VISITING EXPERTS' PAPERS

ECONOMIC CRIME: EMERGING THREATS AND RESPONSES - SINGAPORE'S EXPERIENCE

*Paramjit Singh**[1]

I. INTRODUCTION

The trepidation over economic crime lingers as a significant threat to businesses across all countries and industries. According to the PriceWaterhouseCoopers Global Economic Crime Survey 2003, at least 37 percent of the top 1000 businesses in 50 countries said they suffered from one or more serious frauds during the previous two years. The reasons to be concerned about economic crime however transcend threats to businesses alone. Peter Grabosky of the Australian Institute of Criminology surmised:

> 'The essence of fraud is a breach of trust. Trust is the very foundation of commerce, and the very basis of civil society. Economic crime thus jeopardises basic interpersonal relations, economic development, and in some cases, even the stability of government. The collapse of the Albanian regime following massive losses sustained by thousands of citizens in an investment fraud constitutes another example.'

The President of the World Economic Forum, Klause Schwab also alluded to the recent financial scandals and the matching negative ramifications on the world's economy:

> "Revelations of dishonesty in some of what were once the world's most venerated firms abound; failed CEOs departing with severance packages worth millions, top managers cooking the books, shareholder and employee welfare subjugated to the greed of the few. Even if these cases turn out to be spectacular exceptions, the image of global business has already been tarnished, and along with it, that of the globalised economy. In this context, it is not surprising that stock prices around the world have fallen to such low, barely fighting to come back."

The PriceWaterhouseCoopers Global Economic Crime Survey 2003 underscores the imminent insidious effects of economic crime on the financial markets. At least 47 percent of the more than 3600 corporate leaders at the top 1000 companies in 50 countries surveyed believed that economic crime has long-term effects on their share price. This perhaps indicates that the financial markets no longer view economic crimes as a historical offence with limited future relevance.

The trepidation over economic crime assumes an even greater ominous dimension when one computes the devastating impact of money laundering on the basic structure of the society. Money laundering has been described as the world's third largest business right behind foreign exchange and oil.[2] Around 2-5 percent (US$800 billion to US$2 trillion) of the world's GDP are laundered each year. Macro economic policy makers now have to include money laundering activities in their evaluation of the economy to avoid misdiagnosis.[3] Money laundering makes criminal activities more difficult to detect and can lead to the criminal infiltration of legitimate businesses. Gil Galvao, President of the Financial Action Task Force, cautioned:

---

* Assistant Director, Commercial Affairs Department, Singapore Police Force. The views expressed in this paper are entirely the author's personal views and they do not necessarily reflect the views of his office.

1 The views expressed in this paper are entirely the author's personal views and they do not necessarily reflect the views of his office.

2 See Jeffrey Robinson's "The Laundrymen"(1996).

3 Speech delivered by Mr Tan Siong Thye, Director of the Commercial Affairs Department and Senior State Counsel in Singapore at the 7th Annual Conference and General Meeting of the International Association of Prosecutors in London in Sept. 2002 pg 2.

'Money laundering, organized crime, and economic crime are often integrally linked, and criminal organizations will use their profits to infiltrate or acquire control of legitimate businesses, and to put legal competitors out of business. They can also use those profits to bribe individuals and even governments. Over time, this can seriously weaken the moral and ethical standards of society and even damage the principles underlying democracy'.

The intimate but menacing link between terrorist financing and money laundering exacerbates the insidious impact of economic crime. Mr Tan Siong Thye, the Director of the Commercial Affairs Department of the Singapore Police Force had at the 7th Annual Conference and General Meeting of the International Association of Prosecutors in London in September 2002, beckoned the call for vigilance. He cautioned:

> 'As with criminals, money is oxygen to terrorist. Money laundered represents the fruits of drug trafficking, arms dealing, prostitution, people smuggling, kidnapping, extortion and terrorism. Ignoring money laundering and terrorist financing will result in global mayhem. Besides the apparent social implications, such as the massive loss and destruction following the September 11 attack, money laundering and terrorist financing can also create economic chaos. Allowing the flow of terrorist funds to continue leads to further terrorist attacks and heightened security concerns. That translates into higher costs for airline transport, lower tourism revenue and higher prices and transportation cost for merchandise.'

No one really knows the exact cost of white-collar crime. The US Chamber of Commerce puts the annual financial tab at a massive US$40 billion, the world over.[4] However it is commonly held that unlike most property crimes, victims may not even have detected the more complex of economic crimes. There may also be instances wherein the victims are reluctant to report such crimes. This is attributed to a multiplicity of motivations that range from pure embarrassment to the negative impact reporting may have on business relationships or staff morale, in the case of corporations. Indeed, according to the 2003 PriceWaterhouseCoopers economic crime survey,[5] only 48 percent of companies in the Asia-Pacific region said they had a requirement to report fraud to an external body. It is against this backdrop, that Mr Wong Kan Seng, the Singapore Minister for Home Affairs, had at the opening of 2001 International Economic Crime Conference in Singapore, cautioned that "globally, economic crime of all sorts must cost governments and businesses billions of dollars every year."

Given its perilous potential, there is clearly a public interest and protection element in economic crime that requires an earnest action against such crimes. For some, economic crime is not perceived as a serious crime because unlike violent crime with its noticeable impact on its victim, economic crime is seen as non-violent in nature. Experts, academics and practitioners alike, have however alluded to the pernicious and devastating impact of economic crime. It has at one extreme, the potential to cause social and economic chaos; and at the other, to cause colossal losses to individuals or corporations. There should therefore be no scepticism that economic crime can beget far more grave and momentous ramifications. So, while academics often debate on the definition of commercial crime, white-collar crime, business crime or economic crime, the primary problem lies not in defining it. The challenge lies in developing appropriate strategies to deal with it effectively.

The Singapore experience has shown that for a determined nation, the problem of serious economic crime is not insoluble or insurmountable. Given that Singapore's economic well-being depends in large measure on the success and integrity of the financial institutions, economic crimes are looked upon with a great degree of severity in Singapore. The policy in Singapore has always been to ensure the highest quality of integrity in the financial system. Corporate and national governance is taken very seriously. Indeed, in the PERC Business Environment Report 2003,[6] which ranks the socio-political and economic variables in various countries, including the United States, Australia and Hong Kong, Singapore was ranked as having the best average scores for the quality, accountability and standards of its institutions. These institutions

---

4 Singapore Law Gazette (Sep 2001), "White-collar Crime - Wide Border Crimes" pg 1.

5 The PriceWaterhouseCoopers Global Economic Crime Survey 2003 involved interviews with more than 3600 CEOs, CFOs or those responsible for detecting or preventing economic crime at the top 1000 companies in 50 countries.

6 The Political & Economic Risk Consultancy Ltd's Business Environment Report 2003 comprised a survey of over 1000 senior expatriates living in Asia.

include the legal, judiciary, police, stock market regulatory, monetary authorities and the quality of corporate governance.

As one of the key institutions and bastions for the prevention, detection and investigation of economic crimes in Singapore, the Commercial Affairs Department ("CAD") of the Singapore Police Force is no less resolute in its mission to safeguard Singapore's integrity as a world class financial and commercial centre through the vigilant and professional enforcement of the laws. "The mission of CAD is to make sure no one unlawfully enriches himself/herself at the expense of others...CAD believes it serves the public interest best if it is able to do its job properly and professionally...and how well CAD does its job has a bearing on foreign investor confidence in Singapore,"[7] Mr Tan Siong Thye, the Director of CAD told The Business Times in a wide ranging media interview in July 2003.

The focus, direction and strategies of the Singapore police towards this direction have not gone unnoticed. The World Global Competitiveness Report 2002-2003,[8] ranked Singapore's police services as one of the most reliable (among 80 countries the world over) in protecting businesses from criminals.

This paper will first dwell on the more common serious economic crimes from Singapore's perspective before dealing with the credit card fraud situation in the Asia Pacific region. It is also critical to allude to the challenges that transpire from the new operating environment. Finally, the paper will discuss Singapore's experience in the successful battle against economic crime.

II. SERIOUS ECONOMIC CRIMES

It would not be possible in a paper to deal with the myriad spectrum of the economic crimes that confront us in the 21st century. As serious and complex economic crimes currently occupy a central position as an economic evil in the world, the paper will provide an overview of the serious economic crimes in Singapore. The objective is not to provide an exhaustive and in-depth analysis but to focus on the nature, challenges and suggested responses to these categories of serious and complex economic crimes. The aim in canvassing these trends is to identify areas where fraud prevention efforts can be mobilised in advance, so that nations may enjoy the maximum benefits of social and economic change, while minimising the downside consequence.

The crime situation in Singapore in 2002 was the second lowest in 15 years after 2001. The crime rate per 100,000 total population was 768 cases in 2002. There were 2,669 cases of cheating and related offences such as criminal breach of trust, forgery and counterfeiting. More than 36 percent of these 2,669 cases comprised cases that involved confidence tricksters who used various ruses to deceive victims into parting with their money, such as supplying or making false claims/purchases, deceiving victims into buying fake items or obtaining loans from victims under various pretexts.[9]

Whilst it is clear that the majority of economic crimes in Singapore comprise confidence tricksters, this paper will focus on 4 categories of serious economic crimes where fraud prevention benefits had been proactively mobilised by the Singapore authorities to keep the problem in check.

A. Securities Fraud

A safe and sound financial sector will provide investors with the confidence to participate in the activities of the capital markets. Market misconduct is the very antithesis of efforts to safeguard the financial integrity of the market. Such misconduct offends basic notions of fairness and jeopardizes the integrity of the open markets. Various forms of prohibitive market conduct in relation to securities and futures in Singapore are captured in the Securities and Futures Act. The misconduct range from false trading, market rigging and manipulation, disseminating false or misleading information statements to bucketing and insider trading.

---

[7] The Business Times 14 July 2003.

[8] The *Global Competitiveness Report* is a publication of the World Economic Forum and is widely recognised as the world's leading cross-country comparison of data and information relating to economic competitiveness and growth.The Report comprises, inter alia, an exhaustive survey of senior business executives and rankings of 80 industrialized and emerging economies the world over.

[9] http://www.spf.gov.sg/.

1. Alternative and Borderless Trading Platforms

The digital age has fundamentally transformed the manner in which the capital markets operate. The Internet provides investors with an alternative trading platform that is convenient, cheap and provides easy access to the capital markets.[10] The flip side however, is that these revolutionary trading platforms also present new modes of perpetuating fraud, including those relating to the trading of securities.

Market manipulators who disseminate false or fraudulent information to the public find the Internet a convenient apparatus to reach a wide scope of users within a short span of time. False or misleading information, intended to inflate or deflate the prices of securities, is posted on online message boards or circulated in Internet chat rooms. Likewise, perpetuators of boiler room operations have jumped onto the Internet bandwagon.[11] Instead of employing groups of telemarketers to laboriously reach out to investors to promote worthless or bogus securities, the Internet can now be used to market their wares to more unsuspecting investors worldwide.

The US has already seen the negative ramifications of these alternative trading platforms. In 2001, the US Securities and Exchange Commission filed charges against 19 individuals involved in an insider trading scheme.[12] It was the first case involving the use of the Internet to pass insider information. The originators of the scheme met each other when they began communicating via the Internet and hatched the scheme in an Internet chat room. They used private internet chat rooms and instant messaging capabilities of the Internet to pass material non public information.

Singapore also experienced its first and fortunately, only case involving the use of the Internet to disseminate false information for the purpose of share market manipulation. In 2001, a rogue dealer representative posted a false take-over bid posting of a public listed company on the website of a financial portal for stocks and shares. The false website posting induced the purchase of securities of the company and triggered a knee-jerk buying of its shares, thus resulting in a rise of the share price. Fortunately, swift forensic-led investigation by the CAD led to the identification of the dealer within a span of several hours. In meting out the jail term to the dealer, the District Judge recognised that the Internet can be used as a powerful mechanism to reach a wide and vulnerable class of persons.

National boundaries are also becoming meaningless in the global securities market.[13] There is a growing assimilation of the global capital markets as a result of the emergence of a global economy. Global competitiveness has led various capital markets to reach out to each other and to overseas clients and investors. The merger of the London Stock Exchange with the German Deutsche Borse is a case in point. Other exchanges around the world are linking up with each other in an effort to stay competitive. More countries are also trading shares of foreign companies on their Exchanges. Online Internet trading has facilitated foreign investors to link directly to various capital markets. These developments have blurred the national boundaries in the global securities market.

2. Insider Trading

Integrity of the markets is the cornerstone of maintaining investor confidence. This very integrity can be eroded by insider trading - the buying and selling of securities based on some piece of confidential information which is not generally available and which is "price sensitive", i.e. likely, if generally available, materially to affect the price of a security.[14] Some academics claim that insider trading is actually the quickest way for information about the companies to reach the market, and so produces share prices that better reflect a firms' true value. Others retort that "the possibility of being outfoxed by better-informed insiders makes shares riskier for outsiders, who are therefore not willing to pay as much or may not buy at all"[15]. A study by the Indiana University in the US has however confirmed what many already know - that insider trading inflates the cost of raising funds in the stock market, since investors will pay less for shares

10 Speech delivered by Mr. Tan Siong Thye at the Cambridge Symposium 2000.
11 Richard Walker, "A Bull Market in Securities Fraud?" (April 1999), in a speech by Director CAD at Cambridge International Symposium 2000.
12 US Securities and Exchange Commission Litigation Release No 16469 (14 March 2000).
13 Speech delivered by Mr Tan Siong Thye at the Cambridge Symposium 2000.
14 Council for Securities Industry, 'Statement on Insider Dealing' (1981) CSI No 5, pg 3.
15 www.economist.com/editorial/justforyou/current/fn5060.html,'Insider Trading'.

floated in markets they think are rigged. The study also revealed that those countries which enforced their insider-trading laws had a lower cost of equity".[16]

The Singapore Government, like most regulatory bodies in the world, is unambiguous on its position on insider trading. The MAS encapsulated its undesirable impact: "Insider dealing is a particularly damaging activity as it destroys the trust between investors and issuers. Insider trading erodes the confidence of investors and is antithetical to market fairness and efficiency.[17] This fairness notion rests on the belief that insiders should not have an undue advantage over other investors in the market. The rationale to regulate the potential abuse of advantageous information is that there is public interest in protecting the free market. In cases where there is information asymmetry due to the use and abuse of confidential, price-sensitive information, then market failure is said to occur.[18]

To bring its securities and futures legislation in pace with advancement in capital markets, be consistent with international best practices and introduce greater market discipline, the Singapore government re-looked at the jurisprudential approach to Singapore's insider trading laws. The laws on insider trading were redefined in 2001 by removing the need to prove the defendant's connection with the corporation, and shifting the focus to the possession of inside information by the accused. This means that liability now directly depends on whether the defendant traded whilst in knowing possession of undisclosed market sensitive information ("the information-connected approach"), and is not dependent on how he was connected with the company concerned ("the person-connected approach").

The new information-connected approach creates a more level-playing field among market participants. In the traditional person-connected approach, the burden was on the Prosecution to show the defendant had received the information from the insider, had an arrangement or association with him and was aware that the insider was precluded from dealing. This meant that it was more difficult for the defendant to be convicted as the balance was tilted too much in his favour, to the detriment of other market players. It was also arduous for others down the information chain, i.e. those who received price-sensitive information from some other persons and traded in securities, to be caught. The information-connected approach shifts the core of the offence, i.e., trading while in possession of undisclosed price-sensitive information by the defendant. The new provisions also tightened the mens rea test for directors or connected persons. A refutable presumption was created that connected persons with possession of inside information are deemed to know that the information is undisclosed and price sensitive.

The new standard aims to introduce a greater degree of market discipline for those in fiduciary positions. The regulations curbing the misuse of privileged information also help to create a "level playing field" among market participants. The shift in approach will send a clear message to investors and market participants that use of material non-public information to one's advantage will not be tolerated.

3. 'Bucket Shops'

'Bucket shops' commonly refers to commodities trading companies that lure victims to trade in securities by masquerading as legitimate trading companies offering lucrative 'jobs' with minimal requirements. These 'jobs' include clerical and administrative positions that require no experience, qualification or age limits. Once lured, instead of the promised jobs, jobs seekers are presented with a sales pitch to entice them into trading in commodities. They end up investing with these companies which may "bucket" (claiming to effect transactions for the clients when they did not) or "churn" (make repeated transactions) to earn commissions from clients. The victims usually show initial profits but soon start losing money and are asked by the companies to top up their trading accounts. To cut or recover their losses or retrieve their principal sum, the victims end up investing more money and eventually losing their entire investment.

Singapore effectively dealt with the 'bucket-shops' through a multi-pronged approach. Various government agencies work within a multi-dimensional approach. A new legislation, the amended Commodities Trading Act criminalised inter alia, false trading, bucketing and fraudulently inducing trading in futures contracts and employment of other fraudulent practices in relation to bucket shops. It also broadened

16 Ibid.
17 Monetary Authority of Singapore, 'Consultation Document on Insider Trading' (27 Jauuary 2001) pg 1.
18 Yang Ing Loong, Andy Yeo and Sharon Lee, 'Insider Trading' reported in www.lawgazette.com.sg.

the definition of commodities to include intangible commodities such as band-width and indices. Under the amended Act, harsher penalties also await those who trade without a license.

The legislative effort is complemented by the strenuous enforcement efforts of the CAD. Following reports that bucket-shop operators had "cheated unsuspecting job-seekers of some S$1 million in the first four months of 2001,"[19] CAD successfully launched a major calibrated enforcement blitz. More than 8 corporations and 38 individuals were charged under the amended legislation, effectively curtailing the bucket-shop problem in Singapore.

B. Corporate Fraud

1. Sound Corporate Governance

A good corporate governance regime is central to the sound development of the state. A sound corporate governance regime, comprising a well functioning legal, regulatory and institutional environment helps to maintain overall market confidence, renew industrial bases, attract long term investment capital, sustain economic growth and ultimately enhance the nations' overall wealth and welfare. The integrity of corporations, financial institutions and markets is particularly central to the health of economies and their stability. The corollary of poor corporate governance practices is well expressed by Arthur Levitt, former chairman of the Securities and Exchange Commission in a speech in 2001:

> "If a country does not have a reputation for strong corporate governance practice, capital will flow elsewhere. If investors are not confident with the level of disclosure, capital will flow elsewhere. If a country opts for lax accounting and reporting standards, capital will flow elsewhere. All enterprises in that country, regardless of how steadfast a particular company's practices, may suffer the consequences. It serves us well to remember that no market has a divine right to investor's capital".

Corporate governance has gained global significance in recent years. The President of the World Bank, submitted that, "the proper governance of companies will become as crucial to the world economy as the proper governing of countries".[20] This view is particularly momentous when one takes account of the consensus view that poor corporate governance often causes corporate carnage and failure. The recent spate of corporate calamities, the likes of Enron and WorldCom, prompted the President of the Institute of Chartered Accountants in England and Wales to remark, "behind every headline case is a failure of corporate governance".[21]

Corporate governance of companies may be defined as the processes and structures in which the business and affairs of the individual companies are governed by their board of directors and senior management. The OECD issued a set of corporate governance standards and guidelines to help corporations and other parties that have a role in the process of developing good corporate governance. The OECD paper defines corporate governance as a "set of relationships between a company's management, its board, its shareholders, and other stakeholders."

Corporate fraud and scandals are the very antithesis of good corporate governance. Corporate misconduct generally refers to punishable acts that are committed by directors, agents or those in controlling positions within corporations, using the resources and power derived from the corporate form as a vehicle to achieve ends. These acts may either benefit the individual personally or the corporation. The acts are distinguished from other punishable acts against the interest of the corporation that are committed for personal gain by agents or persons who are not in controlling positions, such as misappropriation of corporate properties.

2. Collapse of Barings

The infamous 1995 collapse of Britain's oldest merchant bank, Barings, offers an unfortunate but succinct illustration of the nexus between lax corporate governance and corporate failure. Much of the circumstances surrounding the collapse revolved around,

---

19 The Straits Times April 18, 2001.
20 Wolfensohn, J.D (1998), 'A Battle for Corporate Honesty, The World in 1999' in The Economist Newspaper.
21 Wyman, P.(2002), Speech given at ICAEW Council on Enron, Feb 2002, reported in http://www.icaew.co.uk.

Nick Leeson, the then managing director of Barings Futures (Singapore) Pte Ltd ("BFS"), Barings Singapore office. Leeson had concealed the spiralling debts which he had chalked up as a derivatives trader in Singapore, causing the 240 year old bank to collapse, under losses of US$1.4 billion. Leeson was sentenced to six and half years in a Singapore prison for charges of deceiving the auditors of Barings and the Singapore International Monetary Exchange Ltd ("SIMEX").

There are several lessons in corporate governance that arose from the collapse of Barings. The main thrust of this section is to underscore some facets of corporate governance drawn from the investigation report on the affairs of BFS by the Inspectors appointed by the Minister of Finance, under the Companies Act ("the Report"). The report was directed to the specific circumstances surrounding BFS and not the Barings Group. The succinct report is reproduced, in part, in this section to assist in the analysis.

Barings set up BFS in 1987 and was granted membership by the Singapore International Monetary Exchange Ltd ("SIMEX"). Leeson was employed by Barings Securities Limited ("BSL") in 1989. In 1992, he applied for registration as a dealer with the Securities and Futures Authority ("SFA") in England. When the SFA queried BSL on a false statement that Leeson had made in the application, BSL eventually withdrew the application to the SFA.

Notwithstanding his failure to register with the SFA, it was decided from the outset that Leeson would also trade at BFS, as its floor manager at SIMEX. In Leeson's application to register with SIMEX, the Exchange was never made aware of the false statement that Leeson had made to the SFA. SIMEX later said that Barings "contributed to the deception by supporting his application which contained false information". Although required to do so, Leeson also did not disclose the outstanding county court judgement against him in the UK.

By 1993, Leeson was trading on behalf of the Barings Group (referred to herein as "proprietary trading"). By the end of 1994, Leeson was thought to be one of the major contributors to the profits of the Barings Group. As a proprietary trader, Leeson's primary activity was to arbitrage or to take advantage of price and interest differences between those quoted for identical contracts on SIMEX on the one hand and on the Tokyo Stock Exchange or the Osaka Securities Exchange on the other.

Almost immediately after BFS began trading on SIMEX as a clearing member, Leeson opened a trading account which he named account 88888. This was the account Leeson subsequently used to conceal errors and to carry out unauthorised trading activities using the banks money up to Feb 1995. The transactions booked in account 88888 by Leeson were "distinguished by three features:

(i) the size of the positions was large from the outset and grew quickly;
(ii) the transactions were not hedged by matching positions. As a result, the Barings Group was exposed to enormous potential losses from even small market movements; and
(iii) the transactions consistently reflected losses from the time the account was opened. In fact the cumulative losses on account 88888 amounted to \135.5 billion (S$2.2 billion) after the collapse of the Barings Group.[22] Leeson required funds to finance the losses and margin deposits. The funds came from other Barings Group companies. Despite this, the Report found that "Barings management consistently contended that account 88888 was an unauthorised account that they had no knowledge of".

The Report found that there were shortcomings in the way in which the persons to whom Leeson reported implemented the matrix management structure. In theory, the Barings Group functioned on a matrix management structure, with Leeson reporting both to his local managers in BFS and his product managers in London. In practice however, Leeson's local managers considered BFS as Leeson's own responsibility and thus did not check Leeson's activities. The local managers also never remedied the problem highlighted in a 1994 internal audit report which identified Leeson's control of both the front and the back offices of BFS as a problem.

The Report also concluded that the vast sums of money remitted to BFS, which exceeded the total value of the Barings Group's assets, failed to attract close scrutiny by the Barings Group. The Barings Group's

[22] See Michael Lim and Nicky Tan's, "Barings Futures (Singapore) Pte Ltd. The Report of the Inspectors appointed by the Minister for Finance" (1995).

risk positions, trading limits and trading performance and the allocation of funding were monitored each day by a high-level Asset & Liability Committee ("ALCO"). It established that at some stage, ALCO did decide that Leeson should be asked to reduce his positions, but this decision was never effectively implemented.

The Barings Group's Financial Controls Department also apparently did not discover the existence of account 88888 although it might have been expected to do so. The Report attributed this partly to the limited view that the Barings Group Finance Director, took of the role of Financial Controls. It established that Financial Controls never had an accurate idea of the true profits and losses of the Barings Group nor properly monitored the cost of funding of the Barings Group's trades executed by Leeson.

The Report found that there was insufficient action taken by the Barings Group to reconcile Leeson's funding request. Leeson kept cabling Barings London office to send him more money, ostensibly to fund client positions or meet demands by SIMEX for margin calls (payment deposited with the exchange as security against loss). In actual fact, the money was to finance the losses booked in account 88888. The Report found that Credit Control made no attempt to verify the identities and creditworthiness of the "clients" receiving these loans. Any such attempt would have revealed that there were no such "clients".

The Report concluded that the Barings Group's management either knew or should have known about the existence of account 88888 and of the losses incurred from transactions booked in this account. This was due to several facts, including the fact "that very large sums of money were remitted to BFS without requiring BFS to justify its requests for funds. Furthermore, the 1994 internal auditors had identified as one key issue to be examined further in Singapore, the fact that Leeson occupied a very powerful position controlling both the front and the back offices of BFS. He was both chief trader and head of settlements and was thus in a position to record the trades that he himself had executed in any way he wished. Nothing was done to remedy this".

The Report also alluded to the inability of Barings Group Treasury and BSL to understand BFS's margin calls. In January 1995, given the magnitude of the Barings Group's positions on the Exchange, SIMEX queried BFS on the adequacy of its financial resources to deal with potential losses and margin calls. A reply by BFS, drafted by the Group Treasurer and approved by ALCO, assured SIMEX of the adequacy of funds to support the positions maintained with SIMEX. ALCO had however made no effort to understand fully the position and the basis for the assurances it gave to SIMEX. The Report found that "had ALCO taken any such step, it might well have curtailed the flow of funds to BFS. This would have deprived Leeson of the funds he needed to place as margins with SIMEX, prevented him from continuing to trade in the way he did, and possibly averted the collapse of the Barings Group".

In addition, the Report concluded that action had not been taken to fully investigate and resolve a discrepancy detected during an audit at BFS. In January 1995, while performing the annual audit of BFS's financial statements for the year ended 31 December 1994, BFS's external auditors discovered a discrepancy of \7.7 billion (S$115 million) between the SIMEX Yen settlement variation account in the general ledger and the balance for the same account as shown on the SIMEX statements. To cover up this discrepancy, Leeson concocted a fictitious deal, a supposed 'over-the-counter' deal that was supposedly brokered by BFS for BFL and Spear, Leeds & Kellogg ("SLK"). He told the auditors that this discrepancy represented a receivable due to BFS from SLK. When further queried, Leeson gave a different explanation, that the balance had in fact arisen from a transaction that he had brokered between SLK and Banque Nationale de Paris ("BNP") without any authorisation from his superiors and that BFS had paid BNP a sum of about \7.7 billion (S$115 million) two months earlier. The Report found that in fact, there was no receivable due from SLK at all. The discrepancy represented part of the funds remitted by the other Barings Group companies to BFS that Leeson had used to finance the losses and margin calls in respect of transactions booked in account 88888.[23]

---

[23] Leeson was subsequently prosecuted and convicted in Singapore for cheating Coopers & Lybrand, BFS's auditors, into giving an unqualified audit clearance. He deceived them into believing that US securities house Spear Leeds and Kellogg (SLK) had paid BFS a sum of 7.78 billion yen through Citibank in Singapore for an Over-the-Counter trade Leeson had brokered. To do this, Leeson concocted an option to deal to balance his company's books. To cover his tracks, he had computer entries faked, confirmation letters as "evidence" for the trade and also falsified bank statements.

In summary, the Report found that:

(i) Almost immediately after BFS began trading on SIMEX in 1992, Leeson opened a trading account which he named account 88888 and booked a large volume of transactions in this account. He then contrived a series of measures to conceal the true nature of the account from the external auditors and supposedly from his superiors. The net effect of these transactions was to artificially inflate the Barings Group's reported profits which was attributed to his performance; and
(ii) Information pertaining to account 88888 and the margin calls on the account was available in London at all times. In spite of the growing discrepancy between the funds remitted to BFS and the transactions in respect of which the funds had been requested, other Barings Group companies continued to remit funds to BFS, and by the date of the collapse, had remitted about S$1.7 billion".

According to the Report, the collapse of Barings "could have been averted if:

(i) the growing difficulty in reconciling Leeson's funding requests had been thoroughly and promptly investigated; or steps had been taken to overcome the inability of Group Treasury and BSL Settlements since, at least, June 1994, to understand BFS's margin calls; or
(ii) the significant risk (i.e. those highlighted by the internal auditors in October 1994, that Leeson could override internal controls by virtue of his command of the front and back offices) had been addressed; or initiatives such as the "middle office" person had been effectively implemented when they were proposed in the last quarter of 1994; or
(iii) Barings high level Asset & Liability Committee had taken Leeson to task for increasing his positions, despite instructions in 1995 that he should reduce his positions; or the discrepancy highlighted in the 1995 audit (the SLK Receivable) had been fully investigated and resolved at the end of January 1995; or
(iv) ALCO had understood and effectively addressed the concerns expressed by SIMEX in its letters to BFS, particularly as to the large positions maintained by BFS, and its ability to fund these positions; or the reasons underlying the requests for very large amounts of funds by Leeson in January and February 1995 had been analysed and understood".

3. Implications for Corporate Governance

The collapse of Barings had therefore much to do with the endemic ineffective corporate management. At its core was the failure of internal controls. A well-informed board did not seem to have been present in this case. W. P. Hogan alluded to the failure of the management in its monitoring and analysis of trading activities as well as the risk associated with them.

Accountability was suspect. The Inspectors Report alluded to the endemic repeated failures by the management to deal with the problems highlighted earlier in this section. W. P. Hogan also observed that the "inefficiencies of Barings accounting, recording and settlement systems meant that data supplied to the leading supervisor was defective and not revealing the true condition of the Group."[24] These views were echoed in 2000 by a three-judge High Court panel in turning down the appeal against debarment by a Barings director. They alluded to the "serious abdication of responsibility" that contributed to the Barings crisis. Likewise in June 2003, the British High Court judge hearing a litigation brought by the liquidators of BFS against BLS, blamed Baring's management, citing "a very high level of fault by BFS, and those to whom the board of BFS delegated their functions".

Leeson himself, in an interview on his side of the story given to the London's Sunday Morning Post after his release from prison, was reported to have said:

> "There are many people who have to look at themselves daily in the mirror and know too that they, too, were not performing properly. I was feeding them complete rubbish to get cash from London to hide the losses: at the end, as much as 40 million pounds or so a day"... I was supposed to report to four people. ...My direct supervisor wasn't interested in the futures and options side of the business. Another boss was in Tokyo and I was having less and less to do with him - only speaking to him occasionally on the phone. Lastly there were my bosses in London. In due course he (Barings Head of Finance Products Group) began to be excited by the size of the profits I was reporting, and he took direct responsibility for me."[25]

---

[24] See W.P Hogan, "Corporate Governance: Lessons from Barings".
[25] The Sunday Morning Post, July 18,1999.

Another significant focus in corporate governance relates to the role of shareholders in monitoring and rendering accountable the directors and management of any company. This aspect was not scrutinised at length in the Singapore Inspectors report, which primarily concentrated on the assessment of what happened at BFS. It is noteworthy however, that W. P. Hogan had alluded to the absence of questioning by outside shareholders as another likely circumstance that may have "bred a complacency towards effective management in the Barings case".

Ultimately, the lesson to be drawn from the Barings fiasco is that 'corporate governance' is not merely a list of procedures or safeguards. It is also a state of mind.

C. Money Laundering - Singapore's Experience in Underground Systems and Non-Financial Institutions

Money laundering refers in general to the process intended to mask ill-gotten gains so that they appear to have originated from a legitimate source. The 'washing' process to 'clean' these ill-gotten gains involves a complicated cycle of transformation, commonly referred to as the 'placement', 'layering' and 'integration' stages.

The concentration of the world's anti-money laundering efforts has shifted over the years. Proceeds from drug trafficking were the focal point of the world's anti-money laundering measures in the 1980s. In the 1990s, different forms of crimes such as corruption and financial crimes engendered the incentives for money to be laundered. Today, terrorist financing has gained prominence in the world's anti-money laundering campaign. Whilst the methods are closely intertwined to traditional money laundering, the purpose of terrorist financing may differ. Additionally, in terrorist financing, a predicate offence may not be occasioned and the money laundered is meant to be used to commit crimes in the future. In both however, the integrity of the financial system is struck at its core.

Singapore is strategically located at the crossroads between Europe and East Asia and is a well reputed and established international financial and commercial hub. It has institutionalised a robust and, as alluded by the Director of CAD, "disciplined, collaborative and holistic approach" to combat the twin evils of money laundering and terrorist financing. In formulating the right strategies, Singapore is mindful of the challenges that we face. These challenges are aptly encapsulated by the Director of CAD at a speech to the 7th Annual Conference and General Meeting of International Association of Prosecutors in London in September 2002:

> "The problem is compounded by the complex nature of money laundering and terrorist financing, which according to the IMF, "cut across several quite separate dimensions (e.g. law enforcement, financial supervision, corporate vehicles, etc);
>
> Moreover, money launders are free to transfer their proceeds of crime internationally but law enforcement is hindered by jurisdictional boundaries and legal technicalities. It means that investigations into international money laundering is hindered and delayed in the process of trying to satisfy the national legislation in different countries;
>
> In addition, the new knowledge based economy with the increasing use of ever changing technology pose new challenges. The Internet and E-Commerce and online financial services provide business conveniences, but financial institutions now find it difficult to implement "Know Your Customers" practices, thereby reducing the quality of information supplied to law enforcers. Modern communication technology offers instantaneous transaction capability but it heightens time constraints on the investigator because criminal funds must be traced and seized quickly before launders can move them."

This paper will focus on Singapore's proactive, collaborative and disciplined approach in ensuring the problem of money laundering through non-financial institutions and underground systems is kept in good stead and check.[26]

---

[26] Speech delivered by Ms Yeo Pia Jee, Assistant Director of the Financial Investigation Division, CAD, at the 20th International Symposium on Economic Crime in September 2002, at Jesus College, UK.

1. Non-Financial Institutions - Proactive Enforcement Efforts

There are about 413 money-changers and 123 remittance houses in Singapore. In 2001, the remittance houses transacted close to S$10 billion. This figure has progressively escalated by at least 35% over the last three years. The sheer volume of public funds passing through remittance houses, make it incumbent on the authorities in Singapore to exercise continued vigilance to ensure that the operators are properly licensed and regulated. The legislative and regulatory safeguards and measures will be alluded to in a later section of the paper.

The complex nature of money laundering and terrorist financing underscores the possibility of remittance houses being used as conduits for transferring illegal proceeds or even for financing terrorist activities. The regulator of financial institutions in Singapore, the Monetary Authority of Singapore ("MAS") has proactively and religiously conducted focused inspections in addition to the regular on-site inspections. A case in point was the MAS move in 2002, to revoke the licenses of two medium-sized remittance houses in Singapore that were transacting several hundred thousand dollars a day. The businesses had failed to comply with accounting and reporting requirements. Whilst there was no suspicion of fraud, the move was a prudent one since any lapse in practices could give rise to opportunities for mal-practices to be committed.

The regulatory effort of MAS is complemented by the strenuous investigative efforts of the CAD. Since 1999, the CAD has successfully investigated 49 complaints against money-changers and remittance houses. Of these investigations, the CAD has successfully prosecuted 20 cases. Convictions were secured for a variety of offences like carrying out business without a license and failure to segregate clients' monies.

The comprehensive regulatory and enforcement efforts have yielded successes in uncovering fraudulent activities. At the 2002 International Symposium on Economic Crime in London, the CAD shared a recent case in which the prosecution of a bank cheat was successful because the money-changer was diligent in adhering to the requirement of maintaining proper records of the customer's particulars and of the transaction details. In the case, two officers from a local bank conspired with others to transfer S$600,000 from the bank customers' account to an accomplice's account. The CAD's investigation revealed that one of the bank officers left Singapore with 26 S$10,000 notes to a neighbouring country, to convert the money into foreign currency so as to avoid detection and convert the S$10,000 notes into smaller denominations. On his return to Singapore, he patronised a local money-changer and changed the foreign currency into smaller denominations in Singapore currency notes. Because the transaction exceeded S$5,000, the money-changer complied with MAS guidelines and he maintained proper records on the identity of the customer and the transaction amount. This information was crucial for the investigation. It would have been difficult otherwise to establish the chain of evidence that the cash held by the accused originated from the proceeds of his crime. The duo was convicted for cheating the bank as well as for money laundering under the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act.

2. Underground Systems

Recent events have drawn attention to the possibilities of the underground systems being used to move "dirty" money. The ease in which money can be moved makes the infamous *Hawala* or *Hundi* systems an attractive and popular avenue for laundering money.[27] In 2001, the CAD carried out an intelligence probe on a group of unlicensed remitters who routinely offered remittance services to foreign workers employed in Singapore. As they were unlicensed, their activities were deemed illegal.

The probe resulted in the arrest of one of the bigger unlicensed operators. The investigators went on to uncover evidence that reinforced our understanding that these *Hawala* operators exist to cater the needs of the foreign workers in Singapore. Unlicensed operators thrive because they charge low or no commissions and they have the necessary network to ensure that remittances reach the beneficiaries, even in remote parts of the world. They also provide value-added services to their customers by delivering letters with the remittance to beneficiaries at no extra cost. Their flexible operating hours and mobile services also provides convenience to their customers.

---

[27] Speech by Mr Tan Siong Thye, "Money Laundering and E-Commerce" delivered at Cambridge Symposium 2001 reported at pg 278 of the February 2002 issue of the Journal of Financial Crime.

There is a possibility that non-financial institutions can be used by money launders to transfer ill-gotten gains. Singapore's multi-faceted approach of licensing, regulation and enforcement, coupled with its world benchmarked practices and legislation are however designed to detect and counter the use of the financial system for money laundering. This approach has in our view, achieved optimal impact.[28]

D. Credit Card Fraud

1. Susceptibilities in Credit Card Fraud

Credit card vulnerabilities are manifested in various forms. They include:

(i) Susceptibility inherent within credit cards

Credit cards have inherent vulnerabilities. Even when credit cards first appeared in the financial payment systems in the 1950s, there were attempts to use them to obtain funds, goods or services fraudulently. The illegally used credit cards are either completely counterfeit, altered (by re-embossing and re-encoding), or genuine credit cards that were lost or stolen.

Legitimate or valid credit card details are highly sought after by fraudsters. The legitimate details are used to either counterfeit a credit card or perpetrate fraud. Legitimate credit cards details may usually be compromised at three main locations, viz.,

(a) at a merchant location or as the credit card data is passed from one organisation to another during the authorisation process via telecommunication lines. The information from a valid credit card's magnetic strip can be obtained through "card skimming." This is the process of replicating the full data encoded in the magnetic stripe of a genuine credit card, and transferring this copied data on the magnetic stripe of a counterfeit card. To complete the process, the blank, white credit cards are then embossed with stolen numbers, and the signature panel on the card installed. Identifying logos, holograms and colour printing are added to imitate a real or valid card. The challenge is that skimming takes place without the knowledge of the legitimate card holder until much later, when he receives a statement of purchase he did not make; or

(b) where the data is stored. Computer hackers can for example, steal credit card data from servers that store credit card details by using brute attacks or compromised passwords. In February 2003, the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) conducted a probe to track down the computer hacker who breached the security system of an entity that processed credit card transactions on behalf of merchants. It was estimated that the hacker may have gotten access to information on as many as 8 million credit card accounts overall. Often, when credit card accounts are hacked, account numbers and other information obtained may be sold to others who turn, may use that information to make unauthorized purchases or counterfeits.[29]

(c) Other sources of obtaining legitimate credit card data include sources such as cloned web sites, faked merchant web sites or web based computer programmes that use mathematical Luhn algorithm to generate credit card details. In 2002 for example, a Pakistani based offender stole credit card numbers by setting up fake online auction sites at Yahoo! and eBay. These stolen credit card details may be sold to others, who can make use of the information to make unauthorised purchases.

(ii) Susceptibility in the application process

It has often been said that the most vulnerable link in the security chain of credit cards relates to the manner in which the cards are issued. Frauds relating to the issue of credit cards may sometimes be perpetuated when an offender obtains the personal details of a real person and uses them to acquire credit cards in that name. The liability of goods purchased with the use of such cards is then passed to the legitimate cardholder. The crime may also be effected with the use of false identification details to overcome the pre-approval identification process. The information is then used to secure a valid credit card in a false name by offenders who later dodge on payment and abscond. The industry is however experiencing a decline in credit card application fraud as credit card issuers have been quite successful in taking preventive measures.

---

28 Speech by Ms Yeo Pia Jee, at the 20th International Symposium on Economic Crime at Jesus College, UK.

29 CNN Money 27 Feb 2003, "Hacker hits up to 8M credit cards".

(iii) Susceptibility in the transaction process

Fraud is most commonly facilitated if the cards are lost or stolen. At least 48 percent of credit card fraud in the world is perpetuated through lost or stolen cards.[30] Some of these cards were also newly issued cards, stolen from the postal service, before they reached the legitimate cardholder. This remains the easiest way to perpetuate fraud with little or no investment in technology.

Secondly, an increasing number of altered or counterfeit cards have also been used to facilitate credit card fraud. As the magnetic stripe of the counterfeit credit card has been replicated with the tracked data encoded on the genuine card, issuers' authorization processes can be easily compromised and the CVV/CVC value is verified and the fraudulent transaction is approved on the skimmed card. Merchants manning frontline credit card point of sales terminals are also easily deceived into believing that the counterfeit credit card that is presented for payment, is a genuine card because of increasingly high quality of counterfeits and simulated security features, including fake holograms, ultraviolet features and micro printing. Merchant fraud, in which the merchant may collude with the presenter of the counterfeit card to generate fictitious sales transactions and share the proceeds of payment, may also be perpetuated.

Thirdly, electronic commerce and online credit card transactions mean that there is no longer a need for the credit card merchant and card holder to be in the same location. Online fraud poses complex challenges as more credit card merchants embark into the global e-commerce arena, a market that Forrester Research expects to soar to US$8 trillion by 2004. Card fraud is increasingly carried out via faceless mediums such as the Internet and other 'card not present' transactions like telephone orders. At present, most commercial transactions which take place on the Internet are undertaken by customers purchasing goods and services by merely disclosing their credit card details. Therein lies the vulnerabilities. Credit card details obtained illegally have been used to incur millions of dollars in losses. A Pakistani based offender for example, had over a three year period obtained more than US$3 million in stolen merchandise from US online retailers by using stolen credit card details he had obtained after setting up a fake web-site. As the magnitude of global online commerce increases, so too will online credit card fraud, if undeterred.

2. Organised Card Counterfeiting Syndicates in the Asia Pacific Region

The Asia-Pacific region is among the fastest growing credit card market in the world. According to some estimates there are currently about 140 million to 150 million credit cards and between 6 million to 7 million credit card terminals across the Asia Pacific region. According to MasterCard, the average growth rate for the region will be in double digits in the next five years. Developments in electronic commerce will also result in a higher proportion of transactions that are carried out remotely. MasterCard International estimated that by 2005, 52 percent of its transactions will be carried out through remote services, rather than physical point of sale terminals.[31]

Unfortunately, the losses sustained through credit card fraud is also an equally fast growing development around the world. In Europe, the proportion of fraud on United Kingdom issued plastic cards committed outside the United Kingdom doubled during the 1990s and will soon amount to one third of all losses.[32]

Organised credit card counterfeiting has been touted as one of the most common and potentially insidious forms of transnational credit card fraud in the Asia Pacific region. The card industry estimates that over 60 percent of fraud losses in the Asia Pacific markets are attributable to losses sustained through card counterfeiting activities. The Australian Crime Commission warned credit card skimming is a booming crime, with banks reporting a 400 per cent increase in losses in 2002 and costing Australian consumers, business and banks a whopping A$300 million a year.[33]

---

30 Tej Paul Bhatla, Vikram Prabhu and Amit Dua, "Understanding Credit Card Fraud" (June 2003).
31 Russell G. Smith, "Plastic Card Fraud" delivered at the International Association of Financial Crimes Investigators 10th Annual Conference in Sydney 20 May 2002.
32 Ibid.
33 The Age, "Counterfeit Credit Card gangs in the Rise" (17 Aug 2003).

According to Russell G. Smith of the Australian Institute of Criminology, offenders most involved in counterfeiting seem to belong to organised groups which emanate from the region bounded by Malaysia, Indonesia, Hong Kong and Thailand.[34] A United States report on Asian organised crime noted that Chinese criminal groups based in Hong Kong were responsible for 40 per cent of the world's counterfeit credit card losses, which are estimated to cost business between A$41 billion and A$2 billion per annum.[35]

The challenges posed in combating organised card counterfeiting syndicates in the region are exacerbated as such organised transnational crime syndicates usually have the influence of:

(i) Capital, which enables the syndicates to operate and establish bases across different jurisdictions, recruit a network of criminal operatives from various jurisdictions and acquire the capability to produce the counterfeit instruments to perpetuate the fraud;
(ii) Organization, which enables the syndicates to effectively command, control and coordinate their illegal operations across more than one territorial jurisdiction; and
(iii) Muscle, which enables the syndicates to effectively discipline lower level syndicate operatives and deter them from absconding with the proceeds of the crime.

Most credit card fraud syndicates in the Asia Pacific are largely involved in organised credit card counterfeiting activities. The 'capital-organisation-muscle' elements of their illegal operations have been apparent in several cases that were crippled by law enforcement agencies in the region. They include:

(i) A syndicate that had established bases across Malaysia, Hong Kong and Korea. In April 2001, an international syndicate involved in the manufacture and use of counterfeit credit cards was crippled in coordinated operations by the Hong Kong ICAC, Korean and Malaysian police. The suspected mastermind had obtained bona fide credit card data through fraudulent means from hotels in Malaysia and retail outlets in Hong Kong, which he transmitted from his base in Hong Kong to recruited operatives in Korea for the manufacture and use of the bogus cards. Close liaison between the 3 police forces resulted in arrest in various jurisdictions.
(ii) A syndicate that operated between Japan and Hong Kong. Close cooperation between the Hong Kong ICAC and the Tokyo Metropolitan Police ("TMP") uncovered a transnational counterfeit card syndicate based in Tokyo in 2001. The syndicate had operatives straddled in Hong Kong as suppliers of credit card data. As a result of coordinated efforts, TMP raided a counterfeit card factory in Tokyo and arrested five people, including a Hong Kong citizen believed to be the syndicate head. During the raid, the TMP recovered more than 1,000 sets of genuine credit card data, over 300 blank plastic cards used for making false credit cards, computer equipment and other tools for manufacturing false cards. A Hong Kong man was subsequently sentenced in Japan. Inquiries in Hong Kong established that the man's accomplices had been using skimmers to collect genuine credit card data from a Hong Kong restaurant for use in manufacturing false credit cards which were subsequently used in retail outlets in Japan. Card issuing banks in Hong Kong had reported losses of over $185,500 due to the criminal use of these counterfeit cards overseas.
(iii) Syndicates that had links in China, Philippines and Japan. Between 1999 and 2001, Hong Kong police uncovered at least four syndicates that recruited employees working at Hong Kong restaurants, cafes, hotels, nightclubs or petrol pumps, as operatives in transnational counterfeit credit card operations. These operatives were paid commissions to use mobile pocket size skimmers to steal credit card data from legitimate cards of their patrons. The counterfeit cards manufactured from the stolen data were subsequently used at retail outlets in Philippines, China, Hong Kong, Japan and Europe to incur more than HK$1 million in charges.
(iv) A syndicate that operated within the Indonesia, Singapore and Malaysia geographical triangle. In 2000, close cooperation between the three regional enforcement agencies resulted in the crippling of a well organised seven-member syndicate that spanned Indonesia, Malaysia and Singapore. The Indonesian masterminds allegedly learned the tricks from their accomplices in Malaysia and recruited operatives from the hospitality services industry in Indonesia. The operatives were paid to secretly copy data from genuine credit cards used in Indonesia and hundreds of cloned cards were made. Several well groomed operatives were recruited as 'tourists' to proceed to Singapore and make fraudulent purchases with the cloned cards. The syndicate's Singapore link trained and guided

34 Russell G. Smith and Peter Grabosky, "Plastic Card Fraud" delivered at the conference on Crime Against Business in Melbourne in June 1998.
35 Ibid.

the 'tourists' as they made hundreds of dollars worth of fraudulent purchases in Singapore. The operatives disposed of the goods through fencers locally and abroad and duly paid the proceeds to the syndicate masterminds.

3. Singapore's Experience

Singapore has a high number of credit card transactions, but a minimum credit card fraud rate. Between January and November 2003 alone, total credit card billings in Singapore amounted to more than S$11.1 billion. Fortunately, in the past 5 years, there was an average of only 235 cases of credit card fraud each year.[36] Industry sources believe Singapore has one of the lowest credit card to 'sales to fraud' ratio in the Asia Pacific region - as low as 0.08 basis points. Of these, the majority comprises losses that were incurred through credit cards that were reported lost or stolen by the card holders.

Credit card skimming activities are also relatively unknown in Singapore. The last known skimming related fraud in Singapore occurred more than two years ago. The case involved an employee of a petrol kiosk who was recruited to run credit cards through a traditional hand held skimming device on behalf of a foreign based syndicate. Much of the low rate of skimming activities or credit card fraud in Singapore, has been attributed to the effective five-pronged countermeasures adopted by the Singapore authorities.

Online credit card fraud poses a complex challenge. There were reports that credit card merchants located in the United States and United Kingdom were duped into accepting fraudulent online credit card purchases, purportedly made by Singapore based fraudsters. The fraudsters had masqueraded as Singapore based individuals and placed online orders with stolen credit card details. The crooks gave instructions to the merchants to deliver the purchases to addresses purportedly within Singapore. A careful examination of the consignee's given name, address, IDD code and telephone number, would however have easily traced the delivery address to a neighbouring country. The Singapore authorities promptly initiated various measures, including working with the credit card industry to avert Singapore's crime free reputation from being soiled by such online criminals. This approach has in our view, achieved optimal impact.

4. Metamorphosis and Shift in Strategies

Developments in the Asia Pacific region suggests that credit card 'skimming' syndicates have switched to safer strategies. The syndicates now rely less on operatives with hand held miniature skimmers to steal data from the magnetic strips of credit cards. They have transgressed to more sophisticated 'chip skimming'. Chip skimming, in which memory chips are implanted directly into the credit card point of sales terminals offer the syndicates a less conspicuous means of stealing credit card data. In 2002, the Hong Kong ICAC discovered an electronic skimmer secretly implanted in a credit card point of sales terminal in a Hong Kong restaurant. In the same year, the Malaysian Police discovered two integrated circuit chips implanted in credit card terminals of two well-established hotels in Malaysia. Whilst the discoveries had prevented losses that could have amounted to millions, the developments suggest the credit card data can be stolen more inconspicuously with the help of a single rogue employee with some basic technical knowledge. This may be the sign of things to come.

Syndicates have also leveraged on modern technology to perpetuate more insidious skimming activities in the hope of frustrating detection. Recent experience in the region shows that skimming activities have progressed to compromising telecommunication networks through wire-tapping at host terminals. In April 2002, the Malaysian police uncovered a Pulau Langkawi based syndicate that had allegedly stolen encoded credit card information by tapping into telephone line junction boxes. The syndicate targeted shopping complexes which used multiple credit authorisation terminals. It is believed the syndicate enlisted telecommunication technicians to help identify telephone lines and secretly steal credit card data. The Malaysian police made another arrest in January 2003 in Johor Bahru, Malaysia when a suspect was caught intercepting a telecommunication line that was illegally connected to a credit card service centre.

Apart from wire-tapping at host terminals, industry sources have also alluded to the possibilities of skimming by running parallel lines from telecommunication networks. The stolen data may then be transmitted wirelessly using GSM technology to remote stations. Commercially available products such as

[36] Based on reports made with the Singapore Police Force.

digital voice recorders or MP3 players can store the data required to produce counterfeit cards. Merchants and card issuers may not discover the compromise until months later when the Common Purchase Point also known as Point of Compromise is identified. By then, evidence of the skimming would have been removed.

The syndicates also tend to shift their activities across different jurisdictions, preferring softer targets, as soon as authorities begin to clamp down on them. Fraudsters who think rationally about the consequence of offending could target countries that have the lowest maximum penalties for relevant offences or those in which sentencing practices result in comparatively low terms of imprisonment. Russell Smith had noted that in the case of credit card fraud, this is likely to be the case, at least with respect to large scale, organised activities. Offenders in China, for example, where the death penalty exists for serious fraud offences, would be well advised to target victims in Australia where in some states they would receive a few year's imprisonment, or less, for offending.[37] In Singapore, anyone caught illegally skimming credit card data may be prosecuted under the Computer Misuse Act, which carries a maximum punishment of ten years. Japan and Taiwan have also passed stricter fraud legislation in 2002.

5. Industry Safeguards

As much of the vulnerabilities in credit card fraud are inherent in the credit card, or lie in the application or transaction process involving the cards, the role of the industry in safeguarding the integrity of the card and the transaction process is paramount. Fortunately, the industry has also leverage on technological advancements in its effort to prevent card fraud. Banks and merchants have deployed fraud prevention technology in their overall risk management strategies.

The "chink in the armour" of most online credit card transactions has been ascertaining that the purchase is indeed made by the cardholder. A combination of tools and technologies has been deployed by the industry. These include the CVM, a 3 or 4 digit code printed but not embossed on the card nor available in the magnetic strip, to help ensure that the person submitting an Internet credit card transaction is in possession of the card. Payer authentication based on (PIN), associated with the card, similar to those used with ATM cards is also being deployed to authorise online credit card transactions. To prevent identity theft related fraud arising from the use of information in sales receipts, a global initiative requiring merchants to truncate account numbers on sales receipts is also being undertaken. Instead of seeing the full 16-digit credit card number on the sales receipt, as is the case currently, the potential fraud perpetrator will only see the last four numbers, while the first 12 numbers have been masked out. The expiry date of the card, now openly displayed, will also be blocked out. The initiative will take full effect by 2006 and is expected to reduce online fraud significantly.

The industry has also proactively leveraged on security technology to authenticate the account information and make it more difficult to copy electronic credit card data. The industry solutions include:

(i) The use of 'magnetic fingerprints' in credit cards. The solution aims to use intrinsic physical properties of a credit card's magnetic stripe to differentiate between an original and cloned card. The combination of unique magnetic stripe characteristics, together with the account number and other encoded data on the stripe will give each credit card a unique fingerprint. The derived algorithmic value or fingerprint is stored in the banks authorisation system so that it will make it difficult for anyone to present a cloned card as the magnetic fingerprint will not match those stored in the issuing bank's authorisation's systems. These are believed to be stopgap measures pending ultimate migration to more secure systems;
(ii) Smart credit cards, embedded with an integrated circuit chip (ICC) are also increasingly being touted as the solution to skimming. Smart chip credit cards can contain between 16 KB and 32 KB microprocessors, which are capable of generating 72 quadrillion or more possible encryption keys, thus making it practically impossible to fraudulently decode information in the chip.[38] Several countries in the region have already began the migration towards the use of ICC in credit cards instead of magnetic strips to provide a much higher platform for secured card transactions; and
(iii) Biometrics have been increasingly used in international travel documents and other forms of

37 Russell G. Smith and Peter Grabosky, "Plastic Card Fraud".
38 Tej Paul Bhatla, Vikram Prabhu and Amit Dua, "Understanding Credit Card Fraud".

documents, requiring high security platforms. The issue of whether biometrics will be used as a standard security feature in the credit card of this millennium will be carefully reviewed by the key industry players, taking into consideration a host of interdependent factors, including the costs associated with credit card security systems vis-a-vis the level of fraud.

Law enforcement and industry players in the Asia Pacific will continue to monitor trends and countermeasures in credit card fraud. Whilst detailed statistics are not available as credit-card companies have a policy of not revealing detailed fraud statistics, industry sources have alluded to credit card fraud to sales ratio in Asia Pacific being "less than half of the global average."[39] This notwithstanding, history has shown that criminal syndicates prescribe to the belief that it is usually possible to triumph over the system. As long as this belief exists, law enforcement and related parties in the fight against credit card fraud are conscious of the dangers of letting their guard down.

III. IMPEDIMENTS TO PREVENTION, ENFORCEMENT AND DETERRENCE

Effective prevention, enforcement and deterrent action in respect to serious economic crimes today are complicated by several challenges. They include:

(i) Economic crime is more dynamic than ever. New fraud patterns emerge swiftly and can quickly transform and migrate. As soon as businesses institute preventive security measures against one type of fraud, it is not uncommon for criminals to move on to a less risky approach soon after. This dynamism, fuelled by today's fast changing technological landscape has not only led to the emergence of new forms of criminality, but also repetition of familiar economic crimes in "electronic clothes".

(ii) The 'boundary-free' nature of transnational economic crimes complicates the difficulties in locating offenders across boundaries and mounting a prosecution. Enlisting law enforcement assistance may be complicated as resources are finite and priorities may differ across jurisdictions. Sometimes the cost of sending law enforcement officers abroad or securing witnesses from abroad to testify in proceedings may be considered exorbitant.

(iii) Advancement in technology has complicated this further - today fewer or no accomplices are needed to stage the fraud schemes that can reach out to a greater scope of potential victims. Some crimes may slip detection or be discovered only much later. With more electronic commerce and little or no face to face interaction with the victim, those who masquerade their identity behind computer networks, anonymous e-mailers and encryption devices are able to shield themselves from most but the most determined and technologically sophisticated enforcement agencies.

(iv) The 'faceless' nature of serious economic crime today complicates the evidentiary limitations of traditional enforcement and investigation. The traditional "smoking gun", paper trial, "eyewitness" testimony and evidential aspects are less applicable in today's context. Modern communication technology offers bountiful benefits but also heightens the constraints on the investigator as evidence can disappear quickly.

(v) To compound matters, there is the complex interplay of legal problems in different jurisdictions. The diminution of national borders in an increasingly global business community complicates the jurisdictionally limited law reform which is largely unsuited to the demands of a rapidly advancing technological environment.

Notwithstanding the enormous difficulties, law enforcement must find ways of overcoming these problems. To do nothing would be, as CAD's Director Mr Tan Siong Thye cautioned, "akin to standing still in the face of an oncoming tidal wave." Economic crimes in the digital age will only become more severe as the nature, scope and magnitude of electronic commercial transactions multiply and increases exponentially.

IV. SUCCESSFUL RESPONSES - FIVE KEY STRATEGIC FRONTS

Crime has never been a big problem in Singapore. Singapore has grown in many ways in the past decades to become a city-state that has sustained levels of high economic growth, political stability and a sense of safety and security. Indeed, in 2002 the World Competitiveness Report, one of the most authoritative sources on the international competitiveness of nations, ranked Singapore the third safest city in the world in terms of the level of personal security and private property. Singapore has been ranked in the top three

---

[39] Edmond Chan, Vice President, Mastercard (Asia Pacific), The New Straits Times dated 24 March 2002: "Stricter controls, enforcement pay off".

positions in this category for the last four years. In 2003, the PERC Business Environment Report 2003, once again ranked Singapore as having the highest level of public security and safety among countries in the region, including Australia, the United States and Hong Kong.

Singapore's experience has shown that to successfully combat economic crime, there are five key strategic fronts that must be simultaneously engaged. The very diverse nature of economic crime necessitates a combination of counter-measures to effectively plug the problem. Singapore's success against the menace has been achieved by a sum total of three elementary but bedrock principles of deterrence, effective enforcement and prevention under a responsive criminal justice system. These principles are crystallized in the tough and relevant laws enacted by a responsive legislature and pushed by a strong and effective executive; in the strong enforcement by incorruptible officers; in the robust and efficient world class court system, and a police force aspiring to be world class in its total policing capabilities.

A. The Legislative Measures

In tandem with a maturing society, Singapore has over the years, enthused from a purely merit based regime towards a disclosure based regime. Along with this, Singapore has pushed for higher standards of corporate governance, greater market discipline and *caveat emptor*. This climate naturally means that there are in existence, a number of relevant and effective statutes in place to combat economic crimes.

The perpetration of economic crimes today, especially those that are 'boundary-free' and 'faceless,' involves demeanour, notions, methods and expressions that may not yet be defined in existing legislation in some countries. Singapore, like many other countries, has responded by outlawing the new forms of fraud with suitable and appropriate legislation to enable appropriate enforcement to counter the appearance of such economic crimes. Whilst the prospects of criminal prosecutions and punishment may have some deterrent effect, Singapore has also regulated business and commerce in such a way as to prevent and control economic crime without unnecessarily stifling the wheels of commerce and industry. This comprehensive framework of control is achieved in part through relevant legislation and statutes. The bare bones of some laws that have been enacted to keep serious economic crime in check are discussed in this section.

1. Money Laundering

Singapore's legislative framework gives legitimacy and empowers law enforcers to combat global money laundering effectively. For example, the Corruption, Drug Trafficking and Serious Offence (Confiscation of Benefits) Act ("CDSA") was introduced in Singapore in 1999 to provide serious penalties for persons involved in the laundering of proceeds of crime. The Act is significant as it, inter alia:

(i) makes the laundering of the proceeds of at least 182 predicate serious crimes, regardless of whether they were committed locally or not, an offence in Singapore. While there is no mention of the word 'money laundering' in the Act, it is an offence when any person conceals, disguises, converts or transfers any property that represents that person's benefit from criminal conduct;
(ii) amended the *men rea* requirement for a money laundering offence to the accused person 'knowing or having reasonable grounds to believe' that the proceeds were derived from serious crimes;
(iii) makes it mandatory for all persons to report suspicious transactions to the authorities. Non-disclosure would attract a maximum fine of S$10,000; and
(iv) the amendments to the CDSA in 2000 facilitates the sharing of information obtained under mandatory Suspicious Transaction Reporting, with our foreign agency counterparts.

The Money-changing and Remittance Business Act (MCRB) is Singapore's protection against money laundering through non-financial institutions. The robust licensing requirement under the MCRB restricts persons of dubious reputation or poor financial standing from entering the money laundering and remittance business. In addition, the obligation to report suspicious money laundering activity under the CDSA is a general one and extends to non-financial institutions such as money changers and remitters.

As alluded to earlier, it is widely believed that many terrorist activities are funded through a series of money laundering operations.[40] Terrorist organisations can thus adversely affect the integrity of the financial

[40] Speech delivered at the 7th Annual Conference and General Meeting of the International Association of Prosecutors in London.

systems. Various legislation such as the United Nations Act 2001, United Nations (Anti-Terrorism Measures) Regulations and the Terrorism (Suppression of Financing) Act ("TSFA"), are significant in Singapore's war against terrorists financing. These laws also give effect to the international conventions signed by Singapore, as with the proper statutory framework in place, Singapore is now in a position to negotiate with foreign countries.

2. Securities and Capital Markets Laws

The Securities and Futures Act 2001 ("SFA") is Singapore's legislative framework to regulate activities and institutions in the securities and futures industry. The SFA was the result of a fundamental re-examination of Singapore's approach to the supervision and development of the financial sector in 1997, including the shift in emphasis from a merit to a disclosure based regime.

The SFA embodies the new regulatory approach. It provides for a module licensing regime and aligns the regulatory requirements and business conduct standards across a similar class of activity. MAS officers are given wide powers to conduct supervision and investigations to carry out their regulatory role. The civil penalty regime that was previously applicable only to cases of insider trading was also extended to other forms of market misconduct.

The legislation has several significant implications, inter alia:

(i) It will make it easier to prove instances of market misconduct, such as insider trading and other market misconduct offences in court. This is because a civil lawsuit, which is won on the "balance of probabilities", can now be waged against the alleged offenders. In the past, only criminal action could be brought by the public prosecutors based on the more difficult process of proving the case "beyond reasonable doubt". This is an important change as the higher standard of proof in a criminal case of suspected market misconduct offences will not be brought to light;
(ii) Perhaps a more significant difference is the law now enables the securities regulator, the Monetary Authority of Singapore to complement the criminal penalty regime enforced by the Commercial Affairs Department. The Monetary Authority of Singapore can now take civil action against alleged market conduct offences instead of criminal action. It is expected that in time to come, this is where the legislative amendments in the SFA will pack a punch since it is the MAS, backed by the Commercial Affairs Department and the Attorney-General's Chambers which can readily marshal the resources and the know-how to take legal action; and
(iii) The new securities trading platforms brought about by globalisation and technological developments are brought into the fold of the regulation. The SFA for example, provides for a wide gamut of laws that include the provision of extra-territorial reach in the security and futures legislation. In this regard, the SFA provides that if the act is partly committed in Singapore and partly committed outside Singapore, or if the act committed outside Singapore, has a substantial and reasonably foreseeable effect in Singapore and if the act is an offence if it is committed in Singapore, the person who committed the act would be guilty of an offence.

The juxtaposition of these developments will enable Singapore to provide an effective yet nuanced approach to punish wrongdoers and further ensure that Singapore's securities markets operate fairly, efficiently and cater to the new challenges in the regulation of the capital markets.

3. Corporate Fraud

The comprehensive framework of control against corporate fraud is achieved in part through relevant legislation and as well as statutes. The offences described in the Companies Act for example, include all acts and omissions of directors and other officers of a company which are contrary to the law.

4. Reviews and Fresh Sentencing Norms

The gamut of laws in the legislative arsenal against economic crimes is periodically reviewed from time to time to ensure laws remain relevant. These include periodic reviews of the Penal Code, which adequately covers general scams and frauds. Where applicable, fresh sentencing standards are set to deter criminal misconduct. The Chief Justice of Singapore Yong Pang How for example, remarked in a criminal case involving credit card skimming, that new sentencing norms for computer crimes must be set to protect the public interest. The accused in that case, procured two others to swipe customers' credit cards through a device that captured data stored on the magnetic strips, and subsequently provided the information to a

counterfeit credit card syndicate. The accused could have been charged for cheating under the Penal Code, with a maximum imprisonment of 7 years. Instead, he was charged under the Computer Misuse Act for using the card-reading device. The offence carried a maximum sentence of 10 years imprisonment and a $50,000 fine.

B. An Effective Regulatory Regime

Much of the battle against economic crimes takes place at the frontline (e.g. financial institutions). An effective regulatory regime is thus as crucial. The Monetary Authority of Singapore (MAS), the regulator of banks and financial institutions plays a significant role to develop a regulatory environment that upholds soundness and safety while encouraging enterprise and innovation.

1. Money laundering

The MAS requires financial institutions to institute rigorous anti-money laundering procedures, such as the 'Know Your Customer" principle.[41] The MAS also issues directives and conducts regular on-site inspections to ensure that financial institutions have adequate control systems, processes and procedures to combat money laundering, terrorist financing and for the reporting of suspicious transactions.

An equally strong regulatory regime to monitor the alternative remittance systems, such as the money changing and remittance business is also necessary. The MAS regulates these businesses through the MCBA. Those who operate such businesses without licences face vigorous enforcement action by the CAD. There are also requirements for annual audits and record keeping to facilitate regulatory inspections and criminal investigations. This is reinforced by Guidelines on Prevention of Money Laundering issued by the MAS to money changing and remittance licensees.

Self-regulatory bodies like that of the law and accounting professions in Singapore, have also promulgated guidelines to report money laundering activities to prevent them from being targeted as intermediaries by money launders. The Law Society of Singapore for example, is currently reviewing its guidelines on anti-money laundering measures. The auditors role and responsibilities in relation to the prevention, detection and reporting of money laundering are also laid out in the Institute of Certified Public Accountants of Singapore's Statement of Auditing Practice. These proactive measures play a part in addressing the vulnerabilities that professionals, such as those in the legal and financial services, face in being implicated in money laundering activities.

2. Building Strong Pillars for Good Corporate Governance

The Singapore Government recognizes that high standards of corporate governance are needed in the financial sector to foster a strong risk management culture, better internal controls, and greater transparency. Good progress is being made towards this direction. The Government implemented several key initiatives in 2002 to improve corporate governance practices. They include:

(i) Formation of the Council on Corporate Disclosure and Governance (CCDG) to review accounting standards, corporate governance and disclosure issues. Established in August 2002, the CCDG comprises members from businesses, professional organisations, academic institutions and the government whose role is to catalyse and advance governance standards in Singapore. The Council prescribes accounting standards in Singapore in consultation with the Institute of Certified Public Accountants of Singapore. It also aims to strengthen the framework of disclosure practices, reporting standards and corporate governance, taking into account trends in corporate regulatory issues and international best practices.

One of the Council's recommendations was quarterly reporting, which is now required of listed companies with market capitalisation of S$75 million or more. Smaller companies have been exempted until 2005 when a review will be conducted. The International Accounting Standards were reviewed to make sure they were applicable in Singapore. Most were adopted as the Financial Reporting Standards (Singapore), and Singapore-incorporated companies had to comply with these starting 1 January 2003.

41 The MAS Notice 626 (Guidelines on Prevention of Money Laundering) to banks for example, takes account, inter alia, of the provisions of the CDSA and the FATF 40 Recommendations.

(ii) The Code of Corporate Governance ("the Code") for all listed companies to comply from financial years beginning on or after 1 January 2003 was put into effect on 1 January 2003. The Code is a critical milestone in strengthening Singapore's disclosure-based and corporate governance regime. The Code sets out principles and almost 70 best practices spanning four main areas of governance, namely, board matters, remuneration, accountability and audit, and communication with shareholders. The Singapore Exchange (SGX) Listing Manual requires all listed companies to disclose in their annual reports, their corporate governance practices with reference to the Code. The provisions of the Code are not mandatory and the emphasis is on self-regulation. Deviations from the Code have to be disclosed by companies. The emphasis is on compliance with the spirit rather than the form of the Code.

(iii) Proposed enhanced corporate governance standards for MAS-regulated financial institutions. In February 2003, MAS obtained feedback on corporate governance guidelines for Singapore-incorporated banks and direct insurers. The guidelines to be issued aim to further strengthen the independence of boards and set out the roles to be played by directors and chief executive officers in relation to their duties towards shareholders, depositors and policyholders.

(iv) More recently, in January 2003, an educational institution had set up a centre to contribute to the research and promotion of best practices in corporate governance and financial reporting. The National University of Singapore Business School set up the Corporate Governance and Financial Reporting Centre to further entrench high standards among corporations in Singapore.

(v) Companies in Singapore are regulated by the common law. In addition, listed companies are subject to such pronouncement of the Singapore Exchange as are found in the Listing Manual. Whilst the Manual does not have legislative force, the Securities and Futures Act makes it obligatory for listed companies to comply with provisions and other exchange rules. Compliance is enforced by means of an appropriate injunction applied for by the MAS or Singapore Exchange. The legal and regulatory regimes are very much in line with those of developed countries.

Singapore's efforts have not gone unrecognised. Singapore was ranked top in Asia for transparency in the World Competitiveness Yearbook 2002. Credit Lyonnais Securities Asia and PERC, both of whom regularly monitor the corporate governance climate, have accorded Singapore the highest ratings in Asia. An Ernst & Young survey of annual reports of 30 large locally listed companies in August 2003 found that all had generally complied with the principles set out in the Code of Corporate Governance. For instance, all 30 companies surveyed have a monitoring committee and had appointed an independent director to be the Chairman of the audit committee as recommended by the Code.[42]

To battle online credit card fraud and e-payment system related fraud, the MAS has developed guidelines to assist financial institutions in recognising and understanding the dynamism of web application and computer and Internet vulnerabilities. The guidelines are designed to promote sound processes in managing technology risk and the implementation of security practices in line with international best practices. The provisions in the MAS Internet Banking Technology Risk Management Guidelines for example, require that credit card validation numbers specified on the credit card should be used for online credit card transactions. Other related regulatory initiatives by the MAS include the Security Guidelines for Mobile Banking and the Payments and Technology Risk Management Guidelines for Financial Institutions.

3. Private Industry Regulation.

Private industry regulation is an equally effective and complementary regulatory platform that complements the efforts of the government. In the battle against credit card fraud for example, Visa International, has set 10 new security directives for online credit card transactions by its member financial institutions and merchant partners to combat online fraud and boost consumer confidence in e-commerce. The rules include keeping security systems up-to-date, encrypting stored data accessible from the Internet and using and regularly updating anti-virus software. Errant Visa merchant members may be liable to fines, restriction of their credit limit through the Visa network or termination of their Visa membership.

An effective regulatory regime requires the amalgamated efforts of relevant government and private agencies to work together within a structured platform. A case in point is the Singapore Police Force's membership in the Alliance for Cyber-crime Experts (ACE), a network of agencies that comprise

[42] Speech by Mr. Tharman Shanmugaratnam, Acting Minister for Education, at the Best Managed Boards Award, on Wednesday, 19 November 2003, at the Regent Hotel, Singapore.

government bodies like the Info-Communication Development Authority and various interested private regulatory parties such as the Internet Service Providers. The ACE members are in constant deliberations on ways to prevent economic crimes perpetuated via cyber space, including Internet credit card fraud and related epayment and e-banking networks. The ACE is a significant player in the promulgation of rules and regulations concerning the 'faceless' nature of the e-revolution. Quarterly meetings are held to ensure that the law enforcement agencies are constantly updated with the latest state-of-the-art technology in the market and possible countermeasures to circumvent its shortcomings in law enforcement.

C. Vibrant and Proactive Institutional and Enforcement Capability

The rationale for an effective, vibrant and proactive institutional capability and policing to combat economic crimes in Singapore was encapsulated by the Singapore Minister of Home Affairs, Mr Wong Kan Seng at the opening of the International Economic Crime Conference in Singapore in 2001:

> "As Singapore develops as a major financial hub, the development of our capital market, banking and financial sectors and electronic commerce is likely to bring about increasingly sophisticated commercial crime. An effective enforcement system is crucial to protect the integrity of our financial market and business environment."

To proactively surmount the imminent challenges posed by the rising sophistication of economic crime, the Singapore Government created a single premier economic crime investigative authority in 2000. The Commercial Affairs Department, then under the Ministry of Finance, was merged with the Commercial Crime Division of the Police. This pooled the scarce resources and the enforcement and intelligence capabilities of the two crime fighting agencies. It positioned the new Commercial Affairs Department ("CAD") under the Singapore Police Force as the de facto specialised serious economic crime investigative authority in Singapore and the "premier investigative authority on white-collar crimes in Singapore."[43]

The reconstitution of CAD was complemented with a revamp of the Attorney-General's Chambers in 2000 to further enhance institutional capacities to combat economic crime in Singapore. Specialised units within the Attorney-General's Chambers were set up to handle the prosecution of complex crimes, including economic crimes and money laundering. The Financial and Securities Directorate was one of the several units set up. The Deputy Public Prosecutors in the Directorate are specialist prosecutors in dealing with serious commercial offences. The state prosecutors involved also play a more hands-on role advising police officers from the start of the investigations until the cases reach the courts. The relationship has significantly enhanced the police's capabilities to unravel the layers of corporate web usually spun by white-collar crooks to cover their tracks.

The reconstituted CAD has become an even more effective economic crime fighting unit. It has introduced several features to proactively ensure its operational effectiveness in dealing with economic crimes and up-keeping the integrity of Singapore's financial markets and business environment. Some of them include:

(i) Structurally, a streamlined organisation structure was created. Dedicated divisions, comprising highly specialised units to investigate corporate fraud, security fraud, money laundering, credit card fraud and other serious economic crimes were created. The streamlined organisational structure also meant that a central agency for the receipt and analysis of Suspicious Transaction Reports (STRs), investigating of money laundering and identifying and seizing proceeds and assets of crime was created. The quantity and quality of STR information has since increased.[44] The last three years have also seen the successful conviction of several money laundering and securities fraud offences. The new structure has also effectively tackled other serious economic crimes, such as credit card fraud.

(ii) The CAD embarked on a highly specialized training programme for its investigators, resulting in highly trained specialist in various corporate and financial fields. Joint training programmes with world-renowned economic crime enforcement agencies and industry leaders have become an

43 The Business Times 18 September 1999.

44 Speech delivered by Mr Tan Siong Thye at the 7th Annual Conference and General Meeting of the International Association of Prosecutors in London.

integral part of the training diet. Training via video-conferencing with specialist agencies around the world has also become a regular feature in the Department's module. A case in point was a training session with AUSTRAC in August 2003. The calibrated training programme has produced a core of highly trained and desired anti-economic crime specialists - in the past three years, CAD officers have increasingly become regular invitees to share their experiences at world renowned economic crime forums.

(iii) The Department has introduced investigation turnaround times as one of its key measurements of effectiveness. In a wide-ranging media interview in July 2003, Mr Tan Siong Thye, the Director of the CAD publicly heralded the 3 to 9 months investigation turnaround times.[45] Eighty-five percent of the cases investigated by the Department already meet the timelines and many of them are completed well within the prescribed turnaround time. A rogue securities dealer who had posted false information on the webpage of a financial portal to manipulate the share market was for example, prosecuted within 10 days after the offence was reported. The Department plans to reduce the turnaround time-line even further to improve its enforcement prowess and professionalism against economic crimes.

(iv) The Department embarked on a programme to proactively leverage on the progress of information technology to enhance the operational capabilities of the police in combating economic crimes. There is an active use of technology, such as computerised investigation, case management and intelligence systems. At the operational level, technology is deployed extensively to aid complex economic crime investigation. A case in point is the introduction of an IT based system to automatically scan trades to help investigators pick up unusual patterns in securities fraud investigation. The system has been effective in overcoming the difficulties and time in analyzing hundreds and thousands of stock trades in investigations.

The Department has also spearheaded processes to effectively integrate info-communication technology into key business processes. A case in point is the deployment of info-communication solutions for business processes like *ex parte* applications to the Subordinates Courts and consultation with the Attorney General's Chambers. These processes have contributed effectively to improving investigation turnaround times.

D. A Sharing of Responsibilities and Partnership

Swift law enforcement action, effective government measures and legal provisions cannot be the only solution to triumph in the battle against economic crime decisively. Collaboration and partnership, particularly with the business and commercial fraternity is a crucial bedrock. The Singapore Minister of Home Affairs aptly reiterated this at the opening speech at the International Economic Crime Conference in Singapore. He advised "... as with all crime, Singapore's commercial and financial integrity cannot be safeguarded by dependence only on appropriate laws and effective enforcement. It must be a joint effort with the community. The Singapore Police Force will build and leverage existing community links to combat economic criminals."

The main thrust of Singapore's police-community partnership in the battle against economic crime is based on the concept of mutual help. The public and business community is persuaded and encouraged to take personal responsibility, both individually and in partnership with others in safeguarding themselves or their business with the advice and assistance of the police. It is based on the principle that prevention is a shared responsibility and crime prevention measures taken by the community and business entities can limit and reduce opportunities for the commission of crime. This philosophy drives the key message that crime is prevented if the opportunity is denied or delayed. The message is put into operation through a robust institutional structure. This includes:

(i) The National Crime Prevention Council (NCPC), set up to act as a catalyst, advisor and partner to mobilise the support of groups, organisations and individuals from the community to work closely with the Police to prevent crime. It is committed to promoting public awareness of and concern about crime and to propagate the concept of self-help in crime prevention. The Council comprises influential representatives from the commercial and industrial sectors, as well as from the public sector and the Singapore Police Force. Working closely with the police, the council holds regular

[45] Business Times dated 14 July 2003 "It's all about timing, says CAD chief".

crime prevention campaigns, as well as regular exhibitions, seminars, workshops and talks on crime prevention.

(ii) At the organisational level, various departmental and divisional structures within the Singapore Police Force have been formed with the primary task to raise awareness of the community to the significant role it plays in crime prevention and safeguarding itself. These units embark on an extensive programme of community oriented and crime prevention activities, including crime prevention talks and exhibitions.

(iii) There has also been a shift in mental models of the police. Apart from its enforcement responsibilities for example, the officers in CAD also place greater emphasis on their roles as facilitators in the pre-emptive and problem solving approach to countering economic crimes. Through this community engagement approach, CAD serves as partners of the people and the business community instead of solely being a white-collar crime investigative agency.

1. Partnership with the Business Community

Given the complexities involved, a partnership with the business and financial community is extremely imperative in the area of prevention, education, exchange of information and policy development. With the community focus concept and structures firmly in place, and strategic networks established with public and private bodies, it becomes possible to leverage on their cooperation and expertise in economic crime prevention. Against this backdrop, the Singapore Police Force and the CAD initiated various initiatives to engage and mobilise the business and economic community on several fronts. These include:

(i) Industry-wide symposiums and conferences to exchange ideas, promote a culture of awareness about serious economic crimes and propagate the concept of self-help amongst the business and corporate community. The Singapore Police Force and the CAD regularly organize symposiums on economic crimes. Participants from the government and private industries such as the legal, banking, financial, economic, service and retail fraternities come together to learn and share their experience. The industry experts dissect a myriad of issues including, lessons on corporate governance, internal controls, accounting and auditing at these forums.

The CAD has organised at least 4 major industry-wide symposiums on corporate governance, e-commerce fraud and economic crimes, as well as money laundering since 2001. An international economic crime conference was also organized in which more than 500 public and private sector participants from more than 33 countries the world over, came together to focus on economic crime trends and prevention initiatives. These initiatives underscore the importance of good corporate governance that Singapore places in its holistic approach in controlling economic crime. They form part of the larger broad based efforts by public and private sector institutions in Singapore to raise awareness among the corporate sector of the value of good corporate governance.

(ii) Regular dialogue sessions and open lines of communication with the industry serve an effective institutionalised platform to promote industry education and exchange of information. CAD's Suspicious Transaction Reporting Office (STRO) conducts regular outreach programmes with members of the business community as part of its strong anti-money laundering regime initiatives.[46] The dialogue sessions help engage and dispel misconceptions that the business community might have on suspicious transactions reporting. Workshops with members of the community on money laundering and terrorist financing are also conducted. STRO has also set up a dedicated hotline and email address to assist members of the business community who may encounter difficulties or problems dealing with suspicious transactions. These programmes have created better awareness among the members of the business community on detecting, reporting and preventing money laundering.

(iii) Leveraging on the cooperation and expertise of the industry via formal arrangements is equally imperative. For instance, the CAD is a member of the Credit Card Security Group, a task force comprising a consortium of representatives of various banks and credit card issuers in Singapore. The Group meets on a monthly basis to discuss development of strategies, programmes and counter-measures against credit card fraud in Singapore. The Group also supports the CAD in the joint education programmes for credit card merchants, businesses and customers to robustly

46 The business community includes all financial institutions under the purview of the MAS. Banks, insurers, fund managers, accountants, lawyers, money-changers are also involved in the business process and are part of the business community targeted by the CAD.

promote credit card fraud prevention measures. The close and symbiotic task force arrangement has been a crucial pillar in keeping a tight lid on the credit card fraud situation in Singapore.

Investigation and prosecution of economic crimes involving an element of market or business practices, such as insider trading, sometimes require the use of expert testimony in prosecutions. In marking the official appointment of CAD's Panel of Experts in 2002, the Director of the CAD, Mr Tan Siong Thye said, "it is imperative that in the collaboration with the business community in this area, an official panel of experts be formed to enhance the stature of the expert's role". The CAD Panel of Experts comprises a cohort of 25 carefully selected private sector business individuals and captains of industry who are readily available to assist the police in investigation and prosecution of serious economic crimes such as insider trading or corporate fraud.

To meet the challenges of economic crimes in the 21st century, the Singapore Police continue to involve the community and fine-tune the system of community engagement. The existing community engagement infrastructures will be periodically reviewed and enhanced to better meet the increasing intricacies of economic crime in the years to come. The CAD will also continuously expand the network of strategic alliances and partnerships with private organisations, trade associations, etc. to control economic crime. This commitment is aptly embodied in the Singapore Police Force's crime prevention slogans, 'crime prevention, a shared responsibility' and 'low crime does not mean no crime'.

E. International Cooperation

Needless to say, international cooperation is a necessary tool in the holistic approach to deal with serious economic crime. The importance of cross border co-operation was succinctly encapsulated by the Singapore Minister for Home Affairs Mr. Wong Kan Seng during his opening remarks at the International Economic Crime Conference in Singapore in 2001. Mr. Wong said, "To fight crime effectively on the local, regional and global level, we need the co-operation of all our partners from foreign enforcement agencies...As criminals leverage on the new economy initiatives to perpetrate their criminal acts, so must we be ahead of the most sophisticated of them. And to do so, it is vital that we share and learn from one another, unleashing the synergies of our collective intellectual resources and experience".

The Mutual Assistance in Criminal Matters Act was passed in 2000. The Act empowers the Singapore authorities to request foreign agencies to perform a variety of investigative tasks to combat serious crime. These include gathering crucial evidence, recovering the proceeds of crime and carrying out searches and raids in foreign countries. It would also make it easier for Singapore to provide similar help to foreign authorities.[47]

The Act positions Singapore as a global player in the battle against economic crime that has taken an international dimension. The Singapore Minister of Law heralded the Act as "Singapore's commitment to be part of the wider network of cooperation in combating crime on a global scale".[48] Such cooperation will focus on combating serious crimes such as money laundering, securities fraud and serious commercial fraud. The Act is essentially an enabling legislation. It also does not affect the close ties that the Singapore Police have already with its foreign counterparts and Interpol in tackling cross-border crimes.

Mutual assistance with foreign counterparts is a necessary and important component in Singapore's fight against economic crimes. Singapore is an active participant in international bodies which have been set up to fight money laundering worldwide. Besides being an active member of the Financial Action Task Force (FATF), Singapore is also a member of the Asia-Pacific Group on Money Laundering, which promotes the adoption and implementation of internationally accepted anti-money laundering standards. Singapore's financial intelligence unit, STRO develops close working relationships and establishes formalised frameworks for the sharing of information and intelligence. STRO is actively involved in the negotiations of Memorandum of Understanding ("MOU") with several foreign countries. Singapore's membership in the Egmont Group in particular, highlights its willingness to work in tandem with its foreign counterparts in exchanging information and intelligence with regard to money laundering and terrorist financing matters. In the area of securities fraud, the provisions relating to mutual assistance to foreign regulatory authorities in

---

47 The Act however does not provide for foreign investigations that are inter alia, not considered a crime under Singapore's laws or when the investigation is aimed at prosecuting someone based on his race, religion, sex or nationality.
48 Straits Times dated 23 February 2000.

the Securities and Futures Act as well as MOUs, that the MAS has entered into with regulators from major financial centres, would also facilitate the enforcement process against securities fraud.

IV. CONCLUSION - STRIKING A BALANCE

The results of the Singapore's proactive strategies to put a lid on crime have not gone unnoticed. The crime rates in Singapore have consistently been relatively low and perhaps more telling, is the negligible impact crime has had on the business environment in Singapore. Indeed, the World Global Competitiveness Report 2002-2003 ranked Singapore and Finland as the top two of 80 countries around the world, where common crime had the least impact on business cost.

We cannot pretend that solutions and countermeasures against economic crime are meant to be a panacea. There is no ultimate weapon against fraud and the war against fraud is one that has no armistice. Criminal activity of any kind usually stems from the belief that it is possible to beat the system. What we can do is to have the systems, the structures, the processes and the will and determination to protect the interests of the honest law abiding citizens or economic community, and to make it difficult for criminals who turn to crime.

In the final analysis however, policies and strategies vis-a-vis control of economic crimes recognise the need to balance enterprise and accountability - that energy against economic crimes should not be at the expense of imposing impractical burdens on commerce and industry. It is a matter of "fine tuning and striking a balance," which the Director of the CAD aptly espoused in his speech at the International Symposium on Economic Crime in Cambridge:

> "The challenges before us today are probably greater than ever before. The public perceives white collar crime to be of growing concern; consumers demand greater protection from fraudsters whilst at the same time want to maintain their privacy online; law enforcement asks for stronger legislation to fight increasingly sophisticated criminals; the international community is actively seeking mutual assistance in criminal investigations; the private sector asks not to be disadvantaged by burdensome new laws that might leave them behind in the global market place. There is a need to fine tune and strike a balance between the demands of various groups in our efforts to seek solutions to the new criminal trends and threats that we face".