with 6 cases, farming credit associations with 3 cases and fishing credit associations with 2 cases. No money laundering case has ever been reported through other types of financial institutions (see Fig. 3.4). Other than use of financial institutions for money laundering, there were 7 cases reported in transactions of real estate, one case of gold bullion purchase, one case involving acquisition of obligatory right, one case involving repayment of debt, one case involving courier in person, and one case involving deposit in a friend's house (see Fig. 3.5).

**Fig. 3.4 Statistics Showing Money-laundering Cases Through Financial Institutions Channels**

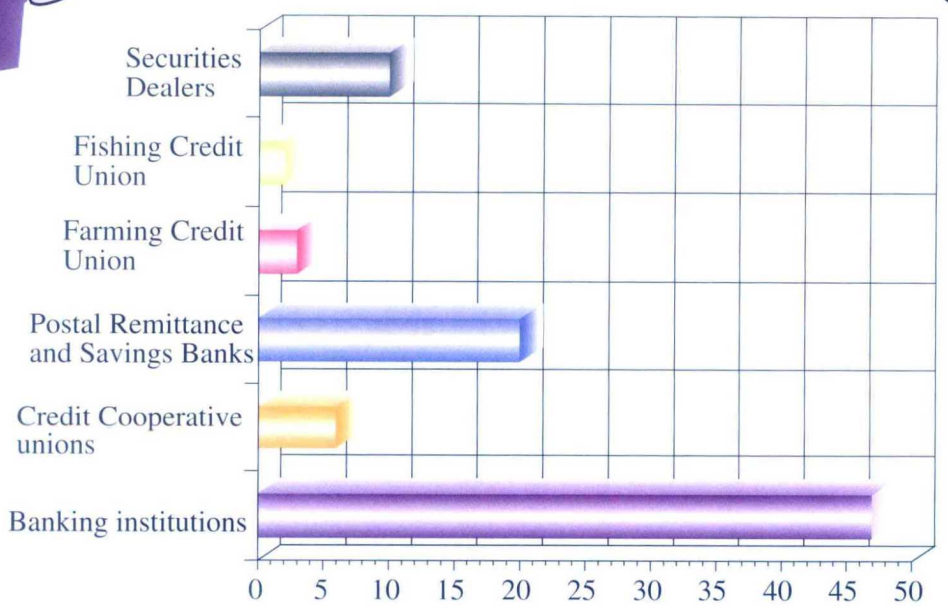
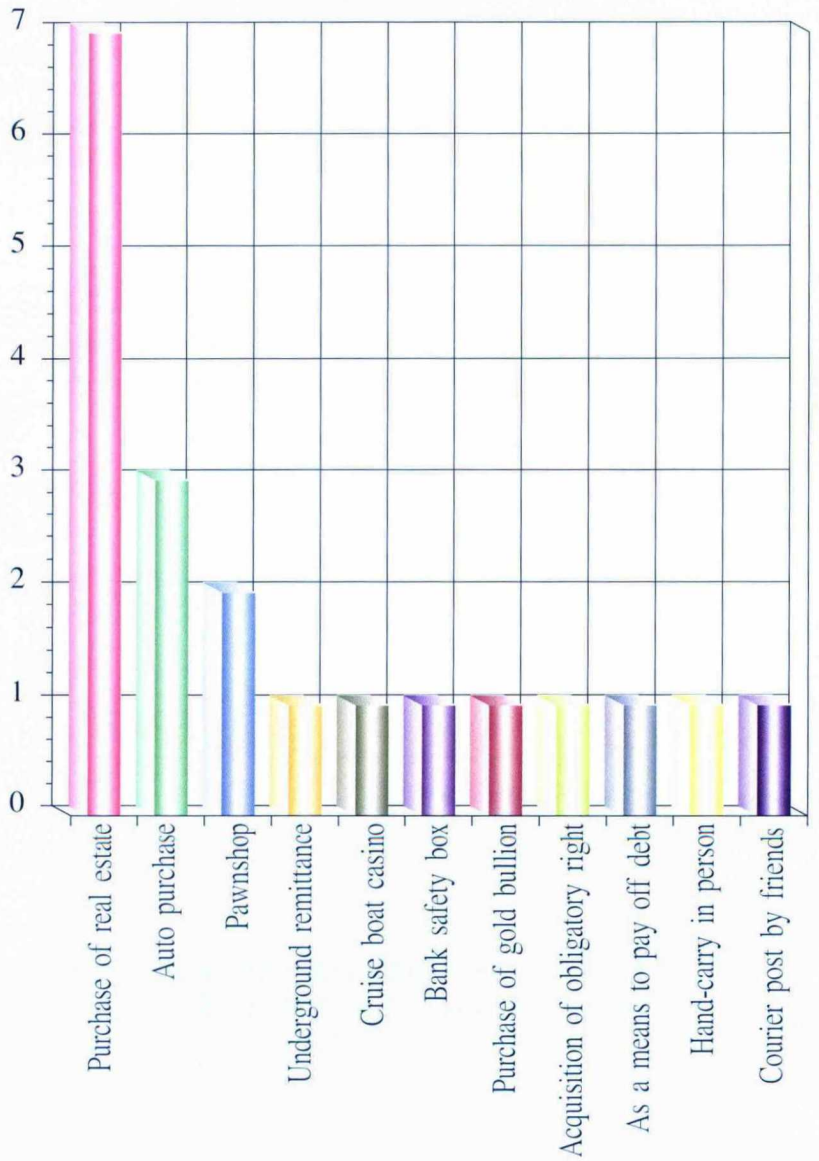


Fig. 3.5 Statistics Showing Money-laundering Cases Through Channels Other Than Financial Institutions



c. Areas where prosecuted money laundering cases took place

By statistics, Taipei County took the lead in all cities/counties with 22 cases prosecuted, following by Taipei City with 19 cases, Kaohsiung County with 10 cases, Taichung City with 9, Kaohsiung City with 7 cases, Tainan County and Ping County with 4 cases each, Yunlin County with 3 cases, Taichung County, Changhua County, Tainan City and Hualien County with 2 cases each, and Keelung City, Nantou County and Ilan County with 1 case each (see Table 3.4 and Fig. 3.6).

**Table 3.4 Statistics Showing Areas Where Money-laundering Cases Had Occurred**

Cases

| Cities/Counties | Number of Cases Occurred |
|---|---|
| Taipei County | 22 |
| Taipei City | 19 |
| Kaohsiung County | 10 |
| Taichung City | 9 |
| Kaohsiung City | 7 |
| Tainan County | 4 |
| Pingtung County | 4 |
| Yunlin County | 3 |
| Taichung County | 2 |
| Changhua County | 2 |
| Tainan City | 2 |
| Hualien County | 2 |
| Keelung City | 1 |
| Nantou County | 1 |
| Ilan County | 1 |
| Total | 89 |

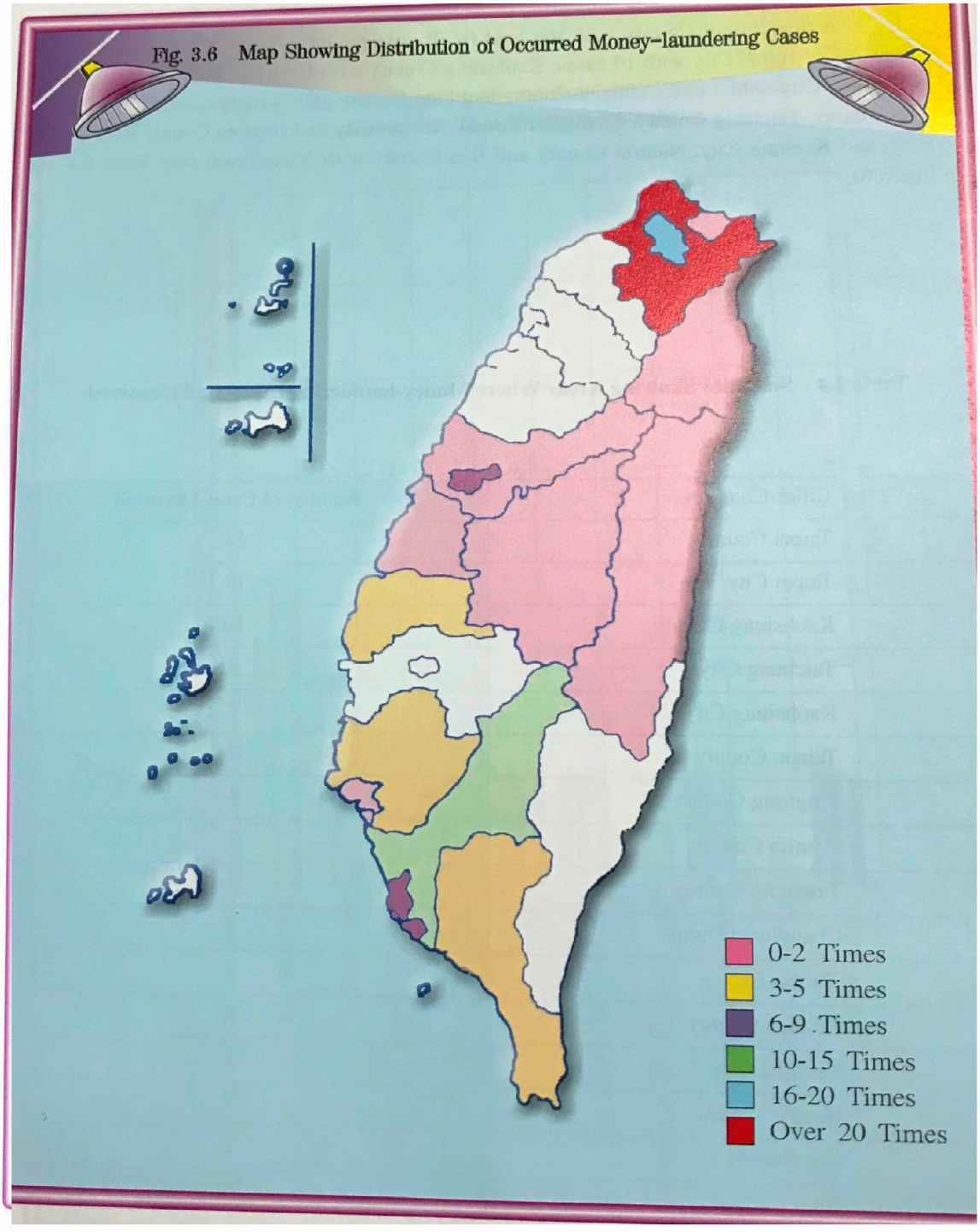



Fig. 3.6 Map Showing Distribution of Occurred Money-laundering Cases

d. Statistics of number of defendants in prosecuted money laundering cases

By statistics, the number of defendants prosecuted under the MLCA showed there were 100 males and 33 females that also participated in commission of major crimes. In addition, prosecuted under the MLCA included also 32 males and 14 females (see Table 3.5).

**Table 3.5 Statistics Showing Number of Defendants Prosecuted for Money Laundering**

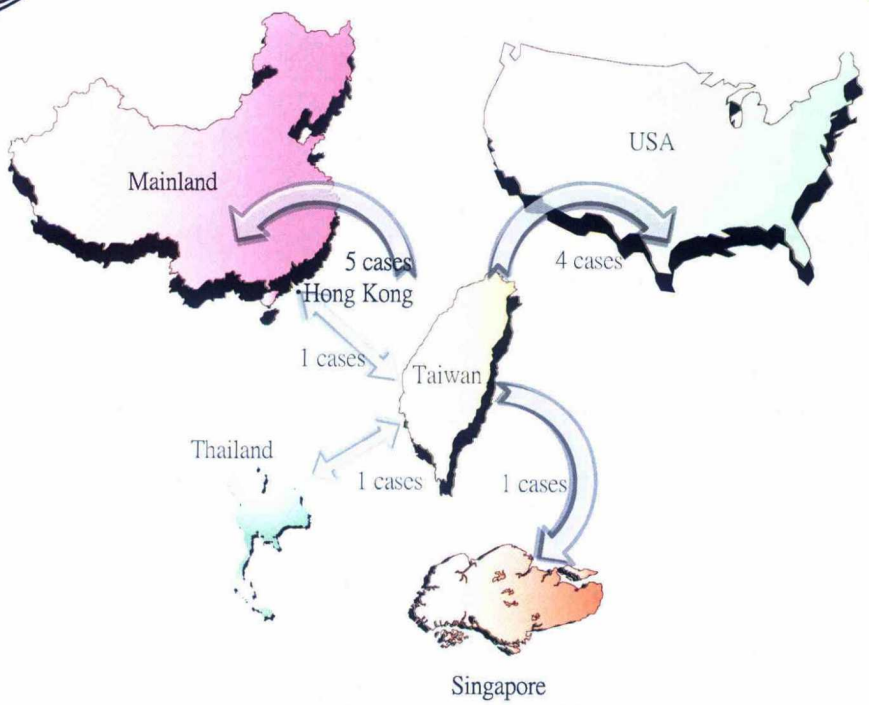
Persons

| Name | Sex | Type of Crime \ Year | 1997 | 1998 | 1999 | 2000 | 2001 | Total |
|---|---|---|---|---|---|---|---|---|
| Severe Crime & Money Laundering | Male | Economic Crime | 1 | 3 | 31 | 24 | 17 | 76 |
| | | Embezzlement | 0 | 2 | 5 | 2 | 6 | 15 |
| | | Narcotic Drugs | 1 | 0 | 1 | 0 | 0 | 2 |
| | | Other major crimes | 0 | 0 | 2 | 0 | 5 | 7 |
| | | Sub-total | 2 | 5 | 39 | 26 | 28 | 100 |
| | Female | Economic Crime | 0 | 1 | 16 | 1 | 5 | 23 |
| | | Embezzlement | 0 | 1 | 0 | 4 | 3 | 8 |
| | | Narcotic Drugs | 1 | 0 | 0 | 0 | 0 | 1 |
| | | Other major crimes | 0 | 0 | 0 | 0 | 1 | 1 |
| | | Sub-total | 1 | 2 | 16 | 5 | 9 | 33 |
| Money Laundering | Male | Economic Crime | 1 | 0 | 8 | 1 | 0 | 10 |
| | | Embezzlement | 0 | 0 | 2 | 6 | 4 | 12 |
| | | Narcotic Drugs | 0 | 0 | 0 | 0 | 1 | 1 |
| | | Other major crimes | 0 | 0 | 1 | 1 | 7 | 9 |
| | | Sub-total | 1 | 0 | 11 | 8 | 12 | 32 |
| | Female | Economic Crime | 0 | 1 | 1 | 1 | 2 | 5 |
| | | Embezzlement | 0 | 0 | 1 | 1 | 2 | 5 |
| | | Narcotic Drugs | 0 | 0 | 0 | 0 | 1 | 1 |
| | | Other major crimes | 0 | 0 | 1 | 1 | 3 | 5 |
| | | Sub-total | 0 | 1 | 3 | 3 | 7 | 14 |
| Total | | | 4 | 8 | 69 | 42 | 56 | 179 |
| | | | 179 | | | | | |

e. Prosecuted money laundering cases involving transnational transactions

Where it comes to transnational transactions of money laundering, Mainland China is on top of the list with 5 cases, followed by the United States with 4 cases, and Hong Kong, Singapore and Thailand with 1 case each (see Fig. 3.7). The leading position by Mainland China indicates the trend of money laundering between the two sides of the Taiwan Strait is on the rise as trade between people residing on both sides of the Strait has gradually become active. The trend also shows it has become obvious that cooperation between law enforcement agencies on both sides of the Strait is an important issue in future.

**FIG. 3.7 Map showing distribution of prosecuted Transnatinal Money-Laundering Cases**



## D. Investigation support

The MLPC offers its assistance not only in money laundering investigations by fellow units inside the MJIB, but also in investigations conducted by other domestic and foreign agencies as well. In 2001, there were a total of 34 cases that the MLPC had provided assistance in investigation, of which 4 cases were for prosecution and investigation agencies, 6 for judicial police agencies, 2 for other agencies and 20 for information exchange with international agencies (see Table 4.1).

**Table 4.1 Statistics Showing Number of Cases Assisted in Investigation in 2001**

| Name of Agency | Number of Cases |
|---|---|
| MJIB Units | 34 |
| Prosecuting Offices | 4 |
| Law Enforcement Agencies | 6 |
| Other Agencies | 2 |
| Information Exchange Under International Cooperation Programs | 20 |
| Total | 66 |

## E. International cooperation

On international cooperation, the year 2001 was quite a challenging one. In January, Asia/Pacific Group on Money Laundering (APG) wrote the MJIB's MLPC, inquiring our willingness to join a mutual evaluation program. We gladly accepted this challenge for we believe the program may be instrumental in reviewing the strengths and weaknesses of our existing money laundering mechanism and, as a member of the APG, to join the mutual evaluation program is our obligation.

The APG mutual evaluation program consists of two parts, questionnaire and on-site visiting. The standard questionnaire is first sent out to all participants while the on-site visiting is conducted by the APG evaluation delegation. To answer the questionnaire, it is noted, a number of government agencies are involved. Therefore, the MJIB has reported the questionnaire to the MOJ requesting through the office of the MOJ comments from the Secretariat of the Judicial Yuan, the MOFA, MOF, MOEA, Central Bank of China (CBC) and the National Police Administration (NPA) of the MOI. The MLPC compiled the comments received from the respective concerned agencies and filled out the questionnaire before it was sent back to APG. In latter March, APG evaluation delegation arrived in Taiwan to make the on-site visiting. Led by APG secretary-general Mr. Rick McDonell, the delegation was composed of Mr. Theodore S. Greenberg of the US, Mr. Robert Perry of Australia and Mr. Ian Wong of Singapore. The evaluation on money laundering prevention mechanism was conducted on three sectors: 1) legal; 2) financial ; and 3) law enforcement. To meet the on-site evaluation, the MJIB requested the MOJ to set up a task force.

The evaluation results by the APG delegation recognize the efforts and determination made by the ROC, praising our practice has reached the international level. The delegation also made few recommendations on how we may improve our money laundering prevention efforts in future, which were duly referred to concerned agencies for reference. The evaluation report was later approved in May when the group held its 4th annual meeting in Kuala Lumpur, Malaysia.

In addition, in support of investigations concerning major crimes conducted by the Anti-dirty Money Center of Taiwan High Court's Prosecutor's Office and various district court's prosecutor's offices, the MLPC exchanged information with Egmont Group and APG members for a total of 20 cases.

On attendance to international conference, MLPC members were dispatched in May to attend the APG 4th Annual Meeting in Kuala Lumpur, Malaysia; in October in Singapore for a workshop. MLPC staff were also present in the Egmont Group 9th Annual Meeting in May in the Hague, Holland; in the working group meeting in Zoetermeer, Holland in October. Due to unavailability of budget, MLPC were absent from the Egmont Group working group meeting in February held in Cyprus. After the September 11 attacks on the US, the global investigation mode of crime investigation has been forced to shift its focus, making fund flow a mainstream item in crime investigation. To discuss on how to prevent fund movement and thereby track the money laundering channels by terrorist groups, the FinCEN of the US had invited Egmont Group members to attend special forum be held on October 31 in Washington, D.C. MLPC was there.

## F. Establishment of databank

Cases of SAR's handled by the MLPC are filed in the computer system after having been verified, induced, compared and analyzed. For the year in question, there were 791 pieces of intelligence filed in the database. All in all, there are 2,031pieces of intelligence on file.

## G. Promotion and training

In order to assist staff in financial institutions in identifying money-laundering signs, and in observation of provisions of the Money Laundering Control Act, the Center, at the request of related financial institutions, has dispatched its agents to lecture on the subject of money laundering at various financial institutions. Details of the lecturing tour are shown as follows:

At Domestic Banks: 49 sessions with 2,990 people attended.
At Foreign Banks: 3 sessions 89 people attended.
At Securities Investment Trust Firms: 4 sessions with 92 people attended.
At Securities Dealers Firms: 34 sessions with 2,789 people attended.
At Insurance Business Development Center:1 session with 50 people attended.
At Bills Financing Firm: One session with 30 people attended.
At Securities and Futures Development Foundation: 2 sessions with 50 people attended.
At Farming and Fishing Credit Associations:4 sessions with 490 people attended.
All in all, 98 sessions were held and 6,580 people attended.
(For details, see Table 7.1)


**Table 7.1 Statistics Showing Promotion and Training Concerning Money-laundering Works Conducted in 2001**

| Name of Financial Institutions | | Number of Sessions | Number of Attendees |
|---|---|---|---|
| Banks | Domestic | 49 | 2990 |
| | Foreign | 3 | 89 |
| Farming & Fishing Credit Unions | | 4 | 490 |
| Securities Investment and Trust | | 4 | 92 |
| Securities Dealers | | 34 | 2789 |
| Securities and Futures Development Foundation | | 2 | 50 |
| Bills & Financing | | 1 | 30 |
| Insurance Business Development Center | | 1 | 50 |
| Total | | 98 | 6580 |

# Part Three

# Case Studies

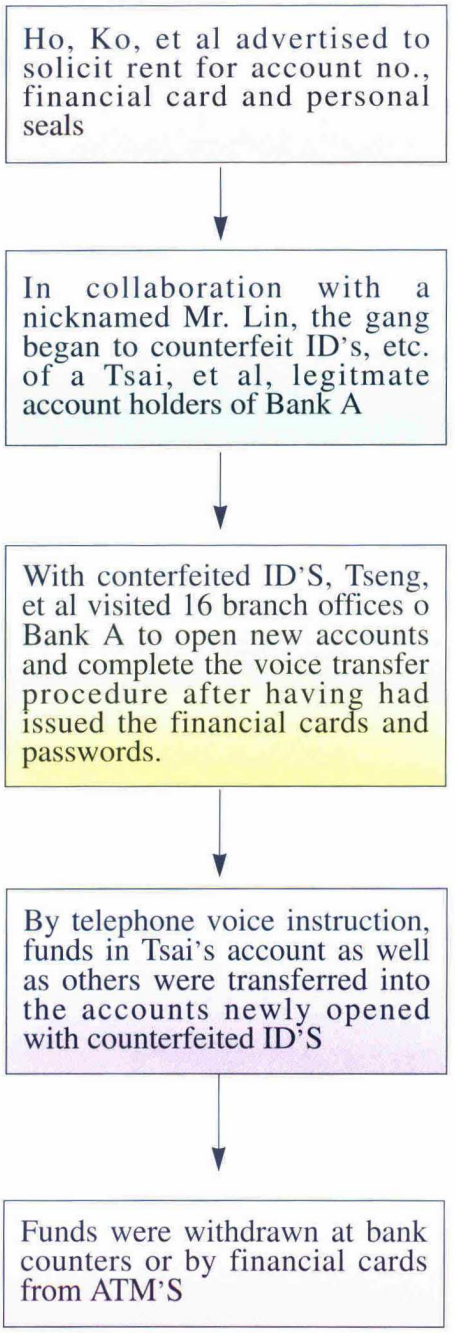
## A. Ho's Case

In the afternoon of April 4, 2001, Bank A reported to MLPC, saying a certain individual was approaching its Branch B to open a bank account with counterfeited ID of existing Branch A account holder. According to the report, this 'certain individual' has stolen the telephone voice password of its Branch A account holder and transferred funds from the existing Branch A account into the account newly opened with counterfeited ID. Later, money was drawn from the counter in the amount of over NT$1.5 million, not to mention use of financial card to draw cash. In all, the fictitious accounts numbered 25 and funds stolen totaled some NT$18 million.

After analysis and filtration of information of fictitious accounts by the MLPC, it was found that a certain Liu once had planned to open an account with Bank A's Branch C. Impatient with the tedious procedures at the counter, this certain Liu went instead to the ATM, trying to draw cash and from the financial card used, it showed the true identity of this certain Liu was actually a Ho.

Since January 2001, this Ho had correlated with a Ko, et al to rent a business premises at 1F, xx, Ta Tun x Street, Taichung City. Meanwhile, the gang advertised in The Liberty Times, Min-chung Daily, offering "cash reward for opening cell phone account number". Apart from applications for cell phone account numbers on behalf of clients, the gang also advertised in the media, saying "passbook + cell phone number = cash" and paid NT$2,000 to NT$4,000 each two months to any one that responded. The act to solicit financial account number, financial card, and personal seal from the general public is in fact used as tools to cover up the crime committed. In March the same year, the Ko and a man nicknamed Lin organized a fraudulent gang, trying to persuade a Tseng, Liu, King, et al as figure heads to open up new account at various branches of Bank A, using photos and counterfeited ID's and personal seals of Bank A's legitimate account holders Tsai, et al provided by the nicknamed Lin. The reward for each account opened was NT$4,000. From March 28 to April 2, the Ho-led gang took the figure heads to visit 16 branch offices of Bank A, opening 25 accounts in succession along with the transfer procedure by voice, using photos and counterfeited ID's and personal seals of Bank A's legitimate account holders. Soon as the financial cards are issued, the nicknamed Lin would use the card to draw cash from the accounts legitimately held by victims Tsai, at el at the bank counter. The Ho-led fraudulent gang was prosecuted publicly by the Prosecutor's Office of Taichung District Court on September 28, 2001.

## Ho's Case Money Laundering Flow Chart



## B. Scandal of county commissioner

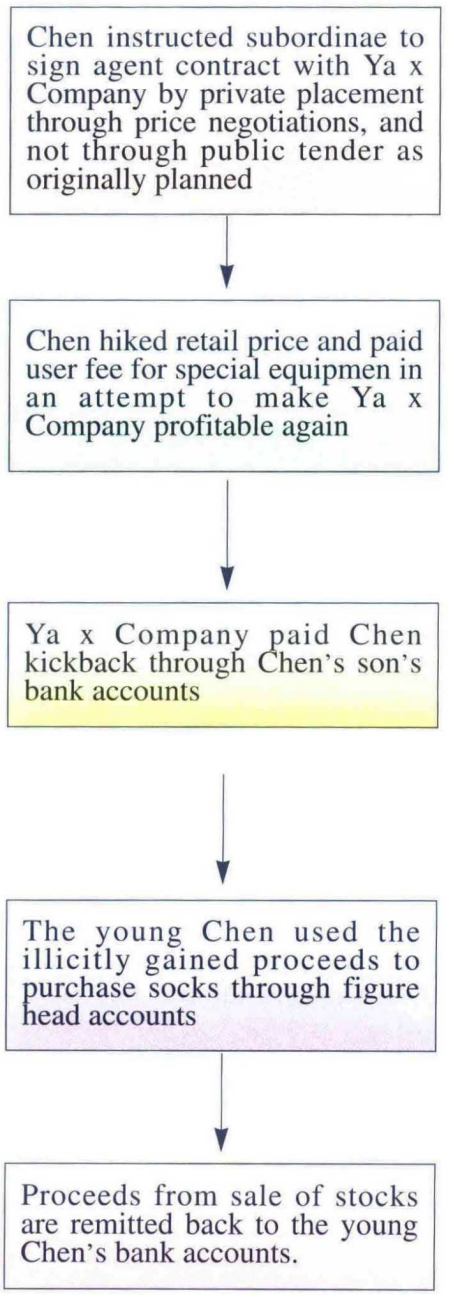
County commissioner Chen of xx County concurrently served as the chairman of a distiller he oversaw. Using his position, Chen exchanged kickback in favor of granting agent status when new brand was distilled. In the process, Chen instructed an Ong, then the head of the bureau of finance, and a Hsing, then the general manager of the distiller, to write untrue liquor-testing record, and change the sale method from public tender to private placement by price negotiation, in an attempt to favor Ya x Company with the agent status for the new brand. Ya x Company further subcontracted the agency contract to a Hui x Company, in violation of the non-subcontracting clause specified in the contract.

In addition, Chen had further violated the Regulations Concerning Management of Price for Wines and Tobacco in the xx Area imposed by the Ministry of Finance for he adjusted the price upward from January 28, 2000 to June 1, 2001. The total illicit gain in favor of a Wu, the person-in-charge of Ya x Company, totaled some NT$54,880,000.00. Chen further instructed to pay Wu additional NT$69,244,741 for patent processing fee for use of the Quick Frozen & Display of Cooked Food Installation Device for Liquid Food that Ya x Company invented.

After Hui x Company illicitly obtained the agent status for the new brand, it went to raise the retail price and paid 20% out of the total profits to Wu, the person-in-charge of Ya x Company. From 2000 to April 2001, the sum amounted to NT$102,973,994, or in all, the illicit gain that Chen helped Wu obtained since the appointment of agent for marketing the new brand of liquor totaled some NT$227,100,000. The kickback that Chen received totaled over NT$3,300,000, as evidenced by Chen's son's bank statements in different banks where the junior Chen had accounts.

In an attempt to cover up and conceal the ill-gained proceeds, the young Chen had taken the advantage of working in a securities dealer's house to purchase stocks of Hui x Company and Li x Electronic Company through accounts of colleagues Yang, Shen, et al, and later resold the stocks with proceeds back-channeled into Chen's account in an act of money laundering for the kickback. On October 18, 2001, prosecutors indicted Chen, Wu, et al on charges of suspected violation of the Regulations Concerning Punishment for Corruption and Embezzlement. The young Chen was also indicted in pursuance of the MLCA for aiding Chen in receiving kickback and money laundering with fictitious accounts.

## County Commissioner Scandal Money Laundering Flow Chart



# Part Four

# Review of the Past and Outlook for the Future

## A. Review of performance for the past year

With the rapid development of hi-tech in recent years, the method used in money laundering has continuously exhibited new tricks. In the past year, the challenge was even greater than years before. Nonetheless, the work on money laundering prevention by concerned government agencies and by financial institutions as well has never ceased to make progress, thanks to the joint efforts made by all concerned. In particular, we may say that outstanding progress was made in intensification of money laundering prevention mechanism, implementation of education and promotion and international cooperation.

First, in the area of intensification of money laundering prevention mechanism, the MOJ's Inquiry System for Account Opening in Financial Institutions was established in August 2001 with the assistance of the MJIB's MLPC. All concerned agencies and institutions nation-wide may, through this System, inquire about a certain specific individual on the overall information on file in each and every financial institution pertaining to the certain specific individual. Compared with the practice in the past when each inquiry had to be addressed to different financial institutions, the system shortens the process, providing tremendous help in tracking the flow of ill-gained proceeds. On the amendment to the MLCA, the bill, after having been forwarded to the Legislative Yuan through the MOJ via the Executive Yuan, had passed the first reading in the joint meeting of the judicial committee and the finance committee. The contents of the amendment cover:

1. Article 2 on sample type of money laundering behavior to include new models of carriage and storage as conducted by the offender in person in the commission of s major crime.

2. Article 3 on the scope of major crimes
   a. The scope of major crime as specified under Article 3(1)(2) through (11) of the MLCA expands to cover the Government Procurement Act and embezzlement. The MOJ version, after discussions, was adopted, which specifies proceeds from a crime committed should be over NT$20 million when it comes to professional fraud, professional usury, violations of the Banking Act, and embezzlement (a new offense).
   b. Deletion of the existing Article 3(2) & (3) with respect to the provisions of manufacturing and trafficking narcotic drugs overseas and on Mainland China as a major crime for the crime mentioned is already covered under Article 5 (6) & (7) of the Criminal Code now in force.

3. The contents of Article 5 on the scope of financial institutions remain unchanged since there has been no consensus between the Ministry of Finance and Ministry of Economic Affairs as to who shall be the regulatory agency overseeing the jewler's shops. Further discussions have been left to the Executive Yuan Council.

4. Addition of Article 5-1 concerning setup of a databank to cover account holders in financial institutions whereas it specifies explicitly judges, prosecutors and administrators may review the information contained in the databank. After discussions, however, it was decided that no addition was necessary and the addition was struck out.

5. Additions to Article 6 on the model points to note for money laundering prevention in financial institutions have been reviewed and passed. The added portion has been referred to the competent regulatory agencies for reference.

6. Amendment of Article 7. The plan was to add, "to report to the designated regulatory agency when the cash transaction exceeds a certain sum." Due to strong objection from some of the attending committee members, the amendment failed to pass the resolution.

7. The wording "may inform the interested party" in Article 8 was deleted.

8. On Article 9 with regard to the term of penalty for money laundering, it was classified into two areas of money laundering, one, money laundering by the interested party alone, and another, money laundering for a third party. The term of penalty varies.

9. The wording "may be exempt from criminal penalty" concerning money laundering for relatives in Article 10 was deleted.

10. The term of penalty for civil service employees when involved in money laundering schemes is raised to below 5 years in prison.

Next, in the aspect of continued enhanced interactivity with financial institutions, we, at the invitation of the financial institution, dispatched our staff to the interested financial institution to lecture on the MLCA with related cases so as to raise the awareness of financial institutional staffers on the issue of money laundering, hoping they may thus act aggressively to prevent money laundering as much as they can. For the year in question, there were 51 domestic and foreign financial institutions that had filed the SAR's, resulting in 791 cases, a remarkable growth compared to the year before. Nonetheless, the SAR's were mostly from the banking institutions and, therefore, extra effort is needed to promote compliance by other financial institutions other than the banking industry.

As to international cooperation, 2001 was the year that the ROC first accepted the APG mutual evaluation program, a first on-site visiting to Taiwan by the APG evaluation delegation since April 23, 1997 when the MLCA went into effect. Since the evaluation results would greatly affect the ROC's international reputation and image, prudent and comprehensive preparation to receive the APG evaluation delegation was made. Under the guidance of the MOJ and the concerted efforts of

the MOF's Bureau of Monetary Affairs, Securities and Futures Commission, Central Bank of China, MOFA's Department of International Organizations, National Police Administration, Bankers Association of the R.O.C., Bank of Taiwan, United World Chinese Commercial Bank, and Financial Information Service Co. Ltd., Taiwan, we had enabled the APG evaluation delegation to fully understand the R.O.C.'s overall money laundering prevention framework. The APG evaluation delegation gave us an affirmative praise over the R.O.C.'s anti-money laundering efforts, believing through filing of the SAR's and contact with domestic and foreign law enforcement agencies with regard to investigations of suspicious money laundering cases would help set a good foundation in the R.O.C.'s efforts in money laundering prevention.

The key points that the APG evaluation delegation had brought up may be summarized as follows:

1. On the aspect of the judicial and law enforcement agencies:

   Primary concerns related to prepositioned crime type in money laundering, number of cases occurred, seizures, confiscation, fund freeze, indictment, provisions set forth in the MLCA and key points of the follow-up amendment, difficulties, if any, in investigations of transnational money laundering cases, and access to banking account information by law enforcement agencies as well as outbound fund flow to foreign countries.

2. On the aspect of financial regulatory agencies and financial institutions:

   Primary concerns covered laws and regulations related to enforcement by financial regulatory agencies, enforcement progress, practice of internal control within financial institutions, training of and implementation by employees of the financial community, status of SAR's, frequency of financial inspections and problems discovered, whether money laundering is included as a major issue in financial inspections, and whether or not employees in financial institutions had acted as accomplice in money laundering.

   After three days of on-site visiting, the APG evaluation delegation released its evaluation results, praising positively the R.O.C.'s efforts in money laundering prevention. On the whole, the R.O.C. was given high scores in its enforcement of money laundering prevention. The APG evaluation delegation was particularly impressed by the R.O.C.'s inquiry system for account opening in financial institutions, citing the system should be patterned after in fellow APG member countries.

   In an effort to expand international cooperation business, MLPC dispatched its staff to be present at the annual meetings, workshops and seminars of APG, Egmont Group for a total of four times, not to mention the presence at mutual evaluation workshop sponsored by APG, the meeting entitled "The Seminar on Asset Forfeiture and Money Laundering" sponsored by the US Department of Justice and the meeting entitled "Special Meeting of Egmont Group Memkers" sponsored by the US Department of Treasury.

It has been close to five years since the MLCA took effect in Taiwan. Naturally, money

laundering prevention work has been gradually led to the right track with outstanding results. Nonetheless, shortcomings exist and further efforts are required so that improvement can be made.

### 1. Source of filed SAR's tends to be concentrated, not comprehensive

Despite increase in the number of financial institutions that filed the SARs and the number of cases reported each year, the informants tend to concentrate in the banking institutions and only few of them showed relatively better results. It is suggested that extensive efforts be made in education and promotion and contact aiming at institutions that fail to respond. In so doing, the source of SAR∏s filing may be expanded and money-laundering prevention may be extended to more levels.

### 2. Analysis of suspicious transactions encounter bottlenecks

Despite continued increase in the number of financial institutions that filed the SARs and the number of cases reported, indictment of major economic crime violation cases has not been correspondingly increased. The bottleneck we found out lies in: 1) lawbreakers have learned how to circumvent the MLCA now that it has been in force for almost five years; 2) deliberate cash draw has dislocated continued investigation in ongoing fund flow cases; 3) rampant figure head accounts have become a stumbling block in investigations of funds flow; 4) quality of filed SARs has not simultaneously upgraded as did the number of filed SARs; and 5) the concept of "money laundering indicators" remains vague in the minds of financial institutional workers.

### 3. Seizure of illicitly gained fund needs intensified enforcement

Illicitly gained funds are the lifeline of crime-committing syndicates. Therefore to cut off this lifeline of the crime-committing syndicates would be one of the most effective means in fighting against money laundering activities by crime-committing syndicates. Consequently the fund flow thus traced could be used as an evidence of crime committed. If the illicitly gained funds can be seized or frozen, it may further serve the goal of dealing a heavy blow to the crime-committing syndicates. However, it must be noted that seizure or freeze of illicitly gained funds has not been quite successful for violators have been on the alert all the times and have adopted a number of countermeasures to circumvent efforts made by investigative law enforcement agencies. Besides, increasing difficulty in enforcement has begun to surface. How to integrate financial institutions and law enforcement agencies in jointly enforcing the MLCA is indeed an important issue that requires immediate attention.

### 4. Discontinuation of roundtable discussions with financial institutions

Financial institutions are where lead of money laundering is first discovered. Quality of the SARs filed affects greatly and deeply the overall effect of money laundering prevention work. The SARs filed by financial institutions need the attention and support of high-level executives. As such, holding of roundtable discussions with high-level executives of financial institutions will not only serve to communicate the concept, but will also enable the financial institutional high-level executives to understand how lawbreakers operate and thereby raise their willingness in filing the SARs . But, much to our regret, we have not been able to hold the roundtable discussions on a yearly basis due to lack of funds. As a result, coordination and cooperation from different financial institutions varies. Improvement is needed.

## B. Focus in future work

### 1. Intensification of task force function in investigation support and sharing of experience

One of the MLPC's functions is to assist all law enforcement agencies in investigation of illicitly gained funds. In the face of the ever-changing and hi-tech new types of crime commission, the only alternative seems to lie in "division of labor, professional service and chase the offender after the money." When a major case breaks out, it requires a specially formed task force to conduct the investigation. The task force, organized with members from fellow law enforcement agencies, is to develop an elite team work function with limited manpower and funding. As a result, experience in investigation is shared and a pool of capable investigators is built up in order to be ready for a more challenging job ahead.

### 2. Promotion of surveillance parameter setup to anti-money laundering through the Internet

With the rapid development of computer and information technique, internet banking is bound to become a major trend in the financial services industry in the 21st century. Due to the special properties of the internet banking as seen in its "privacy, difficult to identify and hard to trace" convenient and swift transaction in e-banking transfer, however, internet banking is easily to become a money laundering tool for illegitimate syndicates. At the time of writing, domestic e-banking, as is noted, remains in the budding stage. Despite this, we need to prepare for the worst by coordinating with all competent financial regulatory agencies to supervise the financial institutions

in setting up an extensive surveillance parameter for internet transactions so as to prevent money laundering through e-banking. The new surveillance parameter would cover all transactions, including those transfers by non-cash.

### 3. Continuous promotion by holding workshops to launch an all-out money laundering prevention campaign

Our work is cut out to continue assisting related financial institutions and regulatory agencies in preparing training & education programs, thereby expanding the level of participants. In principle, each and every person-in-charge or contact person of each financial institution is required to participate in the money laundering prevention workshop. The person-in-charge or contact person shall be responsible for promoting money laundering prevention works in the institution where he/she works, effectively integrating all resources and passing related money laundering information onto fellow workers. In addition, the person-in-charge or contact person is also required to implement holding of workshops for high-level executives and, by law, filing SAR∏s so that an extensive money laundering striking network may be set up.

### 4. Implementation of international anti-terrorist norm and intensification of counter offensive measures

Following the September 11 attacks, anti-terrorism has become a global furor. In response, the MJIB∏s MLPC quickly established files exclusively on terrorists and, in coordination with the investigation into flow of foreign exchange and funds of a few specific individuals of the Middle East, the terrorists files were offered to related agencies for reference. In future, the files on terrorist groups or individuals are to be further enhanced and information on foreign exchange transactions via specific countries or areas will be filtered extensively. At the same time, we are to aggressively implement the 8 points of recommendation concerning prevention of money laundering by international terrorist groups made by the Financial Action Task Force, or FATF.

### 5. Expansion of international cooperation channels to fight against money laundering crime

Since money laundering is in nature a transnational movement of fund, it requires concerted efforts by all concerned governments to trace the flow of fund. As the financial intelligence center for the R.O.C, which is a member of the APG and Egmont Group, the MJIB∏s MLPC has tried hard to build up intelligence exchange partners in the international community. Under our extensive efforts throughout the years, the number of partners has gradually increased, although the limited funding available due to governmental budget retrenchment has greatly confined our participation in

international money laundering prevention activities. What we need to do in future is to try to break through the difficulties and utilize the limited resources to establish counter-part relations with other countries in order to establish intelligence exchange channels to jointly strike against illicit activities.

### 6. Intensification of collection of foreign laws on fund freeze and aggressively promote amendment to the MLCA

In conjunction with the MOJ's initiative to amend the existing MLCA, we would aggressively begin to collect laws on fund freeze in foreign countries to provide the MOJ for ready reference in their initiative to amend the existing money laundering control act so that the amended new act would match the international money laundering standards and effectively seize the illicitly gained funds.

# Part Five

# Essay

# Internet Money Laundering Crime and How to Prevent it

By Lin Chia-Shun

## A. Foreword

## B. Internet banking and information safety

1. What is Internet banking?
2. Development of R.O.C.'s domestic Internet banking

## C. Analysis of crime-committing models of money laundering through Internet

1. Money laundering model by use of smart cards
2. Money laundering model by use of Internet banking
3. Money laundering model by use of e-cash

## D. Money laundering cases and preventive countermeasures

1. Money laundering cases at home
2. Preventive countermeasures against money laundering via Internet

## E. Conclusions

## A. Foreword

Ever since the inception of World Wide Web (WWW), the so-called third industrial revolution or information revolution has brought about a new era of mankind. The rapid development and proliferation of Web[1] has not only discovered unlimited sources of knowledge for mankind, but also catapulted related industries into burgeoning development. Meanwhile, the gradually maturing Web environment has directly stimulated the rapid rise of electronic commerce, providing the opportunity to avoid the usual face-to-face conduct in future commercial activities. This revolutionary manner of transaction, i.e., transactions conducted easily via Internet in virtual space and across national border, is bound to upset traditional commercial behavior via fixed buying, selling, marketing and service channels and become the mainstream of future commercial transactions.

Growth of domestic Web population now is estimated to be a third of the total population, thanks to the burgeoning development of Internet at home. As a result, the quality of users varies, making cyber crime a latest crime-committing means in recent years. For example, shopping via Internet has often caused unauthorized use of credit cards; no merchandise received following completion of a transaction; no payment received after delivery; or even worse, hackers have invaded banking institutions via Internet to embezzle customer's funds in deposit, etc. As such, the ever-changing crime-committing scene in Internet has seriously affected economic development, particularly the financial service industry.

To meet the rapidly developed financial environment in the information age, the financial service industry has initiated a major revolution in its technology and service channels, that is the development of the virtual Internet banking service. Web entries, however, have given criminals opportunities to use the innate characteristics of the 'reality-free irrespective of space and time' Internet to cover up or conceal illicitly gained wealth resultant from a major crime. Consequently, conventional methods and thoughts of money laundering prevention need a facelift to cope with the emerging Internet banking service.

## B. Internet banking and information safety

### 1. What is Internet banking?

Internet banking may present in different names and different forms. It could be called Internet banking, on-line banking, electronic banking, or even cyber banking. As to the substance, it also invites different interpretations, depending on how you look at it. Thus, the definition for Internet

banking, as viewed by Taiwan's MOF's Bureau of Monetary Affairs through the "Sample Copy of Contract for Personal E-Banking and Internet Banking Service", hereinafter called the Contract, promulgated May 26, 1999, indicates "... linked from the customer's computer end, the customer may do his/her banking through Internet with his/her bank, without going to the bank's counter in person...."[2] while the definition of electronic banking given by Bankers Association of the R.O.C. in its "Operating Basis for Safety Control over Electronic Banking by Financial Institutions", hereinafter called Safety Control Basis, filed with Ministry of Finance, refers to "Financial institutions and their customers conduct banking services via electronic equipment and communication equipment without requiring the customer to visit the banking institution in person"[3]. Compared the two, it seems the Contract has directly civilized Internet banking as a tool.

Further, Office of the Comptroller of the Currency, OCC, of the United States defined Internet banking in its Internet Banking, Comptroller's Handbook published in October 1999 as " ... systems that enable bank customers to access accounts and general information on bank products and services through a personal computer (PC) or other intelligent device." The definition is concise and precise.[4] Since Internet banking has the characteristics of 'open 24 hours, instant interactivity, and without the limitation of space and time', bank customers may, regardless wherever he/she is at, fund transfer may be conducted anywhere, and instructions to order purchase of stocks or money transfers may be done any time. The practice may completely upset the existing consuming and money management models for the newly emerging electronic payment mechanism[5] offers a more convenient and comprehensive and anonymous characteristics than conventional currency transactions. The added features in e-banking provide no-limit transfers in a safe and transnational environment, circumventing conventional banking restrictions and overseeing by law enforcement agencies. At the same time, the private, difficult-to-identify and hard-to-trace characteristics concerning customer data offered by both the e-banking institutions and electronic payment mechanism have provided additional incentive to criminals to use the service in money laundering. Furthermore, since the safety measures in present Internet banking leave much to be desired, money laundering offenders may, in theory, reach on-line accounts of others and use fictitious identity to transfer funds in order to circumvent investigation by law enforcement agencies.

## 2. Development of R.O.C.'s domestic Internet banking

Electronic banking in Taiwan started in June 1984 with the ATM system that replaced conventional counter service to enable account holders to draw cash, check banking statement and transfer fund from the automatic teller machine. Starting 1994, banking institutions began to set up the so-called man-less banking service through the ATM and other periphery equipment to replace otherwise the counter service, accomplishing the purpose of branch automation. Apart from offering more convenient services to customers, the move also saves the banking industry massive labor cost. With the approval of the regulatory agencies, banking institutions further provide telephone banking, offering limited banking services through such safety mechanism as password and pre-set

account number. At the same time, under the supervision of the regulatory agency, the then Financial Information Center(now Financial Information Service Co. Ltd., Taiwan) was instructed to draft domestic financial EDI standard and set up common financial EDI system to provide businesses B to B payment system in a closed-end Internet environment, thus enabling businesses to achieve the efficiency of automation operation.

In recent years, with the development of the Internet and employment of various information technology, MOF's Bureau of Monetary Affairs, under the expectation of the general public and the plea of the financial industry, lifted in May 1999 restrictions on Internet banking services that included fund transfer and instructions for transactions imposed on the banking industry. In addition, use of cell phone has become increasingly popular. Together with information technology, innovation in the financial service sector has excelled itself continuously. In October the same year, the MOF's Bureau of Monetary Affairs added mobile banking services that domestic banks have been allowed to operate. In view of the potential development of the Internet banking that may affect the financial turf in future, domestic banks have begun aggressively to deploy Internet banking service. This is particularly true with newly opened banks as they have used their electronic edge to make up their weakness in having fewer branch offices.

In view of the development in the Internet banking and the strong need to set up a comprehensive e-bank for the banking industry, as well as taking into account transaction safety and consumer's interest, the Ministry of Finance instructed in 1998 Bankers Association of the R.O.C. to aggressively draft the operating basis for safety control over electronic banking and a sample contract thereto to be served as a complementary measure to open e-banking business by the banking industry. The operational scope of the basis and contract should include such e-banking businesses as PC banking and network banking. The former enables account holders to be linked with the bank via an exclusive network and value-added network while the latter enables account holders to be linked with the bank via the Internet. [6]

At present, Internet banking service items by domestic financial institutions briefly are divided into: 1) business to customer, or B2C. Under this category, services provided by the bank include statement checking, checking on details of transactions, checking on inward/outward remittances, collection of bills for deposit, and checking on needed supplementary bills by checking account holders. Functions provided by B2C enable account holders to operate independently on-line transfer, pre-reserved transfer and credit card payment between the same account or different accounts; and 2) business to business, or B2B. Under this category, services provided by the bank include transfer of wages, package remittance, package issuance of bills, and pre-reserved financing by remittance. Other functions provided by B2B enable account holders to check the inventory of suppliers and make transaction through the e-commerce transaction platform aligned freely by the account holders, not to mention on-line payment of loans. In addition, to place on-line orders for mutual funds and collection of credit card payments have become gradually a new major indicator service item of domestic banks that provide e-banking financial services.[7]

## C. Analysis of crime-committing models of money laundering through Internet

Compared with conventional financial services, Internet banking uses digital or electronic means for disbursement. The disbursement message carries digital symbol and, in the delivery process, must be encrypted until its reaches the recipient when the message is de-encrypted to return to the original form. As such, money laundering through the Internet may employ the Internet banking facilities and the various new disbursement systems to conduct financial transactions and thereby engage in various criminal activities, inclusive of money laundering[8]. By the estimate of related UN agencies, there are at least some US$300 million worldwide transacted through the cash-less e-banking for money laundering[9]. To analyze by the three-stage theory, money laundering handlers must first bring the illicitly gained funds into legitimate businesses such as the banking institutions, securities dealers or real estate business for placement. At the same time, source of the fund and identity of the owner should be concealed as much as possible, not to mention acceptance of deposit as does conventional financial service industry. The e-banking facilities just provide such high safety and privacy that placement dictates. In the layering stage, movement of the illicitly gained funds must go through a series of reliable and diversified transactions to cover the source, ownership and location. Money laundering handlers may use the Internet disbursement method with encryption to move the illicitly gained funds around the world few times in a day. By virtual technology, substance movement of the illicitly gained funds may be avoided. In the integration stage, e-banking permits cash transfer from person to person, thereby circumventing the regulation for report of transaction. Transactions via ATM by smart cards enable cash movement in practically every country of the world that allows money laundering handlers to completely launder the illicitly gained funds and lead the funds into normal financial system. The following analyze how money laundering handlers may use smart cards, the Internet banking facilities and the various new disbursement systems to conduct money laundering:

### 1. Money laundering model by use of smart cards

The IC chip embedded in the smart cards possesses highly efficient memory that allows cardholders to click on ATM machines or use as a credit card, once value having been stored, in IC-equipped stores or P.O.S. (point of sales) machines. At the time of writing, smart cards are mostly in the experimental stage in most of the FATF (Financial Action Task Force) member countries. As such different operation characteristics have been found. Some systems provide anonymous transactions while some systems offer mechanism to trace transaction information. Since the stored value of the smart card has been charged, financial institutions suffer no losses in case the card is reported lost and, in theory, there is no need to restrict the stored value of the card. Somehow concern by FATF members countries about the development of anonymous transactions has placed a

ceiling in the stored value of smart cards, for example, in England, the limit is 'G50-'G500, or US$74-US$740, converted at the rate of 1:1:48. However in some non-FATF countries, the limit can be as high as US$92,000. In addition, despite most of the systems do not allow direct transaction from card to card, some systems have developed functions that permit cardholders to transfer funds directly without the media of the financial institution, thus leaving no record of transaction. Moreover, there is no restriction on the sum transferred, or any regulations imposed upon cardholders in transaction. In short, there is no way to trace what has been transacted. Further, smuggling of smart cards to cross national borders can hardly draw any attention from anybody. As the value of smart cards can be stored through ATM, telephone, e-wallet, and PC, appropriate preventive measures must be established before money launderers exploit the opportunity to launder money. It is estimated that transactions through smart cards worldwide have grown from 250 million cases in 1966 to  billion cases in 2001. Here at home, we need, in the course of developing this line of business, to prepare the eventuality that smart cards may one day turn to be a tool for money laundering.

## 2. Money laundering model by use of Internet banking

Internet banking offers financial transaction service via the Internet. Under this disbursement system, customers may conduct on-line fund transfer, limited by the sum of transaction or the party on the receiving end and, besides, the parties must have accounts in the financial institution. But what worries people is the whole system lacks uniform regulation by the regulatory agencies. As such despite the on-line transactions are conducted between specific account holders, the identity of people that conduct the transactions via the Internet are hard to identify, once the account is opened. Should the banking institution is situated in an area where protection of customer's privacy as provided by the Bank Secrecy Act or BSA, is superior to the money laundering act, it may not or even not be required to check the identity of people who open on-line account. By computer terminal, funds may then be easily transferred and laundered.

## 3. Money laundering model by use of e-cash

E-cash is the electronic money of the Internet. As different from the smart card, initial purchase and final settlement stage of e-cash both go through the banking institution while the transactions provides no trace to check. Therefore e-cash account holders may store e-cash in the smart card and, once authorized, debit the charge to the e-cash account and finally the charge is deducted from the general banking account. The safety mechanism of e-cash must ensure that the value can be stored only through authorization and not repeated consumption. When e-cash is offered, the issuing financial institutions must face the inevitable issues of verification, execution of e-contract, and protection of the Internet data. Anonymous e-cash is similar to conventional currency, paper money that may too hinder financial institutions from the obligation of reporting the final sources of e-cash

transaction. Further, by the use of electronic encryption, e-cash transaction is protected and difficult to be detected by law enforcement agencies. Characteristics of independence (transfer via Internet and not subject to any specific area) of e-cash transaction and its safety (no copying or repeated use), non-tracking (protection of user's privacy renders it impossible to trace consumption status) off-line disbursement (e-shopping is conducted off-line without going through banking institution), transferability (others allowed to use the same card), and segmentation (segmented into several limits with the final total corresponding), especially, the characteristics of independence, non-tracking and transferability, have provided the best money laundering channels for unlawful characters.

## D. Money laundering cases and preventive countermeasures

### 1. Money laundering cases at home

a. In an attempt to seek the unlawful possession and, on the basis of general guilty intention, Chiu altered a Hong's ID in February 2001 by replacing Hong's photo with his and ordered Hong's seal. With the altered ID along with the unauthorized seal of Hong's and Hong's bogus signature, Chiu opened new bank accounts with telephone banking services at Cosmos Bank, Taiwan, The Chinese Bank, Taoyuan Branch of Taiwan Cooperative Bank, Toucheng Branch of The Chang Hwa Commercial Bank, Ltd., Toucheng Branch of E. Sun Bank, The International Commercial Bank of China Taipei Office, Chungho Branch of Grand Commercial Bank, Bank of Taiwan Head Office, Dah An Commercial Bank, Yingko Branch of First Commercial Bank, Fubon Commercial Bank, Panchiao Branch of Taipei Bank and Toucheng Branch of The International Commercial of China from February 20 to March 15. Separately, in April the same year, Chiu, equipped with altered national ID cards and unauthorized seals of a Peng and a Yu, repeated the same act by opening savings accounts with telephone banking services in the names of Peng and Yu at Cosmos Bank, Taiwan, Yungho Branch of The Chinese Bank, Chungho Branch of First Commercial Bank, Chungho Branch of The Chang Hwa Commercial Bank, Ltd., Yungho Branch of Makoto Bank, Panchiao Branch of Taishin International Bank, Hsintien Branch of The International Commercial of China, United World Chinese Commercial Bank and Chiao Tung Bank.

Later, as of a certain day in April 2001, Chiu, knowing precisely 「TAIWAN-CA. COM Inc.」[10], hereinafter called the Certification Company, provides customers FEDI service that allows users to surf its website via Internet to download information of customers with electronic data interchange (EDI) certificate authority, or CA, already issued, surfed the Certification Company's website from several unspecified cyber cafes to click on the "request for

authorization by use of trading partner's Chinese names" column to obtain consecutively the safety codes and ID numbers, and digital financial vouchers of several corporate and individual account holders and, via the Internet, surfed http://netbank.icbc.com.tw, the website of The International Commercial Bank of China, to test one by one under the columns of user's code and passwords the corporate names, uniform serial numbers, individual's names, ID numbers, etc. obtained from the Certification Company's website previously. In the process, Chiu was able to obtain several groups of ICBC's account holders' codes and passwords. Once succeeded in the individual account holder's page, Chiu went further to surf columns of statement of deposit, balance of filed deposit, inquiry by customer regarding Internet banking services in order to copy user's codes, ID numbers and related information of the accounts visited.

Later, Chiu visited the homepages of The International Commercial Bank of China, Taishin International Bank, United World Chinese Commercial Bank, and Bank SinoPac to repeat the same testing process he did previously. If succeeded, Chiu would, in the name of the account holder, surf the Internet to spot transfer details and duplicate the account number that may be too in other banks to visit the list of codes for financial institutions used for money transfer through ATM shown on the web page of Financial Information Service Co., Ltd. Once the names of the bank for the accounts in question are located, Chiu would repeat his act in the same manner as demonstrated in the preceding paragraph. Through on-line money transfer, Chiu had diverted in several batches the deposit in the accounts into accounts opened in the names of Hong, Peng and Yu. Later, with the financial cards issued by the opening banks, Chiu drew cash from Hong, Peng and Yu's accounts, making all involved banks to surrender cash in the accounts in question and avail Chiu to seize the property of others. As a result, Chiu also concealed the illicitly gained wealth by committing a major crime out of his professional fraud.

b. Analysis of illegal types

So far as money laundering handlers are concerned, they engage in illegal activities or illegal transactions to launder their illicitly gained wealth through financial or non-financial institutions to conceal the source or substance of the illicitly gained wealth. As the move enables them to cut off the correlation between the funds and the illegal activity/transaction, they may circumvent tracking by law enforcement agencies and achieve legalization of the illicitly gained wealth. In general, money laundering offers three steps - placement, layering, and integration - for observation. Take for instance, defendant Chiu in the case cited above used the surfing facilities provided in cyber cafes to obtain information such as names, codes, passwords, etc. he needed to commit the cyber crime. By navigating through the web pages, he tested the authentication of the information he had on hand to further augment his collection of more needed information. By using the convenient characteristics of the Internet banking or telephone banking service for money transfer, Chiu had, with the input of directive, instructed the Internet banking or telephone banking to divert deposit in the legitimate accounts into the accounts of

Hong's, Peng's and Yu's opened under altered ID's, etc. He covered up his illicitly gained wealth and the route through which he obtained, thereby exempting him from criminal prosecution. The process presents placement, layering, and integration, the three steps seen in every money laundering case. Chiu's act meets the description.

In addition, Surveillance Ninth Squadron of Criminal Investigation Bureau has recently cracked a cyber crime committed by unlawful characters. The scheme was to pirate the currently popular on-line game 'Virtual Treasure' and prescribe a specific ratio of exchange rate of New Taiwan dollars as set in the 'Virtual Currency' for the 'treasure' so as to cover up the illicitly gained wealth suspicious of money laundering. [12] Cases like this indicates that offenders have, through the "Louma" software program monitored and intercepted the account number and password of players temporarily stored in the Temp to further pirate the virtual treasure temporarily stored by other players. To do this, all one needs to do is to use the keylog program to read and translate files compiled with garbage codes. Police authorities referred the case to the prosecutor's office on charges of theft, fraud and money laundering. Still it is hard to say, if the case can be prosecuted using Money Laundering Control Act.

## 2. Preventive countermeasures against money laundering via Internet

a. Enactment of laws and regulations related to money laundering via Internet

At present, there are no special laws and regulations pertaining to money laundering prevention. The existing Money Laundering Control Act (MLCA) lists, by the individual business type, different samples of money laundering activities seen in different financial institutions. Meanwhile, it has been noted that the model points to note for money laundering activities given by financial institutions are mostly patterned after the MOF-induced suspicious money laundering signs[13] when it comes to recognition of SAR's, adding or subtracting slightly to suit the business needs of the individual institution concerned. We may therefore suggest that MOF and trade associations of financial institutions add more suspicious money laundering signs in reference of the money laundering models cited in preceding paragraphs so as to be served as a basis for e-banking institutions when filing SAR's.

The current filing system for money laundering prevention is required by Article 8(1) of the MLCA. It relates to suspicious activity report, or SAR, irrespective of the sum involved. To lessen the burden of financial institutions, MOF has, by administrative order, set in principle the minimum requirement of NT$1.5 million in cash transaction, if and when the transaction is suspicious of money laundering. It is recommended that in Internet banking, irrespective of the sum of transaction that is over or below NT$1.5 million, in cash or not, the concerned banking firm establish an auto detecting mechanism and file the SAR's in a timely manner.

In addition, we may further suggest the MOF add provisional provision that allows freeze of a specific account whose activity is suspicious of money laundering. In so doing, the evidence

may be retained intact and the interest of the victim may be protected. As to the existing standard procedure in financial institutions which calls for keeping on file transaction records, we suggest it may be amended from time to time in conjunction with the opening of e-banking so as to enable law enforcement agencies to seek and retain related evidential electromagnetic records in the course of investigation of suspicious money laundering activity.

b. Amendment to related provisions concerning confirmation of account holder's identity and keeping on file transaction records

Article 7(1) of the MPCA provides that when a certain sum in currency is transacted, the concerned financial institution should check the identity of the account holder and keep on file the transaction record. The prevalent recognition of this certain sum in currency is NT$1.5 million or more in cash transaction or change of money that may lead to money laundering through T/T or other channels by criminals. Money transfer through e-banking in future, when currency transaction is not involved, there is no requirement to check the identity of the account holder and keep on file the transaction record, so stipulates the existing MLCA. However, the source of deposit and the flow of the cash after the withdrawal, the banking institutions should in principle strictly observe the rules of checking the identity of the account holder and keeping on file the transaction record. In the intermediary stage, the direction of fund flow is bound to cause a loophole in money laundering prevention. In future when e-banking operation allows fund transfer to and from offshore points, it could even become a tremendous challenge to the work of money laundering prevention. Concerned agencies should be prepared to draft responsive counter measures at an early date. We pay pattern after the United States to draft an act concerning fund transfer via Internet. The proposed bill may administer the increasingly popular e-transactions properly and thus establish effective money laundering prevention mechanism.

c. Intensification of control over financial business via Internet

It has been for some time since the MOF approved electronic transfer by banking institutions and, accordingly, the banking industry as a whole have aggressively set up transfer systems on the Internet with comprehensive security measures in force such as secure electronic transaction (SET) or secure socket layer (SSL). However, should the threshold of transaction use only user code and password whereas the password is fixed, the risk in transactions via Internet is quite high. It works like this: the bank end is responsible for checking the account holder's identity and ensuring security, account holder may, once the personal identify such as ID number and the password are verified, proceed with the transaction via Internet and the system will, in accordance with the instruction, transmit the message to related units to conduct the transaction. In other words, the front end system is responsible for security and the rear end system is responsible for relaying information as instructed to related units to conduct the transaction. As

such, identity checking of account holders in e-banking is extremely important. Apart from the strict requirement for face-to-face contact when new account is opened[14], efforts should not be spared in trying to avoid fictitious figure-head account holders from engaging in money laundering activities via Internet. It is suggested that all account holders banking via Internet are required to apply for an electronic ID, verified by digital process in order to ensure security of transactions via Internet.

As for financial institutions, it is extremely important to check account holder's identity prior to the transaction process, a process preferably requiring digital application and verification. To account holders, user code and password should be strongly protected, trying by all means and at all times to avoid use of such easily thought of numbers as birthday and the like, not to mention change of the password from time to time. At the same time, it is suggested better not to conduct transactions in such public places as cyber cafes for computer software often has the function of memory, just in case the account is invaded by unlawful characters.

d. With the rapid development and technical update of e-banking, smart card, on-line banking, e-cash and all sorts of neo disbursement systems, it is estimated that acceptance and practice by nationals at home of these new e-devices must be continuously on the rise as well. E-wallet and e-credit card, the two models now available in the marketplace, may stop part of the money laundering activities for there is a limit on the amount that can be transacted. But in the face of the impact brought upon by the drive of financial liberalization, it is naturally that more and more new disbursement tools via Internet will be brought in at the home market. Should there be no appropriate restrictions on use of the new tool such as limit on the stored value of smart card or transaction and issuing institution be limited to banking firms only, e-banking would be difficult to prevent unlawful characters from using the service as a new channel for money laundering.

## E. Conclusions

Appearance of the Internet has made it more convenient for transmission of information worldwide. To the banking industry, it produces even a great impact, allowing many of the conventional financial services to be provided on-line. As such, a burgeoning development of financial services via Internet at home would be a trend in future that would be hard to stop. Consequently, it would be the inescapable responsibility of law enforcement agencies to prevent money laundering activities using the latest information technology via the Internet to destroy global financial security system. The innate characteristics of cyber crime have made it necessary that law enforcement agencies must meet head-on the challenge and needs the cyber crime creates. Investigative capability can be only enhanced when related sources, tools and education and training

are provided. Needless to say, further promotion of international cooperation among counterpart law enforcement agencies has become another must in coping with the increasingly changing crime-committing practice used in money laundering.

## Annotation:

1. Statistics released by Euro-Marketing Associates (http://www.euromktg.com) indicates worldwide Internet population has grown from 1 million in 1990 to 150 million in 1998; separately, by the statistics compiled by Focus on Internet News & Data ( http://www.find.org.tw) on August 2, 2001, the Internet population in Taiwan at the end of June 2001 had reached 7.21 million, or a popularity rating of 32%.
2. Please refer to Article 2(2) of the sample contract in question.
3. Please refer to Article 1 of the Basis for Safety Control in question.
4. Legal Issues of Internet Banking, Hsieh Yi-hung, pp. 122-123, 月旦法學雜誌, Issue 71, April 2001.
5. The so-called e-disbursement mechanism generally comprises the following three: 1) function of transfer, i.e., debit card; 2) function of store of value such as stored value card, IC financial card, smart card, electronic wallet and national ID card; and 3) function of on-line payment, referring in general disbursement of e-currency via Internet. For details, please refer to The Rise of e-Disbursement Mechanism and Related Legal Issues Thereof (Volume I), by Kuo Kuan-pu, 資訊法律透析, pp 40-49, January 2000 Issue
6. Please refer to From Development of Internet Banking to the Challenge Ahead for Taiwan Financial Regulatory Agencies, by Lin Yu-ting, 資訊法律透析, March 2000 Issue
7. Please refer to the previous article, page 127.
8. The so-called New Disbursement System refers to electronic transactions by the use of smart card, on-line banking, e-cash, etc. For details, please refer to The Challenge in the Development of e-Commerce - Related Money Laundering Issues via Internet (Vol. I), by Hsieh Li-kung, 科技法律透析, pp 4-7, October 2000.
9. Please refer to Commercial Times, page 6, May 27, 1998.
10. The website for TAIWAN-CA. COM Inc is http/:www.ca.taica.com.tw.
11. Financial electronic data interchange, or FEDI, refers to electronic transmission using a certain standard and data format via an agreed communication protocol to proceed the operation interface of business or individual financial services. Through on-line linking or financial value-added network, business or individual allows the other party via computer to automatically exchange information, process and make appropriate responsive mechanism to access the financial identity issued by a banking institution and verify the identity of the transacting party. After the formalities, transaction may begin via Internet directly for such financial services as transfer of funds, use of e-wallet, payment of taxes, payment of fees, money transfer, transmission of financial documents and exchange.
12. Please refer to social news dispatched by the Central News Agency on September 10, 2000.
13. Please refer to The Model Points to Note for Money Laundering Prevention in the Banking Sector, issued by MOF per Tai-Tsai-Yung-Tze-86086098 dated March 26, 1997.
14. Comptroller of the Currency of the US Department of the Treasury requires financial institutions

engaged in e-banking to specially request account holders banking via Internet to sign an account agreement before transactions can be conducted via Internet.

## Bibliography:


1. The Rise of e-Disbursement Mechanism and Related Legal Issues Thereof (Volume I), by Kuo Kuan-pu, 資訊法律透析, January 2000 Issue.
2. The Impact of e-Cash upon the Financial Industry, by Chang Li-chuan, 台灣經濟金融月刊, Vol. 36, Issue 10, October 2000.
3. From Development of Internet Banking to the Challenge Ahead for Taiwan Financial Regulatory Agencies, by Lin Yu-ting, 資訊法律透析, March 2000 Issue.
4. Legal Issues of Internet Banking, Hsieh Yi-hung, 月旦法學雜誌, Issue 71, April 2001.
5. Money Laundering Prevention and Maintenance of Economic Order, by Hsieh Li-kung, published by Banking & Finance Institute, Taiwan, March 1999.
6. The Challenge in the Development of e-Commerce - Related Money Laundering Issues via Internet (Vol. I), by Hsieh Li-kung, 科技法律透析, October 2000.
7. The Challenge in the Development of e-Commerce - Related Money Laundering Issues via Internet (Vol. II), by Hsieh Li-kung, 科技法律透析, November 2000.
8. Practical Investigation of Cyber Crime, by Chang Shao-ping, training material for Seminar on Investigation and Surveillance of Computer and Network Crime-committing Technique, Cadet Training Institute, MJIB
9. Review of Shortcomings in Money Laundering Prevention by Financial Institutions and Preliminary Suggestions for Improvement, by Chan Te-en, 台灣金融財務季刊, March 2001.
10. The website for Best Green is http://www:fisc.org.tw.

# Appendix

## The Model Points to Note for Anti-money Laundering in the Banking Sector

(On file for reference of Letter re Tai-Tsai-Yung-(A)-Tze-#0900015015 dated January 4, 2002 to Bankers Association of the R.O.C. by Ministry of Finance )

1. The Model Points to Note for Money Laundering Prevention in the Banking Sector are established in accordance with Article 6 of the Money Laundering Control Act (MLCA) and are intended to serve as a guidance in prevention of money laundering.

2. In practice, the points to note for money laundering prevention are as follows:
   a. Points to note when a new account is opened:
      (1) The prospective account holder should present personal identification for verification; if it is a personal account, the national ID card or passport is required; if it is a non-personal account, presentation of registration papers, documents or related identification documents are required, save the tax return. When the prospective account holder refuses to comply, tacit rejection to proceed with the process should be in order or wait until the identification is verified.
      (2) With respect to prospective account holder presented with power of attorney or authorization, the fact of the power of attorney or authorization must be verified; should the verification be difficult to proceed, tacit rejection to proceed with the process should be in order.
      (3) With respect to other points to note, the internal standing operating procedure shall govern.
   b. Points to note when after a new account has been opened:
      (1) With respect to accounts opened in the form of power of attorney or authorization, or suspicion is found after an account has been opened, verification should be followed by telephone, written communication or on-site interview.
      (2) When an account has been opened with official document or other letter, use registered mail to verify.
   c. Points to note with regard to transactions after a new account has been opened:
      (1) With respect to currency transactions of a certain sum or more, it is a must to check the identity of the account holder and keep on file the transaction record.
      (2) The currency transactions of a certain sum or more mentioned in the preceding paragraph refers to NT$1.5 million or more of one or more transactions in cash or its equivalent in foreign currencies deposited or withdrawn in the same business day of the same account or transactions of change of money.
      (3) Should it occur that any of the following events be found to exist in transactions of an

account, special attention must be paid. When it is believed that suspicious money laundering transactions, irrespective of the sum involved, are conducted through the account in question, the case must, in accordance with The Points to Note hereof, be reported to MJIB, in addition to checking the identity of the account holder and keeping on file the record of transaction.

(a) If an account holder suddenly makes an unusually large deposit which is clearly not compatible with their identity and status, or unrelated to their business areas.

(b) If a large sum of cash is suddenly deposited in or withdrawn from a dormant account or one in which no transactions have taken place for a long time, and is then rapidly transferred.

(c) If, immediately after opening an account, an account holder makes a large deposit which is clearly not compatible with their identity and status, and which is then rapidly transferred.

(d) If a large number of small sums are deposited in an account, and the money is then withdrawn, either in one large withdrawal or in several smaller withdrawals, leaving only a nominal balance, and the amounts involved are clearly incompatible with the account holder's identity and status, or are unrelated to their business areas.

(e) If an account holder regularly transfers large sums of money between accounts, or asks to process the transactions in cash.

(f) If all of an account holder's deposits and withdrawals are for similar amounts of money, and only a short amount of time elapses between them.

(g) If a large sum of money is remitted from specified areas (non-cooperative countries) such as the Coke Islands, Dominica, Egypt, Guatemala, Grenada, Hungary, Indonesia, Israel, Lebanon, the Marshall Islands, Myanmar, Nauru, Nigeria, Nieu, the Philippines, Russia, St. Kitts and Nevis, St. Vincent, Grenadines and Ukraine, and then remitted out again a few days later, or if a large sum of money is remitted directly from the ROC to one of the regions mentioned above, and the nature of the transaction is not related to the account holder's identity. (The list of non-cooperative countries or economies is renewed based on information furnished by Financial Action Task Force (FATF).

(h) If an account holder purchases large quantities of foreign exchange, but is unable to give a clear explanation as to what it will be used for, or if the amount purchased is not consistent with their identity or area of business.

(i) If an account holder regularly asks for small bills to be changed for large bills, or vice versa.

(j) If an account holder regularly deposits large sums in a particular account on behalf of another party or parties.

(k) If an account holder regularly deposits amounts slightly smaller than the amount which must be reported, and then has these sums remitted to other cities or regions.

(l) If an account holder suddenly repays a bad debt of large sum, and is unable to offer a convincing explanation as to the source of the funds.

(m) Other transactions which are clearly abnormal.

(n) Information of transactions by terrorists or terrorist groups or the terrorists or terrorist groups being the final beneficiary provided by American Institute in Taiwan.

(o) Deposits or withdrawals of or remittances by those involved in reports of significant special cases in TV, news media, periodicals included, or Internet.

(p) A group of people flock to banking institution to conduct transactions in the form of deposit, withdrawal or remittance.

Where financial institutions have only renewed the list of non-cooperative countries or terrorist groups and have not amended The Points to Note hereof, there is no need to file the update to Ministry of Finance for file and reference.

3. Internal control procedure concerning prevention of money laundering:

a. Filing method and duration of keeping on file for complete transaction vouchers:

(1) Filing method: Complete transaction vouchers and original documents for transactions suspicious of money laundering should be kept on file.

(2) Duration on active file: Minimum of 5 years.

With respect to closed accounts, related documents such as photocopied ID, account statement, and address of account holder should be kept on file for 5 years.

b. Points to note concerning behaviors of account holders and staffers in financial institutions:

(1) Should it occur that any account holder be found to behave in one of the following manners, service may be refused and the case should be immediately reported to the supervisor:

(a) After an account holder has been informed of presenting related information for identity checking in accordance with law in connection with the currency transaction, the account holder steadfastly refuses to comply.

(b) Any individual or group that has coerced banking employee not to keep the transaction record on file or report the transaction to the regulatory agency as required by law.

(2) Should it occur that any banking employee be found to behave in one of the following manners, spot check over the business he or she handles must be conducted and, if necessary, request for assistance from the auditing department may be in order.

(a) Luxurious living, obviously not compatible with income.

(b) Refusal to take leave without proper cause when the leave is due.

(c) Failure to present convincing explanation with respect to deposit and withdrawal in huge sum.

c. Flow process of internal filing regulations and procedure of filing with designated government agencies:

(1) The bank shall assign a VP or an executive in similar level to be in charge of and jointly supervising implementation of The Points to Note hereof and participate in training courses on money laundering prevention. New recruits must complete the course within 6 months after employment begins.

(2) For each branch offices, a senior managerial executive should be assigned to oversee implementation of the program.

(3) Filing flow process:

(a) If the handling clerk in any units finds any transaction suspicious, he or she should immediately report the case to the supervisor.

(b) The supervisor in charge must at the earliest decide whether the case is subject to report to the authorities.

(c) If it is, the handling clerk must fill in the report in accordance with the standard form.

(d) Submit the report to the head office via the usual channel of command.

(e) The business unit at the head office forwards the report with comments to the VP or an executive in similar level before the report is routed to the regulatory agency.

Should the case be obviously of importance and emergency, each unit is required to use fax or other feasible means to file the report at the earliest possible time and immediately prepare the written information for report to MJIB.

(4) Confidentiality requirements to prevent leakage of reported data and information:

(a) Once the report is filed in accordance with established rules, all employees at all levels should keep the information strictly confidential.

(b) With respect to related documents, it must be done in the manner as do secret documents; if anybody is found to have leaked the information, he or she shall be dealt with in accordance with related regulations.

(5) With respect to internal control measures, regular review must be made to determine whether or not it is adequate to serve the goal of money laundering prevention:

(a) This bank shall make regular review of the established points to note concerning anti-money laundering activities.

(b) Where branch offices are numerous and widespread, meetings should be held by region to review the money laundering prevention operation so as to collect different findings from among all concerned staffers.

(6) Job description of the auditing department with respect to the job:

(a) The auditing department shall, in accordance with the internal control measures and

related established rules, hold regular auditing.

(b) Any negligence by the executing units found out by the auditing department shall be reported regularly to the VP or an executive in similar level in charge for perusal and may be used as a reference material in the on-the-job training class.

(c) Should the auditing department find any serious violating incident and conceal the fact without reporting to the executive in charge, the responsible unit at the head office should take appropriate action to deal with the case.

(d) The auditing department of each bank shall assign full-time employee to conduct spot checks of transactions involving huge sum at each unit and try to see if the transaction is legitimate.

(7) When a bank is concurrently engaged in the banking business, The Points to Note hereof also applies to the business department of the bank; if a bank is concurrently engaged in the bills business, The Points to Note hereof also applies to the bills department of the bank

4. Holding of regular seminar or on-the-job training on money laundering prevention

a. Pre-employment training: Minimum few hours of training courses of laws and regulations related to money laundering control and the legal responsibility imposed on employees of financial institutions should be arranged for new recruits so that the fresh employees may understand related regulations and their legal responsibility.

b. On-the-job training

(1) Initial promotion of established law: After the MLCA went into effect, all financial institutions should, within the earliest possible period of time, train their employees to familiarize with the MLCA and related laws and regulations and make known related and complementary responsive measures taken at the bank. Once the money laundering prevention supervising unit completes the preparation, the training unit may take over to arrange training courses for employees.

(2) Regular on-the-job training:

(a) The training department should hold regular annual training courses for employees to study so as to enhance employee's judgment and implement money laundering preventive functions and avoid employees from acting against law.

(b) The training course mentioned above may be incorporated in other appropriate professional training courses.

(c) Apart from the bank-trained lecturers, courses related to money laundering prevention may, depending on actual needs, retain outside scholars and experts from Ministry of Justice, Ministry of Finance, colleges and universities or other institutions.

(d) The money laundering preventive courses may, apart from related laws and

regulations, aid with actual case studies so that employees may fully understand signs and types of suspicious money laundering activities. It will help discovery of transactions suspicious of money laundering.

(e) The planning and supervising units in charge of employee training should regularly keep pace with the training status and urge those who are not participating in the course to enroll, depending on actual needs, in courses related to their job.

(f) Apart from the internal on-the-job training, the bank may assign its employees to enroll in other training courses of outside training institutes.

(3) Theme lecture: In order to enable employees to learn more about money laundering control ordinances, the bank may hold theme lectures by inviting scholars and experts from outside institutions.

5. Incentive measures for employees who have contributed to the work of money laundering prevention:

Appropriate incentive should be awarded to employees who have contributed to the work of money laundering prevention in any of the acts mentioned below:

a. Discovery of suspicious money laundering case and report in accordance with related anti-money laundering laws and regulations, leading law enforcement agencies to enhancing prevention or breaking the case as a result.

b. Employees scoring high points in related money laundering training courses overseas or having collected worthy information of foreign anti-money laundering ordinances that financial institutions may use in anti-money laundering activities.

6. The Points to Note shall, subject to review each year, take effect following resolution by the Board of Directors or the responsible unit delegated with the authority by decentralization of authority and submit to Ministry of Finance for file and reference. The same shall apply to subsequent amendment.

## The Model Points to Note for Anti-money Laundering in the Securities Dealers Sector

Acknowledge is made with reference to the MOF (90) Tai-Tsai-Cheng (Fa)-#174016 of January 4, 2002.

1. The Points to Note is established in accordance with Article 6 of the MLCA.

2. In order to prevent money laundering, the company shall act in pursuance of the following rules:
   a. Apart from the regular procedure required of a prospective account holder, all information of detailed identification concerning the prospective account holder and the agent shall be duly entered in the account holder's file card with photocopied documents as attachment.
   b. All information of the prospective account holder must be reconfirmed and, if necessary, conduct an on-site interview to verify the information so furnished.
   c. Attention must be paid continuously and check the transaction statement of account holders on the regular basis. Set up the transaction model of each and every account holder so that auditing may be conducted in case an abnormal transaction suspicious of money laundering occurs.
   d. In case any of the following events is found to exist, the identity of the account holder must be checked and, if necessary, conduct an on-site interview to verify the information on record.
      (1) If the identity documents or juristic person certification provided by the prospective account holder show signs of having been forged or altered, or if the customer attempts to use a false name to open an account or perform transactions.
      (2) If the prospective account holder's address or workplace is very distant from the place of business of the securities firm, and the prospective account holder cannot give any reasonable explanation for this, or if there is something else clearly abnormal about the account's transactions.
      (3) If the account holder's credit limit suddenly rises significantly, after which an unusually large securities or bond transaction takes place, followed by withdrawal of securities in huge sum (exceeding 400 trading units and over NT$40 million in one transaction or total transactions exceeding 1,000 trading units and over NT$100 million), where this is clearly inconsistent with the account holder's identity and income or the nature of their business.
      (4) If an account in which there have been no transactions for over 2 years suddenly has

securities or bond transactions for large amounts (exceeding 400 trading units and over NT$40 million in one transaction or total transactions exceeding 1,000 trading units and over NT$100 million), or the deposit or withdrawal of a large quantity of securities which are then rapidly transferred.

(5) If, immediately after opening an account, the account holder undertakes a transaction involving the purchase or sale of a large quantity of securities or bonds (exceeding 400 trading units and over NT$40 million in one transaction or total transactions exceeding 1,000 trading units and over NT$100 million), where this is clearly inconsistent with the account holder's identity, income or credit data, and the securities or bonds are then rapidly transferred.

(6) If one person or a group use more than 9 trading accounts or more than 5 margin accounts to buy or sell the stock of one particular company or a group of companies.

(7) If accounts opened by members of the same company are used for frequent purchase or sale of large quantities of securities.

(8) If an account holder uses more than 3 accounts opened in the names of others to break down a large transaction and rapidly made transfer of the proceeds or the transaction appears obviously abnormal.

(9) If an account is used to repeatedly buy in securities at high prices, with few or none of the securities being sold, or to repeatedly sell securities at low prices, with few or no securities being bought in.

(10) If an account holder fails to perform their settlement obligations on schedule, such that the total amount of breach of contract involved comes to NT$10 million or more.

(11) Where the prospective account holders of a securities dealer, or people who trade in securities, settle a trade or act as an agent are terrorists or terrorist groups or the terrorists or terrorist groups being the final beneficiary (see the list of suspicious terrorists or terrorist groups provided by the competent regulatory agencies).

e. If the company is engaged in the business of bond trading, attention should be paid to the following points. Trading of bond could be in the form of outright buy or sale, or with strings attached while the scope of bond covers trading and transfer in kind or by registration of public bond, company bond, financial bond, and foreign debts.

(1) Toward the customers:

(a) In initial trading, the customer is required to appear in person while the securities dealer shall, by the status of the customer, i.e., national natural person, national statutory corporate body, overseas Chinese residing at the home front or offshore, or foreigner, ask the customer to present ID in accordance with law. In case the ID presented is not of the interested party or the power of attorney by the statutory corporate body, or the ID presented appears to be suspicious and the customer refuses to cooperate by providing other auxiliary documents, the transaction should

be rejected or wait until the ID is verified to be true and correct.

(b) Where the transaction is conducted through proxy or by power of attorney indicating it is not the bona fide account holder, or his/her Taiwan representative or agent, confirmation must be conducted with the bona fide account holder, or his/her Taiwan representative or agent by telephone, fax, written communication or other appropriate means.

(2) Points to note when it comes trading and settlement:

(a) When payment is made in cash for amount of over NT$1.5 million, inclusive, the identity of the investor must, in accordance with the above-mentioned provisions, be checked and keep on file the transaction record.

(b) When the customer presents entitative bond for settlement and the amount exceeds NT$1.5 million, inclusive, request for presentation of document to show the source of obtainment or letter of affidavit is in order and the record of transaction as well as related vouchers should be kept on file. In case the customer refuses to comply, the securities dealer may tacitly refuse the transaction.

(c) In the event that an unusual huge sum of buys or sales occurs in the initial transaction, evaluation must be immediately made to determine whether the ID provided by the customer is obviously incompatible or inappropriate. Meanwhile, special attention must be paid and confirmation strengthened and keeps on file the transaction record.

(d) Securities dealers are advised to pay special attention to transactions mentioned below. Apart from reconfirmation of the customer's identity, cognition of motive for buy or sale, the record of transaction should be kept on file. In addition, if the transaction is suspicious of money laundering, report to the designated regulatory agency must be made immediately.

(i) If a customer pays in cash or delivers unregistered entitative bond, and tries to circumvent providing previous transaction record, source of the bond or related vouchers.

(ii) If a customer suddenly buys or sells in huge amount 10 times larger than normal average trading volume and then rapidly sells or buys, different from past trading level in amount or models of buy or sale, apparently incompatible with the customer's status and without reasonable cause.

(iii) If a customer tends to be fond of having entitative bond and without appropriate reason.

(iv) If a customer has extensively bought the bond through sparse sources and then dispensed the bond in a package with large amount or reversed the operation the other way around, different from normal trading pattern.

(v) If a transaction is executed by a third party other than the account holder or

the same customer has executed the transaction on behalf of other customers or through other accounts.

(vi) If a settlement exceeding NT$1.5 million is delivered by transfer to the dealer not from the account where the account holder has his/her record or through multiple accounts other than the account holder's; or the customer requests the dealer to remit the proceedings due to one or multiple accounts other than the account holder's; or more than one customer requests the dealer to remit the proceedings due to the same account.

(vii) If proceeds of a settlement comes from a certain specific foreign countries (see the list of non-cooperative countries provided by FATF) or foreign banks at the home front; or if the customer, following resale after purchase, immediately requests the dealer to remit the proceeds to the territories mentioned above, or foreign banks at the home front, or OBU's.

(viii) All other transactions that appear to be obviously abnormal.

3. The company shall, in accordance with the following regulations, draft internal control procedures with regard to money laundering:
   a. Correct and comprehensive transaction records should be well kept.
      (1) Trading records and vouchers that may provide cognition of the complete transaction should be kept on file for at least 5 years.
      (2) With regard to cases suspicious of money laundering, the trading records and vouchers should be kept in exclusively established book for future reference.
      (3) Where a case is under investigation and despite the limit of time to keep the related trading records and vouchers has expired, the trading records and vouchers shall not be destroyed before the case is closed.
   b. Attention should be paid to customers that have tried to circumvent provisions set forth in the MLCA.
   c. Filing procedure of internal report flow process and report to designated agency with regard to SAR's:
      (1) The internal report flow process requires the employee who first discover the transaction suspicious of money laundering to immediately report the case to the department head and, after approval by the department head, the report is routed to the VP, the president with notice to the General Auditor, and the chairman. Thus the completion of the internal report flow process. Where conflict of interest involves the channel of command, the employee may jump the routing sequence and submit the report to executives in higher position.
      (2) Once the internal report flow process is completed, report to MLPC of MJIB by fax at the earliest possible time, followed immediately by regular written communication.

d. Attention must be paid to ensure that the reported information is kept confidential and no leakage is allowed.
e. Hold regular review of the internal control measures to see if it is adequate to prevent money laundering.
f. The Model Points to Note for Money Laundering Prevention should be incorporated into the internal control system.

4. Hold regular annual training courses or theme lectures or arrange related training classes for employees to study so as to enhance employee's judgment and enable employees to fully recognize signs and types of transactions suspicious of money laundering.

5. Assign a VP or an executive in similar level to be in charge of and jointly supervising implementation of The Points to Note hereof and participate in training courses on money laundering prevention.

6. The Points to Note shall, subject to review each year to determine whether or not revision is necessary, take effect following resolution by the Board of Directors and submit to the competent regulatory agency for file and reference. The same shall apply to subsequent amendment.

## The Model Points to Note for Anti-money Laundering in the Farming & Fishing Credit Associations Sector

1. The Model Points to Note are established in accordance with Article 6 of the Money Laundering Control Act (MLCA) and are intended to serve as a guide in the prevention of money laundering.

2. In practice, the points to note for money laundering prevention are as follows:
   a. Points to note when a new account is opened:
      (1) The prospective account holder should present personal identification for verification; if it is a personal account, the national ID card or passport is required; if it is a non-personal account, presentation of registration papers/license/permits, and legitimate papers of the person-in-charge are required. Should the documents presented appear suspicious, request for additional supplementary documents such as copy of household registration or household booklet is in order. When the prospective account holder refuses to comply, tacit rejection to proceed with the process should be in order or wait until the identification is verified.
      (2) With respect to prospective account holder presented with power of attorney or authorization, the fact of the power of attorney or authorization must be verified; should the verification be difficult to proceed, tacit rejection to proceed with the process for such application should be in order.
      (3) With respect to other points to note, the internal standing operating procedure shall govern.
   b. Points to note when after a new account has been opened:
      (1) When an account has been opened with official document or other written communication, use official correspondence by registered mail to verify.
      (2) When suspicion is found after an account has been opened, verification should be followed by telephone, written communication or on-site interview. Also verification should be conducted with regard to those accounts having no geographical relations.
   c. Points to note with regard to transactions after a new account has been opened:
      (1) With respect to currency transactions of a certain sum or more, it is a must to check the identity of the account holder and keep on file the transaction record.
      (2) The currency transactions of a certain sum or more mentioned in the preceding paragraph refers to NT$1.5 million or more of one or more transactions in cash or its equivalent in foreign currencies deposited or withdrawn in the same business day of the same account or transactions of change of money.
      (3) Should it occur that any of the following events be found to exist in transactions of an

account, special attention must be paid. When it is believed that suspicious money laundering transactions, irrespective of the sum involved, are conducted through the account in question, the case must, in accordance with The Points to Note hereof, be reported to MJIB, in addition to checking the identity of the account holder and keeping on file the record of transaction.

(a) If an account holder suddenly makes an unusually large deposit which is clearly not compatible with their identity and status, or unrelated to their business areas.

(b) If a large sum of cash is suddenly deposited in or withdrawn from a dormant account or one in which no transactions have taken place for a long time, and is then rapidly transferred.

(c) If, immediately after opening an account, an account holder makes a large deposit which is clearly not compatible with their identity and status, and which is then rapidly transferred.

(d) If a large number of small sums are deposited in an account, and the money is then withdrawn, either in one large withdrawal or in several smaller withdrawals, leaving only a nominal balance, and the amounts involved are clearly incompatible with the account holder's identity and status, or are unrelated to their business areas.

(e) If an account holder regularly transfers large sums of money between accounts, or asks to process the transactions in cash.

(f) If all of an account holder's deposits and withdrawals are for similar amounts of money, and only a short amount of time elapses between them.

(g) If an account holder regularly asks for small bills to be changed for large bills, or vice versa.

(h) If an account holder regularly deposits large sums in a particular account on behalf of another party or parties.

(i) If an account holder regularly deposits or withdraws amounts slightly smaller than the amount which must be reported.

(j) If an account holder suddenly repays a bad debt of large sum, and is unable to offer a convincing explanation as to the source of the funds.

(k) Deposits or withdrawals of or remittances by those involved in reports of significant special cases in TV, news media, periodicals included, or Internet.

(l) A group of people flock to banking institution to conduct transactions in the form of deposit, withdrawal or remittance.

(m) Other transactions which are clearly abnormal.

3. Internal control procedure concerning prevention of money laundering:

a. Keeping on file contents and duration of keeping on file of complete and correct transaction vouchers:

(1) Contents kept on file:
  (a) With respect to a certain sum suspicious of money laundering, the complete and correct transaction vouchers in original form should be kept on file.
  (b) With respect to closed accounts, related documents such as photocopied ID, account statement, and address of account holder should be kept on file.
(2) Duration on active file: Minimum of 5 years.

b. Points to note concerning behaviors of account holders and staffers in financial institutions:
(1) Should it occur that any account holder be found to behave in one of the following manners, service may be refused and the case should be immediately reported to the supervisor:
  (a) After an account holder has been informed of presenting related information for identity checking in accordance with law in connection with the currency transaction, the account holder steadfastly refuses to comply.
  (b) Any individual or group that has coerced banking employee not to keep the transaction record on file or report the transaction to the regulatory agency as required by law.
(2) Should it occur that any banking employee be found to behave in one of the following manners, spot check over the business he or she handles must be conducted and, if necessary, request for assistance from the auditing department may be in order.
  (a) Lifestyle of the employee concerned has obviously changed, apparently incompatible with income.
  (b) Refusal to take leave without proper cause when the leave is due.
  (c) Failure to present convincing explanation with respect to deposit and withdrawal in huge sum.
(3) Flow process of internal filing regulations and procedure of filing with designated government agencies:
  (a) The association shall assign the chief secretary or a staff authorized by the chief secretary to be in charge of supervising implementation of The Points to Note hereof.
  (b) Filing flow process:
    (i) If the handling clerk in any units finds any transaction suspicious, he or she should immediately report the case to the supervisor.
    (ii) The department head in charge must at the earliest decide whether the case is subject to report to the authorities.
    (iii) If it is, the handling clerk must fill in the report in accordance with the standard form.
    (iv) Submit the report to the chief secretary or a staff authorized by the chief secretary via the usual channel of command.

Once approved, use fax or other feasible means to file the report at the earliest possible time and immediately prepare the written information for report to MJIB.

(4) Confidentiality requirements to prevent leakage of reported data and information:

(a) Once the report is filed in accordance with established rules, all employees at all levels should keep the information strictly confidential.

(b) With respect to related documents, it must be done in the manner as do secret documents; if anybody is found to have leaked the information, he or she shall be dealt with in accordance with related regulations.

(5) Job description of the auditing department with respect to the job:

(a) The auditing personnel shall, in accordance with the internal control measures and related established rules, formulate auditing matters and hold regular auditing.

(b) Any negligence by the executing units found out by the auditing personnel shall be reported and may be used as a reference material in the on-the-job training class.

(c) Should the auditing personnel find any serious violating incident and conceal the fact without reporting to the executive in charge, the responsible individual should be subject to disciplinary action.

(d) The auditing personnel should conduct spot checks over transactions in huge sum in the credit department and try to see if the transaction is normal.

4. Holding of regular seminar or on-the-job training on money laundering prevention:

a. Pre-employment training: training courses of laws and regulations related to money laundering control and the legal responsibility imposed on employees of financial institutions should be arranged for new recruits in the credit department so that the fresh employees may understand related regulations and their legal responsibility.

b. On-the-job training

(1) After the MLCA went into effect, the training unit should launch a campaign to promotion the law within the earliest possible period of time to train employees to familiarize with the MLCA and related laws and regulations and make known related and complementary responsive measures taken at the association.

(2) The training unit should hold regular annual related training courses or make arrangement for theme lectures for employees to study so as to enhance employee's judgment and implement money laundering preventive functions and avoid employees from acting against law.

(3) The money laundering preventive courses may, apart from related laws and regulations, aid with actual case studies so that employees may fully understand signs and types of suspicious money laundering activities. It will help discovery of transactions suspicious of money laundering.

5. Appropriate incentive should be awarded to employees who have contributed to the work of suspicious money laundering cases leading to crack down by the investigative and prosecutor's offices.

6. The Points to Note shall be subject to regular review each year through meeting of related department heads convened by the chief secretary or the secretary designated by the chief secretary or the head of the credit department.

7. The Points to note shall take effect following resolution by the Board of Directors and submit to Ministry of Finance for file and reference. The same shall apply to subsequent amendment.

## The Model Points to Note for Anti-money Laundering n the Securities Investment & Trust & Consultation Sector

1. The Points to Note for Money Laundering Prevention in the Securities Investment & Trust & Consultation Sector are established in accordance with Article 6 of the Money Laundering Control Act (MLCA) and are intended to serve as a guidance in prevention of money laundering.

2. In practice, the points to note for money laundering prevention are as follows:
   a. Points to note when the account holder requests for fund beneficiary certificate or make investment with full power of attorney:
      (1) When company employee handles the fund beneficiary certificate or investment with full power of attorney for the first time, request the customer to present the following documents in accordance with law:
         (a) When the customer is a natural person and a national of the Republic of China, presentation of the original national ID is required; if the customer is a foreign national, presentation of the original passport is required; if the customer is a juvenile or incapacitated, presentation of the statutory representative's original ID or passport is required.
         (b) Should the customer be a statutory corporate body or other institution, presentation of the customer's power of attorney, the attorney-in-fact's original ID, the customer's registration paper, official document or photocopies of related documents and the photocopy of the statutory representative's ID is required. A tax return alone should not be the only document that can be used as a basis for account opening.
      (2) Should the documents presented appear suspicious, attention must be paid to the point whether the document is counterfeited, altered or the photo identical with the interested party and, depending on actual needs, the company employee may further request for additional supplementary documents such as copy of household registration or household booklet. When the customer refuses to comply, tacit rejection to proceed with the process should be in order or wait until the identification is verified.
      (3) With respect to customer presented with power of attorney or authorization to make purchase or the attorney-in-fact, company employee must check the fact of the power of attorney or authorization and detailed information of the interested party and the attorney-in-fact must be kept on file. When necessary, verification should be followed by telephone, written communication or on-site interview. Should the verification be difficult to proceed, tacit rejection to proceed with the process should be in order.

(4) When it comes to investment by full power of attorney, information on the customer's financial status as furnished by the customer must be fully checked and, when necessary, request the customer to provide more documents or conduct an on-site interview. Should the results show that the customer's status and income are not compatible or no clear indication to show the source of funds, special attention must be paid to make sure that there is no money laundering involved.

(5) In case the purchase is made in cash and the sum exceeds NT$1.5 million or in equivalent foreign currency, or in case the purchase is suspicious of money laundering, the identity of the investor must be fully checked. When the customer is a natural person and a national of the Republic of China, presentation of the original national ID is required; if the customer is a foreign national, presentation of the original passport is required; if the customer is a juvenile or incapacitated, presentation of the statutory representative's original ID or passport is required. Meanwhile, the trading record must be kept on file.

(6) In case it occurs that the investor suddenly makes a purchase involving a huge sum that appears obviously not compatible with his/her income, special attention must be paid to make sure that there is no money laundering involved.

(7) If the purchase or the contract by power of attorney is made by suspicious terrorists or terrorist groups or the terrorists or terrorist groups being the final beneficiary, it must be listed as suspicious money laundering activity and report immediately the case to MJIB with copy to MOF (see List of Terrorists or Terrorist Groups forwarded by MOF).

(8) Al other points to note with regard to purchase of fund beneficiary certificate or investment by full power of attorney, the company's internal operating procedures shall govern.

b. Points to note concerning related trading after fund beneficial certificate is purchased:

(1) Where the purchase is made in cash involving over NT$1.5 million or equivalent in foreign currency, or the customer is suspicious of money laundering, the identity of the customer must be once again fully checked (see Article 2(1)(1) above) and keep the trading record on file.

(2) Special attention must be paid in case the trade appears to have any of the following events:

(a) The customer has made a purchase in huge sum and rapidly redeemed without reasonable reason.

(b) If a large number of purchases are made extensively in small sums for the same or different funds, and the fund is then redeemed in one large sum or in several smaller redemptions, leaving only a nominal balance, and the amounts involved are clearly incompatible with the account holder's identity and status.

(c) If all of an account holder's purchases and redemptions are for similar amounts of money, and only a short amount of time elapses between them.

(d) Payment of the purchase originates by inward remittance from a specific foreign countries (see the non-cooperative countries provided by FATF at website http://www.oecd.org/fatf/pdf/NCCT2001 en.pdf or http://www.oecd.org /fatf/pdf/PR-20010622 en.pdf) and, within a few days, quickly redeemed or request to send the proceeds directly from the R.O.C. to any of the countries named above.

(e) If an account holder regularly makes purchase on behalf of other parties or makes the purchase through different third parties.

(f) Other transactions which are clearly abnormal.

(3) Points to note after an investment contract by full power of attorney is executed:

(a) The identity of the customer must be once again fully checked (see Article 2(1)(1) above) and keep the trading record on file.

(b) After the investment contract by full power of attorney is executed and the customer is found to have any of the following events, immediate notification to the custodian agency should be made and pay attention to the cash deposit or withdrawal in the account to sound out if there is any sign of suspicious money laundering:

(i) There is no such account holder.

(ii) The account holder in question denies the existence of any full power of attorney executed.

(iii) Posted reports or other documents are returned by the post office, marking "no such addressee."

(iv) Sufficient evidence or fact has convinced people to believe that the customer is a figure-head being used by others.

(v) In the application form filled out by the customer, bogus or untrue statement has been found.

(vi) Once the investment contract by full power of attorney is executed, the customer quickly terminated the contract without property reason.

(vii) While the investment contract by full power of attorney is in force and effect, the customer has added large sum of investment fund or extensively increase fund of investment that are obviously not compatible with the customer's status and income.

(viii) While the investment contract by full power of attorney is in force and effect, the customer has requested reduction of the investment fund without reasonable reason.

(ix) While the investment contract by full power of attorney is in force and effect, the customer operates abnormally by extensive increase or reduction of the

investment fund.

c. While the investment contract by full power of attorney is in force and effect, frequent contact with the customer must be made and, from time to time, make notice and grip the customer's financial condition. One interview at least once a year must be made so that the customer's data can be amended or updated for basis of investigating suspicious money laundering activities.

3. Internal control procedure concerning prevention of money laundering:

a. Filing method and duration of keeping on file for complete trading records:

(1) With respect to investment made by full power of attorney or cases involving over NT$1.5 million or equivalent in foreign currency, complete trading records and vouchers that disclose details of the trade should be kept on file for at least 5 years.

(2) In case any trade that is suspicious of money laundering, the trading records and vouchers should be kept in a special book so established.

(3) Where a case is under investigation and despite the limit of time to keep the related trading records and vouchers has expired, the trading records and vouchers shall not be destroyed before the case is closed.

b. Flow process of internal filing regulations and procedure of filing with designated government agencies:

(1) The head office shall assign a VP or an executive in similar level to be in charge of and jointly supervising implementation of The Points to Note hereof and participate in training courses on money laundering prevention. New recruits must complete the course within 6 months after employment begins. For branch offices, a senior executive should be assigned to act as the full-time supervisor in charge of overseeing related work.

(2) In addition to reporting to the full-time supervisor in charge, company employee may tacitly refuse transaction of purchase or consignment in case a customer shows any of the following behaviors:

(a) When informed of presenting related information to check the identity in accordance with law, the customer steadfastly refuses to fill out related information required of transactions in cash.

(b) The customer has tried or intended to coerce company employee not to keep the transaction record on file or report the transaction to the regulatory agency as required by law.

(3) Filing flow process:

(a) If the company employee finds any trade abnormal or suspicious of money laundering in accordance with Article 2(1)(2), (4) or (6), or Article 2(2), and (3)(2) of The Points to Note hereof, he or she should immediately report the

case to the supervisor.

(b) The supervisor in charge must at the earliest decide whether the case is subject to report to the authorities.

(c) If it is, the company employee must fill in the report in accordance with the standard form.

(d) Submit the report to the head office via the usual channel of command where the responsible personnel will, in turn, forward the report to MJIB's PLPC.

(e) After a comprehensive evaluation, should the case be determined of obvious importance and emergency, an oral report to the responsible executive in the head office should be first made, followed immediately by telephone or fax to report the case to MJIB while the written information is being prepared.

c. Confidentiality requirements:

(1) Once the report is filed in accordance with established rules, all employees at all levels should keep the information strictly confidential.

(2) With respect to related documents, it must be done in the manner as do secret documents; if anybody is found to have leaked the information, he or she shall be dealt with in accordance with related regulations.

d. Regular review must be made to determine whether or not money laundering prevention measures are adequate:

(1) The head office shall make regular review of the established points to note concerning anti-money laundering activities and enter such reviews into record.

(2) Where branch offices are numerous and widespread, meetings should be held by region to review the money laundering prevention operation so as to collect different findings from among all concerned staffers.

e. Job description of the internal auditing department with respect to the job:

(1) The auditing unit shall incorporate The Points to Note for Money Laundering into the internal control measures and set auditing items to conduct regular auditing.

(2) Any negligence by company employee in the implementation of money laundering operation found out by the auditing unit shall be reported to the president via the executive exclusively in charge of the work and offer suggestions for improvement as a reference material in the on-the-job training class.

4. Holding of regular seminar or participation in money laundering prevention courses:

a. Pre-employment training: Minimum 3 hours of training courses of laws and regulations related to money laundering control should be arranged for new recruits so that the fresh employees may understand related regulations and their legal responsibility.

b. On-the-job training:

(1) Promotion of established law: After the MLCA went into effect, all financial

institutions should comply with subsequent revisions of said Act from time to time and, within the earliest possible period of time, train their employees to familiarize with the MLCA and related laws and regulations and make known related and complementary responsive measures taken at the company.

(2) Regular training:

(a) The training unit should hold regular annual training courses for employees to study so as to enhance employee's judgment.

(b) The training unit should introduce actual case studies on a regular basis so that employees may fully understand signs and types of suspicious money laundering.

5. Incentive measures should be awarded to employees who have contributed to the work of money laundering prevention, attended to related money laundering training courses overseas or having collected worthy information of foreign anti-money laundering ordinances that financial institutions may use in anti-money laundering activities.

6. The Points to Note shall, subject to review each year, take effect following resolution by the Board of Directors and submit to Ministry of Finance for file and reference. The same shall apply to subsequent amendment.