GROUP 2

ECONOMIC CRIME AGAINST THE PRIVATE SECTOR

Chairperson	Mr. Asif Nawaz	(Pakistan)
Co-Chairperson	Mr. Teruo Taniguchi	(Japan)
Rapporteur	Mr. Patrick Ochieng Obimo	(Kenya)
Co-Rapporteur	Mr. Marino Francisco Sagot Somarribas	(Costa Rica)
Members	Mr. Saadi Lahcene	(Algeria)
	Mr. Ramon Crespo Carrilho Machado	(Brazil)
	Mr. Tetsuo Nagakura	(Japan)
	Mr. Tetsuo Ogura	(Japan)
	Mr. Yoshihiro Ono	(Japan)
Advisers	Deputy Director Masahiro Tauchi	(UNAFEI)
	Professor Tomoko Akane	(UNAFEI)
	Professor Ryosuke Kurosawa	(UNAFEI)

I. INTRODUCTION

At the outset the group would wish to place on record its gratitude and thanks to the advisors and visiting experts for their valuable advice and guidance in the workshop sessions. This group workshop was assigned to deliberate on the issue of economic crime against private enterprise. It was agreed that we will consider crimes where private enterprise is the victim. However, it was felt that many a times, crime against private enterprise will have its effects on investors.

It was observed that economic crime is rampant in both developing and developed countries, and is eating at the very roots of society. It is vitiating the business atmosphere and the public in general is loosing faith in the regulatory apparatus of the State/criminal justice system. The gravity of the problem is highlighted by the finding of an international survey conducted by Earnest & Young regarding the effect of fraud on business (May 1998). As per its findings, more than half the respondents (those enterprises who responded to the questionnaire) had been defrauded in the last 12 months; 30% had suffered fraud more than five times in the last five years; 84% of the worst frauds were committed by employees (nearly half of whom had been with the organization for over 5 years) and most of the worst frauds were committed by management.

The group decided to tackle the subject by discussing the actual situation of economic crime in various countries. Facts and figures were gathered to appreciate the preponderance of crime in these countries. Case studies were undertaken to identify problems/difficulties faced by criminal justice officers at various stages of investigation, prosecution, and trial of offenders. Solutions were explored and recommendations formulated.

II. ACTUAL SITUATION OF ECONOMIC CRIME AGAINST THE PRIVATE SECTOR

Most of the countries represented in the course do not have any definition of economic crime in their penal codes.

Offenders are punished under various laws pertaining to fraud, cheating, breach of trust, misappropriation and embezzlement, etc. It was agreed that crime is a complex phenomenon and offers no easy solutions. There are multiple socio-economic factors affecting the state of crime in a particular society. It has to be understood in relation to a particular time and social milieu. However, effort was made to explore commonalties and find ways to manage criminality.

It was noticed that crime in general, and specifically economic crime is being committed on a larger scale and becoming more sophisticated in member countries. The group will discuss crime against private enterprise under the categories listed below:

a) (i) Breach of trust by executives/staff of the enterprise
   (ii) Embezzlement by executives/staff of the enterprise/others
   (iii) Fraud/fraudulent management by executives/staff of the enterprise/others
b) Infringement of intellectual property rights
c) Counterfeit credit cards/prepaid cards
d) Computer-related crime

The above categorization is not mutually exclusive. However, ingredients of all these criminal acts/behavior may be present in a particular crime. Since breach of trust, embezzlement, and fraud/fraudulent management by executives/staff of the enterprise may include similar kinds of elements constituting the respective crimes, the group decided to categorize them for the sake of convenience in discussion.

III. BREACH OF TRUST, EMBEZZLEMENT, AND FRAUD/ FRAUDULENT MANAGEMENT BY EXECUTIVES/STAFF OF THE ENTERPRISE

Algeria

These crimes are dealt with under the Penal Code of Algeria and are on the increase due to the process of change from a government controlled economy to a free market economy. The regulatory apparatus to deal with such crimes is still not firmly in place. There is a need to develop institutions and regulations to handle this transformation. The total number of cases convicted during the last three years are given below.

CRIME (ALGERIA)	1995	1996	1997
Breach of trust	20	122	53
Embezzlement	10	30	72
Fraud	42	336	160
Total	72	448	285

Source: Ministry of Justice, Algeria.

The total number of cases prosecuted in 1998 from January to July was 1115, much higher than previous years. Fraud was committed against private enterprise both by insiders and outsiders.

Brazil

Brazil experienced a succession of bankruptcies since 1970. The Central Bank decreed intervention in financial institutions which revealed cases of fraudulent management/embezzlement, and in a few cases, breach of trust committed by owners/executives of these institutions. The Government of Brazil enacted new legislation to ensure stricter control over and inspection of financial institutions, which resulted in a decrease in such incidents/cases. Criminal interest has now shifted to the government sector and consumers, against whom a significant number of fraud cases are being

perpetrated, such as off-the-book sales, tax evasion, misappropriation of public funds, etc. Law 7492, enacted in 1986, is the main provision presently used in fraud/ embezzlement cases. Although statistics related to the private sector are not available, overall 4304 cases have been registered since 1986, and out of them, 1639 have been concluded at investigation level.

Costa Rica

The Costa Rican Penal Code provides punishment for economic offences. Fraud in private enterprise is mostly committed by insiders. The following chart reflects the state of this crime in Costa Rica. The cleared cases are as follows.

There was a slight increase in cleared cases but the situation in Costa Rica regarding economic crime in private enterprise is not very serious. The public in general is more concerned about corruption in government departments.

Japan

The so-called 'bubble economy' swelled in 1986 to 1990, with a dramatic rise in stock and land prices. With the objective of countering this phenomena, the government of Japan switched to a belt-tightening policy. The bubble then burst; stock and land prices tumbled and around 1991 the economy experienced a severe slump causing bankruptcy in various enterprises. This contributed to revealing misconduct done by private companies during the bubble economy, with a resultant increase in fraud, breach of trust and embezzlement cases by executives of financial institutions. The table below illustrates crimes committed by executives of financial institutions in 1997.

Kenya

Economic crimes against the private sector are on the increase. Victims do not report these offences to police for fear of negative business repercussions, so statistics are not reflective of the real

CRIME (JAPAN)	1992	1993	1994	1995	1996
Fraudulent Management	149	142	141	162	194
Embezzlement	121	89	122	160	169
Fraud	2063	1878	2097	2397	2481
Bankruptcy	24	4	1	2	16
Total	2357	2113	2361	2721	2860

Note: Fraud includes all frauds, not specifically private enterprise (source: Supreme Court of Justice of Japan).

Beach of Trust	Number of cases	6 (-3)
	Number of persons arrested	28 (-2)
	Amount of damage	2.6 billion yen (-78.2 billion yen)
Embezzlement	Number of cases	23 (+5)
	Number of persons arrested	25 (+6)
	Amount of damage	3.2 billion yen (-0.2 billion yen)
Fraud	Number of cases	56 (+35)
	Number of persons arrested	113 (+83)
	Amount of damage	5.8 billion yen (-3 billion yen)

Note: Figures in parentheses show the increase or decrease from the previous year (source: National Police Agency of Japan).

situation. Global economic turmoil has affected the Kenyan economy and quite a few companies have gone bankrupt. Receivers appointed over the companies have reported many cases of fraud/ fraudulent management. These cases are tried under the Penal Code of Kenya.

Pakistan

The Pakistan Penal Code prescribes punishment for offences like breach of trust, cheating, misappropriation etc. The economic crime which impacted the national economy, was a co-operative scandal in which executives of financial corporations indulged in large scale frauds/ embezzlement, resulting in the bankrupty of these corporations. Banks are also the common victims of fraudsters, who obtain loans under various schemes on fake securities. The table below indicates cases regarding economic crime investigated and cleared by the Federal Investigation Agency. Through statistics of one agency are not a true reflection of the state of crime in the country, they do indicate a trend which is on the rise.

Other Countries

Crime data was not available regarding other developing countries represented in the course. However many private enterprise/banks have been defrauded by executives/others in India. In the famous securities scandal in India (1992), management of a bank of Karad misused the funds of the bank in the securities market, causing huge losses to the bank. No significant case of breach of trust/fraud has been reported in Nepal. Such crimes however, registered an increase in the Republic of Korea, with rapid growth of the economy (1991-1996). There are numerous cases in which more than ten million U.S. dollars were embezzled or swindled by Korean executives. These executives were later arrested and indicted by public prosecutors.

The Economic Crime Investigation Bureau of the Police Department of Thailand has reported 57, 66, 64, 46, 71 and 92 cases involving financial institutions and commercial banks in 1992, 1993, 1994, 1995, 1996 and 1997 respectively. In 1997, damage caused by these offences was more than USD$ 233 million.

Case Studies

1. Fraud/Fraudulent Management in Banco Nacional (BN) of Brasil

Facts

BN ranked 8th among Brazilian banks and had 13,000 employees and 335 branches throughout the country. In 1986, the Brazilian economy experienced a rapid growth, whilst BN provided a great number of loans to small enterprises. When high inflation struck, hundreds of such companies went out of business, leaving non-performing loans.

PAKISTAN

YEAR	CASES INVESTIGATED	CLEARED	REFERRED FOR DEPARTMENTAL ACTION	CLOSED
1993	222	79	9	26
1994	224	69	6	10
1995	189	60	25	8
1996	240	61	3	7
1997	303	146	4	45

Note: Figures include economic crime in government organizations as well.

Executives of the Bank managed to alter the due dates of these loans in BN's computerized accounting system and applied high interest rates to keep them looking as good credits. Instead of writing off bad loans, they were shown as performing/active loans providing interest income, generating positive results at the end of the fiscal year. Fictitious income from interest earnings amounted to nearly US$ 17 billion from 1988 to 1995. When adjusted, fiscal year positive results turned into a loss of US$ 10 billion. A total of US$ 145 million was paid as dividends from 1990 to 1995. Undesirable effects were generated at same time, such as taxation on profits and compulsory withdrawals from the Central Bank.

Independent auditing of balance sheets and financial demonstrations were conducted by a private multinational auditing company during this period. They granted BN approval based on misleading assessments from insufficient evidence, contrary to legislation and accounting procedure requirements. This crisis brought problems to stockholders/investors and to the country's financial system, provoking Central Bank intervention in November 1995. The Brazilian government created a bail-out program for the banking system through which BN demanded US$ 4.98 billion. Investigation identified inside employees, at the vice-presidency level and executives heading two other areas, as responsible for conceiving and implementing changes in the accounting system. They were indicted for fraudulent management, for providing false information to the market and for preparing false balances.

Difficulties / Problems raised by Participant

Stretched over the period 1988 to 1995, requiring the services of police experts in the fields of accounting and computer technology.

Countermeasures / Solutions shown by Participant

Investigation agencies should be staffed with skilled investigators and allowed to request specialist cooperation from other institutions.

Discussion in the Group

The participant from Pakistan pointed out that, in his view, this does not qualify as a case of fraud/fraudulent management as the investigators have neither indicted the president of the bank nor proved the bad intention of the executives. Management of the bank might have misrepresented the situation to avoid negative business repercussions. He was of the view that the banking industry is facing problems in many countries due to world-wide recession. In Indonesia, Thailand, Pakistan and Republic of Korea, over 30 % of loans granted by banks have gone bad.

The participant from Brazil asserted that falsification of records amounts to fraud and Brazilian law provides punishment for that. The participant from Kenya opined that management might have been driven to misrepresent their financial position due to fear of losing the confidence of the public. Fraud/fraudulent management involving misappropriation may well follow in the wake of misrepresentation, as inhibitions which discourage fraud have already been overcome. In the actual case, had the management of the bank identified overall bad loans from good ones at the outset, and shown them in a high risk category, they could have avoided aggravating consequences such as paying taxes, dividends to share holders and compulsory withdrawals by the Central Bank.

The participant from Japan introduced a similar case regarding Yamaichi Securities Corporation, in which executives

of Yamaichi concealed debt of 260 billion yen on the balance sheet in November 1991. Since the investigators required specific expertise and knowledge to understand the transaction of securities and bonds, the services of inspectors of the Security and Exchange Surveillance Commission were co-opted to assist the investigators, and the executives of Yamaichi were indicted in this case.

The participants pointed out the importance of establishing special investigation agencies, and close co-operation between criminal justice officers and executives of the regulatory bodies, such as SESC, which may provide necessary expertise to investigate such cases.

2. Breach of Trust in Inditex of Algeria

Facts

A case regarding breach of trust/ embezzlement was detected by Algerian Authorities in 1997, in which a manager and two executives of the Inditex (a textile company) manipulated the company's funds for their own interests. They entered into a partnership contract with a fictitious off-shore company called Radco (situated in Spain), purported to be a producer of raw material which would provide Inditex:

(a) Raw material at whole sale price.
(b) Technical know-how.
(c) Sale of goods of Inditex to other countries.

In return, Inditex would pay 30% of its annual profit to Radco.

During investigation, it was established that the Spanish company was not the producer of the raw materials. Inditex was purchasing raw materials at 5 to 8 % higher than the market price, and the profit so gained was shared among the group of perpetrators. Similarly, 30% of the profit being paid to the Spanish company was transferred to various banks in Switzerland, France and Algeria through "bank-drafts". So accessing those accounts was not possible for investigators.

Difficulties / Problems raised by Participant

(a) It was difficult to gather evidence because the proceeds of the illegal profits were stashed away in foreign banks.
(b) Secrecy laws of the banks made it impossible for investigators to get material evidence of accounts in foreign banks.
(c) Investigating officers lacked knowledge of commercial law operations.

Countermeasures / Solutions shown by Participant

(a) Regional and international co-operation be strengthened.
(b) The rules regarding bank secrecy be reviewed.
(c) Services of specialized agencies may be co-opted i.e. audit departments.

Discussions in the Group

The Algerian participant explained that it is legal in his country to hold anonymous bank accounts, and the rights of depositors are protected by law. However this creates problems for investigators in tracing the flow of a suspect's transactions in the bank. In this case, the problem was further compounded as the profits/money was kept in foreign banks and the accomplice was a foreign national (Spanish). So gathering evidence required international co-operation and an extradition treaty with Spain. He pointed out that the confession of the accused, recorded by prosecutors, was the main evidence in this case, and it would not be possible to convict the offenders if they convince the court that confession was recorded under duress.

It was pointed out by a participant that, ordinarily, it is very difficult and time

consuming to get a person extradited or to get information from foreign banks. He suggested greater mutual assistance in the international field and informal contact between criminal justice officers of various countries for resolving this problem. The Japanese participant told that it is not possible to hold anonymous accounts in Japan and investigators can thoroughly examine bank records.

Some of the participants expressed the view that anonymous bank account systems and the secrecy laws of banks should be reviewed/changed. However it was perceived that Algeria is keeping this system to attract deposits/capital so that the financial resources of the country will not be drained by competing European banks.

The participant from Brazil explained that many financial institutions in his country established off-shore companies in the Caribbean Islands to indulge in illegal trade/money laundering. The Central Bank of Brazil is making efforts to enter into bilateral agreements with the Central Bank of Caribbean Islands for allowing inspectors of the Central Bank to carry out audits of such affiliated companies.

3. Embezzlement in a Large Financial Institution of Costa Rica

Facts

From July 1983 to May 1984, in Costa Rica, four executives of a large financial institution embezzled money from the institution. These executives, who were authorized to issue cheques, gave cheques to fictitious companies, which in turn, through various accomplices, endorsed the cheques many times, and finally deposited them in the bank accounts of companies owned by these executives. The total amount of cheques resulted in damage to the financial institutions of $1.5 million dollars.

Difficulties / Problems raised by Participant

(a) Judges are overburdened and avoid taking up cases of a complicated nature. They tend to postpone hearings in economic crime cases.
(b) A lot of evidence is to be collected. Investigators require special knowledge of commercial laws/ operations.
(c) Cheques were endorsed many times, therefore it was difficult to determine offenders.
(d) Although the investigators proved the flow of cheque transactions, illicit profits could not be recovered.

Countermeasures / Solutions shown by Participant

(a) In Costa Rica, a new law was enacted to prohibit endorsing cheques more than once.
(b) Special investigators offices, one in the judicial police and another in prosecution, have been established. The offices specialize in economic crimes.

Discussions in the Group

The participant from Costa Rica informed that the law regarding endorsements of promissory notes/cheques has been revised in his country, to discourage malpractice, and now only one endorsement is allowed.

The participant from Japan was of the view that use of promissory notes provides ease of transaction in business and is very common in Japan. Restricting their endorsement can adversely affect the business atmosphere. Further, the efficacy of restricting endorsements is doubtful as promissory notes without endorsement (blank) often circulate in the business world.

4. Breach of Trust in a Bank of Pakistan

Facts

Mr. HL, president of a bank in Pakistan, transferred USD$ 5 million to the account of A.O.Y. via American Express in New York. The amount was debited to the bank branch in Karachi. This case was registered in 1997 for committing criminal breach of trust. Both the president of the bank and directors of A.O.Y. were abroad. The Federal Investigation Agency procured warrants of arrest from the Special Banking Court in Karachi and moved Interpol for their arrest. Mr. H.L. went to the High Court in Punjab, challenging the jurisdiction of the F.I.A. to investigate this case. The Chief Justice of the High Court directed that the accused shall not be arrested, pending the writ petition. No date has been fixed for the regular hearing of the petition.

Difficulties / Problems raised by Participant

(a) Affluent offenders involved investigators in legal cases to frustrate the purpose of criminal justice.
(b) Defendants, being abroad, were out of reach of the local authorities.

Countermeasures / Solutions shown by Participant

(a) Greater co-operation between various organs of the criminal justice system.
(b) International co-operation for extraditing offenders.

Discussions in the Group

The participant from Pakistan expressed the view that economic crime offenders are generally affluent people. They have money to spend on entertaining bureaucrats and financing campaigns of politicians, who in turn provide necessary assistance when required. Further they can engage competent lawyers to create impediments by raising legal issues in the course of investigation, and such delay in investigation buys them time to wriggle out of a situation.

Criminal justice officers enjoy high social status in developing countries and wield considerable discretion/influence, but their salary structure is not commensurate with that status, making them prone to corruption. Political systems in most of these countries are still struggling to shed a colonial past. Political executives try to use the criminal justice system to perpetuate its rule, so it is necessary to provide a better salary structure for criminal justice officers and operational autonomy to insulate them from political influence.

General Discussion of the Group

A participant raised the issue of the expertise required of investigators in dealing with complicated business transactions and the plethora of commercial laws. Participants from Brazil and Japan pointed out that they have a system of auditing private enterprise by external auditors and various regulatory bodies, i.e. Security & Exchange Surveillance Commission, Tax Agency, Ministry of Finance and Central Bank etc, all have authority to inspect banks/companies. Such inspections sometimes provide the beginning of a case. Better co-ordination between regulatory bodies and criminal justice officers can ensure co-operation, and the experts of these bodies can provide necessary assistance in the investigation.

Some participants expressed the view that better training of officers in investigation techniques will improve their skills and arranging common training programs will foster goodwill amongst officers of various countries and result in better informal international co-operation. The group deliberated to find effective measures to deal with crime. It was agreed

that the nature of private business is such that over-regulation may kill the atmosphere of free enterprise and pose problems to genuine entrepreneurs in effectively exploiting business opportunities. The following countermeasures were proposed by some of the participants:

(a) Organizations should develop and refine their fraud control systems, and encourage a culture of integrity.
(b) Raising the awareness of the public regarding pitfalls of the market culture.
(c) Procedures for public disclosure of the basic aspects of a company's operations can help safeguard against such crime.
(d) Criminal justice officers be made conversant with commercial laws/ operations.
(e) The agencies dealing with economic crime may be provided with the services of experts in the field of accounting.
(f) Regional and international mutual assistance in the field of criminal justice matters.
(g) Role of regulatory bodies may be strengthened.
(h) To prevent the emergence of shell companies, rules may be framed to require them to be registered with the Chamber of Commerce and Trade of the host country.
(i) Operational autonomy to various enforcement bodies to insulate them from political pressure/external influence.
(j) Better service conditions for criminal justice officers.

IV. INFRINGEMENT OF INTELLECTUAL PROPERTY

Algeria

The old Penal Code prescribed very lenient punishment for infringement of these rights, which is being reviewed to enhance punishment of imprisonment from 2 months to 1 year, and fine from 5000 to 20,000 DA. Special provisions dealing with infringements of trademark and copyright law are included in the Competition Law. The figures regarding these crimes were not available, however violations of these laws are common. Both the public and law enforcement does not attach much importance to these violations. Further, the victims are reluctant to lodge complaints due to the apathy of the regulatory bodies.

Brazil

The usual practice in the past was related to software copying and official support for the production of patented computer technology and pharmaceutical products. With the recent enactment of specific laws protecting intellectual property rights, the previous freedom to copy any foreign patented item ended, and enforcement was put in place, thus significantly reducing its occurrence. Presently, the most common infringement relates to counterfeiting brand name consumer products.

Costa Rica

The Penal Code of Costa Rica provides for punishment of offences regarding infringements of intellectual property rights. Special legislation provides for the setting up of regulatory bodies to deal with issues regarding the Trademark Law, Illegal Competition Prevention Law, Copyright Law, Utility Model Law and Patent and Design Law. However infringement of these rights are common, as the criminal justice system attaches low

priority to these violations, and the victims normally don't come forward to lodge complaints.

Japan

The products inscribed with fake brand names are banned, but can still find their way into the market. However a few cases have been registered and successfully prosecuted in the criminal courts. As most of the cases are handled by the civil courts, violations of intellectual property rights are not frequently reported to the police. The available statistics from Japan indicate that violations of trademarks and copyright are more common than other laws concerning infringement of intellectual property rights. The table below shows the cleared cases in Japan during the last five years.

Kenya

Copyright and trademark laws are violated with impunity, as victims do not report these offences to law enforcement agencies. The officers of law enforcement agencies lack special knowledge of the laws and expertise to deal with such violations. Video and music cassettes are the most affected items, and markets abound with garments, shoes, bags, and medicines using fake brand names. Few reports received originate from our local artists. These cases are considered to be petty and are never submitted to the statistical bureau for record.

Pakistan

Pakistan has special legislation regarding copyright, trademarks, patents and design. The Penal Code of Pakistan also prescribes punishments for offences regarding infringement of intellectual property rights. However cases regarding infringement of these rights are rarely lodged with the police. Society in general does not attach much importance to such infringements, which take place without much resistance from either public or law enforcement bodies. However people do differentiate between goods on the basis of quality, and protection of these rights is mainly determined by market forces or the zeal of the aggrieved party.

Other Countries

The situation in Nepal is almost similar to Pakistan. In India, the Copyright Act deals with such crimes. Offences under this Act are mainly committed in urban areas. In 1996, the highest incidences of violation of this Act were reported from the city of Bombay (100) and Delhi (55). The Philippines has, under certain conditions, criminalized the infringement of intellectual property rights under the new Intellectual Property Code. In Korea, a joint investigation team was formed in 1991 in every District Prosecutor's Office to specifically investigate this type of crime. Figures of indicted cases during the last three years in Korea are 13683,15166 and 13460 respectively.

JAPAN	1993	1994	1995	1996	1997
Trademark Law	465	251	342	517	442
Illegal Competition Prevention Law	40	34	43	99	56
Copyright Law	384	138	172	348	433
Patent Law	1	1	2	0	0
Design Law	5	4	2	0	0
Utility Model Law	0	0	0	0	0
Total	895	802	901	964	933

(Source: National Police Agency of Japan)

Case Study

1. Infringement of Intellectual Property Case in Japan

Facts

Company A was a legal producer of video-game machine software, bearing the copyright 'Arukanoid'. B was a director of C company, which dealt in the production, sale or lease of video-game machine software bearing a different copyright. During the period between 1986 and 1987, B was found to have sold 18 pieces of Arukanoid video game machines without consent or permission from company A. Company C was found guilty and fined 500,000 yen. B was also found guilty and sentenced to 8 months imprisonment with 2 year's suspension of execution of the sentence.

Difficulties / Problems raised by Participant

(a) It was difficult to gather evidence to prove that B knowingly purchased the software violating the copyright of Arukanoid video.

(b) The investigators had difficulty in distinguishing the software which B was selling from the genuine Arukanoid product, due to the similarity of appearance.

Countermeasures / Solutions shown by Participant

(a) The analysis of the accounts book seized from Company C containing sales records showed variation in prices between the genuine and the copied software.

(b) The victim cooperated with investigators to recognize the difference between the genuine and the copied software.

Discussion in the Group

The situation in member countries clearly indicates that low priority is attached to the infringement of intellectual property rights by both society and the criminal justice system. Information technology has further facilitated the piracy of software programs through the internet. This is causing a huge loss to private enterprise. The Software Publishers Association has estimated that $ 7.4 billion worth of software was lost to piracy in 1993, with $2 billion of that being stolen from the Internet.

Japanese participants pointed out that products using fake brand names are mostly smuggled into Japan from other Asian countries. This makes it difficult for investigators to collect evidence, i.e understanding the whole process of their production. So international co-operation is necessary to deal with the situation. Some of the participants proposed that there is need to protect the business interests of entrepreneurs and suggested that the regulatory apparatus should play a pro-active role, and punishments regarding infringement may be enhanced to deter perspective offenders.

V. COUNTERFEIT CREDIT CARDS AND PREPAID CARDS

Algeria

Credit cards are not commonly used in Algeria, and there is no special enactment to deal with fraud relating to credit cards. Few cases were cleared and prosecuted under the traditional provisions dealing with forgery, swindling and counterfeiting of securities.

Brazil

Some counterfeit credit card cases have been detected and investigated in Brazil, usually connected to organized crime. However, the prevalent form of credit card offence is related to the use of stolen cards and cards obtained through false information. Prepaid cards are not yet widely used.

Costa Rica

There are various types of credit card fraud in Costa Rica. Depending on the type of the fraud perpetrated, the sufferer of the loss can either be the issuer, card holder, bank or merchant. Counterfeit credit cards and prepaid card fraud are not known to have been reported.

Japan

There are few cases of the use of counterfeit credit cards. Most crimes relating to cards are cases in which regular cards issued to authorized holders were used by unauthorized persons. There are many cases in which used prepaid cards are counterfeited (especially telephone cards, cards for pachinko games and so on). Card crimes are sometimes committed by organized groups involving foreign organized crime group members. Statistics of cases relating to various card frauds are tabled below.

Kenya

The use of plastic money or cards in consumer spending has exerted considerable influence in the growth of financial transactions in Kenya. The major frauds so far experienced relating to credit cards are as follows:

(i) Use of stolen and lost cards.
(ii) Use of fraudulently acquired or issued cards.
(iii) Running of extra vouchers (i.e. merchants can bill the card company by fraudulently preparing extra vouchers of cards presented to them).

No case involving the use of counterfeit credit cards or prepaid cards has been reported.

Pakistan

Pakistan is still a cash economy and use of plastic money is still very limited. A few large stores and hotels located in big cities entertain credit cards. People belonging to affluent classes normally keep credit cards for use abroad. Prepaid cards of small denominations are used at telephone booths. There is hardly any cases reported to police regarding counterfeit cards.

Other Countries

Credit cards are widely used as a mode of payment in Korea. In most of the criminal cases related to credit cards, authorized card holders made excessive use of the card with the intention to evade payment, constituting a fraud under the Penal Code of Korea. However sometimes stolen or lost cards, and in a number of cases, counterfeit cards are used. Provisions of the Credit Card Act are invoked to punish offenders along with the Penal Code. A number of suspects are arrested and indicted every year. In the Philippines, credit card fraud has almost disappeared due to the adoption of new procedures by business establishments, i.e.

JAPAN		1991	1992	1993	1994	1995	1996	1997
Number of Cases Detected	Total	7,740	11,045	8,585	8,740	6,671	6,396	11,714
	Credit	6,195	9,596	7,056	7,173	4,951	4,282	8,594
	Cash	1,452	1,303	1,314	1,291	1,514	1,408	1,926
	Others	93	146	215	276	206	706	1,194
Number of Cases Cleared	Total	7,544	11,539	8,268	8,122	6,204	5,586	11,368(31)
	Credit	6,270	10,205	7,216	6,998	5,061	4,070	8,860(26)
	Cash	1,178	1,177	923	877	948	845	1,240(1)
	Others	96	157	129	247	195	671	1,268(4)

The numbers in parenthesis indicate cases using counterfeit cards (source National Police Agency of Japan).

verification of credit cards passed onto them through an Omron Card Authorities Terminal (OCAT). Credit card companies have also introduced the system of requiring photographs of holder on the card itself for easy identification.

The problem of stolen and counterfeited cards is becoming serious in Thailand. As per the statistics from the Economic Crime Investigation Bureau of the Police, there were 58, 54, 57, 71, 79, and 87 cases regarding counterfeited credit cards in the years 1992, 1993, 1994, 1995, 1996, and 1997 respectively. In 1997 damage caused by these crimes exceeded USD$ 561,000.

Case Study

1. Counterfeit Prepaid Card Case of Japan

Facts

In June 1995, the suspects ran a counterfeiting machine in an apartment within Itabashi Ward in Tokyo. The suspects used the machine to counterfeit prepaid cards for accessing Pachinko machines. They collected used prepaid cards from various sources and copied the magnetic data of genuine cards, using the used prepaid cards, and the counterfeiting machine. Within two months they had succeeded in producing approximately three hundred thousand counterfeit prepaid cards, out of them one hundred thousand cards were used by the suspects and their agents, thereby causing the card company a loss of about 500 million yen. The suspects were indicted on allegations of forgery of securities.

Difficulties / Problems raised by Participant

The crime was committed by an organized gang involving a lot of suspects. They changed their place of residence frequently to perpetrate this crime.

Countermeasures / Solutions shown by Participant

Co-operation of police from various jurisdictions was solicited to arrest members of the gang.

Discussion in the Group

Participants noted with concern that where credit cards have provided ease of transactions, at the same time they provide immense opportunity for criminals to use or appropriate cards, or the stored information in the card. According to one estimate, losses amounting to USD$1.3 billion were caused to credit card companies in the year 1995.

The participant from Japan pointed out that counterfeit credit card crimes are dealt with under the normal provisions of Penal Code in Japan, such as illegal use or production of electromagnetic records, using forged securities and so forth. However it was pointed out by a participant that certain countries have amended their Penal Codes to provide for crimes related to credit cards. In Canada, section 342 (1) (c) of the Criminal Code provides that it is an offence to possess, use or traffic in a forged or falsified credit card, knowing that it was obtained, made or altered by the commission of an offence either in Canada or elsewhere. The participant from Pakistan pointed out that possession of counterfeit cards may be criminalized to discourage the forgery of cards. Participants from Japan were of the view that the public in general is not ready for such legislation in Japan.

The participant from Kenya pointed out that this crime has a transnational nature as the card issuer, card holder, merchant and offender may be in different jurisdictions. He suggested that laws in various countries need to be harmonized to facilitate trials in multiple jurisdictions. The participant from Brazil opined that the best countermeasures have to come

from the industry itself, by streamlining procedures regarding issuance and the use of credit cards and in improving the security features of the card. The participant from Japan stated that credit card crime is often perpetrated by organized gangs/ mafia. He suggested that end users may be provided immunity from prosecution to rope in the members of the organized gang.

It was agreed that the challenge can be met by a coordinated effort by industries and governments. The credit card industry should streamline procedures and improve security features, while cardholders and merchants should act more responsibly in handling the cards. At the same time, governments should enact necessary laws to keep pace with new technological challenges and finally, laws may be harmonized in various jurisdictions so that criminals may not take advantage of the discrepancies.

VI. COMPUTER RELATED CRIME

The use of computer technology in business and governmental organizations has created unprecedented opportunities for the storage/dissemination of information in all areas of human activity. At the same time, it has created unprecedented opportunities for crime. It is perceived that the challenge is so great that the law enforcement apparatus in itself will not be sufficient to deal with the situation. Consequently, new forms of control and harnessing non-governmental organizations will become essential.

Various forms of crime have already surfaced; i.e. theft of telecommunication services where hackers get unauthorized access to the telephone facilities and make many millions in telephone calls. Electronic funds transfer assist in concealing and removing the proceeds of crime. Given the fact that computer crime transcends national boundaries, effective countermeasures will also require enhanced international co-operation. It was agreed that for the purpose of this paper, computer crime may be defined as crime in which computer technology has been used to perpetrate the crimes.

Algeria

There is no special provisions dealing with high-tech crime, so the few cases where the computer was involved were prosecuted and convicted under the ordinary stipulations of the Penal Code. However the draft of the new amendments of the Penal Code and the Code of Criminal Procedure, submitted to the parliament, prescribe new penalties and regulations related to computer crime and to data seizure, and to admissibility before the court.

Brazil

Although legislation still lacks specific computer crime law, other legal provisions are being used to prosecute rampant computer-related offences. Brazil has witnessed a rapid expansion of computers connected to the Internet. Fraudulent purchases through this system are being perpetrated against credit card companies and other supplier of goods. All other forms of Internet-related offences, i.e. child pornography, hacking, etc are also being registered in increasing numbers.

Costa Rica

Actually Costa Rica doesn't have a specific law to apply in respect to these cases, but at the moment computers and the Internet are very popular. Proliferation of computers is changing social life and bringing new forms of computer-related crime. Child pornography and hacking are prevalent. Offences relating to computers are punished under the Penal Code of Costa Rica.

Japan

In 1987, the Japanese Penal Code was amended to enable punishment of three types of computer-related crime. The first is the illegal production of certain types of electromagnetic records. The second is the obstruction of business by destroying computers/electromagnetic records. The third is computer fraud, since under the former Japanese Penal Code, the article of the fraud was applicable only to human beings. However, unauthorized access to protected computers is not punishable under the current Japanese Penal Code. Computers are now indispensable tools in Japanese daily life. The following data shows the proliferation of information technology in Japan. The number of host computers connected with the Internet in Japan was 300,000 for 1995, 700,000 for 1996 and 1,150,000 for 1997. Increase in use of computers has resulted in a tremendous increase in computer-related crimes. The following tables shows this trend.

NUMBER OF HIGH-TECH CRIMES IN JAPAN

YEAR	REPORTED NUMBER	CLEARED
1995	111	110
1996	178	176
1997	263	262

Note: cleared figures may contain reported cases from previous years (source: National Police Agency).

Kenya

Computer-related crimes are on the increase. There is no statutory interpretation of the term 'computer crime', and for the purpose of investigations and prosecutions, provisions of the Penal Code are used to deal with these cases. So far the most prevalent cases reported are those that target the computer data and those which are committed using the computer as the instrument to facilitate the commission of the crime.

The kenyan legal justice system, which is based on common law, has difficulties in addressing cases falling under the first category. In the first category of cases, the data exists as electric impulses which are not tangible objects. Common law only punish acts against property which is tangible. Victims are normally advised to seek a civil remedy.

Pakistan

Computer technology is gaining ground in Pakistan and the use of computers is becoming more popular. However no new legislation has been enacted and cases, if

BREAKDOWN OF HIGH-TECH CRIME IN JAPAN 1997

CRIME TYPE	Reported	Cleared
Computer fraud	162	163
Illegal production of private electromagnetic record	4	5
Illegal production of official electromagnetic record	8	7
Obstruction of business by destroying a computer, etc.	4	2
Destruction of official electromagnetic record	1	1
Destruction of private electromagnetic record	0	0
Network using crime	83	83
Others	1	1
Total	263	262

(Source: National Police Agency of Japan)

any, are tried under general penal laws. No serious cases involving computer technology has been reported so far.

Other Countries

Computer-related crime is increasing in Korea. The Information Crime Investigation Center was established in the District Prosecutor's Office of Seoul in 1995, and the Information Crime Countermeasures Headquarters was established in the Central Investigation Office of the Supreme Prosecutor's Office in 1996. From April 1995 to August 1997, 263 cases were investigated and 75 suspects were arrested, out of them six suspects were arrested for hacking.

Computer technology is gaining ground in the Philippines but no cases have been reported so far. In India, 22,000 counterfeit share certificates of reputed companies which were allegedly prepared by using desk top publishing (DTP) systems were seized. Several cases of software piracy have been registered by Delhi police on the initiative of NASSCOM, India. South Africa has specific provisions in the South African Police Services Act 1995 which criminalizes unauthorized access or modification of computer material belonging to or under the control of the police service. However the practice of search and seizure is based on common law. The computer crime investigation unit of the South African police service deals with computer-related crime. There is no specific legislation regarding computer-related crime in Thailand and if any, cases are dealt with under normal penal laws.

Case Study

1. Online Computer Fraud in a Bank, Nagoya, Japan

Facts

A and B defrauded a bank in Nagoya by illegally using the bank's computer system. They pressurized C, a clerk of the bank, to take secret data of the host computer, including descriptions of the bank customers. A and B, being outsiders, deciphered the data code and obtained passwords and account numbers of other companies. Posing as customers, A and B used their own computer to access the bank's computer system from a hotel room and sent false remittance information. They acquired illicit profits by producing false records. About 1.6 billion yen in total was remitted to accounts, which the other accomplice had established in other banks. The accomplice was able to withdraw about 140 million-yen from one bank.

However, when the other bank inquired of the bank in Nagoya regarding payment of the 1.5 billion yen, the fraud came to the notice of the Nagoya bank, which prevented payment and prompted reporting to the police. During police investigation, it transpired that C had acquired data from the bank in Nagoya. Next, police suspected A, since he had a close relationship with C. A often stayed in a hotel, where the telephone was suspected of being used to access the bank in Nagoya. The police finally acquired the telephone record and found that A, along with another accomplice B, were involved in this case.

Difficulties / Problems raised by Participant

(a) Intense anonymity of offenders at the initial stages of investigation. Telephone records at the hotel had already been deleted and the telephone company did not volunteer information due to secrecy of communication.

(b) Special knowledge of computer technology was required in gaining and examining evidence.

Countermeasures / Solutions shown by Participant

(a) Search and seizure warrants for the

bank's telephone records were carried out so as to identify the person who accessed the bank in Nagoya. This obtained necessary information which would not have been otherwise available due to the secrecy of communication.

(b) Investigators to be provided better training in high technology.

(c) Improve co-ordination/co-operation between private enterprises and law enforcement agencies.

2. K Securities Case of Kenya

Facts

A was employed by K Securities Ltd as a computer operator. He was sharing his office with other employees. His duties included entering all data relating to the buying and selling of shares for the firm's clients. During the period between 1996 and early 1998, A colluded with B, the firm's dealer at the stock exchange, to form fictitious companies through which they perpetrated theft of the client's shares. Following frequent complaints by the clients, the matter was discovered by C, the executive director of K securities Ltd. However A destroyed all the data in the computer by invoking the delete command on all the contents of the computer's directory.

The latest backup of data was done late in 1997. The companies operations were paralyzed as the computer system held 85% of the information required to run the day to day operations. C enlisted the services of an expert who managed to recall most of the data from the computer database. Subsequent examination of the recalled data revealed that A and B had defrauded K Securities of about Ksh.5 million. They were arrested five months later and charged with the offence of 'stealing by servants'.

Difficulties / Problems raised by Participant

(a) It was difficult to recall the deleted data from the computer hard disk.

(b) Both the director and the investigators had inadequate knowledge about the operating systems of computer.

Countermeasures / Solutions shown by Participant

(a) Regular training of law enforcement agencies to update their knowledge of modern technologies.

3. Computer Fraud Targeting KDD of Japan

Facts

A, with a view to evade telephone fees, developed software which was capable of obstructing the KDD computer system from recognizing telephone calls and charging a fee. Later B and C shared in such software and evaded telephone fees individually. However KDD had an alarm system which was activated when a subscriber continuously engaged its line for more than two hours with more than two minutes silence during that hour. The suspect held the line for two hours, resulting in detection. So by this alarm system the case was found out and KDD reported it to the police in December 1993. Police found out that A, B and C had in total incurred a bill of 27 million yen which was not recorded by KDD, during a period of one year and seven months. A, B and C were arrested on allegations of computer fraud and all were convicted after trial.

Difficulties / Problems raised by Participant

(a) Though KDD was the victim, it was reluctant to volunteer evidence claiming its right to secrecy of communications.

(b) The exhibits included personal computer and data which was very difficult to preserve. The computer

was special because one had to enter a password before switching it off, otherwise part of the data would be erased.

Countermeasures / Solutions shown by participant

(a) The evidence was secured by search and seizure after the search warrant was issued by a judge.
(b) Services of experts were solicited for preserving the computer data.

Discussion in the Group

It was generally agreed that crime involving high technology poses difficulties for investigators and requires special expertise and skill to successfully prosecute offenders.

The participant from Japan pointed out that under the usual interpretation of search and seizure, the target is supposed to be tangible, while computer data is intangible. It is also difficult to identify the exact location of the data in a computer system. Further, computers are multifunctional and hold large amounts of data. Seizure of entire mediums/systems containing evidence could affect the interest of others or obstruct the business of the enterprise. Network computers can be multi-jurisdictional. In most countries, prior judicial authorization is required to carry out searches and courts demand particularity, i.e. the location, the equipment to be searched (hard drive, diskettes etc). He suggested that to solve this problem new legislation may be considered making it obligatory upon the computer operator to cooperate with investigation authorities, and new international arrangements (bilateral and multilateral) may be made to deal with emerging challenges.

Another participant from Japan reported that in the KDD case, the offender destroyed significant evidence by one key-touch during the police search. He proposed that investigators should be accompanied by experts in computer technology during search and seizure operations, so as to ensure the preservation of data.

The member from Kenya observed that in common law countries, the best evidence during criminal proceedings is primary evidence and in multi-functional computers, seizure of the original medium may obstruct the business operations of an enterprise. He proposed that there is need to enact new legislation that would allow admissibility of computer generated copies as evidence, in special circumstances.

Members from Pakistan, Kenya and Costa Rica pointed out that computer-related crimes are dealt with under normal penal laws in their countries. Most common law countries prescribe punishment in relation to mischief to property, and as property is defined as something tangible, it may not be possible to punish an offender who, by tapping computer keys, destroys data, because data exists as electromagnetic impulses which are not tangible.

The participant from Japan stated that unauthorized access to the computer is not an offence in Japan, while some other countries have prescribed punishment for this offence. He opined that due to the dual criminality principle in international law, it may not be possible to extradite such an offender. He proposed the harmonizing of law by enacting new legislation.

The participant from Brazil expressed the view that in order to prevent computer-related crime, it is necessary to co-operate with industry to establish security systems, saving log data systems, and improvement of encryption. A participant pointed out

the need to have informal contact between law-enforcement agencies of various countries to ensure better co-operation at the international level, especially in high-tech crime, as data can be destroyed very quickly.

It was observed that it is necessary to impart training to investigators in computer technology and co-opt the services of experts in these fields. Establishing special investigation departments for computer crime (Cyberpolice) may be considered. Countermeasures suggested by the participants are summarized as follows:

(i) Training of investigators in computer technology.
(ii) Establishing special investigation departments for computer crime (Cyberpolice).
(iii) Soliciting services of experts in the relevant fields while investigating cases of a complicated nature.
(iv) Better co-ordination between regulatory bodies and criminal justice officers.
(v) New legislation regarding computer-related crimes, and search and seizure of electronic data in certain jurisdictions.
(vi) Computer generated copies made admissible pieces of evidence in special circumstances.
(vii) Unauthorized access to information made an offence.
(viii) Mutual legal assistance among nations in the field of computer crime.
(ix) Government and private industry to work in close collaboration to improve the security of information.

VII. DIFFICULTIES COMMONLY FACED BY CRIMINAL JUSTICE OFFICERS AND SUGGESTED COUNTERMEASURES

A. Globalization of Crime

1. Difficulties

The advent of technology has made it possible for a person sitting in one part of the globe to transact business thousands of miles away. The world is now characterized by unprecedented mobility of information, finance, goods, services and people. This globalization has also provided opportunity to criminals to operate transnationally. They commit crime in one country and find safe havens elsewhere in the world, where criminal justice officers cannot keep track.

Even if one is able to advance the law, the chances of locating the offender, obtaining extradition and launching successful prosecution or recovering compensation is almost impossible. The shear cost of sending officers from one country to another for collection of evidence may be prohibitive. The operation of different laws in different countries further accentuates the problem.

2. Countermeasures

International cooperation in the field of Criminal Justice Administration should be enhanced. Governments should enter into bilateral and multi-lateral treaties for the extradition of offenders and to ensure mutual legal assistance. In the absence of treaties, governments may co-operate with each other on the basis of reciprocity. Informal contacts between law enforcement officers of various countries may be encouraged by having common training programs. The United Nations may assist member countries, when requested, by providing model treaties which have been already developed.

B. Lack of Technical Know-how

1. Difficulties/Problems

Modern information systems provide an effective means by which offenders can communicate in order to plan and execute their activities. Emerging technologies of encryption and high speed data transfer can greatly enhance the capacity of criminal organization to place their communication outside the reach of police. The offenders are able to disguise their identities through the use of complex electronic technologies. Computer technology calls for knowledge beyond the expertise and skill of most investigating officers. Further, complex commercial and financial transactions require special knowledge of these laws/operations. So criminal justice officers find it difficult to successfully prosecute offenders.

2. Countermeasures/Solutions

Criminal justice officers may be trained in the latest technologies and provision may be made for hiring the services of experts in these fields to assist investigators. Services of investigators from regulatory bodies like SESC (Security Exchange and Surveillance Commission) may be co-opted to assist police investigators. Governments should encourage research in the field of computer technology so as to ensure the safety of data and its retrieval, when required by criminal justice officers.

C. External Influences in the Criminal Justice System

1. Difficulties/Problems

Most of the developing countries have remained under the colonial yoke. The colonial rulers had designed the criminal justice system to ensure their rule over the population. The justice/rights of citizens were secondary to their predominant desire to rule. The political authorities in the developing countries inherited that legacy but political institutions being nascent were not strong enough to put the system on its right track, i.e. ensuring the rule of law and democratic control of the criminal justice system. Instead they tried to gain control over criminal justice officers with a view to perpetuate their rule. Thus criminal justice officers were made to act as servants of the political executives rather than as custodians of the rule of law. This has bred corruption in the system and created a gap between the criminal justice officers and the public in general, resulting in loss of support/cooperation from the citizens.

2. Countermeasures/Solutions

Criminal justice officers should be provided operational autonomy by institutional arrangements, so as to insulate them from external interference. In Japan, operational autonomy of the police is ensured by the Public Safety Commission, where members of commission (five in number, not more than two from the same party) are selected by the Prime Minister with approval of both houses of Parliament. They have a fixed tenure and can only be removed by the Prime Minister with consent of both the houses of Parliament. This institution appoints the Commissioner General of Police, with approval of the Prime Minister, and also supervises the working of the National Police Agency.

The concept of accountability of officers, both external and internal, should be strengthened. Review of executive actions, by having the office of Ombudsman, will provide citizens a forum for redress of their grievances. This will restore public confidence and also help earn their cooperation in combating crime.

D. Lack of Cooperation by Victims to Criminal Justice Officers

1. Difficulties/Problems

Business enterprises are reluctant to report crime committed against them to the

police for fear of negative business repercussions. Employees of these organizations are not ready to report their colleagues/seniors. Further, corruption in the criminal justice system of developing countries erodes public confidence in the system. Witnesses will not come forward to depose as the inquiries by investigating agencies take a long time and protracted trials further tax their time and money. High rates of acquittal in developing countries further dampens the enthusiasm of plaintiffs and witnesses.

2. Countermeasures/Solutions

Close co-operation between government and industry will help in building the confidence of entrepreneurs in the criminal justice system. Better training of officers and operational autonomy will bring professionalism to criminal justice officers and earn them the confidence of the public.

E. Poor Coordination Among Various Agencies

1. Difficulties/Problems

It has been observed that at many times, regulatory agencies like the Central Bank, Corporate Law Authority, Income Tax Bureau and other financial bodies detect fraud/crimes but they do not pass on this information promptly to investigation agencies, resulting in destruction of evidence and losing material witnesses. At times, investigating officers hardly communicate with prosecutors during the investigation and prosecutors only learn about cases when the file is submitted to them. This can be detrimental to the successful prosecution of offenders.

2. Countermeasures/Solutions

Common training courses consisting of officers from various fields will promote understanding among various organs of the State. In Japan, various kinds of training courses, conferences and other inter-action activities are organized to provide police officers, public prosecutors, national tax administration officers and officers of other agencies to promote understanding of the activities of various agencies and to improve technical knowledge in other fields. Such inter-actions also help to establish personal contact points in the event of actual investigation, and promote better coordination for the future among different organizations.

F Search and Seizure of Digital Data

1. Difficulties/Problems

Collection of digital data from computers poses problems to investigators, as the computers are not just storage mediums but are performing multiple functions in an organization and hold large amounts of data. The exact location of data in the computer system may not be known. Data may be stored in the server, hard drive, diskette or paper printouts. Data, at times, may be mingled with other irrelevant information. Courts in certain jurisdictions require that investigators should intimate the exact location of data for issuing search and seizure warrants. Further, the seizure of entire mediums/systems containing evidence could affect the interests of others and may cause obstruction to legitimate business. Selective retrieval of data may damage the information contained in the computer system. Problems can further be compounded where cross-border searches may be involved in the future.

2. Countermeasures/Solutions

To ensure proper search and seizure of data, investigation agencies may be staffed with computer experts for identification/safety of data. Courts should flexibly interpret the principle of particularity of data when issuing search and seizure warrants. Criminal procedure laws should also permit investigating authorities to search computer systems and seize data

under similar conditions as in the traditional powers of search and seizure. Computer generated copies may be made admissible as evidence in special circumstances.

Specific obligations should be imposed on service providers, who offer telecommunications services to the public either through public or private networks, to provide information to identify the user, when so ordered by the competent investigating authorities. International agreements should be negotiated as to how, when and to what extent, search and seizure should be permitted. Development of mutual legal assistance treaties may be encouraged.

VIII. CONCLUSION

Economic crime is a complex phenomenon acquiring greater significance in this global era. Economic offenders do not act on the impulse of the moment, rather they carefully plan their crime and execute it in a manner so as to leave no trace. Present day technology has provided the opportunity to act transnationally with ease. It is imperative that governments, over the world work in close cooperation by entering into formal/informal assistance arrangements. Regulatory agencies may be strengthened to play a proactive role in combating such crime. It is important to enhance their investigative capacities, facilitate coordination of their tasks and encourage cooperation amongst them. Awareness of the problem in itself is only part of the solution.