APEC Working Group on Electronic Financial Transactions Systems (E-FITS)

Final Report
26 July 2002

Contents

INTRODUCTION

1. The rapid growth of the Internet in recent years has led to a proliferation of on-line financial services offered by both the public and private sectors. Financial institutions have rapidly expanded their range of banking, securities and insurance business in the on-line environment, while governments have begun to harness the Internet to deliver not just information, but also transactional services that require payments. While the electronic delivery of financial services and electronic payment and settlement of financial transactions (commonly referred to as "e-finance") to consumers, businesses and financial institutions has generally lowered the costs of business operation, it has also created new risks.

2. E-finance also changes the nature of competition for financial institutions. A borderless environment that drives transaction costs to almost nil could mean footloose customers and businesses. Cyberspace blurs physical distinctions, allowing financial institutions to root themselves anywhere yet seamlessly offer the same services on-line. Jurisdictional boundaries become harder to enforce, while new business models potentially raise new operational, strategic and systemic risks.

3. E-finance is evolving so rapidly that few regulators have put in place regulatory frameworks for e-finance in areas such as prudential restrictions on financial institutions, consumer protection, data privacy, and cross-border transactions. Most governments have responded by expanding the scope of existing laws and regulatory provisions to cover electronic transactions. In a few instances, economies have enacted laws and regulations specific to electronic transactions, though some are in draft form or are non-binding yet.

4. With endorsement from APEC Finance Ministers in September 2000, the Electronic Financial Transactions Systems (E-FITS) Working Group was established to develop and implement programmes to foster and promote the use of electronic means for conducting financial transactions within the region. The Working Group submitted an interim report to Finance Ministers in September 2001

which provided a current status of e-finance development in the APEC economies and the relevant frameworks governing the provision of such services, and identified issues for further development of e-finance in the region. The report also gave an overview of the current state-of-play of e-finance work done by other international fora.

5. The interim report highlighted several observations in the development of e-finance in the APEC region. First, policy coordination among government ministries and agencies was identified as a key prerequisite for the development of a coherent strategy to promote and deliver e-finance services. The Internet revolution challenges our traditional notions of government and increasingly requires it to operate as a networked, "joined-up" entity, rather than just as a collection of departments. Governments must begin to think "horizontally" from the perspective of their customers, instead of only "vertically" from the perspective of their agencies.

6. Secondly, governments need to maintain flexibility in their regulation and supervision of e-finance activities, and to avoid overly burdensome regulation of new activities that may stifle the development of e-finance. There is room to encourage authorities to regulate with a light touch, to depend more on market self-regulation (to the extent possible), and to eschew one-size-fits-all solutions. They may have to move from rules to guidelines, from a positive list approach that spells out what is allowed to a negative list approach that spells out only what is prohibited. Governments should also work more closely with the private sector to develop regulations that are sensitive to evolving market conditions, and which allow new technologies to flourish.

7. Thirdly, in recognition of rising consumer demands for security in e-finance transactions, particularly those of a cross-border nature, economies should engage in closer dialogue and co-operation. E-finance is transcending borders and effective regulation of this growing sector will require an international response.

8. Fourthly, by its very nature, e-finance would benefit from straight-through processing and this can be facilitated by robust and secure domestic payment and settlement systems and also cross-system and cross-border linkages to achieve

payment versus payment (PVP) and delivery versus payment (DVP) settlements to reduce settlement risks.

9. In light of these observations, the Working Group members embarked on an exercise that aims to identify sound practices, prioritise among prospective improvements, and formulate sound regulatory policies in the area of e-finance. Members saw merit in undertaking case studies to share experiences and expertise in the development of e-finance in the APEC region. Several members of the Working Group (namely Brunei Darussalam, Hong Kong, Korea, Malaysia, Singapore and Thailand) contributed case studies that addressed particular horizontal and vertical policy issues in areas such as e-government, e-banking, on-line securities trading, infrastructure and regulatory approaches. These case studies are summarised in Chapter 1 and attached to the report in Annex A.

10. E-banking has developed explosively in recent years, but the accessibility and dynamism of the Internet brings both benefits and risks. Though most types of risks inherent in e-banking are not fundamentally different from traditional banking, technology risks have become more prevalent and grown in complexity and magnitude. In the new technology-driven environment, it is critical that banks have flexible and responsive internal operating processes as well as sound and robust risk management systems. Regulators should encourage adoption of sound practices by financial institutions offering e-banking. Regulators should also allow scope for industry innovations in e-finance, but they cannot do this without regard for the soundness of the institutions, the interests of the depositors and customers, as well as the potential impact on financial sector stability.

11. In the securities industry, on-line trading has empowered individual investors with access to information and markets at reduced cost. However, the importance of investor protection and reliability of on-line trading systems should not be underestimated. Investor confidence in the security and soundness of on-line trading depends on the existence of investor protection measures to prevent manipulative or fraudulent activities and their own understanding of market risks.

12. In the area of e-payments, the Working Group emphasised the significant roles that governments could play. At the strategic level, governments should establish the national IT vision and affirm their support for the development of e-finance. More practically, governments have a catalytic role to play in the establishment of payment architectures – both public and private – that are open, robust, scalable and that can be linked across borders to reduce settlement risks. Governments could also work with the private sector to promote the connectivity between their systems so as to foster greater consumer take-up of e-finance. Finally, governments could leverage on some of its monopolistic functions – such as the collection of taxes and charges – to generate the critical mass of e-payers that are comfortable with on-line payments. This also helps private payment gateways achieve the economies of scale they otherwise could be hard pressed to achieve.

13. The growth of e-finance is making consumer protection a more important function of public policy on financial services. To gain greater understanding of the policy stance in APEC economies, the Working Group undertook a small-scale survey to identify policy issues concerning legal infrastructure governing cross-border e-finance and consumer protection. The survey found that it is a common practice by member economies to amend existing banking, securities or financial legislation to address e-finance transactions and consumer protection concerns. There is also a lack of information exchange on economies' legal infrastructure. An option may be to post major legislation on financial transaction, e-finance and e-commerce in English on the regulatory authorities' website and to encourage dialogue between regulators in the region.

14. The survey also noted the importance of consumer confidence to the promotion of e-finance and the need to establish reliable dispute resolution mechanisms for cross-border electronic financial transactions. A summary of the survey findings is found in Chapter 2 and the survey is attached in Annex B.

CHAPTER 1 VERTICAL AND HORIZONTAL CASE STUDIES

OVERALL CASE STUDY SUMMARY

15. Working Group members were invited to conduct case studies on e-finance developments in their economies. These studies contribute to a better understanding of the role of relevant legal, regulatory, and market frameworks and encourage the sharing of experiences and technical expertise among APEC economies. Two types of studies were conducted – vertical case studies that focused on a single type of business and horizontal studies that considered cross-sectoral issues.

16. Vertical case studies were prepared on the development of on-line securities trading by Korea, e-banking by Malaysia and payments system infrastructure by Brunei Darussalam and Thailand. Horizontal case studies were prepared by Hong Kong on its strategy for strengthening its financial infrastructure and by Singapore on its e-Government initiative.

17. Case studies prepared by Korea and Malaysia illustrated the significant development in the delivery of financial services to consumers. The success of on-line securities trading in Korea has been driven by several factors including advances in information technology resulting in lower trading costs, faster speed and more convenient trading platforms. This success is also a result of the marketing of these advantages by brokerage firms and of measures taken by government. Legislative changes were made to allow on-line trades to take place and capital requirements for commission brokers were significantly lowered. As a result, two-thirds of all equity trades in Korea are conducted on-line. In Malaysia, developments in information technology along with combined government and private sector initiatives have contributed to significant changes in electronic banking services. Under the Multimedia Super Corridor (MSC) initiative, two types of multi-application smart cards are being issued. The MyKad issued by the Malaysian Government contains both government and payment applications. The Government applications include national identity, driving license, health information, immigration information and

Public Key Infrastructure (PKI), and payment features such as electronic cash and the ATM application. Payment Multi-purpose Cards, on the other hand, are issued and branded by banking institutions, and incorporate payment functions of ATM and e-money.

18. Similar observations are made from case studies prepared by Brunei Darussalam and Thailand regarding their payments systems. In Brunei Darussalam, financial institutions were found to have the capacity to move to paperless payment and bill presentment systems. Utility departments and telephone companies have expressed interest in these services because of the potential cost savings. In this regard, the government has been involved in developing a supportive legal infrastructure and recognizes the need for a strategic framework to encourage paperless payment. The Bank of Thailand has upgraded its system for large value electronic funds transfers among financial institutions through the use of advanced technology and by enhancing features for system users. The enhancements in enabling straight-through processing and providing a Web interface will benefit smaller-scale members, facilitate greater interoperability among a variety of users and support cross-border initiatives.

19. Case studies prepared by Hong Kong and Singapore illustrated horizontal (cross-sectoral) aspects of e-finance. To enhance its financial infrastructure, Hong Kong introduced a comprehensive financial market reform program that included a fundamental change in the market structure, enhancement of the financial infrastructure as well as regulatory and legislative reform. With a vision to support a move towards an e-economy, the Hong Kong SAR Government has set up the Steering Committee on the Enhancement of the Financial Infrastructure (SCEFI) to study and recommend necessary improvements in financial infrastructure. The SCEFI has recommended an infrastructure that would allow local and global market participants to assess the full spectrum of financial products and services interconnected by an open, robust, secure, scalable and high performance network. This infrastructure would enable transactions to be processed electronically in a straight-through manner. Singapore designed its PSi system (Public e-Services Infrastructure) to provide a complete infrastructure for the development and delivery of electronic services for public sector agencies in recognition of the changing nature

of public services. PSi provides the necessary infrastructure and tools to help public sector agencies deal with the complexity of developing and deploying electronic services including on-line payment systems such as cash cards, credit cards and Internet direct debits.

20. These case studies show that a variety of factors have affected the development of e-finance, including legal infrastructure, advancements in information technology and efforts by governments. It is obvious that e-finance has been recognized as an important initiative for both government and the financial services sector. These case studies have exhibited some of the benefits that can be gained from efforts in e-finance development and some of the ways in which governments have participated in these efforts. Governments have been involved in a variety of efforts from legislative and regulatory changes to public-private partnerships to wide-spread market reforms. It is clear that a proactive approach by government can be instrumental in spearheading the development of e-finance and encouraging the implementation of necessary legal, physical and human infrastructure. Further efforts of individual economies may vary depending upon existing laws, practices and consumer behaviour.

INDIVIDUAL CASE STUDY SUMMARIES

21. The section presents the summaries of six individual case studies by Korea, Malaysia, Brunei Darussalam, Thailand, Hong Kong and Singapore. Full reports of the case studies are attached at Annex A.

KOREA: ON-LINE SECURITIES TRADING - DEVELOPMENTS AND TRENDS

22. Recent advances in information technology, the Internet in particular, have been revolutionizing the way of trading securities all over the world. The securities industry in Korea is at the forefront of this revolution.

23. The 0.2 million on-line accounts opened in 1998 have increased more than twenty-fold to reach 4.6 million by 2001. On-line trading volume has also increased dramatically over the last several years. According to the data from the KSDA (Korea Securities Dealers Association), on-line trading volume has increased from US$17 billion in 1998 to over US$1.6 trillion in 2001. The percentage of equity trades conducted on-line has reached to 66.6 percent of all equity trades in 2001, which is the highest level recorded in the world.

24. How could on-line trading in Korea be so active? The success of on-line trading in Korea is driven by several factors. First of all, on-line trading has advantages over the traditional trading method. Lower trading costs, faster speed, and more convenient trading platforms can make on-line trading very attractive. Second, the marketing efforts of brokerage firms accelerated the increase of trading volume. Third, the major securities market participants in Korea are individual investors. Most individual investors in Korea tend to use on-line trading. Finally, without the appropriate policies of the Korean government, on-line trading would not be possible. The Ministry of Finance and Economy allowed securities transactions through electronic communication by amending the Securities and Exchange Act in 1997. Also, capital requirement for a commission broker was reduced to 3 billion won from 10 billion won in 1999.[1] These financial market-related policies that were introduced provided a new means of securities trading in Korea. Other indirect policies were established regarding the Internet infrastructure. The Government has constantly encouraged development in information technology and infrastructure. As a result, the nation has the highest proportion of on-line trading users in the world.

25. On-line trading has significantly changed the securities market in various ways. First, traditional trading has been shrinking and the trading patterns have changed remarkably. The daily trading volume increased as trading became easier than before. Thus, the convenience of trading caused the appearance of short-term on-line day trading on the markets. Second, for the first time ever, investors can directly access financial information and tools to analyse the securities markets by themselves. In addition, investors can act quickly on the information through on-line

[1] 3 billion won is about US$ 2.3 million based on latest exchange rate.

services. The changes in the securities markets have enabled investors to participate more directly in the markets. Finally, securities firms face severe competition in providing information and services as well as setting commission rates.

26. The convenience of on-line trading, developments of information and communication technology, competitions between securities companies have fuelled the development of on-line securities trading in Korea. Currently, we can expect a continuing rise of on-line trading in the future. According to the recent survey, Korean securities firms estimate that 71~80% of total equity trades will be executed through on-line by the end of 2005. However, the increasing trends will reach a saturation point at some time.

27. Securities firms will continue to seek other business areas as well as brokerage service. They have to diversify their business to survive in a new competitive environment. Providing financial advice on-line will be the next area of focus for the brokerage industry.

28. The reduced costs and increased ease of on-line securities trading are appealing to active traders. However, we can find some negative factors linked to investors' trading behaviour. For example, as day trading became possible, investors are exposed to potential price and market distortions caused by speculative trades. Many individual investors in Korea participate in undesirable short-term trades. As securities markets are more dynamic and volatile than before, various risks caused by on-line trading occur. Therefore, the government will focus more on investor protection. First of all, the reliability of on-line trading system will be critical. When the system breaks down, a backup or an alternative system will be needed. Protection of on-line customers' personal information is also important. Secondly, in order to prevent market manipulation, monitoring and punishment to the manipulation should be strengthened. In the on-line domain, it is easier for market manipulators to conduct fraudulent activities. The role of the regulator will be important in maintaining an orderly market. Lastly, investor education should be emphasized. As on-line trading has reduced personal interaction between the securities firms and investors, professional advice and knowledge have been less available. Thus, investor education to protect investors from market risks will deserve more attention.

MALAYSIA: ELECTRONIC BANKING IN MALAYSIA

Development History and Trend

29. Developments in information technology and telecommunications have introduced a myriad of changes to the banking industry. In Malaysia, the principal effect was on counter services, which had seen new and innovative delivery channels with the advent of electronic banking.

30. Electronic banking in Malaysia had its roots in the Automated Teller Machines (ATM), which were introduced in 1981. This was followed by PC banking, and telebanking in the mid-1990s and e-money in 1998. Further developments came with the giro services and Internet banking in 2000.

Factors affecting the Development of Electronic Banking

31. Several issues have been identified as being contributory factors in the evolution to e-banking.

(a) **Regulatory** - Bank Negara Malaysia had paved the way by installing a sound and progressive regulatory framework that encompasses prudential requirements, while allowing for financial innovation by the banking institutions.

(b) **Institutional** - The banking institutions themselves have been instrumental in introducing IT driven products and services to meet the needs of an electronic market place.

(c) **Physical Infrastructure** - PC penetration is increasing rapidly with the growth of fixed line telephone services and mobile telephony, with the latter outpacing the former. Efforts are being driven by the Government to educate the public, reduce the digital divide and require the relevant service providers to increase the level of their services.

(d) **Legal Infrastructure** - the Malaysian Government had introduced a range of cyberlaws ranging from the Digital Signature Act to amendments to the Evidence Act to facilitate the introduction of electronic transactions.

(e) **Security** - A special body, Malaysian Institute of Microelectronic Systems (MIMOS), had been entrusted with addressing information security management relating to the Internet.

(f) **Social and Political** - Both the Malaysian Government and Bank Negara Malaysia had taken a proactive role in promoting electronic financial services with the Multimedia Super Corridor (MSC) initiative, the e-Government agenda and the Government and Payment Multi-purpose Cards.

Conclusion

32. Competitive pressures as well as demands from consumers will ensure that e-banking services continue to evolve into more sophisticated products and services, as well as being more widely accessible to the general consumer. Much is also being done by the authorities by way of structure and process at national and industry level to resolve impediments to e-banking.

BRUNEI DARUSSALAM: ENVIRONMENTAL SCANNING ON PAPERLESS PAYMENT[2] CHANNELS

Introduction

33. The case study examined the status of the paperless payment channels

[2] Paperless payment refers to paperless governance and information/data exchange through multimedia technologies.

taking place in Brunei Darussalam. The project implementation was led by the Ministry of Finance. In order to get information for the case study, the Financial Institutions Division, Ministry of Finance has targeted at banks to conduct the followings:

(a) surveys on the volume of transaction on payments for goods, services and financial transfers including Automated Teller Machines (ATM) transactions; and

(b) questionnaires on banks' plans to implement electronic financial services.

Analysis and Findings

Banking

34. 100% of the respondents responded to the surveys. Summary findings are as follows. The total transaction volume for the period January to December 2001 showed a seasonal trend for different types of transactions. The volume of cash withdrawals was about 75% of the cash payments at ATMs and counters. Paper credit transfers showed the highest volume, followed by automated payments and cheque payments. Credit cards purchases have increased steadily and still exceeded debit card purchases. The number of ATMs has increased from 98 ATMs in 2000 to 102 ATMs in 2001.

35. The returned questionnaires (6 out of 9) from banks showed that at present 3 banks (2 domestic and 1 foreign) have embarked on Internet banking services, however all banks showed interest in setting up such services. The market is quite small and local culture is cash-based driven with less outgoing but more incoming goods and services.

Utilities and Others

36. The utilities departments and telephone companies were interviewed and though they have not utilised Internet payments, they are certainly looking at

more ways to allow the public to make payments conveniently, especially electronically.

Location Advantage for Paperless Payment

37. The Government has emphasized on the importance of Information and Communication Technology (ICT) development in Brunei Darussalam. The Brunei Darussalam Information Technology Council (BIT Council) has been established to spearhead and provide guidance on the implementation of the National IT Strategic Plan. Through the BIT Council, the Government aims to lead and facilitate the strategic development and diffusion of state-of-the-art IT for the entire nation. The e-Government Program Executive Committee and the e-Business Program Executive Committee have been formed as affiliates of the BIT Council as part of the institutional infrastructure to assist in achieving the mission and goals of the National IT Strategic Plan for the National Drive Towards Paperless Society.

38. The two Internet Service Providers (ISPs) currently in operation are BruNet (www.brunet.bn) operated by Brunei Telecommunications Department (JTB) since September 1995 and Simpur.net (www.simpur.net.bn) operated by DataStream Technology (B) Sdn Bhd (DST) since October 2000. Brunei Darussalam's Internet subscribers have also doubled to nearly 30,000 in year 2001 compared to year 2000, which is almost 10% of the entire population of the country.

39. Legal infrastructure for promoting and supporting e-Government and e-Business in Brunei Darussalam has been given priority implementation. This includes the Trademarks Order and Copyright Act, the Computer Misuse Order, the Electronic Transactions Order 2000, the Patent Order, the amendment to the Evidence Act to accept "computer evidence", the Class License Notification and the Internet Code of Practice are introduced under the Broadcasting Act. An Order to establish and incorporate the Authority for Info-Communications Technology Industry (AiTi) of Brunei Darussalam Order, 2001 has also been gazetted in May 2001. Overall the legal framework is undergoing enhancement to create a favourable environment for electronic use and allow provision for cyber laws based on international standards

such as United Nations Conference on International Trade Law (UNCITRAL) Model Law.

40. The Brunei Global Multimedia Info-communication Network or 'RaGAM 21' for the Brunei Darussalam's info-communication superhighway, will eventually link up every major town, village, school, institution and commercial area in the country. Currently, almost every strategic area in Brunei-Muara District is linked to 'RaGAM21' network, which in turn is linked globally via satellite and the South-East Asia, Middle-East, Western Europe 3 (SEA-ME-WE3) and Brunei-Singapore submarine cable systems.

Conclusion

41. Based on these findings, it indicated that the financial institutions in Brunei Darussalam have the capacity to drive paperless payment system in the very near future.

Opportunities / Challenges

42. The availability of the paperless payment system (without or less paper) to the various sectors of society can be drivers for resources saving and also improving the overall efficiency in financial transactions in Brunei Darussalam. However, it would require management to change for it to be sustainable and implementable. There has to be a paradigm shift of everyone's attitude towards paperless payment. People are generally hard to change but with good education on the benefits of paperless payment and confidence in the system, they can adapt. With wider use of electronic means to settle payments and as society goes towards paperless, legal issues may be involved when problems arise. Legal framework needs to address the issues of concern yet allow flexibility in the implementation and operation of the paperless payment system. This may require technical measures to overcome lack of confidence for payment through Internet say, due to fear of hackers or viruses.

Critical Success Factors

43. Secure environment and public confidence in paperless payment system are critical success factors.

Strategy

44. There has to be a strategic framework on e-finance that needs to be developed in Brunei Darussalam and aligned with the national IT framework, i.e. to encourage paperless payment in Brunei Darussalam, in line with the core strategies of the National IT Strategic Plan, *"IT 2000 and Beyond"* i.e. paperless society, e-government and e-business.

THAILAND: THE BAHTNET INITIATIVE

45. The vertical study on the BAHTNET system of Thailand covers one of the highly developed financial infrastructures of the country. Since 24 May 1995, the Bank of Thailand (BOT) developed the BAHTNET (Bank of Thailand Automated High-value Transfer Network) System for electronic funds transfers among financial institutions in Thailand. Due to the changing business requirement of the market and the technology advancement as well as, the BOT's policy, the BOT has upgraded the existing BAHTNET system by enhancing the facility for the settlement of Thai government securities in a delivery versus payment (DVP) manner since 11 December 2001.

46. Additionally, the new system incorporates the dual technology, which include S.W.I.F.T. and Web interface for sending and receiving messages between BAHTNET members and the BOT. As a main interface, the use of S.W.I.F.T. interface would enable straight-through processing (STP) and be consistent with international practice. Meanwhile, the Web-based technology would be an effective channel in handling interactive inquiries and message transmission for smaller-scale members. Hence, the development of the BAHTNET system would increase scope of

the services as well as the efficiency and safety in the payment system, and should prove invaluable in the development of the money and capital markets.

47. Factors affecting the development of the BAHTNET system are identified. Major financial institutions are key drivers behind the use of S.W.I.F.T. gateway, which would allow their internal systems to be compatible with the BAHTNET system and be able to perform STP. From a legal perspective, many laws are under development aiming to promote efficiency by encouraging use of electronic payments. Additionally the technology deployed in the previous BAHTNET system became obsolete and limited its services to a closed system. Hence, the upgrade of the BAHTNET system is required by using advanced technology to develop a secure and efficient infrastructure. The other environmental issues, such as social, economic, and global, are also included.

48. With the objectives of promoting efficiency and minimizing risks in payment systems by developing an RTGS infrastructure, key achievements have been reached. The BAHTNET system helps substitute the use of cheque, which is deemed to be a costly and higher-risk mean of payment. The development of a DVP system supports the same-day settlement of securities transactions. Hence, it reduces the settlement risk and minimizes the use of manual procedure. Several mechanisms, including intraday liquidity facility, gridlock resolution, and queue management, have been introduced to facilitate members in managing their liquidity needs. Additionally, the development of the BAHTNET system is consistent with BIS Core Principles for Systemically Important Payment Systems and international practice as well as supporting future cross-border linkages with other payment systems.

49. With limited timeframe of development period and the cutover in a big bang scenario, as well as, the varying natures of participants, the BOT confronted challenging tasks in preparing all members to be ready for the cutover of the upgraded BAHTNET system. Nevertheless, the migration of upgraded BAHTNET system was implemented with satisfactory result. The success was owing to close co-operation between the BOT and all related parties and effective project management, which drove the teams towards the same goals in compliance with the scheduled plan.

50. The future plans of the further development of the payment infrastructure need to be considered. First, the BOT would continue to support potential cross-border linkage, which would allow a reduction in the settlement risk for payment versus payment of foreign exchange transactions and delivery versus payment of securities settlement. Second, the BAHTNET system will be continuously developed in order to respond to the rapid changes of business needs and advanced technology. Third, the BOT has been currently revising the provision of the intraday liquidity facilities to ensure the fair market value of the deposited securities and the consistent calculation methods across the liquidity window provided by the BOT. Finally, the BOT is considering an ideal infrastructure, which would provide the same window for trading and settlement for both government sector and private sector securities.

HONG KONG: THE FINANCIAL INFRASTRUCTURE IN HONG KONG

51. This study on the financial infrastructure of Hong Kong covers one of the Hong Kong SAR Government's key initiatives in its financial market reform.

Environmental Analysis on the change drivers

52. The environmental analysis on the Hong Kong financial markets identified two key change drivers, namely the advent of information technology and the globalisation of financial markets.

53. The advent of information technology has stimulated productivity growth and lowered transaction and operational cost for financial service providers, which give rise to the emergence of e-commerce and e-trading. The exponential growth of e-commerce and e-trading has however resulted in fundamental and irreversible changes in business models of the financial markets. The marketplace is no longer bounded by national geography and traditional franchises are under threat. New market players and new sets of customers emerged in the explosive information age. The rapid growth in e-commerce has also created a new group of powerful, low

cost and competitive intermediaries, like the Electronic Communications Networks in the securities market and similar on-line networks in the derivatives market.

54. In the light of these market developments, exchanges and clearinghouses in various financial centres, including Amsterdam, Frankfurt, Singapore and Sydney, have transformed themselves into customer-centric and market-driven commercial entities. Strategic alliances among the exchanges and clearinghouses were established to facilitate cross-market products development and to achieve economies of scale on their technology investments.

Strengths and Weaknesses of Hong Kong's Financial Infrastructure

55. In the past ten years, electronic trading and clearing systems in both securities and banking industries have been introduced in Hong Kong, including the securities settlement systems (Central Moneymarkets Unit for bonds and Central Clearing and Settlement System for equities), electronic trading systems (Automated Order Matching and Execution System for securities and Hong Kong Automated Trading System for futures) and electronic payment systems (Hong Kong dollar and US dollar RTGS).

56. However, the lack of connectivity and common standards among these systems and others within the economy impedes the development of the straight-through processing (STP), which is believed to enhance the processing efficiency for the whole value chain in the securities and futures transactions and reduce the operational cost.

Market Reform Program

57. On 3 March 1999, the Financial Secretary of the Hong Kong SAR Government announced in his budget speech a comprehensive financial market reform program to strengthen Hong Kong's competitiveness and to sustain Hong Kong as an international financial centre. The reform program consists of three major components:

(a) Fundamental change in the market structure accomplished through the demutualisation and merger of the exchanges and clearinghouses;

(b) Enhancement of the financial infrastructure to improve risk management, increase efficiency and reduce cost; and

(c) Regulatory and legislative reform to improve the supervisory framework and protection of market participants.

The study and recommendations of the Steering Committee on the Enhancement of the Financial Infrastructure (SCEFI)

58. To proceed with the reform program, the Financial Secretary appointed the SCFEI to study and recommend necessary improvements in Hong Kong's financial infrastructure. Four major recommendations were put forward in the study:

(a) Setting up a single clearing arrangement for securities, stock options, futures and other exchange-traded transactions in order to achieve liquidity and risk management excellence. The single clearing arrangement will improve risk management for market participants, exchanges, clearinghouses and regulatory authorities and money settlement efficiency. It also enables cross-margining and cross-collateralisation such that liquidity can be pooled and asset utilization can be improved.

(b) Enhancing the financial technology infrastructure to facilitate STP. A robust financial infrastructure that links the exchanges and clearinghouses together using industry-standard computer protocols and message standards improves the connectivity and interoperability of various systems.

(c) Moving towards a scripless securities market. A scripless securities market provides the enabling environment for STP. As a first step towards a scripless market, Hong Kong introduced the Electronic Transactions Ordinance in early 2000 to provide legal standing and protection to electronic documents, records and signatures.

(d) Building a robust technology infrastructure. To remove the entrance barrier and attract more people to involve in the financial markets, a financial infrastructure anchored on technologies and architectures that are open, robust, scalable and supportive of continuous innovation is needed. It is intended to integrate various systems/networks into a hub by utilizing a single technology platform called FinNet (Financial Network).

Conclusion

59. To enhance the financial infrastructure of Hong Kong, changes in the current business practices, legal and regulatory framework and relationships among various stakeholders are required. The Hong Kong SAR Government plays an important role in driving the project with a vision to establish an financial infrastructure that allows local and global market participants to access, via a single window, the full spectrum of financial products and services on an open, robust, secure, scalable and high performance network.

SINGAPORE: E-GOVERNMENT - THE PUBLIC E-SERVICE INFRASTRUCTURE (PSi) AND E-PAYMENT CAPABILITIES

60. This study examines the Singapore Government's Public e-Services Infrastructure, with a specific emphasis on its e-payment capabilities.

Challenge of E-Government

61. The Singapore Government recognises that the nature of public services needs to be fundamentally different in the digital era. The challenges for governments are to harness infocomm technology (ICT) to offer e-services that are convenient[3] to the users, leverage on web portals to reduce governments' complexities

[3] 24/7 availability, fast delivery, customer focus and personalisation

and organise services according to the needs of the users, and reduce cost by using ICT to improve internal processes and service delivery.

The Public E-Services Infrastructure (PSi)

62. The Singapore Government's PSi was conceived to help public sector agencies deal with the complexity of developing and deploying e-services, especially cross-agency ones. As a public-sector wide project, PSi is able to reap economies of scale, reduce the costs of implementing e-services and offer a simplified development and delivery environment in which government agencies are able to delegate many issues to the safe hands of PSi. These issues include security, reliability, speed and ease of deployment, scalability and upgrading.

63. PSi is an enterprise level amalgam of hardware and software designed to deliver a complete infrastructure for the development and delivery of e-services. The design of PSi consists of (i) the *e-Service Generator* as a complete design environment (ii) *EDX (Electronic Data Exchange*) which integrates e-services hosted on PSi with back office/legacy data systems (iii) *Authentication & Authorization* which enables PSi to differentiate users and grant different access levels (iv) the *System Management Console* which provides backend management facilities (v) the *Intermediate Zone* which provides a means to host databases on PSi, enabling e-services to access and update data in an efficient manner (vi) the *Payment Module* which enables e-services to effect on-line payment transactions in a secure and reliable manner.

E-Payment Services on Psi

64. The payment options available for e-services are often critical in determining how mature[4] and useful that service is to its customers. This usually requires the availability of convenient and low-cost on-line payment mechanisms that allow customers to complete their transactions on-line.

[4] There are generally 3 levels of e-service maturity (i) Publish (users can only obtain information, i.e. a one way process) (ii) Interact (users can undertake a part of the transaction electronically, ie there is some interaction but the service is not completed on-line) (iii) Transact (users can complete the entire transaction electronically)

65. PSi offers the latest payment methods as a *common service* to the e-services hosted on it. The e-Payment module features a number of key capabilities: it shields technical complexities from designers of e-services, provides a reliable and secure environment, provides appropriate reports for service/product fulfilment, reconciliation and dispute settlement, allows PSi to link with various e-payment service providers while maintaining payer's confidentiality, allows future payment mechanisms to be added without disruption to existing services, and aggregates payment requirements from all its e-services, and so allows users to benefit from lower transaction costs.

66. Currently, PSi has the following methods available for electronic payment:

(a) NETSCash - Utilising the cash card (smart card encoded with cash value) with a cash card reader, users are able to fulfil payment instantly on-line.

(b) Credit Card Payments - Payments using major credit cards, such as Visa and MasterCard are supported on PSi, with the Development Bank of Singapore (DBS) being the processing bank for the credit card transactions effected.

(c) Internet Direct Debit - Making payment with an Internet banking account is possible on PSi. Currently, anyone with an Internet banking account with DBS is able to perform a direct debit payment transaction with e-services on PSi. This mechanism will be made available to the Internet banking account holders of other banks when they are ready to offer such services.

Current Challenges

67. The existing set of payment options on PSi is by no means complete. For example, the NETSCash option requires a smart card reader and is limited by the maximum stored value of cash cards of S$500; the credit card option is relatively expensive and less secure; and the Internet direct debit option is currently limited to the customers of one bank only.

68. The challenges that PSi faces with respect to e-payment include enabling multi-bank payments, introducing GIRO-on-Demand[5] to reach out to a much wider target audience than only those with Internet bank accounts and launching a Virtual Wallet which removes the need for a card reader. Besides introducing more e-payment options on PSi, the Singapore Government has also embarked on a project to present consolidated government bills to members of the public and to collect consolidated payments on-line. When rolled out, PayPoint will offer the public a single point of access to various government fees, charges and fines.

Conclusion

69. PSi provides the necessary infrastructure and tools that enable the rapid deployment of e-services without the need for the service owner to handle complex issues such as system availability, security, reliability, connectivity and scalability. It provides a suite of common services widely used by most e-services, enabling the Government to reap the benefits of increased efficiency and scale. With highly developed payment capabilities, PSi also enables on-line payment for all e-services requiring such capabilities in an efficient and cost-effective way.

[5] An electronic Internet payment mode which enables users to issue payment instructions on-line with settlement via a credit transfer system between bank accounts

CHAPTER 2 SMALL-SCALE SURVEY: ISSUES ON CONSUMER PROTECTION IN CROSS-BORDER E-FINANCE

Introduction

70. Through the development of information technology and deregulation in the recent years, opportunities for consumers in APEC economies to engage in cross-border financial transactions have increased in general. In particular, the popularity of the Internet since the 90s has had significant impacts on cross-border communication, contributing to expansion of channels for consumer access to financial services.

71. An important benefit of e-finance for consumers is that they can directly access financial institutions in foreign jurisdiction. However, this may also increase the possibility for consumers to be exposed to cross-border disputes. Consumers' concerns about safety and security as well as prudential or regulatory restrictions, tend to be the major impediments to cross-border e-finance.

72. As there has been little systematic research on consumer protection issues arising from cross-border e-finance in the APEC region, a small-scale survey covering fifteen APEC economies has been conducted[6] on

(a) Laws and regulations concerning consumer protection in e-finance,
(b) Laws and regulations concerning cross-border transactions, and
(c) Dispute resolution systems for cross-border e-finance.

[6] The conduct of this survey was approved at the fourth meeting of APEC Working Group on Electronic Financial Transactions Systems (E-FITS) held in Brunei Darussalam in October 2001. The fifteen economies selected for the survey were Australia, Brunei Darussalam, Canada, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Singapore, Chinese Taipei, Thailand, and the USA, which are mainly participants of the WG on E-FITS. While the actual research activities in each economy were conducted by the Australian National University (ANU), Canberra, Australia in consultation with the Japanese Government, the summary and interpretation of the research are the WG's and not the ANU's. The results of the surveys of individual economies are attached at Annex B.

Laws and regulations concerning consumer protection in e-finance

73. Most members have trade practices legislation governing improper behaviour and usually providing a certain degree of consumer protection. Most members also have general consumer protection legislation that is "technology neutral", which accordingly covers Internet transactions, but not specifically designed for e-commerce. For example, Japan and Chinese Taipei treat Internet transactions as comparable to mail order sales which are already covered by their consumer protection laws. Many members (Australia, Brunei Darussalam, Canada, Hong Kong, Japan, Korea, New Zealand, Singapore, Chinese Taipei, Thailand and the USA) have additional consumer protection regulations or guidelines specific to e-commerce, although some of them are still in draft form or are not legally binding[7]. Australia, Brunei Darussalam, Canada, China, Hong Kong, Malaysia and Singapore already have explicit cybercrime laws prohibiting hacking, denial of service attacks, etc, while Indonesia and Thailand have them still in draft form.

74. The result of the small-scale survey shows a certain level of common ground in the legislation on e-commerce in the region. A majority of members has established basic legislation which defines the nature of electronic contracts and clarifies the conditions under which an electronic contract and/or electronic signature will be given legal status. Australia, Brunei Darussalam, Canada, Hong Kong, Japan, Korea, Mexico, New Zealand, Singapore, Chinese Taipei and the USA all have similar law generally based on the United Nations Commissions of International Trade Law Model Law on Electronic Commerce (UNCITRAL model law), which also covers the area of consumer protection. On the other hand, China developed legislation that is not related to the UNCITRAL model law whereas Indonesia and Thailand still have draft laws under discussion. Malaysia also amended its existing commercial legislation to provide legal recognition to electronic documents along

[7] Privacy protection might be another important aspect of consumer protection. There is a distinction between members using a more restrictive approach giving stronger protection for individuals, and those that use a less restrictive approach that emphasises freedom of information but gives less protection to individuals. Eight members (Australia, Canada, Hong Kong, Korea, Malaysia, Mexico, New Zealand and Chinese Taipei) have privacy laws or are considering having them. Seven members (Brunei Darussalam, China, Indonesia, Japan, Singapore, Thailand and the USA) do not have explicit privacy laws. Most members that have privacy laws follow the ten privacy principles in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

with the Digital Signatures Act, rather than developing separate legislation for e-commerce. It appears therefore that there is a reasonable degree of consistency across the region with regard to basic legislation on e-commerce including consumer protection.

75. In comparison, the result of the survey shows that there are few economies in the region with legislation specifically covering e-finance. Thus, e-finance rules reflect the diversity in financial laws and regulations among the member economies. The majority of members (Australia, Canada, Hong Kong, Indonesia, Japan, Malaysia, Mexico, New Zealand, Singapore, Chinese Taipei and the USA) have amended existing banking, securities or other financial laws to be "technology neutral" so that financial transactions will be treated alike regardless of the transaction medium. In addition, Hong Kong, Malaysia, Singapore and Chinese Taipei have additional codes of practice or guidelines specifically for e-finance or Internet banking. Korea is developing separate legislation for e-finance focused on e-banking and e-payment, to set up separate inspection and supervision systems for e-finance, while Thailand is now drafting Royal Decree under the Electronic Transaction Law.

Laws and regulations concerning cross-border transactions

76. Most APEC members maintain broadly open regimes in regard to cross-border financial transactions except for a few economies including ones which temporarily imposed restrictions on capital movements after the Asian financial crisis. Members vary greatly in the extent they allow foreign financial institutions to provide services to their residents. Some economies such as China and Indonesia restrict non-residents from owning or trading shares listed on the local stock exchanges. These restrictions also apply to cross-border transactions carried out by electronic means.

77. It also appears that some e-finance transactions such as on-line bill payments from bank accounts can only be possible within an economy but rarely possible across borders in practice. Also, some types of cross-border transactions such as wire and mail funds transfers to overseas bank accounts are possible by conventional means but usually not by electronic means. In most economies, it is not clear whether there are regulations impeding such transactions or financial institutions

choose not to offer such e-finance services due to security or other considerations. Mexico is the only economy which has regulations barring cross-border electronic transactions by consumers from individual accounts.

78. The survey also shows that many economies (China, Japan, Malaysia, Mexico, Singapore, Chinese Taipei, Thailand and the USA) maintain special restrictions against certain activities by non-resident financial institutions such as solicitation of businesses and acceptance of deposits from domestic residents. Some economies explicitly prohibit the establishment of Internet-only banks. Such restrictions could have negative impact on the development of cross-border e-finance.

Dispute resolution systems in cross-border e-finance

79. In several economies, consumer protection policy planning and enforcement are vested in one agency, while others have such roles shared among various government bodies or agencies. In some economies such as Hong Kong, Korea, New Zealand, Chinese Taipei and Thailand, an independent agency responsible for consumer protection in general commerce also handles consumer protection issues in e-finance.

80. The enforcement powers against breaches of consumer protection law vary among agencies, ranging from administrative "cease and desist" orders to reliance on court judgements. In some economies there is a combination of administrative enforcement, "name and shame" actions and civil proceedings. There are economies like Korea and the USA with Internet-specific enforcement system. The US Office of Internet Enforcement (OIE) was formed in 1998 as a part of the Securities and Exchange Commission to identify areas of surveillance, formulate investigative procedures, provide enforcement guidance nation-wide, and conduct Internet investigations and prosecution in order to combat on-line fraud. In Korea, the Ministry of Finance and Economy introduced regulation to protect consumers engaged in electronic transactions by enabling the authorities to issue orders to cancel improper contracts and refund money against exaggerated advertisement.

81. Whether the domestic consumer protection scheme applies to cross-border transactions varies among economies. Some economies (including Australia, Hong Kong, Japan, Korea, Singapore (limited application), Thailand and the USA) apply their consumer protection laws to foreign providers. Of these economies, Australia, Japan, Korea and the USA also apply their consumer protection scheme to foreign consumers to a limited degree, for instance, on-line consumer complaints desk is established but no action by the authorities was guaranteed.

82. In practice, differences in the enforcement systems among APEC economies may create loopholes in resolving cross-border disputes. The small-scale survey shows an example of "cold call" (sales practice of approaching potential customers without any prior introduction) case using web site/email; a market regulator in Country X received criminal complaints from authorities in Country Y and other countries. The authority in Country Y worked closely with the market regulator and other regulators in Country X, because a large number of consumers in Country Y had been cold called by sales people in the South East Asia and ended up purchasing fake securities in Country X. While international collaboration among enforcement agencies has successfully prosecuted the case, no authority was able to recover money on behalf of investors. This suggests that international collaboration could be improved to facilitate more satisfactory resolution of cross-border disputes.

CHAPTER 3 CONCLUSION AND RECOMMENDATIONS

(3A) REGULATORY ISSUES

83. As discussed in the Interim Report, recent years have seen rapid technological advances, which have brought fundamental changes to the way financial services, both banking and securities trading, are produced, distributed and consumed. E-banking has resulted in greater efficiency and reduced transaction costs to the consumers. Similarly, in the arena of on-line securities trading, the Internet allows significant cost savings for market participants and unparalleled opportunities for enabling consumers to be well informed and undertake transactions on an immediate basis. It has facilitated a financial landscape for both e-banking and on-line securities trading that is no longer bounded by natural borders and geography. Further, transactions utilising electronic modes of payment provide a better audit trail than corresponding transactions involving physical cash. However, despite its ready acceptance by IT savvy consumers, issues relating to security of the Internet and reliability of the electronic environment continue to remain as areas of concern to regulators and consumers alike.

84. The reality of e-commerce as the new market place poses serious challenges to regulators and the existing regulatory framework as the nature of services tends to be fundamentally different. Looking ahead, the financial institutions can be expected to offer more enhanced services such as account aggregation, direct debits and credits, bill presentment and other sophisticated services through multiple delivery channels e.g. mobile phone and TVs. Although the present legacy systems may not in some cases be adequately equipped or appropriate to support a wide range of e-commerce transactions, the traditional regulatory and legal framework may still be applied to ensure continued stability in the financial system. It should be noted, however, that no regulator can promise complete absence of system failures or has the capacity to totally eliminate fraud. However, the regulator can undertake a series of measures to reduce the likelihood of failure. Accordingly, to support the orderly development of e-banking and on-line securities trading, it is necessary for policies to

be adjusted, and the regulatory and legal framework revised, to ensure that the right institutional and structural environment is created to nurture its growth. The role of the authorities concerned would, therefore, be to plan and develop suitable regulatory policies with a view to promoting financial stability and a sound financial infrastructure, whilst supporting the continued growth of e-finance activities.

85. After taking into consideration case studies and feedback on e-banking and on-line securities trading from Working Group economies, we would like to propose several regulatory philosophies and approaches to be undertaken by APEC economies to provide a conducive environment for the development of e-banking and on-line securities trading. These are all the more critical given that financial institutions have already tapped their supply of early adopters.

E-BANKING

Recommendation 1: Deployment of Sound Practices

86. Sound practices for financial institutions offering e-banking should be developed and deployed. These may encompass technology, security, internal audit procedures, customer service, consumer protection, problem resolution, business continuity planning and communications. In addition, the sound practices promulgated by the BIS in "Risk Management Principles for E-Banking" should be carefully scrutinised.

Recommendation 2 : Risk Management

87. The management of financial institutions should be required to implement a sound system of internal controls, policies and procedures for managing material risks. Measures should also be in place to ensure that e-banking systems are operated in a safe and sound manner, including the availability of contingency and business resumption plans. Technology solutions, key business principles and strong management commitment play a critical role in establishing a rigorous framework for sound risk management and security practices.

Recommendation 3: Consumer Protection

88. Consumers need to be protected against potential unfair practices by financial institutions. They should enjoy an equivalent level of protection whatever the medium of commerce. Therefore, it is advisable for financial institutions to implement proper and effective policies, procedures and controls to effectively protect customer information and ensure its integrity, availability and confidentiality. It would also be advisable for sound practices to cover effective consumer protection in the on-line environment, such as full and fair disclosure of essential information, advertising, complaint handling, dispute resolution and legal redress, in an effort to help build consumer confidence in electronic commerce and assist implementation of on-line consumer protection without erecting barriers to trade. In addition, financial institutions should initiate a pro-active approach to educate consumers about their rights and responsibilities and how to protect their own privacy on the Internet, as technology is the source of many concerns involving personal privacy.

Recommendation 4: Regulatory Frame work

89. The regulatory authorities should establish a comprehensive regulatory framework for e-banking. Appropriate regulations, policies and practices should be introduced at an early stage to regulate e-banking to maintain safety and public confidence, while respecting competition and innovation. The regulatory framework has to balance the trade-off between efficiency and financial system stability. It is advisable for regulators to move from the traditional "regulator knows best" approach to a "supervision based on market discipline" approach. This would facilitate a move away from micromanagement.

Recommendation 5: Entry requirements

90. The regulatory authorities should establish clear and transparent criteria on entry requirements for both existing financial institutions and new entrants to e-banking. The criteria may need to reflect the current and projected penetration of e-finance products in the local market.

Recommendation 6: Common Standards and Specifications

91. To facilitate cross-border transactions, common standards and specifications should be adopted to ensure compatibility or interoperability of systems. Common standards would also facilitate system enhancements, generate cost savings as well as establishment of a firm platform for future innovation.

ON-LINE SECURITIES TRADING

Recommendation 1: Legal framework

92. The legal framework should facilitate the development of on-line securities trading. Appropriate measures should be taken to ensure that the legal framework is facilitative, technology friendly and neutral, whilst not compromising the basic tenets of securities regulation.

Recommendation 2: Secure and Reliable System

93. The technological reliability of on-line trading systems is critical. When a system breaks down, a backup or an alternative system needs to be in place. In addition, protection of customers' account and trading information is also important.

Recommendation 3: Investor Protection

94. In the on-line domain, it is easier for unscrupulous players to conduct manipulative fraudulent activities, leading to potential price and market distortions. There should be appropriately strengthened monitoring and enforcement to mitigate the risks of market manipulation.

Recommendation 4: Investor Education

95. As on-line trading has reduced personal interaction between the securities firms and investors, investor education to alert investors to market risks deserves more attention.

(3B) PAYMENT ISSUES

96. As noted in our Interim Report, payment and settlement systems constitute an important link in the value chain of e-finance, and if underdeveloped could even become a bottleneck in the processing of e-finance transactions. However, APEC economies are in somewhat diverse stages of development in IT infrastructure supporting payment and settlement systems. Such infrastructure would need to be kept updated with technological advances to enhance system functionality and promote compatibility. As many APEC economies have rather small domestic markets, it would be sensible to achieve economies of scale through cross-border co-operation and linkages to create a larger, regional market.

97. Most APEC economies have already introduced certain models of real-time gross settlement (RTGS) systems for settlement of payments in domestic currencies. Many of such RTGS systems also have DVP (delivery versus payment) capability for the settlement of securities (often debt securities) transactions, often as an adjunct to the RTGS system to provide intraday or overnight liquidity via repurchase agreement. However, there is generally a lack of ability to settle foreign currency transactions simultaneously on a PVP (payment versus payment) basis in order to reduce the settlement risk. Such DVP and PVP linkages would be important elements that could help promote the development of regional financial markets, and e-finance in particular because the potential benefits of cross-border securities or payments transactions will be diminished if such transactions executed via electronic means cannot be cleared and settled seamlessly and instantaneously. It is recognised

that while PVP settlement has so far been implemented only in one jurisdiction, there is room for wider application of PVP linkages among the regional members of APEC.

98. Through innovative system designs and adoption of latest information technology, payment system infrastructure can be developed to provide fast, convenient, low-cost, direct, user-friendly and secure services to their users in both domestic and cross-border context. Having considered the contributions from the WG economies through surveys and case studies, we would suggest the following recommendations regarding payment infrastructure that APEC economies could consider in further developing e-finance.

Recommendation 1: IT Infrastructure for payment systems

99. Unwavering government vision and affirmative support for well-established IT infrastructure to be put in place to foster the development of e-finance.

100. To facilitate efficient processing throughout the value-chain of e-finance, transactions should best be conducted on seamless networks anchored on technology architectures and infrastructure that are open, robust, scalable and supportive of continual improvement and innovation. Depending on the stage of economic and market development, the aim should be to introduce RTGS system, DVP and PVP linkages. Government should consider e-payment as an essential element in formulating e-agenda or establishing national IT strategic plans. Besides encouraging competition through market liberalisation, co-ordination in public and private sector resources to facilitate the development of e-payment systems is required.

Recommendation 2: Legal Framework

101. A secure and reliable e-payment environment should be safeguarded by relevant legislation.

102. E-payment should be conducted in a legally robust environment such that payments could be effected in a safe and secure environment. The question of finality of settlement of payments or securities (equities or debt securities) would also need to be addressed, if necessary through explicit legislation providing for the finality. Participants in different e-payment systems should be well informed of the rules, rights, obligations and procedures of the system such that they are well aware of their credit and liquidity exposure in the process of settlement. Apart from domestic transactions, legal risks arising from cross-border settlements involving other jurisdictions should also be dealt with.

Recommendation 3: Scope of Payment Infrastructure

103. Payment infrastructure for both high-value payments and retail payments should be developed in such a way to facilitate e-payments.

104. It appears that most government efforts in developing payment infrastructure are focussed on wholesale or high-value payments. This may be appropriate for B2B or B2G transactions, but for B2C and C2C transactions, that would entail the development of infrastructure catering for retail level transactions. The use of open platform technology and standardised computer protocols could facilitate straight-through processing from various front-end e-trading platforms (covering physical or financial assets) to different back-end settlement systems. Such high-value payment systems and respective linkages/interfaces should be robust and tamper-resistant with reliable encryption algorithms and intrusion detection tools.

105. At retail level, various payment mechanisms or systems should be made suitably safe, secure and user-friendly. While there may be no lack of private sector initiatives on retail payment systems, some of them might operate with little supervision, particularly those operated by non-regulated institutions. An appropriate degree of public sector oversight should be in place in order to protect the interest of the general public. Also, some proprietary systems, e.g. e-banking offered by banks, lack connectivity and could benefit from a more open approach to encourage connectivity to promote electronic transactions across banks or payment systems.

Recommendation 4: Government Initiatives

106. Proactive government policies in encouraging e-payment should be developed to improve the popularity of e-finance.

107. Government initiatives in promoting electronic payments for tax and government charges could enhance the popularity of e- payments. This could help to generate the critical mass of e-payers, who would then feel more comfortable in making on-line electronic payments to commercial entities. Private payment gateways could thus achieve economies of scale on their technology investments with the widened on-line customer base. It would be even more efficient if a common payment platform could be used for both public and private sector transactions.

Recommendation 5: Cross-border Transactions

108. The interoperability between systems and development of common standards for data format should be promoted to facilitate efficient cross-border payments and linkages.

109. Interoperability and interconnectivity between payment systems locally or overseas are becoming indispensable to the development of payment infrastructure. In the process of integration, close co-ordination between various government bodies and private sectors is required in streamlining the legislative and regulatory obstacles, setting standards and harmonising tax practices to ensure the effectiveness of cross-border payments.

110. Establishment of regional or international electronic payment standards could improve cross-border payment and settlement efficiency. Apart from enhancing system connectivity, efforts from APEC economies in initiating common standards could save investment cost in building up cross-border payment systems and induce interest of private sectors to develop new products, services and interfaces for payment systems.

Recommendation 6: Education and Consumer Protection

111. Educational and training programs to the general public should be enhanced to improve their understanding and acceptance of electronic transactions, hence strengthening the awareness of consumer protection.

112. Relevant educational programs could help to overcome the social barrier, reduce the digital divide in the society, and enhance the awareness of consumer protection. In particular, public understanding of the availability of e-commerce assurance, certificate authorisation and technology audit services could increase their confidence and demand for using electronic transactions.

(3C) CONSUMER PROTECTION IN CROSS-BORDER E-FINANCE

113. E-finance has been expected to lead to the rapid penetration of financial service transactions beyond national borders. However, this expectation has not been fully materialized so far. The overriding factor influencing e-finance seems to have been clients' concern about safety and security, which applies even stronger to cross-border services. Other frequently cited obstacles are the differences among national regulatory systems and regulatory approach. Furthermore it may be highly possible that consumers would be involved in cross-border disputes over financial services provided by overseas financial institutions.

114. Based on the contributions from the member economies through the small-scale survey, in addition to the propositions in the previous parts, we would like to suggest the following four points as recommendations.

Recommendation 1: Improvement of Regulatory Environment

115. To enhance consumer protection, it is recommended that further improvement of the regulatory environment for e-finance be pursued.

116. The majority of member economies uses existing banking, securities or financial legislation to cover e-finance transactions including consumer protection issues. However, it should also be noted that legislation has always lagged behind the development of e-finance and there is considerable variation in the level of readiness to deal with consumer protection issues across the region.

Recommendation 2: Information Exchange

117. Further exchange of information on legal framework of each economy should be recommended.

118. A lack of awareness and knowledge of laws and regulations in each economy itself may be a barrier to cross-border transactions. It might be particularly pertinent for financial sectors that changes in laws and regulations in each economy are rarely announced abroad. Therefore consumers, and even overseas regulators, may find it difficult to keep up with the details of such changes. To enhance efficiency in the exchange of information on financial laws and regulations, it is recommended that major legislation on electronic transactions, e-finance, and e-commerce be posted in English on the authorities' websites, and dialogue be encouraged between regulators in the region.

Recommendation 3: Trust Mark Systems

119. Development of internationally recognized trust mark systems should be recommended.

120. Along with the increase of e-finance transactions, the need to ensure consumer confidence has also become greater. The recent developments in the systems of identifying reliable on-line traders and service providers show that consumers find them helpful and almost essential in e-commerce. One such mechanism is a "trust mark" system, helping consumers to identify reliable on-line business enterprises by means of a certain mark posted on the website of those enterprises that follow an agreed code of practices. Developing such trust mark

systems that are internationally recognized would contribute to building more consumer confidence in cross-border transactions.

Recommendation 4: Dispute Resolution Mechanisms

121. Establishment of reliable dispute resolution mechanisms for cross-border e-finance should be recommended.

122. The result of the small-scale survey reveals that the dispute resolution system varies among economies and in particular lacks cross-border effectiveness. It is important to ensure that all on-line consumers have easy access to dispute resolution systems for small-value disputes at a low cost, in particular for e-finance transactions. Further studies for making dispute resolution mechanisms effective for non-resident consumers are recommended.

KOREA: ON-LINE SECURITIES TRADING - DEVELOPMENTS AND TRENDS[1]

I. Introduction

1. Recent advances in information technology, the Internet in particular, have been revolutionizing the way of trading securities all over the world. The securities industry in Korea is at the forefront of this revolution.

2. In this paper, we provide a description of on-line securities trading in Korea. We also describe changes in the securities industry and trading behavior that take place when investors go on-line. The 0.2 million on-line accounts opened in 1998 have increased more than twenty-fold to reach 4.6 million by 2001. On-line trading volume has also increased dramatically over the last several years. According to the data from the KSDA (Korea Securities Dealers Association), on-line trading volume has increased from US$17 billion in 1998 to over US$1.6 trillion US$ in 2001. The percentage of equity trades conducted on-line has reached to 66.6 percent of all equity trades in 2001, which is the highest level recorded in the world.

3. On-line trading has significantly changed the securities market. One of the biggest changes is individual investors' relationship with brokerage firms. For the first time ever, investors can directly access financial information and tools to analyse the securities markets by themselves. In addition, investors can act quickly on the information through on-line services. The changes in the securities markets have enabled investors to participate more directly in the markets.

4. The success of on-line trading in Korea is driven by several factors. First of all, on-line trading has advantages over the traditional trading system. Lower trading costs, faster speed, and increased convenience have made on-line trading attractive. Second, the marketing efforts of brokerage firms accelerated the increase of trading volume. Third, without the appropriate policies of the Korean government, on-line trading would not be possible. The Ministry of Finance and Economy allowed securities transactions through electronic communication and other manners by amending the Securities and Exchange Act in 1997. Also, capital requirement for a commission broker was reduced to 3 billion won from 10 billion won in 1999.[2] At the same time, the Financial Supervisory Commission established detailed requirement conditions for obtaining a license of a securities company. These financial market-related policies that were introduced provided a new means of securities trading in Korea. Other indirect policies were established regarding the Internet infrastructure. The government has constantly encouraged development in information technology and infrastructure. As a result, the nation has the highest proportion of on-line trading users in the world.

5. The trading volume, the number of on-line accounts, and the proportion of on-line trading have grown dramatically. The reduced costs and increased ease of on-line securities trading are appealing to active traders. However, we can find some negative factors linked to investors' trading behavior. For example, as day trading became

[1] prepared by Jinho Byun, Research Fellow, Korea Securities Research Institute
[2] 3 billion won is about US$ 2.3 million based on latest exchange rate

possible, investors are exposed to potential price and market distortions caused by speculative trades. Many individual investors in Korea participate in undesirable short-term trades. Thus, investor protection, including investor education by the government or self-regulatory organizations (SROs), should be emphasized in the new trading environment.

6. This paper proceeds as follows. In Section II, we describe the current state of on-line securities trading in Korea. In Section III, we present reasons behind the rapid proliferation of on-line trading and their impact on the securities markets. We close by making several concluding remarks and discussing future trends in Section IV.

II. On-line Securities Trading in Korea

A. Background

(1) Definition

7. On-line trading is defined as the technology and services for buying and selling stocks and securities over the Internet. It is also called cyber-trading, Internet trading, web trading or electronic trading. In Korea, on-line trading is usually called "Home Trading", which includes Internet, ARS (Auto Response System), and wireless devices.[3] The table below shows that most on-line trades in Korea are executed through the Internet. The percentage of Internet trading to total on-line trading was 94.3% in 2001.

Table 1: On-line Trading by Types of Devices Used[4]

Year	***Internet***	ARS (telephone)	Wireless Devices
1999	89.9%	7.8%	2.4%
2000	92.1%	2.7%	5.3%
2001	94.3%	2.2%	3.4%

Source: KSDA (Korea Securities Dealers Association)

(2) Products Currently Offered On-line

8. On-line investors can log in a brokerage firm's own on-line trading system[5](or website) and, frequently at no charge, find market data, historical charts, securities analyses, and customized home pages.

9. On-line firms offer trading in equities, options, futures, fixed income securities, and ECN trading. The proportion of equity, futures, and options to total on-line trading volume in 2001 are 55.8%, 41.9%, and 2.3%, respectively. In particular,

[3] For example, brokerage firms provide wireless trading devices for investors. PDA (Personal Digital Assistants) and Cellular Phones are also used in Korea.
[4] Data was collected from 35 firms out of total 38 on-line service providing companies.
[5] Brokerage firms' trading system based on on-line network is called Home Trading System (HTS).

the proportion of on-line futures trading has increased by 40% in 2001, which could have been partly affected by the terrorist attack on the World Trade Center in September 2001. Many on-line firms also offer access to after-hours trading.[6] Investors can opt to have these services delivered not only to their PC's, but to wireless communication devices as well.

(3) New Way of Trading

10. Before 1997, the Korean investors sent orders to brokerage firms via documents or telephone, according to the Securities and Exchange Act (SEA). However, the Internet made a significant impact on the means of business. It has become possible to communicate instantaneously with millions of people at a low cost. Individuals can also access much more information quickly. As a result, the Internet became a new and powerful tool for the financial marketplace. Lastly, the Korean government allowed securities transactions by means of electronic communication and other manners[7] in 1997. Following the amendment, Cho-Heung Securities provided the first on-line trading service in May 12, 1997; at that time, the securities firm charged the same commission rate as before.

11. In 1999, the Ministry of Finance and Economy amended the SEA to lower the capital requirement for commission broker to 3 billion won from 10 billion won. Also, the Financial Supervisory Commission established detailed requirement conditions for obtaining a license of a securities company.[8] Under the new and transparent conditions, securities firms can also establish on-line brokerage firms as a subsidiary company. These policies related to the securities markets opened a new way of securities trading in Korea. On-line brokerage firms were established more easily after the amendment. Thus, competition among on-line firms took place dramatically in reducing commission rates.

B. Overview of Current State

(1) Progress of On-line Trading

12. On-line securities trading has increased tremendously. Table 2 shows the on-line trading volumes from 1998 to 2001. Figure 1 indicates the trends of on-line equity trading volume over the year.

[6] Through an ECN (Electronic Communications Network), which has operated since December 2001, investors can trade during after regular trading hours.

[7] They are telephone, telegram, facsimile, computer, and other similar electronic communication manners [Securities and Exchange Act - Article 109; Enforcement Decree of SEA - Article 66-2].

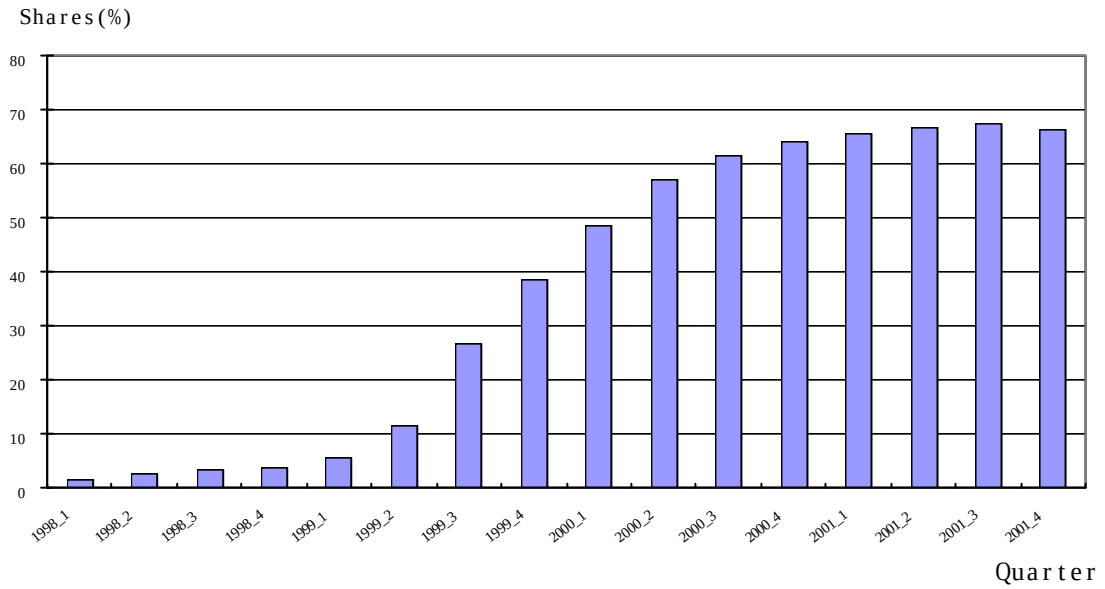
[8] The Financial Supervisory Commission set the conditions for (1) capital requirement, (2) financial structure and qualification of shareholders, (3) competence of management, and (4) propriety of business plan.

Table 2: On-line Securities Trading Volume (US$ billion*, %)

Year	On-line Equity Trading Volume		On-line Futures Trading Volume		On-line Options Trading Volume		Total On-line Trading Volume	
	US$ bill.	%	US$ bill.	%	US$ bill.	%	US$ bill.	%
1998	8.60	2.9%	8.22	1.3%	0.08	3.1%	16.90	1.9%
1999	373.50	25.4%	140.26	11.3%	2.34	18.1%	516.10	19.0%
2000	1,016.60	55.9%	437.22	33.7%	8.90	35.5%	1,462.72	46.6%
2001	920.60	66.6%	692.10	40.7%	38.38	53.7%	1,651.08	52.3%

*(2001.12.31. Exchange Rate)

Figure 1: Trends of On-line Trading Shares of Equity Trades



13. Although the on-line equity trading volume has decreased in 2001,[9] the proportion of on-line trades has grown steadily. Table 2 shows that the proportion of on-line equity trading to total trading volume is 66.6% in 2001, which is the highest level recorded in the world.[10]

14. Figure 2 and 3 shows the trends of on-line trading and individual investors' trades in stock markets, KSE (Korea Stock Exchange) and KOSDAQ (New Market in Korea). On-line equity trade shares in 2001 are about 60% in the KSE and 78% in the KOSDAQ. Most of the investors are individual investors participating in both markets. Figures show that the major market participants are individual investors. They occupy about 75% of KSE and 95% of KOSDAQ trades.

[9] Many attribute the decrease in stock trading in 2001 to the collapse of the venture market bubble.
[10] According to the Salomon Smith Barney, the on-line proportion of equity trades in US is about 38% in 2000.

Figure 2: Trends for On-line trades and Individual Investors in the KSE

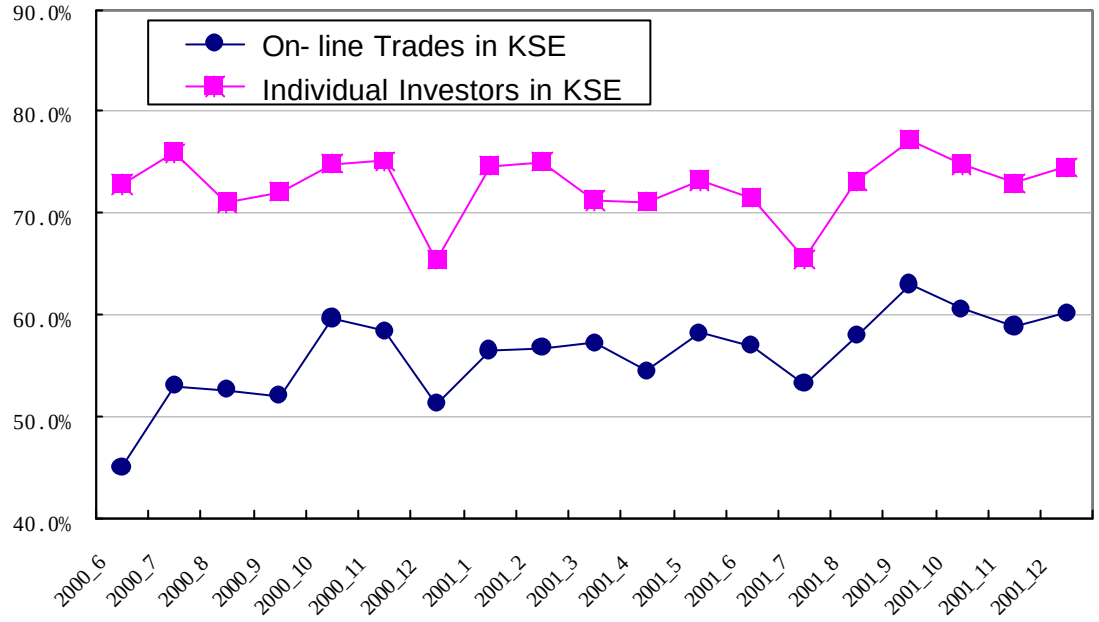
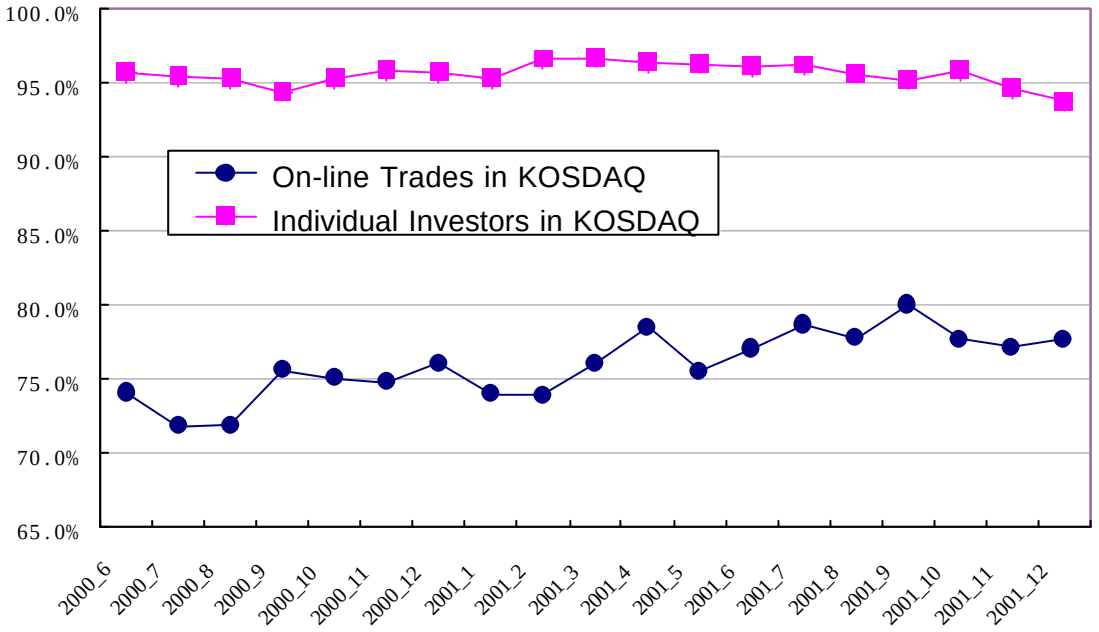


Figure 3: Trends for On-line Trades and Individual Investors in the KOSDAQ



15. Korea Securities Dealers Association (KSDA) estimated that by the end of 2001 there were 4.6 million on-line accounts; 3.8 million were recorded in 2000 and 1.9 million in 1999. However, the total number of accounts has decreased by 4.3% in 2001. The main reason for the expansion of on-line trading is a reduction in the commission rate for on-line trades.

Table 3: Number of On-line Accounts (million)[11]

Year	On-line Accounts	Total Accounts	On-line Shares (%)
1998	0.2	3.8	6.0%
1999	1.9	7.6	24.9%
2000	3.8	8.7	44.4%
2001	4.6	8.4	54.6%

(2) On-line Trading Changes the Securities Industry

16. Of the 44 domestic securities firms, 38 firms offered on-line trading in 2001; 20 foreign brokerage firms, however, did not participate in on-line business in Korea. The number of on-line trading firms was 27 in 1999.

17. The recent increase of the number of on-line trading firms is partly due to lower entry barriers to brokerage business as a result of the amendment in the Securities and Exchange Act in 1999. As we discussed before, the minimum capital requirement for brokerage firms was reduced to 3 billion won from 10 billion won.

Table 4: Number of On-line Trading Securities Firms

Year	Domestic Firms	Foreign Firms	Total
1999	27	0	27
2000	37	0	37
2001	38	0	38

18. While 38 firms offer on-line trading, a few large firms currently dominate the market. The five biggest firms occupied 50% of on-line markets in 2001, although their proportion recently has declined a little. On the contrary, the market share of five on-line brokerage firms[12] doubled to 17.2% in 2001 from 8.8% in 2000.[13]

Table 5: On-line Trading Market Share

Year	Top 3 Firms	Top 5 Firms	Top 10 Firms	5 On-line Firms
1999	49.3%	66.0%	85.2%	-
2000	46.1%	61.9%	79.4%	8.8%
2001	37.6%	50.5%	73.7%	17.2%

19. During the first few years of on-line trading, competition among securities firms led to a dramatically reduced commission rate. In 1997, the commission rate for

[11] Number of accounts is calculated at the end of the year.
[12] On-line brokerage firms only provide on-line brokerage services.
[13] The rising market share of on-line brokerage firms can be attributed to their lower brokerage fees. Usually, the commission rates of on-line brokerage firms are lower than those of full-service securities firms because they can save some fixed costs.

equity trading was fixed at 0.5% per trade. However, the average equity commission charged by on-line firms recently has been reduced to 0.07% per trade in 2001.

Table 6: Average Commission Rate of On-line Trading[14]

Year	Equity Commission		Futures Commission		Options Commission	
	range	average	range	average	range	average
1997*	-	0.5%	-	0.05%	-	1.5%
1999	0.05 ~ 0.25%	0.14%	0.01 ~ 0.18%	0.02%	0.40 ~ 0.75%	0.55%
2001	0.025 ~ 0.5%	0.07%	0.002 ~ 0.0225%	0.01%	0.15 ~ 0.50%	0.45%

* In 1997, only off-line trades were available.

(3) Characteristics of On-line Investors

20. Investors who trade equities on-line tend to be individual investors. The proportion of individual investors in both the KSE and KOSDAQ are above 90% of total on-line trading volume. Especially, the KOSDAQ on-line trading was executed by more individual investors (99.2%) than KSE (95.9%) in 2001.

Table 7: Composition of On-line Trading Investors (US$ billion, %)[15]

	KSE		KOSDAQ		KSE + KOSDAQ	
	Volume	%	Volume	%	Volume	%
Institutional	9.65	4.1%	2.19	0.8%	11.84	2.3%
Individual	225.77	95.9%	268.75	99.2%	494.53	97.7%
Total	235.43	100.0%	270.94	100.0%	506.37	100.0%

21. The frequency of on-line trading has stabilized to approximately 11~13 trades per account a month from 5.66 trades in 1988. Since there are about 20 trading days in a month, investors usually make one trade per 1.65 day. The high frequency of on-line trading implicitly shows that there are many day traders in Korea.

Table 8: Frequency of On-line Trading per Accounts

Year	Monthly Trades
1998	5.66
1999	13.29
2000	12.83
2001	10.51

[14] The commission rates vary according to the trading amount. For comparison purpose, we selected the commission rates for large orders of brokerage firms.
[15] It is estimated from the data of 24 brokerage firms.

22. The increase in the securities trading of on-line investors can be explained by an overconfidence hypothesis. According to the recent papers of Barber and Odean (2000, 2002),[16] on-line investors in US trade more actively, more speculatively, and less profitably than before. Barber and Odean argue that several cognitive biases reinforce the overconfidence of on-line investors. First, people tend to attribute their successes to their own abilities, such attribution is a self-attribution bias. Thus, recent investment success is likely to foster overconfidence in one's stock picking abilities. Second, on-line investors have access to vast quantities of investment data; these data can foster an illusion of knowledge, which increases overconfidence. Finally, on-line investors generally manage their own equity portfolios and execute trades at the click of a mouse; this fosters an illusion of control, which reinforces overconfidence. Overconfident investors are inclined to trade excessively like Korean on-line securities traders.

Table 9: Money used for an On-line Trade

Year	Thousand US$
1998	2.10
1999	3.60
2000	2.91
2001	2.82

23. The amount of money used for a trade was highest in 1999 as 3.60 thousand US$ (4.78 million won) when the stock market was boom. It seems to have positive relationship with market condition. Last year it was 2.82 thousand US$ (3.74 million won), down by 3.1%.

III. Growth of On-line Trading

A. Reasons for Prosperity

24. On-line securities trading share of the total trades in Korea was 52.3% in 2001. Especially, on-line equity trading is 66.6% of the total equity trading for the year. Certainly, it is the highest level in the world. How could on-line trading in Korea be so active? The success of on-line trading in Korea is driven by several factors. First of all, on-line trading has advantages over the traditional trading method. Lower trading costs, faster speed, and more convenient trading platforms can make on-line trading very attractive. Second, the marketing efforts of brokerage firms accelerated the increase of trading volume. Third, the Korean government has encouraged development in information technology and made favorable infrastructures for on-line trading. Finally, the major securities market participants are individual investors. Most individual investors in Korea tend to use on-line trading.

(1) Advantages of On-line Trading

[16] Barber and Odean, "Trading is Hazardous to Your Wealth: The Common Stock Investment Performance of Individual Investors," *Journal of Finance*, 55, 2000, pp. 773-806.
Barber and Odean, "Online Investors: Do the Slow Die First?," *Review of Financial Studies*, forthcoming. 2002.

25. The first advantage of on-line trading is its lower cost. As Table 6 shows, the commission rates for on-line trading has reduced on average from 0.5% to 0.07% per trade for last four years. It is possible to lower the trading cost because on-line trading removes many unnecessary costs that are common with traditional trading such as an office building, paper works and sales staff.

26. The second advantage is improved trading speed. The orders are routed to the trading system of the KSE or KOSDAQ market instantaneously by using the computer. The electronic communication between the point of order and the execution system produces no time delay.

27. The convenience of usage is another advantage of on-line trading. Investors can consult market data, charts, and real-time news, and make their orders using the same screen. A wide range of market information is available through the Internet and other wireless devices. Also, on-line trading overcomes many obstacles related to the time and place. Investors can access the on-line system 24 hours a day from anywhere.

(2) Competition among Brokerage Firms

28. Marketing efforts of small and medium sized brokerage firms accelerate the industry's move to on-line trading. They reduced commission rates and effectively promoted their cost advantages to the market.[17] The availability of on-line trading at reduced commission rates has forced large firms to reconsider their pricing models.

29. To cope with challenges from on-line trading, large brokerage firms participated in "virtual price war" over commission rates and reformed their services in areas including ease of access, pricing of services, and information resources.[18] Large brokerage firms in Korea could not avoid the needs of on-line investors because the proportion of on-line trading has been increasing. In addition to execution costs, on-line service firms will continue to compete with each other to offer their customers more convenient access to research, portfolio management tools, and financial planning.

(3) Government Policies Supporting the Internet Infrastructure

30. The Internet has continued to grow at an extremely fast pace, playing a critical role in the development of on-line trading. Since most on-line trades are executed through the Internet, the growth of on-line trading has a direct relationship to Internet infrastructure.

31. The average usage of the Internet is increasing in many countries. Table 10 shows Internet subscribers in OECD countries.[19] At the end of 1999, there were at least 49 million Internet subscribers in the US, about 11 million in both Japan and Korea, 9 million in Germany, more than 7 million in the UK and 6.2 million in

[17] In US, on-line firms (discount brokerage firms) differentiated themselves from traditional brokerage firms by reducing commission rate instead of offering more services. They grew in a niche market.
[18] As a large brokerage firm, Samgsung Securities reduced commission rate by 50% on May 1999.
[19] An Internet subscriber is the number of subscribers to the Internet services of the telecommunication carriers. Total 29 OECD countries are compared.

Canada. A ranking based on the number of Internet subscribers out of 100 persons shows high levels for Korea, Sweden, Denmark, Canada, the US, and Netherlands, and relatively lower levels for Hungary, Greece, the Czech Republic and Mexico. Actually, among the OECD countries, the rankings in Internet usage for Korea are number two in total subscribers and number one in subscribers per 100 persons.

Table 10: Internet Subscribers in OECD (January 2000)[20]

Country	Internet Subscribers	Ranking	Subscribers per 100	Ranking
Australia	2,407,407	11	12.9	10
Canada	6,169,500	6	20.4	4
Czech Republic	199,000	24	1.9	23
Denmark	1,135,393	14	21.4	3
Germany	9,000,000	4	11.0	13
Greece	199,960	23	1.9	24
Hungary	114,033	25	1.1	26
Japan	10,590,000	3	8.4	19
Korea	**10,860,000**	**2**	**23.4**	**1**
Mexico	1,350,000	13	1.4	25
Netherlands	2,834,375	10	18.1	6
UK	7,400,000	5	12.5	12
US	49,723,100	1	18.4	5

32. How could Korea have the highest level of Internet usage? The Korean government basically triggered the expansion of Internet users. The government introduced policies to encourage development in the infrastructure of information technology and communication, which made a favorable environment for on-line trading.

33. Table 11 summarizes the government policies encouraging the use of Internet driven by the Ministry of Information and Communication and the Ministry of Education and Human Resources Development. For the network infrastructure, the Ministry of Information and Communication established a plan for "Korea Information Infrastructure (KII)" in 1993. Accordingly, Korea constructed high-speed optical transmission networks. Also, the government adopted a flat-rate system and a low-price-policy for high-speed Internet and created a competitive service environment by licensing multiple common carriers.[21] As a result, the number of high-speed Internet users has explosively increased.

Table 11: Government Policies supporting Internet Usages

Area	Policy	Contents
Network	Plan for "Korea Information Infrastructure" Phase 1: 1995~1997 Phase 2: 1998~2000 Phase 3: 2001~2005	Nationwide optical backbone High-speed Internet access Open competition between service providers (1996)

[20] OECD, "Internet Infrastructure," 2000.

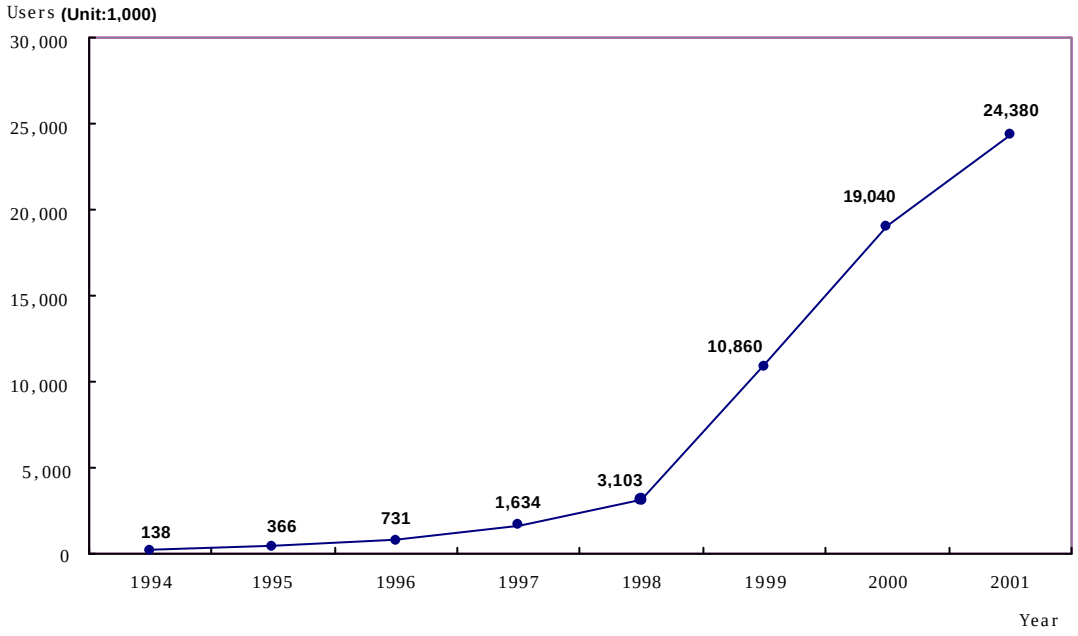
[21] The average cost of high-speed Internet access in Korea is US$ 22.45 while Japan $67.1, Hong Kong $31.8, Singapore $25.6, Malaysia $18.4, and US $30.1[source: Korea Network Information Center].

Education	Plan for "Education-Computerization" (1997~2002)	Provisions of Multimedia Instruments Building the Electronic Network

34. Also, the Ministry of Education and Human Resources Development has invested a total of 486.6 million US$ in the "Comprehensive Plans for Education-Computerization". In this ambitious plan to build the infrastructure for Education-Computerization, the government intended to expand the information-use base. Following the project, schools have been provided with access to multimedia instruments and electronic network.

35. In addition to the expansion of home or school computers, Internet cafes[22](or PC game room) boomed in Korea. The number of Internet cafes was about 3,600 in 1998, which then quadrupled to 12,050 a year later. Figure 4 shows the number of Internet users in Korea. As it shows, the number of users grew eight-fold in three years, which is from 3.1 million in 1998 to 24.4 million in 2001.

Figure 4: Number of Internet Users in Korea



Source: Korea Network Information Center

(4) Active Participation of Individual Investors

36. In addition to plans for Internet infrastructure, Korea experienced a venture boom in the information technology (IT) sector with the advent of "New Economy" in 1998. Many venture firms were established and their stocks were traded on the KOSDAQ market. As a result, the stock markets boomed. After the financial crisis in 1997, 1998-99 may be remembered as the period during which the Internet bubble (or

[22] In Korea, the Internet Cafe is called the PC game room in which people can play on-line games and trade securities through the Internet without any difficulty.

venture bubble) was created and expanded. On-line securities trading also increased at this time. We may find positive relationship between the growth of on-line trading and stock market bubbles. Although the government allowed on-line trading in 1997, substantial amounts of on-line trading started taking place from 1999.

37. The major securities market participants are individual investors. Individual investors occupy about 75% of KSE and 95% of KOSDAQ trades. The advantages of on-line trading are still attracting many individual investors on-line. Now, Internet and on-line trading have deeply penetrated into the daily lives of Korean investors.

B. Impact on the Securities Market

38. The development of on-line trading has affected securities markets in various ways. First, traditional trading has been shrinking and the trading patterns have changed remarkably. The daily trading volume increased as trading became easier than before. Second, as individual investors could access the securities market without any professional help, on-line trading has improved their status in the securities industry. Finally, securities firms face severe competition in providing information and services as well as setting commission rates.

(1) Short-term Trading Prevails

39. Table 12 shows the average daily trading volume in the KSE and KOSDAQ. The average daily trading share volume in the KSE was 98 million in 1998. The KOSDAQ trading share volume was even smaller. However, the trading volume in 2001 has passed 300 million shares. Although the direct cause of trading volume increase in the stock markets is not easy to find, we may infer that on-line trading has increased the daily trading volume. Because time and costs are tremendously reduced, stock trading via on-line is much more convenient than using traditional means.

Table 12: Average Daily Trading Volume (unit: million shares)

	KSE		KOSDAQ	
Year	Daily Trading	% change	Daily Trading	% change
1998	98	-	0.7	-
1999	279	184.7%	35	-
2000	306	9.7%	212	505.7%
2001	473	54.6%	384	81.1%

40. The convenience of trading may also cause the appearance of short-term on-line day trading on the markets. According to the KSE,[23] the proportion of day trading was 46.1% in 2001. The on-line day trading has been criticized for causing high volatility in the markets. However, it also provides the market with liquidity. The potential problems of day trading are beyond the scope of this paper. However, it has been cautiously indicated that investors are exposed to potential price and market distortions caused by speculative day trades. Thus, investor protection, including

[23] KSE, "Day Trading in 2001," Press release, 2001.12.26. They define a day trading as “buy and sell the same stock within a day”.

investor education by government or self-regulatory organizations (SROs), will be more emphasized in the new trading era.

(2) Individual Investors Access Markets with Greater Ease

41. The change in the securities markets has enabled investors to participate more directly in the securities markets. On-line trading has significantly changed the dynamics of the marketplace, causing one of the biggest shifts in individual investors' relationship with their brokers.

42. For the first time ever, investors can access financial information on the same terms as market professionals, including news developments and market data. In addition, on-line service provides investors with tools to analyse information such as research reports, calculators, and portfolio analysers. As the information gap between individual investors and institutional investors narrowed, the status of individual investors in securities markets has improved. Therefore, the role of brokerage firms as a middle-man is shrinking.

(3) Securities Firms Face Severe Competition

43. On-line trading has had a tremendous impact on securities firms in many ways. First of all, sharply reduced commission rates forced securities firms to diversify their business. Korean securities firms highly depend on brokerage fees as income. In maintaining low commission rate, the securities firms that are not able to attract sufficient customers will disappear or be merged in the future. Thus, securities firms are seeking other business areas in addition to brokerage service.

44. Second, as competitions between securities firms intensify, securities firms are shifting their focus from institutional investors to individual investors. Severe competitions require heavy spending on advertisement and investments on computer network systems to enhance the convenience of customers.

45. Finally, because the earnings of securities firms have deteriorated, securities firms are trying to differentiate themselves from competitors by offering various services and high quality investment information to their customers.

IV. Concluding Remarks and Future Trends

46. The convenience of on-line trading, developments of information and communication technology, competitions between securities companies have fueled the development of on-line securities trading in Korea. Currently, we can expect a continuing rise of on-line trading in the future. According to the survey, Korean securities firms estimate that 71~80% of total equity trades will be executed through on-line by the end of 2005. Also, they expect that the ratio will be over 80% by 2010.[24] However, the increasing trends will reach a saturation point at some time.

[24] Historically, the highest ratios of equity, futures, and options to the total equity, future, and options trades were 69.3%(2001.9), 50.9%(2001.1), 57.7%(2001.9), respectively.

47. Securities firms will continue to seek other business areas as well as brokerage service. They have to diversify their business to survive in a new competitive environment. Providing financial advice on-line will be the next area of focus for the brokerage industry. For example, if website users set their preferences, then on-line firms will send information tailored to these preferences. Also, securities firms can either classify users and offer different information to different categories of users or recommend products based on user profiles that they have developed.[25]

48. The government will focus more on investor protection. As securities markets are more dynamic and volatile than before, various risks caused by on-line trading occur. First of all, the reliability of on-line trading system will be critical. When the system breaks down, a backup or an alternative system will be needed. Protection of on-line customers' personal information is also important. Second, in order to prevent market manipulation, monitoring and punishment to the manipulation should be strengthened. In the on-line domain, it is easier for market manipulators to conduct fraudulent activities. The role of the regulator will be important in maintaining an orderly market. Lastly, investor education should be emphasized. As on-line trading has reduced personal interaction between the securities firms and investors, professional advice and knowledge have been less available. Thus, investor education to protect investors from market risks will deserve more attention.

V. References

Korean

Korea Network Information Center, "Analysis on Rapid Growth of Internet Users in Korea," Analysis Report, 2000.7.

Korea Securities Dealers Association, "On-line Trading in 2001," Research Department, 2002. 1.

Korea Stock Exchange, "Day Trading in 2001," Press Release, 2001.12.26.

Lee, Jeong-Beom and Joo Lee, "Current Issues on Cyber-brokerage Industry," Survey Report, Korea Securities Research Institute, 1999.8.

English

Barber and Odean, "Trading is Hazardous to Your Wealth: The Common Stock Investment Performance of Individual Investors," *Journal of Finance*, 55, 2000, pp. 773-806.

Barber and Odean, "Online Investors: Do the Slow Die First?," *Review of Financial Studies*, forthcoming, 2002.

[25] For example, Charles Schwab & Co., Inc. allows viewers to create a personalized web page. "Schwab, Excite to Launch Personalized Web Pages," *Institutional Investors*, May 10, 1999.

Ministry of Education and Human Resources Development, "Infrastructure for Education-Computerization," Korea, 2001.5.

Ministry of Information and Communication, "Korea Information Infrastructure & Broadband Service," Korea, 2001.6.

OECD, "Internet Infrastructure," DSTI/ICCP/TISP(2000)10/CHAP5, 2000.

MALAYSIA: ELECTRONIC BANKING IN MALAYSIA[1]

I. Introduction

1. The vertical case study on Electronic Banking in Malaysia will focus on the wider spectrum of activities in so far as these contribute to building a consumer base for e-commerce in cross-border trade. This is because developments in retail financial services, inter-bank services and e-commerce gateway initiatives will indirectly influence the process of establishing a paperless trading mechanism for regional e-commerce activities. The case study will be presented in two sections, namely, Development history and trend in e-banking activities (Section A) and Factors Affecting the Development of Electronic Banking (Section B).

A. Development History and Trend in e-Banking Activities[2]

1981 – 2001

2. The evolution of e-banking in Malaysia up till now has largely been to substitute over-the-counter services with remote services, and hence reduce the overheads associated with conventional branch-based banking. Electronic banking in Malaysia has its roots in Automated Teller Machines (ATM) introduced in 1981 in Malaysia. The range of services grew rapidly from balance inquiry and cash withdrawal to transfer of funds between checking, savings and credit card accounts, bill payments, IPO subscriptions, cash and cheque deposits. The widespread adoption of ATM units also created several ATM networks in the late 1980s. In the 1996, these networks were amalgamated to create a single system, known as the Malaysian Electronic Payment System (MEPS), a private payment channel provider which is jointly owned by the Malaysian banks. MEPS provides a common platform for retail or micro, electronic payment services, and is currently engaged in various projects to promote the use of micro-payment services using advanced card technology. Additional information is available at www.meps.com.my. Apart from advanced ATM services, banks in Malaysia offer PC Banking, wireless banking and deposit-taking machine services.

3. To support the development of e-commerce, MEPS launched an internet payment gateway in March 1999 to process card-based payments for its member banks.

4. In June 2000, Bank Negara Malaysia (BNM) allowed all domestic Malaysian banks to provide full transactional / interactive Internet banking services as an additional delivery channel. Foreign owned banks were allowed to offer Internet banking services from the 1st of January 2002. Although it is still too early to form a firm conclusion about the success of Internet banking, there is evidence to suggest

[1] Prepared by Bank Negara Malaysia

[2] See 'Electronic Banking in Malaysia: A Note on Evolution of Services and Consumer Reactions', by Balachander Krishnan Guru, Santha Vaithilingam and Norhazlin Ismail of Multimedia University Malaysia, and Rajendra Prasad of BSN Information Technologies & Services Sdn. Bhd., 1999/2000.

that many urban customers are attracted to the convenience of paying bills from home or the office.

5. In October 2000, MEPS launched the Inter-bank GIRO service, allowing small value inter-bank payments to be effected. The number of transactions grew rapidly (from 3,951 in January 2001 to 16,321 in December 2001), as did the value of transactions (from RM37.9 M in January 2001 to RM 137.5 M in December 2001).

6. The Malaysian Government was the first Government in the world to implement a national strategy for a multi-application smart card. The Multipurpose Card (MPC) Flagship Application is one of the MSC Flagship Applications that seeks to develop a single common platform for a MPC enabling the Government and private application providers to implement smart card solutions.

7. Two types of cards are being issued under this project, MyKad, issued by the Government contains critical government applications such as the national identity, immigration particulars, driving license, medical information as well as payment applications, namely the MEPS Cash and ATM application. The second smart card application, the Payment Multi-purpose Cards (PMPC), incorporates the ATM, debit and MEPS Cash applications to be individually issued and branded by banking institutions.

8. Progress has also been made in the implementation of the electronic money scheme, MEPS cash, which was first introduced in 1998 during the Commonwealth Games. The banking institutions are now in the final stages of implementing a nationwide roll out of the MEPS Cash application. Besides being introduced as a stand-alone card, MEPS Cash will also be issued as an application in MyKad, and the PMPC, which will contain ATM and debit applications.

9. It would be reasonable to conclude that e-banking services have proliferated in recent years in the Malaysian banking scene. Competitive pressures as well as consumer demand will ensure that e-banking services continue to evolve into more sophisticated products, as well as being more widely accessible to the general consumer.

2002 and Onwards

10. The rapid growth of credit card transactions and inter-bank GIRO services is due to the attractiveness of the business application. Credit cards are widely accepted, and the readers are now installed even in comparatively small business establishments. Inter-bank GIRO saves on clearing time and transaction costs, and hence is attractive. However, micropayment applications are not yet that attractive, for several reasons. The card readers need to be installed at enough merchant sites for the product to be a practical alternative to cash. The ATM machines must be modified to allow re-loading of cards, anywhere, anytime. The cost of setting up this infrastructure has to be factored into some sort of pricing mechanism.

11. It is for this reason that a joint initiative between the government and the private sector has been established to manage the problems associated with infrastructure and connectivity. Bank Negara Malaysia acts as the chair for this joint

initiative, which includes commercial banks, technology vendors and MEPS as the principal players. If the project is successful, and the transactions are cost effective, the incentive to create e-commerce applications will be much greater.

12. It would be reasonable to expect that the PMPC and other card-based services (like Touch N Go) that are aimed at retail purchases will gradually reduce the dependency on cash and cheques. The work being undertaken by MEPS together with the banking industry will also promote connectivity within the retail payment systems infrastructure. Once the cost factors have been absorbed by the pricing mechanism, the incentive to provide this added feature to consumers will spur growth in micropayment products.

B. Factors Affecting the Development of Electronic Banking

Regulatory Factors

13. BNM has put in place a regulatory framework that encapsulates prudential requirements, while giving the banking institutions considerable leeway for innovative financial products. Apart from the guideline regulating electronic fund transfer systems, BNM had also issued a comprehensive guideline that covers financial services offered through Internet banking delivery channels. Micropayment service providers are not currently regulated on a stringent basis, but they do come under the jurisdiction of the central bank. Hence, the issue of minimum service standards and prudential controls can be more easily addressed.

Institutional Factors

14. Generally, the banks have been instrumental in introducing technologically sophisticated products. The advantage of having sufficient capital and incentive, driven by greater competition had resulted in many of the local banks moving towards greater use of technology in doing business.

15. Factors that inhibit the development of electronic banking products include the difficulty in cutting costs associated with system enhancements and changing consumer mindset. Migrating the bulk of customers to the on-line platform has proven to be slow and cumbersome. Other institutional factors include the shortage of qualified information technology staff, particularly in the areas of software development, strategic management of technology and risk management for vulnerabilities typically associated with electronic banking services provided through an open network.

16. Activities underway to address these issues include increasing the scope for private education centers to fill the gap in the IT labor market, and educating the public about off-branch banking.

Physical Infrastructure Factors

17. The telecommunications infrastructure in Malaysia is growing rapidly, with mobile telephony currently outpacing the growth of fixed line telephone services. PC penetration into homes is increasing rapidly, and together with the wide availability of Internet cafes, Malaysia has a rapidly growing population of Internet savvy consumers (current estimate by MDC is 15 million Internet subscribers in Malaysia). Efforts to close the 'digital divide' are on going, for instance by implementing special projects through the Malaysian National Computer Confederation's Open Source Special Interest Group (MNCC-OSSIG). Further information can be obtained at www.mncc.com.my.

Legal Infrastructure

18. In terms of a legal infrastructure, the Malaysian government has introduced a range of cyberlaws, as shown below:
- Computer Crimes Act 1997
- Digital Signature Act 1997
- Amendments to the Evidence Act
- Communications and Multimedia Act
- The Copyright (Amendment) Act 1997
- Personal Data Protection Bill (under development)

ICT Security Factors

19. The main technological issue revolves around security systems for the secure provision of financial services over an open network environment, like the Internet. The occasionally alarming signs of virus threats, as well as presence of hackers, can only be resolved through cost effective technology solutions in the form of firewalls and other intrusion detection and prevention devices.

20. The body that plays a key role in information security management for the Internet environment is the Malaysian Institute of Microelectronic Systems (MIMOS). MIMOS was established as the Malaysian Institute of Microelectronic Systems on 1 January 1985. In the early days, MIMOS functioned as a small unit in the Prime Minister's Office. By 1990, MIMOS had evolved into a full-fledged organisation under the Ministry of Science, Technology and the Environment (MOSTE.) In January 1995, MIMOS was appointed Secretariat to the National IT Council (NITC.) The NITC envisions an information-rich society in line with the National Vision Policy, Vision 2020, and actively promotes the application and development of Information and Communications Technology (ICT) in nation-building efforts. On 1 November 1996, MIMOS underwent a 'corporatisation' exercise. It emerged as MIMOS Berhad, empowered with greater flexibility to create value-added innovations for industry, society and the nation. MIMOS Berhad continues to be an ICT R&D (Research & Development) organisation that functions as an advisor to the Malaysian Government on technologies, policies and strategies relating to ICT development.

21. MIMOS established the Malaysian Computer Emergency Response Team (MyCERT) in March 1997. MyCERT handles ICT security problems such as

intrusion, spamming, and many more. In 1998, the National Information Technology Council (NITC) formed another body, NISER (National ICT Security emergency Response center), to address ICT security issues covering both proactive and reactive measures.

Social and Political Factors

22. The Malaysian government and the central bank have both been extremely keen to promote innovation in financial services. The development of the Malaysian Multimedia Super Corridor (MSC) initiative, the e-government agenda and the proposed introduction of Government and Payment Multi-purpose Cards, using smart card technology, all contribute to a positive environment for electronic banking services. Further, the more intense use of information technology and teaching of the same in all levels of the education system will accelerate the adoption rate of new electronic banking products.

23. Bank Negara Malaysia has a dedicated unit to conduct periodic information systems audits on all banking institutions. The information systems supervisory function plays an important role in mitigating the risks, in particular the possibility of systemic risks, associated with the widespread adoption of electronic banking delivery channels.

24. It can be concluded that although there are still many issues that must be dealt with in order to promote e-banking in the country, there is a lot being done by way of structure and process to resolve these issues at the national and industry level. The individual banks can leverage off these developments to enhance their own e-banking services.

BRUNEI DARUSSALAM: ENVIRONMENTAL SCANNING ON PAPERLESS PAYMENT[1] CHANNELS[2]

I. Introduction

1. This report examines the status of the paperless payment channels taking place in Brunei Darussalam. The project implementation was led by the Ministry of Finance via the Financial Institutions Division and with the support from Information Technology and the State Stores Department (ITSSD) and Brunei Currency Board. In order to get information for the case study, the Financial Institutions Division, Ministry of Finance has targeted at banks to conduct the followings:

(a) surveys on the volume of transaction on payments for goods, services and financial transfers including Automated Teller Machines (ATM) transactions; and
(b) questionnaires on banks' plans to implement electronic financial services.

II. Analysis and Findings

2. For the surveys in (a), 100% of the respondents responded to the above survey. Summary of the findings is as below. The total transaction volume for the period January 2001 to December 2001 showed a seasonal trend for different types of transactions. For cheque payments, it showed the highest during the month of January and November. For paper credit transfer, it showed the highest during the month of March and June. Automated payments showed a random movement, fluctuating during the months. Credit cards purchases have increased steadily and peaked during the month of November. Debit card purchases have increased steadily and peaked during the month of November and December. Cash withdrawals at ATMs and counters showed the highest during the month of February and November. This coincided with the festive seasons of Chinese Lunar New Year and Hari Raya Aidilfitri where money gifts are a tradition. Cash payments showed the highest during the month of November. The number of ATMs has increased during the last 12 months from 98 ATMs to 102 ATMs. ATMs withdrawals showed the highest during the month of December.

3. For the questionnaires in (b), the response rate was 66.7% (6 out of 9 banks), and the results are summarised as follows:

(Q1) Has your bank planned to or already has implemented internet banking?

Implemented (2)	Planned (0)	No response (4)

[1] Paperless payment in this report refers to paperless governance and information/data exchange through multimedia technologies.
[2] Prepared by the Ministry of Finance of Brunei Darussalam

(Q2) Has your bank offered electronic banking services to your customers? For example, a simple static web sites. Do you have intention to upgrade their on-line presence?

Yes (6)	No (0)	No response (0)

(Q3) Do your bank has the ability to offer a payment clearing facility for electronic commerce transactions (on line services)?

Yes (0)	No (6)

(Q4) Do your bank has a payment gateway strategy planned or in progress for your merchants?

Yes (2)	No (4)

(Q5) Do you prefer to have a third party providing a gateway or to have one in-house?

In house (4)	3rd party (1)	No response (1)

(Q6) What do you think in regards to enabling merchants to accept on-line credit card payments form internet customers?

Secure environment (4)	No response (2)

(Q7) Do you have internet investment plans on the coming year?

Investment plan (2)	No response (4)

(Q8) Do you have plans to offer interactive banking website?

Yes (3)	No response (3)

(Q9) What is your proposal on how to get returns from your investment for this project?

Volume (4)	Bigger customer base, competitive pricing, access to technology, defensive strategy (2)

(Q10) Is there a company or do you anticipate that there will be companies with web store fronts in Brunei Darussalam that will offer payment gateway services?

Yes (3)	No (2)	No response (1)

(Q11) What is your bank target group, reservations, perception to image, etc?

Target groups: Internet savvy client, input export, corporate customers, added value customer service (5)	Perception (0)	No response (1)

(Q12) Do you have merchants asking your bank to provide the appropriate payment infrastructure to enable them to accept credit card transactions over the internet?

Yes (4)	No (1)	No response (1)

(Q13) What do you think in regard to the risks of merchants fraud and non-delivery of goods?

Measurable risk (4)	No response (2)

(Q14) Do you think the market in Brunei Darussalam (transaction volume) is enough to cover the costs of payment gateway infrastructure? If internet, larger audience, may be will reduce the cost of servicing customers' relationship?

Facilitator: Customer services (1)	Inhibitors: Market is too small, local culture cash-based driven, less outgoing goods & services, more incoming goods & services (5)

(Q15) If we have all the above, the banks might require technology auditor to hack into your systems on a regular basis to monitor system security and reliability, what do you think about that?

Preference more to internal auditor than external auditor (6)

III. Bill Presentment and Payments

				Payment Methods				
Type of bills	No. of Subscribers	Bill presentment	Bill Despatch	Cash	Cheque	Credit card	Internet payment	Pre-paid
Telephone	70,000 - 80,000	Paper / Internet	Post /Internet	✓	✓	✓		✓
Water	60,000	Paper	Post /spot billing	✓	✓			
Electricity	88,000	Paper	Post /spot billing	✓	✓	✓		✓
Internet	14,000	Paper / Internet	Post /Internet	✓	✓	✓		✓
Mobile phone	143,000	Paper / Internet	Post /Internet	✓	✓	✓		✓

IV. Location Advantage for Paperless Payment

4. The Government has emphasized on the importance of Information and Communication Technology (ICT) development in Brunei Darussalam. The Brunei Darussalam Information Technology Council (BIT Council) has been established to spearhead and provide guidance on the implementation of the National IT Strategic Plan. Through the BIT Council, the Government aims to lead and facilitate the strategic development and diffusion of state-of-the-art IT for the entire nation. The e-Government Program Executive Committee and the e-Business Program Executive Committee have been formed as affiliates of the BIT Council as part of the institutional infrastructure to assist in achieving the mission and goals of the National IT Strategic Plan for the National Drive Towards Paperless Society.

5. The two Internet Service Providers (ISPs) currently in operation are BruNet (www.brunet.bn) operated by Brunei Telecommunications Department (JTB) since September 1995 and Simpur.net (www.simpur.net.bn) operated by DataStream Technology (B) Sdn Bhd (DST) since October 2000. There have been three other ISP licences issued but not in operation yet. Brunei's Internet subscribers have also doubled to nearly 30,000 in year 2001 compared to year 2000 which is almost 10 percent of the entire population of the country.

6. Legal infrastructure for promoting and supporting e-Government and e-Business in Brunei Darussalam has been given priority implementation. This includes the Trademarks Order and Copyright Act, the Computer Misuse Order, the Electronic Transactions Order 2000, the Patent Order, the amendment to the Evidence Act to accept "computer evidence", the Class License Notification and the Internet Code of Practice are introduced under the Broadcasting Act. An Order to establish and incorporate the Authority for Info-Communications Technology Industry (AiTi) of Brunei Darussalam Order, 2001 has also been gazetted in May 2001. Overall the legal framework is undergoing enhancement to create a favourable environment for electronic use and allow provision for cyber laws based on international standards such as United Nations Conference on International Trade Law (UNCITRAL) Model Law (source: Attorney General's Chamber).

7. In 2001, at least three of the commercial banks have offered Internet Banking services with one recently launched its Mobile Banking service (November 2001). Brunei Darussalam is expected to see its second mobile operator in operation in 2002 with the invitation to tender issued recently.

8. Brunei Darussalam has one of the best basic telecommunication infrastructures in this region. The Brunei Global Multimedia Info-communication Network or 'RaGAM 21' for the Brunei's info-communication superhighway, will eventually link up every major town, village, school, institution and commercial area in the country. Currently, almost every strategic area in Brunei-Muara District is linked to 'RaGAM21' network which in turn is linked globally via satellite and the South-East Asia, Middle-East, Western Europe 3 (SEA-ME-WE3) and Brunei-Singapore submarine cable systems.

V. Conclusion

9. Based on these findings, it indicated that the financial institutions in Brunei Darussalam have the capacity to drive paperless payment system in the very near future.

A. Opportunities / Challenges

10. The availability of the paperless payment system (without or less papers) to the various sectors of society can be drivers for resources saving and but also improving the overall efficiency in financial transactions in Brunei Darussalam.

11. The measures that focus on the services and change management for the better are to be sustainable and implementable. There has to be a paradigm shift of everyone's attitude towards paperless payment. People are generally hard to change but with good education and awareness programme on the benefits of paperless payment and confidence in the system, they can adapt.

12. With wider use of electronic means to settle payments and as society goes towards paperless, legal issues may be involved when problems arise. Legal framework needs to address the issues of concern yet allow flexibility in the implementation and operation of the paperless payment system.

13. This may require technical measures to overcome lack of confidence for internet payment say, due to fear of hackers or viruses.

B. Critical Success Factors

14. Secure environment and public confidence in paperless payment system are critical success factors.

C. Next Action Plan

15. There has to be a strategic framework on e-finance that needs to be developed in Brunei Darussalam and aligned with the national IT framework, i.e. gned with the two points below: to encourage paperless payment in Brunei Darussalam, in line with the core strategies of the National IT Strategic Plan, "IT 2000 and Beyond" i.e. paperless society, e-government and e-business.

THAILAND: THE BAHTNET INITIATIVE [1]

Executive Summary

1. The vertical study on the BAHTNET system of Thailand covers one of the highly developed financial infrastructures of the country. Since 24 May 1995, the Bank of Thailand (BOT) developed the BAHTNET (Bank of Thailand Automated High-value Transfer Network) System for electronic funds transfers among financial institutions in Thailand. Due to the changing business requirement of the market and the technology advancement as well as, the BOT's policy, the BOT has upgraded the existing BAHTNET system by enhancing the facility for the settlement of Thai government securities in a delivery versus payment (DVP) manner since 11 December 2001.

2. Additionally, the new system incorporates the dual technology, which include S.W.I.F.T. and Web interface for sending and receiving messages between BAHTNET members and the BOT. As a main interface, the use of S.W.I.F.T interface would enable straight-through processing (STP) and be consistent with international practice. Meanwhile, the Web-based technology would be an effective channel in handling interactive inquiries and message transmission for smaller-scale members. Hence, the development of the BAHTNET system would increase scope of the services as well as the efficiency and safety in the payment system, and should prove invaluable in the development of the money and capital markets.

3. Factors affecting the development of the BAHTNET system are identified. Major financial institutions are key drivers behind the use of S.W.I.F.T gateway, which would allow their internal systems to be compatible with the BAHTNET system and be able to perform STP. From a legal perspective, many laws are under development aiming to promote efficiency by encouraging use of electronic payments. Additionally the technology deployed in the previous BAHTNET system became obsolete and limited its services to a closed system. Hence, the upgrade of the BAHTNET system is required by using advanced technology to develop a secure and efficient infrastructure. The other environmental issues, such as, social, economic, and global, are also included.

4. With the objectives of promoting efficiency and minimizing risks in payment systems by developing an RTGS infrastructure, key achievements have been reached. The BAHTNET system helps substitute the use of cheque, which is deemed to be a costly and higher-risk mean of payment. The development of a DVP system supports the same-day settlement of securities transactions. Hence, it reduces the settlement risk and minimizes the use of manual procedure. Several mechanisms, including intraday liquidity facility, gridlock resolution, and queue management, have been introduced to facilitate members in managing their liquidity needs. Additionally, the development of the BAHTNET system is consistent with BIS Core Principles for Systemically Important Payment Systems and international practice as well as supporting future cross-border linkages with other payment systems.

[1] Prepared by the Bank of Thailand

5. With limited timeframe of development period and the cutover in a big bang scenario, as well as, the varying natures of participants, the BOT confronted challenging tasks in preparing all members to be ready for the cutover of the upgraded BAHTNET system. Nevertheless, the migration of upgraded BAHTNET system was implemented with satisfactory result. The success was owing to close cooperation between the BOT and all related parties and effective project management, which drove the teams towards the same goals in compliance with the scheduled plan.

6. The future plans of the further development of the payment infrastructure needs to be considered. First, the BOT would continue to support potential cross-border linkage, which would allow a reduction in the settlement risk for payment versus payment (PVP) of foreign exchange transactions and DVP of securities settlement. Second, the BAHTNET system will be continuously developed in order to respond to the rapid changes of business needs and advanced technology. Third, the BOT has been currently revising the provision of the intraday liquidity facilities to ensure the fair market value of the deposited securities and the consistent calculation methods across the liquidity window provided by the BOT. Finally, the BOT is considering an ideal infrastructure, which would provide the same window for trading and settlement for both government sector and private sector securities.

I. Development History and Trend

A. Background and Development Path

7. The Bank of Thailand (BOT) developed the BAHTNET (Bank of Thailand Automated High-value Transfer Network) system as a financial infrastructure for electronic funds transfer among financial institutions in Thailand. The BAHTNET system has been in operation since 24 May 1995 by supporting high-value funds transfer on the on-line real-time gross settlement (RTGS) basis. The transactions are completely settled on a transaction by transaction basis in order to reduce the settlement risk and, more importantly, to enhance financial stability.

8. The BOT has realized the importance of developing the government'domestic securities market, reducing the government's securities-related costs and risk as well as ensuring that system infrastructure conforms to an international settlement standard. Consequently, the BOT has upgraded the existing BAHTNET system by enhancing the facility for the settlement of Thai government securities on a real-time basis or in a DVP manner since December 2001. Moreover, the upgraded system uses S.W.I.F.T. Interface as the main interface for sending and receiving messages between BAHTNET members and the BOT.

9. Types of the transactions sent through the BAHTNET system are:
   (a) Funds Transfer,
   (b) Pre – Authorized Debit Transfer,
   (c) Third Party Funds Transfer,
   (d) Deliver Free / Receive Free,
   (e) Delivery Against Payment / Receive Against Payment, and
   (f) General Messaging.

10. Members, who are S.W.I.F.T members, are able to access the BAHTNET system by using standard S.W.I.F.T. interface already installed at many institutions, whereas, other BAHTNET members, who may not be ready to become S.W.I.F.T members, the BOT has provided an alternate channel for them to access BAHTNET by using Web browsers on the BOT Webstation via BOTNET/X. Types of transactions available for this interface are the same as for the S.W.I.F.T. Interface.

11. Additionally, from the members' viewpoint, whereas the S.W.I.F.T. Interface is most suitable for straight-through processing (STP) with their internal systems, it is not suitable for interactive use. The Web Interface then also offers interactive inquiries for the balance and movement of their cash account and securities account , as well as providing queue inquiries and management services for all members.

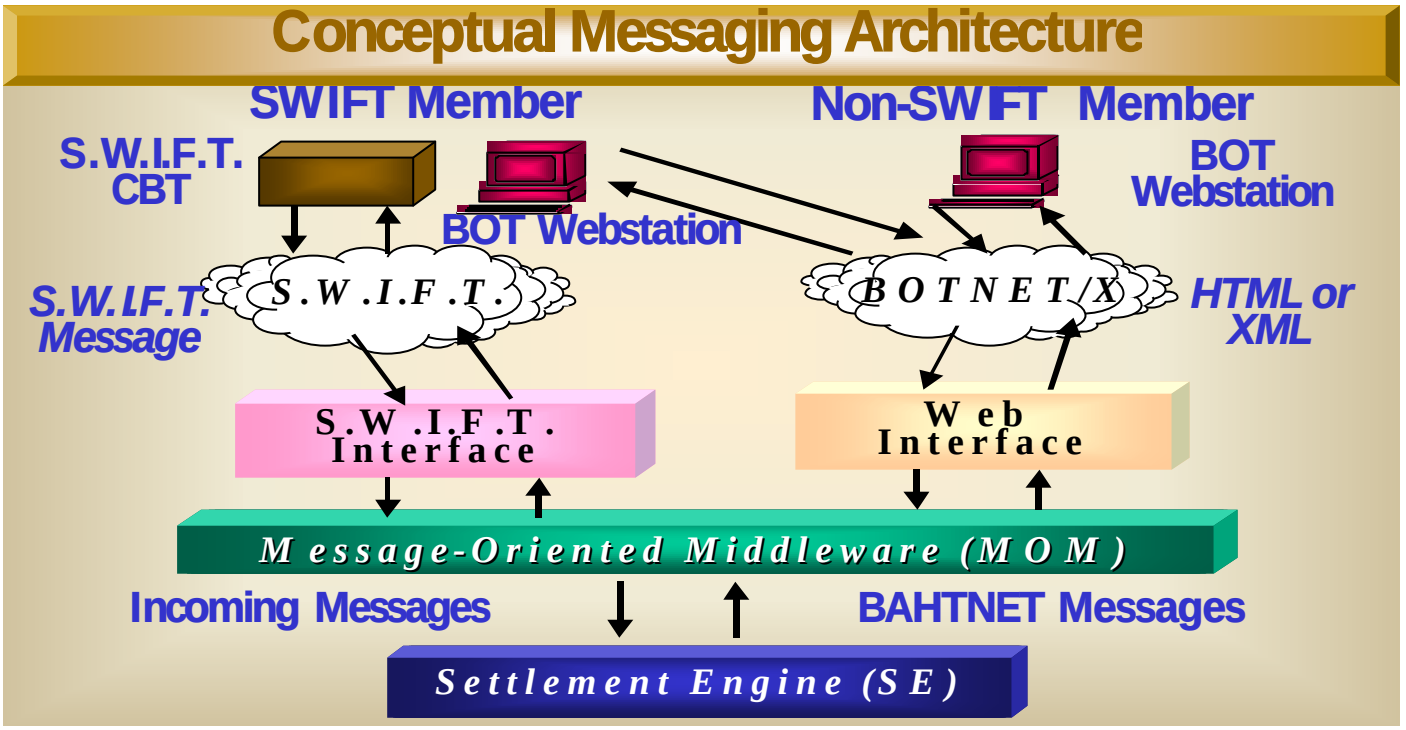


Figure 1 Conceptual Messaging Architecture

B. Factors Affecting the Development

Regulatory Factors

12. Currently, there is no specific legislation governing electronic funds transfer. The lack of a specific law on electronic funds transfer means that electronic payment transactions fail under the Civil and Commercial Code. However, the BOT and other concerned government agencies have been well aware of the rapid pace of technological developments, and hence the need to improve the process of legal framework.

13. Many laws are under development aiming to promote efficiency by encouraging use of electronic payments. The Ministry of Justice and responsible agencies have been in the process of revising the Civil Procedure Code in order to support the admissibility of electronic data as evidence in court. The Electronic Transactions Act, giving the legal recognition of electronic data messages, was enacted in December 2001 and enforced in April 2002. In addition, the National Electronics and Computer Technology Center is currently working on four related legislations. The draft Universal Access Act and draft Data Protection Act are awaiting parliamentary review, while the planned Computer Related Crime Act and Electronic Funds Transfer Act are undergoing the drafting process. The BAHTNET system has been designed to employ sufficient security mechanisms to ensure the integrity and confidentiality of the system and to support the enforcement of new legislation, which would help promote the use of cost-saving means of payments.

Institutional Factors

14. Throughout the development of the BAHTNET system, members and relevant institutions had worked closely with the BOT, which is one of the key factors that drive the project toward the success. The BOT arranged consultative meetings with the BAHTNET Working Group, members and relevant parties on a regular basis. They have shown interest to become involved and actively participated in defining the requirement specifications of the system in cooperation with the BOT. One of their requirements is to allow their internal systems to link with the BAHTNET system.

15. Since major financial institutions already used S.W.I.F.T gateway for their international transactions, they are therefore a key driver behind the use of S.W.I.F.T gateway for their domestic transactions via the BAHTNET system. The use of S.W.I.F.T interface would support compatibility between members' internal systems and the BAHTNET system. This, in turn, fulfills the requirement of members to implement straight-through processing. Consequently, the BAHTNET members would benefit from the elimination of rekey tasks and any human error that may have incurred.

Infrastructural Factors

16. The availability of the network infrastructure either in the form of leased line or dial-up lines is another infrastructure issue that facilitates the connection between the BOT and BAHTNET members either via the S.W.I.F.T gateway or the BOTNET/X (router-based network). The strong relationship between the BOT and the Telecommunication Authority of Thailand has also attributed to the successful network linkage to the BAHTNET Web Service for both primary and back-up site within a limited timeframe.

Technological Factors

17. The constraints of the technology utilized in the previous BAHTNET system do not allow for further enhancement and extension of new services. Since at that point in time the existing technology became obsolete and the previous BAHTNET system has proprietary message format and standards, such features would only allow the settlements between the closed BAHTNET members. Hence, it neither supports

compatibility with members' internal systems nor connection with other payment systems. As a result, the upgrade of the BAHTNET system was required to ensure that the advanced technologies are utilized to develop a secure and efficient infrastructure and to provide flexibility in implementing the STP.

18. Additionally, the enhancement aims to improve the security of the system by adopting the globally accepted methodologies. Public key infrastructure (PKI) and digital certificate are key security devices for user and message authentication deployed in the BAHTNET Web Service. Other security methodologies include secure socket layer, digital signature and firewall being employed to ensure the confidentiality and integrity of the instruction message. In addition, the BOT will validate instructions and verify user rights at the institutional level. With regards to the above, the sufficient security safeguards have been put in place to ensure the safe and sound BAHTNET system.

Social and Political Factors

19. The Ministry of Finance and the BOT recognize the importance of the electronic funds and securities transfer, which provides a necessary infrastructure to support the implementation of the nation's economic policy. Additionally, the infrastructure would provide a basis for the development of the bond market and boost up the business transaction in the financial market. Therefore, the development of the BAHTNET system has been strongly supported and, additionally, the power and authority in overseeing the performance of the BAHTNET system is fully delegated to the BOT.

Economic Factors

20. Due to the vulnerable condition of the economy after financial crisis, the BOT realizes that any failures in the settlement systems would bring hazardous impact to the economy. To ensure financial stability and to reduce settlement risk in the payment systems, the BOT implemented the strategy to encourage the use of RTGS system, including, funds and securities transfers through the BAHTNET system. By developing an RTGS system and enforcing members to settle certain types of business transactions through the BAHTNET system, the financial institutions tend to use lesser amount of risky means of payment, such as, cheques.

Global Factors

21. The BOT's project in developing the BAHTNET system to incorporate both RTGS and DVP process is consistent with the practice of the vast majority of industrialized countries and at the forefront of developing countries. The project would help minimize payment systems risk and hence systemic risk, as well as, enable the complete STP, resulting in the efficiency of the payment system.

II. Policy Concerns, Policy Initiatives and Policy Objectives

22. The BOT pursues the objectives of developing an infrastructure to support the development of the money and capital markets, as well as, promoting efficiency and minimizing risks in the payment system.

A. Developing Nation's Infrastructure

23. Payment systems are a major part of a country's economic and financial infrastructure. They contribute towards promoting economic activity and improving macroeconomic management in the following ways:

(a) Release of funds from the clearing and settlement,
(b) Functions for more productive use,
(c) Reduction of float levels,
(d) Lowering of transactions costs, and
(e) Control of monetary aggregates.

24. The additional real-time DVP system would provide a national infrastructure for the development of domestic government securities market and the use of globally accepted format and standard would ensure that system infrastructure conforms to the best international practice.

B. Promoting efficiency

25. The development of the BAHTNET system enhances efficiency in payment systems which can be viewed as operational efficiency and economic efficiency. First, the payment transactions can be processed in a fast and reliable manner, facilitating the turnover of money in the economy. In technical terms, settlement represented by T, moves from, for example, a two-day settlement (T+2) to a real-time settlement (T+0). This is said to achieve operational efficiency.

26. Second, economic efficiency concerns the promotion of cost-saving means of payment. Thus, as an electronic payment system, the BAHTNET system has the advantages of scale economies, reducing the transaction cost as volume increases, they are more economical than the use of cheques.

C. Reducing risks

27. While an efficient payment system facilitates the flow of funds, potential risks may also arise when payment failures occur, ranging from liquidity shortages to credit problems among participants. Moreover, such risks may develop into systemic risks that are transmitted from one member to another in the system, disrupting the smooth functioning of the payment system and the stability of the financial system. The development of real-time gross settlement and delivery against payment system would ensure that the settlement will be occurred on a transaction by transaction basis. The payment failure would then produce an impact to a lesser extent, reducing the systemic risks of the payment system.

D. Pricing Policy

28. While the BOT has developed the BAHTNET system as a financial infrastructure to increase the efficiency and to reduce systemic risks within the payment system, there is no profit motive. In fact, the BAHTNET fee structure is meant to entice potential electronic funds transfers away from paper-based system. With regards to the setting of service fees charged by member banks to their clients, the BOT lets the market mechanism work freely, recently eliminating the ceiling price level.

III. Key Achievements

A. Replace the Use of Cheque with the Settlement Through BAHTNET System

29. Given Central Banks' objectives in payment systems of reducing risk and promoting efficiency, the development of a large value payment system covering all of Thailand is a logical step. It will assist in the reduction in the usage of cheques for high value payments between banks, between banks and the central bank and between the customers of banks. Reduction in cheque usage reduces the direct cost of cheque processing to the clearing house and financial institutions, the settlement risk inherent in a deferred debit instrument and the opportunity for fraud. By providing a large value payment system with same day settlement, the system liquidity tied up in 'float' (which is a form of credit) will become available for productive use.

B. Enhance Efficiency and Reduce Risk inherent in Securities Settlement Process

30. The BAHTNET system has incorporated the new securities transfer service on a DVP basis. The transfer will be limited to scripless debt securities for which the BOT is the registrar. The transaction of scripless securities transfer in the book entry system amounted to 4,000 million Baht each day on average. With the DVP system, members will be able to make direct transfers to and from their securities accounts instead of the previous procedure of sending documents to the BOT for further processing. Additionally, members can provide securities transfer service for their customers by using custodian accounts or by directly accessing their customer accounts in the settlement agent scheme.

31. In complying with an international practice, the DVP process is to automate the transfer of all types of securities for settlement in order to minimise the use of manual documentation and thereby create process efficiencies, lower costs and position for further automation in the securities trading, clearing and settlement cycle including Straight-Through Processing. In addition, the automation will enable shorter settlement times (potentially from the existing T+2 to T+0), minimise the risk of failed transactions, and decrease the number of high cost cheque and cash-based payments.

32. In addition, the securities transfer is offered as an alternative for the liquidity management of financial institutions. The DVP is expected to boost trading

transactions in the secondary market, which leads to the establishment of benchmark interest rates and to further development of the capital market.

C. Facilitate Liquidity Management and Enhance Convenience and Services

33. As a leading edge RTGS, the designs of the BAHTNET system focus on increasing convenience and service to members and the ability of financial institutions in managing their liquidity needs and cash flow. The design of the BAHTNET Web Service is based on the requirements of members and the environment in which they operate. The system facilitates the connectivity via Proprietary Payment Systems (PPS) and CBTs for S.W.I.F.T members and connectivity via Web browser technology for non-S.W.I.F.T members. With the latest IP technology, users are able to monitor their liquidity status, including, the balance and movement of their current accounts and securities accounts as well as status and details of transactions.

34. In order to accommodate intraday liquidity needs and inherent risks arising from the RTGS system which results in the instantaneous settlement, several mechanisms and facilities have been employed. Queuing mechanism and gridlock resolution are the mechanisms that have been developed to handle the queue of the funds transfer instructions that cannot be settled due to insufficient funds in the sending institution's account. Additionally, intraday liquidity facilities are provided to members on a fully collateralized basis. The BOT allows its members for the unlimited amount of this facility without any charges during the day. The above mechanisms allow members to efficiently manage their liquidity needs and help achieve smooth operation of the settlement process.

D. Conform with International Standards

35. Due to the fact that the BAHTNET, as a national payment and settlement system, is deemed to be a Systemically Importantly Payment Systems, the design and implementation phase have been carefully undertaken with respect to the recommendations of the BIS Core principles. Furthermore, the system also sets a standard for funds and securities transfer by utilizing S.W.I.F.T message type and message format standard, enabling participating institutions to implement Straight-Through Processing according to a widely accepted and global standard. For securities instruction, the format is designed to conform with ISO15022 by applying standard Bank Identification Code and ISIN Code (International Securities Identification Number). Public Key Infrastructure (PKI), which is an international practice for reliable security system, is one of the key methodology deployed in the system. It can be seen that the new mechanisms employed in the BAHTNET system is consistent with the practice of major industrial countries and at the forefront of developing countries.

E. Groundwork For Future Cross-Border Linkage

36. The BAHTNET system lays the groundwork for potential cross-border linkage with other payment systems for PVP of FX transactions as well as the DVP of

securities transactions. This is due to the fact that it is both a RTGS system and it is using S.W.I.F.T message standards and the S.W.I.F.T Network for S.W.I.F.T members. The main rationale behind future linkage across borders is to significantly reduce foreign exchange settlement risk or principal risk. Alternative payment systems incorporate distinguished features and mechanisms, resulting in their own advantages and disadvantages. Other common benefits of cross-border linkage include reducing the costs of risk management, promoting operational efficiency, and enabling members to undertake a greater volume of business with a broader range of counter parties, as well as, facilitating foreign trade and supporting the growth of cross-border settlement.

IV. Impediments Encountered over the Course of the Development

37. With limited timeframe of total 13 months for the development of the BAHTNET project, aggressive work schedules were planned, leaving small room for delay or adjustments. The discrepancies from expected results required immediate decision for adjustment of the schedule plan to ensure successful migration within the target deadline.

38. The cutover of the upgraded BAHTNET system is implemented in a big bang scenario. The previous system was shut down when the upgraded came into operation. Therefore, the BOT must carefully monitor the readiness status of the all members and make assessment of the environment before making a cutover approval, since the setback of even one member would lead to the industry-wide impact.

39. The participants of the BAHTNET system comprise of large number of financial institutions and government bodies. With different characteristics of participants in terms of organizational size, scope of service, experience, and stage of preparation and development, the BOT confronted challenging tasks in preparing all members to be ready for the cutover of the upgraded BAHTNET system.

V. Ways to Overcome the Impediments

40. Project management is one of the critical success factors of the project. Active participation of executives tremendously drives the project to its goals and helps gain well cooperation from related parties and facilitate quick decision making. The steering committee meetings were held on a monthly basis to closely monitor the progress of the project is in line with the work plan and that all the incurring problems receive early attention and being quickly resolved. The well plan of the development project with detailed procedures and assigned responsible person has also contributed to the successful development of the project.

41. Throughout the development of the BAHTNET System, the BOT worked closely with selected vendors, BAHTNET members, and the related internal departments, as well as external organizations. Close cooperation and open communication would allow all related parties to have a clear understanding of their responsibilities and move toward the same goals. The BOT regularly held a meeting with BAHTNET members to explore and define the consensus on the BAHTNET

requirement specifications as well as to monitor their readiness status for the migration to the upgraded BANHTNET system. The project teams have also made site visits to members, who encountered any unsolved problems. Active involvement from relevant parties would allow the project teams to receive useful comments and to reach the best solution among the alternatives.

VI. Challenges and Future Plans

A. Cross-Border Linkage

42. The BOT is keen to support the potential cross-border linkage which would allow a reduction in the settlement risk for PVP of foreign exchange transactions and DVP of securities settlement. Therefore, the payment system committee established a working group to conduct an analytical study on the feasibility and impact of the cross-border linkage with various national payment systems and international payment systems. The working group comprised of the representative from related departments of the BOT, including Financial Institutions Policy group, Monetary Policy Group, Financial Markets Operations Group, Legal Group, Information Technology Group, and Payment Systems Group.

B. Continuous Enhancement of the System

43. The BAHTNET system will be developed on a regular basis in order to respond to the rapid changes of business needs and advanced technology. The enhancement of the BAHTNET system aims to increase efficiency, convenience, and scope of services available in the system and to increase the STP rate as well as to ensure the BAHTNET system stay at the forefront with latest technology. The new requirements are derived from member's comments and related parties' recommendations. The meetings with BAHTNET members will be held from time to time to ensure that members understand and agree with the enhancement as well as to ensure their readiness status for the implementation.

C. Improve Intraday Liquidity Facilities (ILF)

44. The BOT has been currently revising the provision of the intraday liquidity facilities to ensure that the permitted ILF amount reflects the fair market value of the deposited securities and that the BOT will receive the fair price in case member fails to buy back the securities at the end of the day. The new scheme takes into account of the daily mark to market of securities and the reasonable haircut rate, in contrary to the existing scheme which offer ILF funds at 90% flat rate on the face value of the securities. The new scheme is consistently applied to other loan window facilities offered by the BOT, such as, a repurchase operation.

D. Single Window for Government and Private Securities

45. An ideal infrastructure for the Thai securities market is to provide players in the market with the same window for trading and settlement for both government sector and private sector securities. The BOT implemented the BAHTNET system to accommodate the settlement of government sector securities and in the meantime, coordinating with the Thai Securities Depository (TSD) and the Thai Bond Dealing Center (TBDC) for the rationalization of the best infrastructure and linkages in the future. The future consideration aims to support Thailand's competitiveness in terms of risk management and enhanced convenience and efficiency.

HONG KONG: THE FINANCIAL INFRASTRUCTURE IN HONG KONG

I. Introduction

1. The horizontal studies on the financial infrastructure of Hong Kong cover one of Hong Kong's key initiatives in its financial market reform instituted by the Hong Kong SAR Government in 1999. The financial market reform program entails fundamental changes in the market structure, enhancement of the financial infrastructure and, regulatory and legislative reforms across the securities, futures and banking industries in Hong Kong.

2. This report is made up of seven sections. Starting with an environmental analysis on the change drivers, the strengths and weaknesses of the existing Hong Kong financial infrastructure are identified. The financial market reform program is then introduced followed by a recap of the essence of the study of the Steering Committee on the Enhancement of the Financial Infrastructure in Hong Kong ("SCEFI"). A vision for success is then defined for Hong Kong supported by four major SCEFI recommendations. The report is concluded with a section on the lessons to be learned from this cross-sectoral initiative.

II. Environmental Analysis

3. An environmental analysis performed for the Hong Kong financial markets has identified two key change drivers. They are the advent of information technology and the globalisation of financial markets. Whilst the former had bought cost reduction pressure and lead to the development of e-commerce and e-trading, the latter had lead exchanges and clearinghouses to establish strategic alliance on a global scale.

A. Advent of Information Technology

4. Recent developments in the United States demonstrate how relentless improvements in technology can compensate for high costs. The U.S. Department of Commerce's report on "the Emerging Digital Economy II" (June 1999) indicated that the decline in U.S. inflation despite three years of robust GDP growth of 4% per annum was attributable to the massive price declines in the IT-producing industries. For example, in 1997, the falling prices of IT goods and services (a 7.5% decrease) offset the 2.6% price increase for the rest of the economy to give an overall inflation rate of 1.9%. This demonstrates that it is imperative for Hong Kong to use IT to help boost productivity, reduce costs and enhance competitiveness.

5. The exponential growth of e-commerce and e-trading enabled and facilitated by the Internet has brought fundamental and irreversible changes to how businesses are being conducted. The marketplace is no longer bounded by national geography. Traditional franchises are under threat, as new players, especially small and medium sized enterprises, can start up electronically to compete with minimal investment. A

new breed of customers, groomed in the sophistication of the information age and the Internet, demand virtual channels for services.

6. Given such changes, on-line trading in securities has witnessed explosive growth, especially in the United States. By the end of 1998, there were an estimated 7.3 million on-line brokerage accounts; and by mid-1999 this number reached the magnitude of 11 million. More than one-quarter of the trades in Nasdaq and NYSE are now channeled through the Web. In Asia, trading in Korean equities has been stimulated by the emergence of over one million on-line accounts.

7. The rapid advance of e-commerce in recent years has also enabled the creation of a new breed of very powerful, low cost and highly competitive intermediaries, the Electronic Communications Networks ("ECNs") in the securities market (e.g., Instinet, Island ECN), and similar on-line networks in the derivatives market (e.g., BrokerTec). These alternative markets have increasingly eroded significant trading volumes from the traditional markets. For example, by 1999, nine of the ECNs account for about 25% of the total equity trading volume in the U.S.

B. Globalisation of Financial Markets

8. Facing up to these market challenges, exchanges and clearinghouses in many financial centres (e.g., Amsterdam, Sydney, Frankfurt, Singapore) have taken strategic steps to transform into customer-centric and market-driven commercial organizations. Exchanges and clearinghouses also established strategic alliances to better enable their development of cross-market products and to realize economies of scale on their technological investments. Examples of these alliances include the use of the NSC trading system by the GLOBEX Alliance of CME, ParisBourse, SGX and the Brazilian futures exchange BM&F; the use of the Eurex system by DTB/SOFFEX, CBOT & HEX; as well as the merger/ vertical consolidation between Cedel and Deutsche Börse to form Clearstream Banking.

III. Strengths and Weaknesses

9. While Hong Kong has ridden on the advent of information technology in the 1990s by introducing a number of electronic trading and clearing systems in both the securities and banking industries to enhance efficiency and increase productivity, the lack of connectivity and common standards among these systems and others within the economy are obstacles to straight-through processing ("STP").

A. Strengths

10. In March 1990, the Central Moneymarkets Unit was established to provide a computerized clearing and settlement facility to the Exchange Fund Bills and Notes and the facility was subsequently extended to other debt securities issued in Hong Kong. In 1992-1993, the Stock Exchange of Hong Kong launched its modern Automated Order Matching and Execution System (AMS) for securities trading. The Central Clearing and Settlement System (CCASS) was also launched during this

period by Hong Kong Securities Clearing Company Ltd. to help reduce risk and improve the efficiency of securities settlement. In December 1996, the Hong Kong Monetary Authority (HKMA) introduced the Hong Kong dollar Real Time Gross Settlements (RTGS) System, one of the most advanced interbank payment system in Asia. The Stock Exchange developed a new generation of securities trading system - AMS/3 - in 2000, while the Hong Kong Futures Exchange migrated from the open out-cry market to a full electronic trading system in the same year. In August 2000, the HKMA launched an US dollar RTGS system to facilitate efficient settlement of US dollar transactions in Hong Kong and the region. In addition, the Government has embarked on the journey of the "Digital 21" strategy and the Electronic Service Delivery initiative.

11. Despite these strengths and achievements, Hong Kong cannot afford to become complacent. Many economies in Asia and the Pacific have also embarked on the journey to build or upgrade their infrastructures, based on modern and e-commerce enabled technology. The China's National Automated Payment System (CNAPS), the Korean Information Highway, the Malaysian Multimedia Super Corridor (MSC), and SingaporeONE are examples of responses to the challenges outlined above.

B. Weaknesses

12. Key obstacles for implementing STP in Hong Kong were identified by various studies and reviews. They include, inter alia:

(a) Lack of connectivity among market participants,

(b) Inadequate deployment of best practice procedures among industry participants (e.g., different timing and procedures for trade confirmation and amendments),

(c) Lack of standards for data communication,

(d) Lack of timeliness and completeness of settlement instructions to custodians,

(e) Varying standards from country to country (e.g., tolerance limits),
(f) Inaccessibility or unavailability of standing settlement instructions,

(g) Manual pre-matching processes, and

(h) Lack of support for efficient use of consistent static data (e.g., standing delivery instructions).

13. SWIFT was commissioned to conduct an STP audit of the savings that could be achieved if Hong Kong's securities sector maximizes STP in 1999. SWIFT estimated that the cost (from payroll alone) of non-STP associated with SWIFT messaging was approximately US$600 million globally per annum. Hong Kong's SWIFT STP rates of 40-45% were comparable with those of Singapore, but were

below those of Australia and Japan. Based upon a limited STP audit of users in Hong Kong, SWIFT estimated that the Hong Kong financial market could save between US$15-20 million (from payroll alone) per year by attaining 80% STP rates. Since SWIFT accounts for an estimated one-half of securities settlement instructions messaging in Hong Kong, the true savings, including rent and other overheads, could be as much as double that to US$30-40 million.

IV. Market Reform Program

14. A market reform program, as a result, was instituted by the Hong Kong SAR Government in 1999 to overcome such weaknesses.

15. In his Budget Speech on March 3, 1999, the Financial Secretary of the Hong Kong SAR Government announced a comprehensive financial market reform to strengthen Hong Kong's competitiveness and to enable Hong Kong to remain in the premier league of international financial centres.

16. The Financial Secretary recognized, while Hong Kong's securities and derivatives markets have achieved tremendous growth and success in the last decade, recent developments in the global market, such as the rapid advent of the e-Economy, emergence of alternative electronic trading systems, increasing sophistication of investors, and the globalisation of markets and investments, have created increasing competition and challenged the position of Hong Kong as a leading regional and international financial centre.

17. Responding to these global market challenges, the Financial Secretary announced a three-pronged reform program for the securities and futures markets in Hong Kong:

(a) Fundamental change in the market structure accomplished through the demutualization and merger of the exchanges and clearinghouses;

(b) Enhancement of the financial infrastructure to improve risk management, increase efficiency, and reduce cost; and

(c) Regulatory and legislative reform to improve the supervisory framework and protection of market participants.

V. The SCEFI Study

18. To address the strengthening of the technology base in the securities and futures market, the Financial Secretary appointed the SCEFI in March 1999 to study and recommend the necessary improvements to Hong Kong's financial infrastructure.

19. The SCEFI study aimed to specifically address the following issues with the objective of enhancing the competitiveness of Hong Kong as an international financial centre in terms of risk management, increased efficiency and cost reduction:

(a) Setting up a single clearing arrangement for securities, stock options, futures and other exchange-traded transactions;

(b) Enhancing the financial technology infrastructure to facilitate straight-through processing of transactions across financial markets;

(c) Moving towards a secure, scripless securities market; and

(d) Building a robust technology infrastructure.

VI. Vision for Success

20. SCEFI put forward a future vision for the Hong Kong financial markets as an integrated global market as shown in Figure 1.

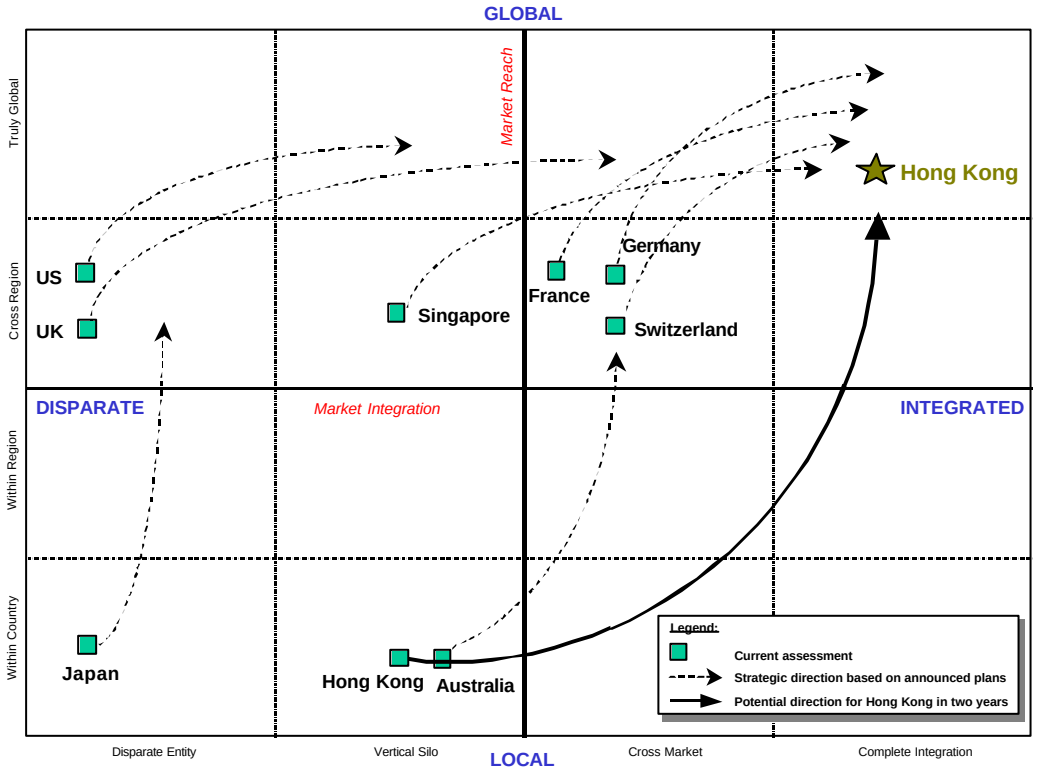


Figure 1: Vision for Success

21. The vision of an e-Economy that Hong Kong should embrace is that of an infrastructure that allows local and global market participants to access the full spectrum of financial products and services, which are interconnected by an open, robust, secure, scalable and high performance network. Within this infrastructure, transactions are processed electronically and straight-through (i.e., without human intervention and rework), and electronic documents (e.g., contract notes) are readily

accepted. This infrastructure will not only provide market participants with a wider choice of products and faster and better services, but also allow transactions to be executed securely at lower cost and with reduced risks.

22. With this vision in mind, SCEFI has observed the following guiding principles in defining Hong Kong's target financial infrastructure:

(a) Achieving risk management excellence;

(b) Maximizing the possibility of STP;

(c) Ensuring instantaneous finality and legal certainty of transactions;

(d) Complying with international standards and suitable best practices;

(e) Seeking strategic partnerships with leading financial centres; and

(f) Embracing open and web-enabled technology for universal connectivity and continuous innovation.

VII. SCEFI Recommendations

23. To achieve the future vision, the enhanced financial infrastructure of Hong Kong must include four components:

(a) a single clearing arrangement for better risk management,

(b) end-to-end straight-through processing for improved cost-effectiveness,

(c) a scripless securities market for enhanced efficiency and legal certainty, and

(d) an open, robust and scalable technology structure for local and remote connectivity and high performance.

A. Single Clearing Arrangement

24. A single clearing arrangement for the securities and futures markets is the foundation for Hong Kong to achieve risk management excellence – an attribute that is vital for attracting global investors to the Hong Kong market. Increasingly, investors will migrate to those markets that guarantee the finality of trade settlement, provide prudent and transparent practices for risk management to best international standards and improve their liquidity across markets and products. The increasing trend of demutualization and merger of exchanges and clearinghouses globally is indicative of this market imperative.

25. A single clearing arrangement will provide the following key benefits to Hong Kong:

(a) Improve risk management (of systemic risks) for market participants, exchanges, clearinghouses, and regulatory authorities by providing a holistic view of risks across markets, products and users;

(b) Simplify and improve the efficiency of money settlement. Reduce the settlement and liquidity risks by clearing through the inter-bank RTGS; and

(c) Allow more efficient use of capital and liquidity through unified money settlement, cross-margining and cross-collateralization.

B. Straight Through Processing

26. Processing inefficiencies generate risks and increase costs. STP involves electronically capturing and processing financial transactions in one pass, from the point of first "deal" to final settlement and confirmation. Current practices involve costly multiple data re-entry from paper documents and other sources that are susceptible to errors, discrepancies, delays and possible fraud.

27. In order for Hong Kong to strengthen its competitiveness in an increasingly global securities marketplace, it is imperative that it continues to focus on eliminating inefficiencies (e.g., reworked transactions and failed deliveries) that increase costs and risks.

28. STP requires:

(a) A robust financial infrastructure that links the main exchanges and clearinghouses together;

(b) Cooperation with the regulatory and tax authorities in ensuring that electronic data/documents and electronic signatures are legally acceptable;

(c) Uniform computer protocols and message standards that are in compliance with best international standards; and

(d) Cooperation between the different market participants and users to ensure that common practices are established and followed.

C. Scripless Securities Market

29. A scripless securities market provides the enabling environment for STP, eliminates the risks associated with paper scrip, reduces the cost of ownership transfer and enhances the processing efficiency of securities transactions.

30. The enactment of the Electronic Transactions Ordinance in Hong Kong in early 2000 has provided legal standing and protection to electronic documents (e.g.,

contract notes, instruments of transfers), records (e.g., Registers of Members), and signatures. This legislation provides a necessary first step towards a scripless market.

31. Through STP, the scripless securities market structure will also provide significant opportunity for efficiency improvement and cost reduction for non-trade activities, such as eIPO and corporate actions.

D. Robust Technology Infrastructure

32. To compete and prosper, Hong Kong's enhanced financial infrastructure must be anchored on technologies and architectures that are open, robust, secure, scalable and supportive of continuous innovation. Such technologies help to remove barriers to entry and makes it easier and more convenient for anyone to participate in the market from anywhere at anytime. A single clearing arrangement, an STP operating environment and a scripless securities market will not become a reality without such world-class technology structure in place.

33. The vision of a robust technology structure for Hong Kong's enhanced financial infrastructure encompasses the following best practices and international standards:

(a) Support unified and open access for trading and clearing of securities and futures;

(b) Provide an integrated platform for risk management and STP for all markets and products;

(c) Enable connectivity and interoperability with standard interactive and message-based interfaces;

(d) Adopt best-of-breed approach or use proven solutions provided by leading players; and

(e) Provide a unified, secure, high performance and high resilient network, enabling both local and remote open access.

34. In relation to the above attributes, the concept of *FinNet* (*Fin*ancial *Net*work) was put forward. It is a secure, open, scalable and high performance community network built to interconnect all financial institutions including securities, futures, banking, insurance and all other licensed financial entities in Hong Kong, to effect STP and ultimately real-time financial transactions such as delivery versus payment. The rationale behind is to integrate many systems/ networks into a hub by utilizing a single technology platform called *FinNet* as shown in Figure 2.

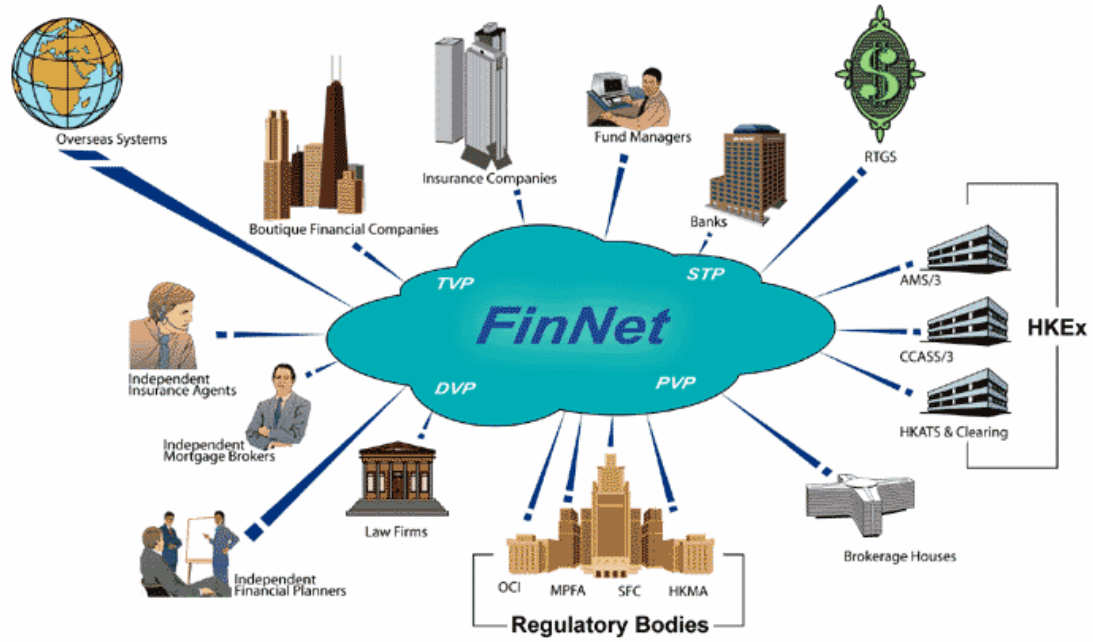


Figure 2: The Concept of *FinNet*

VIII. Lessons to be Learned

35. The enhanced financial infrastructure calls for changes in the existing business practices and relationships among various stakeholders. For example, market participants would be permitted to participate across markets, contract notes would become electronic, and legal certainty would be granted upon settlement of transfers in the CSD, etc.

36. Appropriate updates, therefore, need to be made to the related legal and regulatory framework to enable these changes. The key legal and regulatory changes required are summarized as follows:

(a) To set up a single clearing arrangement, relevant legislation and exchange rules need to be amended to permit cross-market participation and to be consistent with the rules on the issuance of trading rights. The merged clearinghouse needs to be recognized by the SFC and the legal structure for cross-market risk management needs to be established;

(b) To achieve STP, new contractual relationships between the STP counter-parties need to be established. Enactment of the Electronic Transactions Ordinance in Hong Kong has provided legal standing and protection to electronic documents and signatures. Pre-agreed collection arrangements need to be made with the Inland Revenue Department and registrars on the collection of stamp duty on off-exchange transfers; and

(c) To transform into a scripless securities market, the Companies Ordinance needs to be amended to accommodate the dematerialization of shares. Legislative changes by overseas authorities are envisaged for dematerializing issues of companies incorporated overseas. The

mechanics as well as the legislation of the new arrangements to facilitate and protect the creation, holding, transfer and exercise of security interests (in particular equitable interests) in scripless issues will have to be worked out.

37. The Hong Kong SAR Government and the SFC have important roles to play in driving and expediting the appropriate updating of the legal and regulatory framework. For example, the Government is instrumental in driving the enactment of the Electronic Transactions Ordinance, the amendment of the Companies Ordinance to accommodate dematerialization of issues, introducing any necessary statutory provisions in order to clearly recognize and protect property rights in scripless issues, making arrangements for stamp duty collection on electronic registration of transfers and the simplification of stamp duty calculations. The SFC also plays a crucial role in sanctioning the setting up of the single clearing arrangement, the new roles of the CSD and new registration model and in facilitating the dematerialization discussions with overseas authorities.

Final Note

38. The above discussion and illustration are what Hong Kong considered as the best for its economy. Other markets might need to take into account their own circumstances.

SINGAPORE: E-GOVERNMENT - THE PUBLIC E-SERVICE INFRASTRUCTURE (PSi) & E-PAYMENT CAPABILITIES

I. Aim

1. This case study presents an overview of the Singapore Government's Public e-Services Infrastructure (PSi), with a specific emphasis on its e-payment capabilities.

II. Overview of E-Government Efforts in Singapore

2. The Singapore Government recognises that the nature of public services needs to be fundamentally different in the digital era. First, as citizens become exposed and accustomed to the speed and quality of services offered on the Internet, they will increasingly expect Government services that are available anytime, anywhere, and designed in a way that suits their **convenience**. The challenge for Governments is to harness infocomm technology (ICT) to offer the same 24/7 availability, fast delivery, customer focus and personalisation in their services. By adapting and applying the same technologies and principles that are fuelling the e-business revolution, we can achieve a similar transformation in public services.

3. Second, we see e-Government as a means of **reducing Government's complexities** for our customers – citizens and businesses alike. With more than 100 public sector agencies in Singapore, dealing with the Government can sometimes be a time-consuming and frustrating affair. This is due to the fact that while the Government is vertically organized, the needs of our customers are often horizontal in nature and cut across a few agencies. By leveraging on web portals that organize services according to the needs of users rather than agency lines, e-Government enables us to hide Government's complexities and provide customers with a single points of access and service delivery. Since the launch of eCitizen – the Singapore Government's main web services portal – in 1999, the number of e-services has increased from 120 to more than 400 today.

4. Third, e-Government helps to **reduce costs** and make tax revenues go further. The cost savings are partly the result of internal process improvements that e-Government brings, but also the result of electronic service delivery being cheaper than traditional forms of service delivery, e.g. mail, customer service counters.

5. The strategic importance we place on e-Government was reflected in the S$1.5bn investment in the e-Government Action Plan over a three year period beginning in Jun 2000. The Action Plan has six strategic programs:

(a) Knowledge-based workplace: this program aims to empower public officers as knowledge workers who engage in active and collaborative learning and knowledge sharing.

(b) Electronic Service Delivery: this program seeks to provide a one-stop interface with the public through the integration of services offered by public sector agencies. The PSi project puts in place a common

infrastructure that will facilitate the seamless integration of front-end services with the back-end systems of public sector agencies so that services can be developed and deployed quickly.

(c) Technology Experimentation: this program seeks to foster creativity and experimentation in the adoption of new technologies.

(d) Operational Efficiency Improvements: this programs aims to identify and invest in new infocomm projects as well as to review, re-design and re-engineer systems due for replacement.

(e) Adaptive and Robust ICT infrastructure: this program focuses on service-wide infrastructure projects that are scalable, robust and cost-efficient.

(f) Infocomm Education: the ICT education program targets all levels of the public sector and facilitates the participation of public servants in the process of "re-inventing Government".

6. The e-Government Action Plan is driven by the Ministry of Finance's Managing for Excellence (MFE) Office. The office spearhead public sector-wide ICT initiatives in partnership with the Government Chief Information Office (GCIO) of the Infocomm Development Authority (IDA) and other public sector agencies.

III. The Public E-services Infrastructure (PSi)

7. The major challenge facing most e-Governments today is the delivery of "complete", end-to-end services in a seamless, integrated fashion. The challenge is increased where the service cuts across a number of government agencies. The Singapore Government's PSi was conceived to help public sector agencies deal with the complexity of developing and deploying e-services, especially cross-agency ones. As a public-sector wide project, PSi is able to reap economies of scale, and reduce the costs of implementing e-services. More critically, it offers a simplified development and delivery environment in which government agencies are able to delegate many issues to the safe hands of PSi. These include:

(a) **Security**: PSi provides a secure environment that insulates e-services on PSi from many potential security attacks/breaches.

(b) **Reliability**: PSi has high availability, an expensive process requiring significant planning, operations management and redundancy.

(c) **Speed and Ease of Deployment**: PSi enables rapid deployment of e-services using intuitive tools that are easy to use

(d) **Economy**: By aggregating demand, PSi is able to benefit from economies of scale and reduce the cost of development and delivery of e-services.

(e) **Scalability**: PSi is designed to be scalable, accommodating both its own growth as well as the growth of the government agencies' e-services, without disruption to the capabilities of existing e-services.

(f) **Upgrading**: PSi is designed in a way that allows for upgrading without affecting the capabilities of existing e-services deployed on PSi. This allows for better features to be incorporated into PSi without affecting service levels.

8. PSi is an enterprise level amalgam of hardware and software designed to deliver a complete infrastructure for the development and delivery of e-services. The design of PSi consists of:

(a) The *e-Service Generator* features a complete design environment which enables users (i.e. public sector agencies) to create e-services using simple tools. These e-services are then hosted on PSi, and will go through a standard software development lifecycle of development, testing, quality assurance and finally production.

(b) *EDX (Electronic Data Exchange)* provides e-services hosted on PSi with the ability to integrate with back office/legacy data systems, resulting in better services to the end customer.

(c) *Authentication and Authorization* enables PSi to differentiate users and grant access levels based on the user's credentials. This is also extended to end users accessing PSi-hosted e-services. In addition, numerous authentication methods are available, ranging from simple user password to public key infrastructure (PKI) authentication.

(d) The *System Management Console* provides backend management facilities through a clean and efficient web browser interface, enabling authorized users to manage their e-services.

(e) The *Payment Module* enables e-services to effect on-line payment transactions in a secure and reliable manner. The Payment Module has the capabilities to accept new forms of payment methods developed by financial service providers and adding them as additional payment options for customers.

(f) The *Intermediate Zone* provides a means to host databases on PSi, enabling e-services to access and update data in an efficient manner. Agencies are able to choose deployment of the databases in this Intermediate Zone or in their own backend systems and connect to them via EDX services.

9. Another key strength of the PSi, besides its aggregation of demand, is its ability to de-couple the common services required by most e-services and deploy them in a standard interface understood by all e-services deployed on PSi. This dramatically improves the speed and efficiency of developing an e-service. Such common services, which include payment, authentication and back end database

integration, are carefully designed to cater to the largest possible number of scenarios. PSi can be thought of as a step beyond a specialized Application Services Provider. It provides a *complete* environment to create application services by utilizing tools and common services and then deploying them.

IV. E-payment Services on PSi

10. The payment options available for e-services are often critical in determining how mature and useful that service is to its customers. At its most basic, a service could just offer information on the Internet – this is commonly referred to as "publishing". Some go further to offer on-line forms that can be filled up and sent to the agency, referred to as "interacting". An e-service has "transacting" capabilities when users can complete the entire application on-line, e.g. renew a driving license, register for a course, and pay fines or bills. For e-Government to reap its full potential, services that require two-way interaction between the public sector agency and the customer should be available at the "transact" level. This usually requires the availability of convenient and low-cost on-line payment mechanisms that allow customers to complete their transactions on-line.

11. The ability to securely and reliably effect payment with a few keystrokes revolutionizes traditional modes of payment, offering levels of convenience and efficiency previously thought impossible. PSi offers the latest payment methods as a *common service* to the e-services hosted on it. The e-Payment module features a number of key capabilities. First, it shields technical complexities from designers of e-services, and provides a reliable and secure environment utilizing the latest industry-standard security features. Second, it provides appropriate reports for service/product fulfillment, reconciliation and dispute settlement. Third, its plug-in architecture allows PSi to link with various e-payment service providers to effect a smooth transaction, while maintaining the payer's confidentiality. This is possible as PSi transfers control to the service provider for authentication and is not privy to any password or authentication details that the payer provides. Fourth, PSi is extensible in that it allows future payment mechanisms to be added without disruption to its other functions and the e-services hosted on it. Finally, PSi aggregates payment requirements from all its e-services, and so allows users to benefit from lower transaction costs.

12. Currently, PSi has the following methods available for electronic payment:

(a) *NETSCash*: Utilizing the cash card (smart card encoded with cash value) with a cash card reader, users are able to fulfil payment instantly on-line.

(b) *Credit Card Payments*: Payments using major credit cards, such as Visa and MasterCard are supported on PSi, with the Development Bank of Singapore (DBS) being the processing bank for the credit card transactions effected.

(c) *Internet Direct Debit*: Making payment with an Internet banking account is possible on PSi. Currently, anyone with an Internet banking account with DBS is able to perform a direct debit payment transaction with e-

services on PSi. This mechanism will be made available to the Internet banking account holders of other banks when they are ready to offer such services.

V. Current Challenges

13. The existing set of payment options on PSi is by no means complete. Payment by cash card is not attractive to customers who do not already possess a smart card reader. It is also limited by the maximum stored value of cash cards of S$500. Payment by credit card is relatively expensive – it costs the Singapore Government 1.85% (of the transacted amount) in commission charges each time a credit card transaction is effected. Credit card payments are also less secure and for this reason, we have limited credit card payments to less than S$500. Internet direct debit is a promising e-payment option now available in the market. It is a suitable payment method for almost all amounts, and currently levies a relatively low transaction fee of S$0.50 per transaction. However, it is currently limited to the customers of one bank.

14. The challenges that PSi faces with respect to e-payment are as follows:

(a) **Enabling multi-bank payments:** A natural extension of the current Internet direct debit option is to enable users with Internet banking accounts from *any* participating bank to perform payment transactions on the Government's e-services. A key issue here is inter-operability between the various e-payment solutions in the market. We are currently in the process of implementing one of these multi-bank options on PSi, and evaluating another for suitability.

(b) **Introducing GIRO-on-Demand**: GIRO (or inter-bank fund virements using an automated clearinghouse system) is already an extensive payment method available to almost all Singaporeans with a bank account. Implementing a GIRO-on-Demand facility on PSi will allow it reach out to a much wider target audience than only those with Internet bank accounts as it can be used by anyone with a bank account. It is not real time and settlement is done on T + 2. However, most government payments do not need real-time settlement, as unlike e-commerce it does not involve sales of goods but payments of Government bills and licences.

(c) **Virtual Wallet:** PSi will be evaluating a virtual wallet payment method offered by a local service provider as a possible future payment option.

15. Besides introducing more e-payment options on PSi, the Singapore Government has also embarked on a project to present consolidated government bills to members of the public and to collect consolidated payments on-line. When rolled out, PayPoint will offer the public a single point of access to various government fees, charges and fines. The customer can also choose to pay on-line using the various e-payment modes available on PSi, e.g. cashcard, credit card, Internet direct debit and Giro-on-demand. Furthermore, the customer needs only to supply and update his

personal information once, due to data exchange and information sharing within PayPoint.

16. From the Government's perspective, PayPoint will reduce the duplication of work for public sector agencies arising from each of them managing and maintaining its own billing, collections, accounting, tracking and enquiry systems. It will also reduce costs for Government, as agencies would no longer have to incur large expenses and developmental time in establishing or upgrading their proprietary systems. Moreover, they will benefit from the experience and reliability of the service provider that will aggregate the various fees and charges being levied by Government.

VI. Conclusion

17. PSi is a provides the necessary infrastructure and tools that enable the rapid deployment of e-services without the need for the service owner to handle complex issues such as system availability, security, reliability, connectivity and scalability. It provides a suite of common services widely used by most e-services, enabling the Government to reap the benefits of increased efficiency and scale. With highly developed payment capabilities, PSi also enables on-line payment for all e-services requiring such capabilities in an efficient and cost-effective way.

Australia: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to Finance and E-finance

- There is no separate legislation covering e-finance. Existing laws have been amended to cover it with the exception of the *Electronic Transactions Act* (see below)
- *Banking Act 1958* - licences banks to operate in Australia
- *Financial Sector Reform Act (FSR) 2001* and several recent amendments. From 1 July 1998 a new financial regulatory framework came into effect. Under the new structure a single prudential supervisor, the Australian Prudential Regulation Authority (APRA) took over responsibility for the supervision of banks, life and general insurance companies and superannuation funds. The Australian Securities and Investments Commission (ASIC) assumed responsibility for market integrity and consumer protection across the financial system.
- *Electronic Transactions Act 1999* (based on UNCITRAL Model law) - regulates the use of electronic signatures, and therefore the definition and legality of contracts created in e-commerce. Each State & Territory has enacted, or is enacting, complementary legislation.
- *ASIC Act 2000* gives ASIC functions in consumer protection. It is responsible for market integrity and consumer protection by promoting and monitoring the adoption of and compliance with approved industry standards and codes of practice, including promoting sound customer-banker relationships.

Are any special licenses or permits required for E-finance business?

- None

1.2 Laws and regulations related to Cross-Border transactions

- There are no special laws relating to cross-border financial transactions (no separate Foreign Exchange Law)
- Residents may hold accounts abroad (there are tax implications but no other legal obligations).
- Residents may freely transfer money abroad and bring money into Australia although it is not yet possible to make Internet banking transfers between domestic and foreign bank accounts (it appears this is a limitation of the payments system used by banks, rather than of legislation).
- It is possible to buy and sell foreign listed securities via listed brokers and (as shown below) it has recently become possible to do this on the Internet via the link between Australian Stock Exchange and the Singapore Stock Exchange.

1.3 Laws and Regulations for Consumer Protection in E-finance

- There are no special laws relating specifically to consumer protection in e-commerce generally or in e-finance. The existing consumer protection laws are considered to cover Internet business. (There are a number of specific laws relating to other aspects of the Internet such as the *Cybercrime Act 2001*, *Telecommunications (Interception) Act 1979), and Interactive Gambling Act 2001.* The government's overall policy is in principle to support self-regulation backed up by a legislative framework.
- *Trade Practices Act 1974* – is the main consumer protection legislation. The consumer protection provisions of the Trade Practices Act are found in Parts IVA, V and VA of the Act. Part IVA contains provisions dealing with unconscionable conduct. Part V prohibits a number of unfair practices, and also covers conditions and warranties, and product safety standards and information. Part VA relates to the liability of manufacturers and importers for defective goods. The provisions apply equally to business on the Internet. The consumer protection provisions prohibit unfair practices such as: misleading and deceptive conduct; false representations; misleading statements; harassment and coercion; bait advertising; referral selling; and pyramid selling. There are also provisions relating to unsolicited goods and credit cards.
- *Privacy Act 1988* and the *Privacy Amendment (Private Sector) Act 2000* (the Amendment Act). This amendment extends the application of the Privacy Act (which previously mainly covered public sector agencies) to most private sector organisations as well. The Privacy Commissioner is empowered to investigate privacy complaints against private sector organisations. The new scheme came into effect for most organisations covered by the *Privacy Act* on 21 December 2001. It has 10 standards for handling private information, based on OECD Guidelines on the Protection of Privacy. It applies to information held both on-line and off-line. It prohibits unsolicited marketing (and therefore spamming) when obtaining permission is "practicable". This is considered to be the case for email approaches, so spamming would likely be considered a breach of the National Privacy Principles.
- *Uniform Consumer Credit Code* (UCCC) is the main code affecting finance. The legislation is based on the principles of truth-in lending which will allow borrowers to make informed choices when purchasing credit. The Code applies rules which regulate the credit provider's conduct throughout the life of a loan, but without restricting product flexibility and consumer choice. The policy of the legislation is to rely generally on competitive forces to provide price restraint but to provide significant redress mechanisms for borrowers in the event that credit providers fail to comply with the legislation. The Code is designed to apply to a deregulated credit market and provide standards for the provision of credit which will not be overtaken by changes in the financial marketplace.The legislative structure of the Code is based upon a template scheme. This means that template legislation has been passed (in Queensland: Consumer Credit (Queensland) Act 1994 and Consumer Credit (Queensland) Regulations 1995/6).Other States and Territories have passed enabling legislation which adopts the template legislation and applies it in the State or Territory as "in force from time to time".

What types of Internet activities would be prohibited by the legislation?

- Sale of unsolicited goods and services – consumers would be protected. Also the use of private data to make sales approaches is likely to be limited under the legislation.
- Misleading statements and unconscionable acts – the provisions would apply to Internet in the same way as to other sales.

Are there any laws and regulations related to data protection (particularly private information)?

- Data protection is covered in the Privacy Act.

2. Self-regulation and Codes of Practice

2.1 Codes of Practice

- The model in Australia has been for government to take a leading role in drafting model guidelines which are then adopted by industry groups. In the case of the *Electronic Funds Transfer Code* (see below), the rules are mandatory.
- The *"Policy Framework for Consumer Protection in E Commerce"* and the practical guidelines for business set out in "*Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business (BPM)"* (May 2000), were drafted by Department of Treasury – Competition and Consumer Policy Division, which is the main body responsible for consumer protection policy. The BPM was based on the OECD *"Guidelines for Consumer Protection in the Context of Electronic Commerce"*, 1999. The BPM encourages businesses to provide information to consumers identifying themselves and setting out terms of transactions. The BPM also supports the "opt-in" approach for commercial email.
- Banking Industry Ombudsman - sets codes of good banking practice and has some powers to handle disputes .
- *Electronic Funds Transfer (EFT) Code* came into effect on 1 April 2002. It was developed by a working group of government, industry and consumer representatives and is a voluntary code which protects consumers transferring funds electronically. It sets out the disclosures consumers must receive before they first use a new form of electronic banking; the information consumers must receive on receipts; liability for unauthorised transactions and system or equipment malfunction; protection of a consumer's privacy; complaints investigation and dispute resolution processes (more information is available on ASIC's website).
- The Government also set up an independent Taskforce on Industry Self-Regulation which reported in Dec 2000, and established the website www.selfregulation.gov.au .

2.2 Trust Mark/Seal of Assurance Schemes

- There is no government sponsored Trust Mark scheme, although the government recommends the Best Practice Model as a basis for trust mark schemes.

- Some private schemes exist e.g Westpac Bank has a scheme for identifying approved companies.
- Credit card companies mostly operate "charge back" schemes to cover customers against fraud and theft. This also covers Internet transactions.
- The privately-owned ADRon-line (see below) symbol may be used by Internet retailers who are committed to the resolution of customer disputes either directly, or through one of the independent services provided by ADRon-line.

2.3 Dispute Resolution

- *Financial Services Reform Act* (FSR Act) now requires financial institutions to provide customers with access to internal and external dispute handling procedures. Previously this was required by the *Banking Code* (which was voluntary, but is now mandatory). The requirements under the FSR Act are based on Treasury *"Benchmarks for Industry-Based Customer Dispute Resolution Schemes"* which recommend accessibility, independence, fairness, accountability, efficiency, effectiveness, and outside scrutiny.
- The Government (Treasury) issued *"Discussion Paper: Dispute Resolution in Electronic Commerce"* in October 2001. The Discussion Paper served as a basis for discussion of the importance of dispute resolution mechanisms in B2C e-commerce. It also aimed to collect data on the nature and extent of e-commerce complaints. The consultation period ended in February 2002.
- Within Australia there are several privately operated dispute resolution schemes. One example is ADRon-line Pty Ltd, that is a private company offering Alternative Dispute Resolution services to industry and consumers generally, as well as B2B, B2C and B2G e-commerce markets. It offers a settlement service – more details at http://www.settlementon-linesystems.com.au – and a mediation service at www.mediateon-line.com.au where the dispute can be resolved through the mediation process. Their system operates by having merchants identify themselves as offering third party, neutral dispute resolution to its customers i.e. a trust-mark scheme as well as ADR. It also allows consumers to request resolutions with non-registered companies.
- The National Alternative Dispute Resolution Advisory Council (NADRAC) is an independent advisory council charged with providing the Attorney-General with policy advice on the development of methods of resolving disputes without the need for a judicial decision. It covers the whole area of ADR, not just on-line.
- Australia (through the Competition and Consumer Division of the Treasury) participates in the OECD Committee on Consumer Policy, including its Working Group on ADR in cross-border disputes. It also participates in the APEC ECSG Group on Consumer Protection in E-commerce, which is working on similar principles to those of the OECD group.

3. Enforcement System

- E-finance problems which are pursued under the *Trade Practices Act 1974* (e.g. misleading advertising, unconscionable conduct) would be enforced by the ACCC

- a statutory authority responsible for ensuring compliance with the *Trade Practices Act 1974* and the provisions of the Conduct Code.

- Problems with a domestic financial institution would be enforced by ASIC, which is responsible for enforcement of consumer protection laws in financial services and products covering investments, superannuation, life insurance, general insurance and bank deposit taking (but not lending).
- For problems under the *Privacy Act 1988* the Federal Privacy Commissioner is able to assist consumers who have complaints regarding Commonwealth or ACT government agencies, consumer credit reporting activities, tax file numbers and spent convictions. Where the Privacy Commissioner forms the view that there has been a breach of the *Privacy Act*, the respondents may be required to undertake actions which can include a written apology, retraining of staff, changing procedures, amending or deleting personal information. Occasionally monetary compensation may be offered to compensate the individual for any loss or damage they have suffered. In a very small number of complaints where the respondent is unwilling or unable to adequately resolve the complaint, the Privacy Commissioner has a power to make a complaint determination either dismissing or substantiating the complaint.
- The Hague Conference on Private International Law convention on international jurisdiction and foreign judgements in civil and commercial matters provides the basis for Australia's approach to cross-border cooperation.
- The ACCC is identifying test cases to clarify problems in enforceability of foreign judgements and cross-recognition of judgements from foreign courts.
- Australia participates in the International Marketing Supervision Network (IMSN) and in *eConsumer*, which is a pilot project run by the IMSN http://www.econsumer.gov. *eConsumer* focuses on cross-border e-commerce B2C transactions, and provides an on-line portal for consumers to obtain information about the approaches to enforcement of consumer protection law within the participating countries, and to make a complaint on-line. Consumers consent to this information being viewed and used by the law enforcement agencies which participate in *eConsumer*. The consumer web page is supported by a secure database accessible only by participating agencies. The project is intended to facilitate dialogue between agencies and to streamline investigations of complaints with an international dimension.
- The ACCC has co-operation agreements with overseas agencies covering information sharing and enforcement co-operation(with US FTC, NZCC, Canada Competition Bureau, PNG Consumer Affairs, Taiwan FTC) and is a member of International Marketing Supervision Network. The Consumer Sentinel database operated by USFTC provides shared information on consumer complaints.
- ASIC participates in international regulatory groups on e-commerce particularly through the IOSCO Internet Task Force.

4. Cases

4.1 Consumer Education

Millennium Bug Insurance Scam

- Australian finance regulator ASIC delivered consumer education through a spoof website in 1999. The April Fool's joke convinced more than 233 people to part with more than AU$4 million over the Internet. The fake investment site claimed investors could triple their money in 15 months if they invested in Millennium Bug Insurance (MBI). Over a period of a month, 10,200 people visited the fake site, 233 people committed themselves to AU$10,000 and AU$50,000 investment packages and 1212 people asked for more information about the investment.
- The people who fell for the scam received a return email from ASIC telling them it was an April Fool's Day joke and giving them advice on how to protect themselves. After that, all record of their having responded to the scam, including the record of their addresses, was destroyed.The Competition and Consumer Division of the Treasury has recently produced the 'Little Black Book of Scams' which aims at educating consumers on how to avoid scams. The publication includes references to financial scams.

4.2 Cold Calling Cases

- The principal form of action by ASIC is "name and shame" and ASIC maintains information links with other enforcement agencies abroad with information about this practice.
- ASIC also maintains information about current cold calling cases on its consumer webpage. It gives advice that consumers should contact ASIC if: they have sent money offshore to an unlicensed cold calling outfit or they receive a call from an overseas organisation that is not named on the list of unlicensed overseas cold callers. The comprehensive list of cold calling cases notified is given at http://www.asic.gov.au/fido . One personal experience of cold calling, notified to ASIC, is given at http://www.asic.gov.au/fido/fido.nsf/byheadline/

4.3 Criminal Prosecution for Spam Email

- ASIC believes a criminal prosecution involving spam email relating to investment opportunities may be one of the first of its kind in the world. The case involved a US company that traded on the small cap market of NASDAQ. In May 1999 messages were posted on a bulletin board and between 500,000 and a million spam messages were sent out in the US and Australia. The messages said the company's stock would increase by up to 900% over the next few months. The next day the stock doubled on trading volume, which was at least ten times the normal average daily trading volume of the company's shares.
- The US SEC received complaints about spam and consulted the company, which denied that the messages had originated with them. Investigations showed that the bulletin board messages were posted from accounts held with Australian-based ISPs.
- A joint investigation between SEC and ASIC served notices on the Australian ISPs and suspects were identified within Australia. Search warrants yielded documentary and computer data. The perpetrators pleaded guilty to making statements or disseminating information that was false or misleading and likely to induce the purchase of securities, by way of transmission of electronic mail messages and posting messages to Internet websites.

4.4 International Cooperation

Thai Illegal Securities Operation

- A well-publicised case of illegal securities selling occurred in Thailand in mid 2001. The Securities and Exchange Commission, Thailand (SEC Thailand) filed criminal complaints against several foreigners on the ground that they conspired to conduct unlicensed securities businesses in Thailand.
- The Thai authority's raids of the premises were conducted as part of an investigation following complaints from ASIC, the Securities and Futures Commission in Hong Kong and the Securities Commission in New Zealand. ASIC had worked closely with the SEC Thailand and a number of other regulators in South East Asia, because a large number of Australians had been cold called by salespeople allegedly based in the region.
- Officers from the Royal Thai Police visited Melbourne and Sydney and interviewed some 20 investors over four days and took their statements.
- Most of the assets that were recovered were stock certificates, and were held as evidence and could not be returned to investors until the Thai Court reached a decision (which is expected to take quite some time).
- Most of the transfers of money were made through the accounts of commercial banks in Hong Kong. Investors have been advised to take legal action to recover their money in that jurisdiction but neither the Australian nor Thai authorities are able to recover money on behalf of investors. It is not clear whether any money has been returned.

4.5 Private sector developments to overcome cross-border jurisdiction difficulties

Australian Stock Exchange on-line link with Singapore Stock Exchange

- ASX/SGX link (Worldlink) has been set up by the Australian Stock Exchange (ASX) to facilitate investment in international securities. Initially the link has been established with the Singapore Stock Exchange (SGX).
- The purpose of the ASX/SGX link (Worldlink) was to promote cross border securities trading between Australia and Singapore by allowing investors direct access, via their domestic exchange, to the other exchange's stocks. Brokers have been doing this for years via their branch offices or through partnership arrangements with a broker in the other market. However such transactions tend to be paper based, are not as direct, and execution time is longer than the exchange to exchange model offered by Worldlink. The latter doesn't cut out brokers altogether, but it means investors do not need to have a broker in each market to complete the transaction.
- In order to give effect to Worldlink, ASX needed to be able to receive orders from SGX (and vice versa). Initially, it was proposed that SGX should become a broker in the Australian market (and vice versa). However, this would have required SGX to be regulated by ASIC with all the associated compliance costs. To avoid this double regulation, the model adopted was that ASX would become a 'broking

entity' in its own market and SGX would become a broking entity in its own market. ASIC does not regulate the ASX 'broker entity' as heavily as it does other brokers in recognition of its regulation as an exchange and the fact that it is just routing Singapore orders. Orders are routed from investor to broker to SGX 'broker entity' to ASX broker entity to the ASX market (and vice versa). So the cross jurisdictional issues were dealt with through the 'broker entity' arrangements

Brunei: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- Research has not revealed to date a significant body of law related to e-finance in general terms. However there are significant developments in the financial system and in the policy making process which are relevant.
- There are strategic diffusion and development programs on national information technology drives towards the paperless society (e-Brunei), e-government and e-business (http://www.e-government.gov.bn and http://www.bit.gov.bn).
- Brunei Darussalam has no central bank and the Ministry of Finance exercises most of those functions. His Majesty became the first Minister of Finance with the formation of the Ministry of Finance on the 1st January 1984. (http://www.bifc.finance.gov.bn/)
- It is assumed that the Ministry licences banks under The Banking Act Cap. 95. Banks pay annual licence fees varying with the nature of the facilities they offer.
- The following legal infrastructure would apply to any matters about information technology: Broadcasting (Class License) Notification 2001, Internet Code of Practice Notification, Computer Misuse Order. Electronic Transaction Order, Copyright Order (http://www.bit.gov.bn/dwnload.htm)
- The Banking System in Brunei Darussalam comprises of 9 commercial banks, of which 6 are foreign owned and represented by branch operations. One banking institution provides Islamic banking services .
- The Securities Order, 2001 regulates all financial and investment advisers, as well as putting in place a framework for the establishment of a Stock Exchange. The Securities Order governs the trading of securities. It provides a framework for the establishment of a financial exchange or exchanges in Brunei Darussalam, and for the licensing of "dealers", "investment advisers" and their representatives.
- The Department of Information Technology and State Stores of the Ministry of Finance is the Secretariat to the Brunei Darussalam National Information Technology Council. It is also the joint secretariat of the E-Government Program Executive Committee.

Are any special licenses or permits required for E-finance business?

- All Internet Service Providers and Internet Content Providers licensed under the Broadcasting (Class Licence) Notification 2001 are required to comply with a Code of Practice and to satisfy the Minister responsible for broadcasting matters that they have taken responsible steps to fulfil this requirement. Under the Broadcasting Act the Minister responsible for broadcasting matters has the power to impose sanctions, including fines, on licensees who contravene this Code of Practice. It appears that any banks offering Internet banking would be regulated under this regulation.

1.2 Laws and regulations relating to Cross-Border transactions

- Brunei Darussalam's dollar is linked to the Singapore Dollar and there is parity between the two. There are no exchange controls.
- Brunei has a strategy of developing its role as an international financial centre. It has established a detailed regulatory structure for this purpose including a large body of legislation. The legislation includes various anti-crime measures as well as several pieces of legislation covering international business [http://www.bifc.finance.gov.bn/ lists: International Banking Order, 2000 ("IBO"), International Business Companies Order, 2000 ("IBCO"), Registered Agents and Trustees Licensing Order, 2000 ("RATLO"), International Trusts Order, 2000 ("ITO"), International Limited Partnerships Order, 2000 ("ILPO"), Mutual Fund Order, 2000 ("MFO"), Securities Order, 2001 ("SO").
- Commentary on this legislation points out that "…the Money Laundering Order, the Criminal Conduct (Recovery of Proceeds) Order, the Mutual Funds Order and the Securities Order regulate those areas both domestically and internationally.
- It is also relevant that Brunei is a "dual jurisdiction", whereby the international legislation offers "offshore" facilities, alongside the usual range of "domestic" legislation drawn from that of England and Wales. The jurisdictional distinction is thus jurisprudential rather than physical.
- In contrast, the "anti-crime" measures (the Mutual Funds Order and the Securities Order) govern both domestic and international activities in these areas.
- The International Banking Order of 2000, for example, concerns the provision of banking services to non-residents. This covers all forms of banking and securities services.

1.3 Laws and regulations for consumer protection in E-finance

- There is not yet specific legislation relating to electronic transactions but some consumer protection is provided in the financial sector legislation. For example, the Securities Order provides for penalties for any person acting as an investment adviser or investment representative without a license or in breach of the standards set for the financial industry. This is considered by the government to provide a level of protection " for all international clients, citizens, residents and businesses of and in Brunei to the highest international standards".
- There is a proposed changed of Brunei Legislation to include a Consumer Rights Act. (http://www.bit.gov.bn/webpage/archives/press/2001/jun/consumer_body_put_up_website.htm)

Are there any laws and regulations related to data protection?

- There is nothing specifically about electronic data protection but the Banking Act requires banks to maintain privacy.

What types of Internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- Internet service providers must be licensed. To date the focus of the licensing regime is related to the material provided. Internet licensees must use their best efforts to ensure that nothing is included in any programme on Internet which is against the public interest or national harmony or which offends against good taste or decency. The specified areas do not appear to relate to e-finance.

2. Self-Regulation and Codes of Practice

2.1 Codes of Practice

- *The Internet Code of Practice* came into force in February 2001 under section 9 of the Broadcasting Act. As noted above the Code relates to the nature of material provided.

3. Enforcement System

- Under the *Broadcasting Act* the Minister responsible for broadcasting matters has the power to impose sanctions, including fines, on licensees who contravene the Internet Code of Practice.
- The "international" legislation is supervised by "the Authority", a segregated unit of the Ministry of Finance acting through the Head of Supervision (BIFC). The Authority comprises a multi-disciplinary unit with appropriate banking, insurance, corporate and trust supervisory skills. It is a one-step with line command passing directly from the Minister of Finance, the Minister responsible for the international legislation.

4. Cases

4.1 Consumer education

- The Consumer Association of Brunei Darussalam (CAB) is studying opening up an Internet website where people can lodge complaints. The association is still fairly small and new and has had limited experience of handling complaints. Most complaints seem to have involved goods not services and it is not clear whether there is expertise relating to electronic transactions.

Canada: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- The federal government's *Personal Information Protection and Electronic Documents Act* was enacted to make existing statutes and regulations compatible with an electronic environment including the replacement of a legal requirements for paper documents and to allow disclosure in electronic means. The Act went into force on January 1, 2001. In a comment on the Act, Industry Canada noted that " The Act will apply to the federally regulated private sector, and to personal information that is sold inter-provincially and internationally. Three years after coming into force, the personal information provisions will apply more broadly to all information collected, used, or disclosed in the course of commercial activities. Where and whenever a province adopts legislation that is substantially similar, the organisations or activities covered will be exempted from the application of the federal law." The Canadian Bankers Association noted that "Prior to January 2001, banks conducted a thorough review of their operations to ensure they complied with the Act and designated a senior officer responsible for upholding its rules. Most bank customers have noticed little change, as the Act's guiding principles and most requirements are the same as the voluntary standards banks have followed for many years."
- The *Personal Information Protection and Electronic Documents Act* also introduces the concept of "secure e-signature".
- The use of information held by governments is covered by separate legislation (eg the federal government is covered by the *Federal Privacy Act of 1982*).
- The *Uniform Electronic Commerce Act* is similar to Part 2 of the *Personal Information Protection and Electronic Documents Act*, in authorising governments to use electronic technology to deliver services and communicate with citizens. The "Act' was drafted by the Uniform Law Conference of Canada in an attempt to promote uniformity in the approach to provincial legislation. It was designed to implement the principles of the UN Model Law.

Are any special licenses or permits required for E-finance business?

- No special licences are required.

1.2 Laws and regulations related to Cross-Border transactions

- Constitutional jurisdiction over consumer protection in the financial services sector is shared between the federal and provincial governments, depending on the financial institution in question and the activity being carried on by the institution.
- There are no specific laws relating to cross border e-finance.

1.3 Laws and regulations for consumer protection in E-Finance

- The *Financial Consumer Agency of Canada Act (2001)* sets up the FCAC to supervise the financial institutions in Canada which are subject to Federal regulation. The FCAC will also deal with complaints from consumers. The Commission also monitors the voluntary codes of the institutions and provides consumer education. The establishment of the Commission was part of a larger package of financial sector reform measures.

What types of internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc.)?

- No activities are specifically prohibited.

Are there any laws and regulations related to data protection (particularly private information)?

- The *Personal Information Protection and Electronic Documents Act* was enacted to ensure the protection of personal information in e-commerce

2. Self-regulation and Codes of Practice

2.1 Codes of Practice

- A group of governments and business organisations, including the banks, have developed a set of principles to guide consumer protection. These are the *Principles of Consumer Protection for Electronic Commerce and Supporting Documentation*. In a commentary on these principles, Industry Canada notes that "the principles are intended to guide the actions of businesses, consumers and governments within Canada in the development of a consumer protection framework for electronic commerce. The principles were drafted by a working group of representatives from Canadian businesses, consumer associations and governments, recognizing that a sound framework for consumer protection will promote consumer confidence and facilitate the acceptance and growth of electronic commerce. The working group has agreed to review the principles regularly to ensure their continued relevance in the rapidly changing electronic marketplace."
- The Canadian Standards Association (CSA) also developed an *International Model Privacy Code* which addresses how to collect, use, and disclose personal information.

2.2 Trust Mark/Seal of Assurance Schemes

- Government On-Line is a Government of Canada initiative to provide information and services on the Internet. The goal of the Government On-Line initiative is to use information and communication technology to provide Canadians with enhanced access to improved citizen-centred, integrated services, anytime, anywhere and in the official language of their choice.

- The Canadian Payments Association (CPA) is a not-for-profit organization created by an Act of Parliament to establish and operate national systems for the clearing and settlement of payments and other arrangements for the making or exchange of payments. The CPA and its members - virtually all Canadian deposit-taking financial institutions - are working on a public key infrastructure under which Canadian businesses and consumers will be able to receive digital certificates from participating CPA members for use in Internet-based transactions.
- The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have jointly developed a service, called WebTrust, to address security and privacy concerns in e-commerce. The WebTrust Seal enables consumers and businesses to purchase goods and services over the Internet with confidence that vendors' web sites meet high standards of business practices disclosure, transaction integrity, and information protection.
- The Better Business Bureau has a trustmark program (privacy and reliability) for its North American members including Canada.
- Internet authentication services, such as VeriSign, have also emerged in e-commerce.

2.3 Dispute Resolution

- The CSA has suggested a number of steps in relation to privacy issues, including use of the Quality Management Institute (QMI) which is a division of CSA International. QMI offers a program whereby organizations can demonstrate their compliance with the CSA *Privacy Code* to customers, employees, trading partners or fellow members of their industry. CSA notes that complaints can be registered with QMI and that while QMI cannot act as a mediator to resolve your complaint, it will investigate a case for compliance with the code.
- The *Principles of Consumer Protection for Electronic Commerce and Supporting Documentation* include specific terms on redress which state that consumers should have access to fair, timely, effective and affordable means for resolving problems with any transaction. It also recommends that vendors should provide adequate resources to handle consumer complaints efficiently and effectively. When internal mechanisms have failed to resolve a dispute, vendors should make use of accessible, available, affordable and impartial third-party processes for resolving disputes with consumers. However, vendors should not require consumers to submit to such processes. The principles also recommend that governments, businesses and consumer groups should work together to develop appropriate standards for dispute resolution mechanisms.
- It is notable that one of the clauses of the Principles refers to cross-border issues and recommends "So that consumers are not disadvantaged, governments should cooperate in the development of clear rules regarding the applicable law and forum, and the mutual enforcement of judgements, in the event of cross-border disputes."
- The Competition Bureau of Industry Canada is the administrative and law enforcement body charged with the preservation of a competitive marketplace in Canada. Its role is to promote and maintain fair competition so that Canadians can benefit from lower prices, product choice and quality services. General

enquiries and complaints regarding deceptive business practices can be made on-line or by contacting the Bureau.

3. Enforcement Systems

- The Privacy Commissioner is an advocate for the privacy rights of Canadians with the power to: investigate complaints and conduct audits under two federal; laws; publish information about personal information-handling practices; in the public and private sector; take matters to the Federal Court of Canada; conduct research into privacy issues; and promote awareness and understanding of privacy issues by the Canadian public.
- The Commissioner works independently from any other part of the government to investigate complaints from individuals with respect to the federal public sector and the private sector. Canadians may complain to the Commissioner about any matter specified in Section 29 of the Privacy Act. This Act applies to personal information held by the Government of Canada. For matters relating to personal information in the private sector, the Commissioner may investigate complaints under Section 11 of the *Personal Information Protection and Electronic Documents Act*. This Act now applies to federally regulated businesses across Canada and all businesses in the three territories of Canada. The Commissioner prefers to resolve complaints through negotiation and persuasion, using mediation and conciliation if appropriate but it also has the power to summon witnesses, administer oaths and compel the production of evidence if voluntary co-operation is not forthcoming.
- In the enforcement and administration of legislation, the Competition Bureau uses a balanced approach with a variety of education, compliance and enforcement instruments.

4. Cases

4.1 International Co-operation

- Canada and the US have co-operated to deal with telemarketing scams. On the Canadian side both law enforcement agencies and the Competition Bureau joined with US agencies (FBI, United States Customs Service (USCS) and United States Postal Service (USPS)) to form a task force to deal with the schemes. A memorandum of understanding to this effect has been signed between the Royal Canadian Mounted Police and the Competition Bureau to give this partnership formal status. The Competition Bureau is a federal agency whose mandate is to enforce the Competition Act, which contains provisions making telemarketing fraud a criminal offence. The joint co-operation in the Centre of Operations Linked to Telemarketing Fraud (COLT) is confirmation of the multi-jurisdictional aspect of its mission. Ever since its inception in 1998, COLT has been successful as regards both the charges laid and the amounts, close to $25,000,000, that have been returned to the victims.
- Canadian business participates in the North American Better Business Bureau (BBB) system. With the Electronic Commerce Promotion Council of Japan

(ECOM) in February 2002 BBB has jointly launched a new approach to resolving cross-border disputes. The BBB system will handle Japanese consumers' complaints against businesses located in areas served by U.S. and Canadian BBBs, and ECOM will provide a reciprocal service for U.S. and Canadian consumers who have complaints against merchants located in Japan. ECOM will perform translation services for the project. Until now, the BBB system has only been able to manage complaints from people based in North America.

- Canada participates in the www.econsumer.gov initiative. The project has two components: a multilingual public Web site, and a government, password-protected Web site. The public site provides general information about consumer protection in all countries that belong to the IMSN (International Marketing Supervision Network), contact information for consumer protection authorities in those countries, and an on-line complaint form. All information is available in English, French, German, and Spanish. Using the existing Consumer Sentinel network (a database of consumer complaint data and other investigative information operated by the U.S. Federal Trade Commission), the incoming complaints will be shared through the government Web site with participating consumer protection law enforcers.

China: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- There is no comprehensive legislative framework on internet and e-commerce regulation but there have been some developments since 2000.
- The *Contract Law of the People's Republic of China* (the "Unified Contract Law") came into effect on 1 October 1999 and has two articles on e-commerce related contract law. The *Contract Law* authorises the validity of electronic contracts and defines when a contract has been offered and accepted. The contract is formed when the acceptance becomes effective. The offer or acceptance becomes valid as soon as it goes through the gateway of a company's internal computer network. As is common in most e-contract law, the Law does not make allowances for the possible failure of a company's internal computer system to deliver a message from the gateway, nor does it address the issue of whether the offer or acceptance has ever actually been opened or read. The Law does not cover electronic signatures.
- The People's Bank of China (http://www.pbc.gov.cn) recently promulgated *The Circular on Standardising Fees on Electronic Transfers*. Banks which transfer funds through electronic transfer systems shall abide by the relevant provisions of *The Circular* by the State Development Planning Commission and the PBC and may not charge postage and telegraph fees. Institutions that transfer funds through telegraph or mailing may charge telegraphic or postal fees according to standards set by the postal authority but may not charge transfer fees.
- *The Provisional Regulation on Online Stock Trading* were brought into effect in April 2000 by the China Securities Regulatory Commission. (http://www.csrc.gov.cn/CSRCSite/default.htm)
- Since China's entry into WTO authorities have indicated they will be amending legislation to make it more compatible with WTO standards and, in particular, this will include drafting of new judicial interpretations focussing on economic crimes such as financial fraud, violations of intellectual property rights and crimes in the futures markets.

Are any special license or permits required for E-Finance business?

- Banks providing services over the internet will be regarded as engaging in Commercial Internet Information Services. Commercial IIS is the provision of services, such as information and website production etc., to on-line users through the internet. Commercial IIS providers are required to obtain an operating permit either from the Ministry of Information Industry or from the provincial telecommunications authorities.
- Parts of the Telecommunications Regulations are relevant to e-finance. Regulations will treat on-line funds transfer, on-line payment, and other on-line transactions offered by banks as Value-Added Telecommunications Services. For VATS an applicant must be a company legally established in the PRC and must

fulfil other conditions. Operating permits will be issued by the provincial telecommunications authorities or by the Ministry of Information. It is not clear whether these regulations are superseded by :

- The Provisional Regulation on Internet Bank established by the People's Bank of China in July 2001. It provides that banks can't establish on-line banking systems without the PBC's approval (Article 4, the Provisional Regulation on Internet Bank).
- The Interim Regulations for the Online Brokerage Sector and the Procedure for the Examination and Approval of Securities Companies for Engaging in Online Brokerage Activities severely restrict the electronic securities trading system. Only companies licensed by China Securities Regulatory Commission may run on-line securities and only securities on the Shanghai and Shenzen Stock Exchange are eligible to be traded. Foreign companies are therefore, excluded.
- Since there is a separation of banking and securities business under the Securities Law there are restrictions on banks offering on-line securities trading, while securities companies are not permitted to facilitate on-line funds transfers.
- The PBC is drafting guidelines for the management of financial risk on the Internet.

1.2 Laws and Regulations related to Cross-Border transactions

- There are limits imposed by PBC on the amount of foreign exchange which individuals may take (or transfer) out of the country. Approval is required for any payment in foreign currency.
- The Provisional Regulations of the People's Republic of China Concerning Administration of International Connection of Computer Information Networks (the "International Network Regulations"), have been interpreted to mean only domestic internet service providers can apply for operating permits. Foreign investment in internet service provision is therefore prohibited.
- Foreign investment in internet content provision is also not allowed under Chinese law. As a result foreign enterprises, including foreign banks, may send e-mails and create their own websites, but if they provide information on their websites which is more than simply a description of their own companies and services, they are likely to be classified as internet content providers and are, therefore, subject to the prohibition.
- Without the PBC's approval, China's banks (HK, Macau and Taiwan's excluded) can not offer cross-border electronic financial transaction services to people resident outside mainland China. (Article 4, The Provisional Regulation on Internet Bank).
- Currently there is no other legislation or regulation dealing with cross-border supervisory issues but the People's Bank of China is planning to formulate such policy.

1.3 Special laws and regulations for consumer protection in E-Finance

- *Law of the People's Republic of China on Protecting Consumers' Rights* and Interests: http://www.qis.net/chinalaw/prclaw26.htm came into effect in 1994.

- State Administration for Industry and Commerce has the functions of protecting consumer's privacy on the Internet and protecting consumer's rights related to on-line transactions.
- *The Provisional Regulations on Online Brokerage* cover data security.

Are there any laws and regulations related to data protection (particularly private information)?

- There is no general data protection law in China although the Computer Information Network and Internet Security, Protection and Management Regulations specify that individuals may not violate the privacy of users of networks. There are no regulations specific to internet financial services. In fact China maintains quite close control of use of the Internet and the above regulations also specify that Internet businesses and users must accept the "security supervision, inspection, and guidance of the public security organization". This can include providing information and digital documents to assist in legal enquiries.
- Law on Commercial Banks requires that banks have a duty of confidentiality on depositors accounts and may refuse inquiries about individuals' deposits except when specified by law.
- Various other pieces of legislation have requirements on data security (e.g. Telecommunications Regulations)
- Online Brokerage Regulations impose requirements on on-line securities companies relating to data security, encryption and back-up.

What types of internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- There is no comprehensive legislation on e-commerce so specific prohibitions tend to emerge from public statements from the authorities. For example, the Ministry of Public Security announced in 2000 that the sale of email address lists would be illegal under a number of laws.
- Regulations for the Control of Secrecy on Computer Information system set out a number of restrictions on the type of content which can be transmitted. These are mainly aimed at "state secrets" but since the service provider is held responsible these could be quite onerous for providers (including banks).
- State Administration of Industry and Commerce has discussed a licensing system for on-line advertising.

2. Self-regulation and Codes of Practice

2.1 Codes of Practice

- China Merchants Bank has its own "on-line shopping mall" in which all products sold may be paid for in real-time using China Merchants Bank's on-line payment system. China Merchants Bank also provides merchants wishing to join the "on-line shopping mall" with technical support in developing on line sale platforms.

3. Cases

3.1 Financial Pyramid Selling Schemes

- ANWAY scheme was a well-publicised pyramid selling scheme that was brought to court but could not be successfully prosecuted.

3.2 Investment Fraud

- Lanzhou - a case of a securities company offering on-line trading which disappeared with investors' money. Details of how the case was resolved are not available at this time.

Hong Kong, China[1]: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- The e-finance services related to the banking sector, securities sector and insurance sector are regulated by the Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC) and Insurance Authority (IA) respectively.
- To facilitate the use of electronic transactions and promote e-business development, the Electronic Transactions Ordinance (ETO) was enacted in Hong Kong to give electronic records and digital signatures the same legal recognition as that of their paper-based counterparts. The ETO was modelled on the UNCITRAL Model Law on E-commence.
- The Banking Ordinance of Hong Kong forms the basis of the legal and statutory framework for supervision of authorized institutions ("AIs", i.e., banks and deposit taking institutions) in Hong Kong and also grants the authority to the HKMA to regulate AIs. The HKMA has implemented a comprehensive e-banking and technology risk management supervisory framework to ensure a secure and sound control environment for e-banking development in Hong Kong, without stifling technological innovation. The supervisory framework is in line with the best international regulatory standards and practices, particularly the guidance of the Basel Committee on Banking Supervision.
- A series of guidelines and guidance notes on e-banking have been issued since July 1997, which covers authorization of virtual banks, the regulatory approach of e-banking and the HKMA's recommendations on e-banking risk management.
- In the securities and futures markets, the SFC issued its first *Guidance Note on Internet Regulation* in March 1999. Supplemental *Circular on Provision of Financial Information on the Internet* and *Guidelines for Registered Persons Using the Internet to Collect Applications for Securities in an Initial Public Offering* were issued in 2000. Following the enactment of the Electronic Transactions Ordinance in early 2000, a *Guidance Note on the Application of the Electronic Transactions Ordinance to Contract Notes* was issued. The recent supplements include a *Collective Investment Schemes Internet Guidance Note* issued in May 2001 and *Guidelines for the Regulation of Automated Trading Services* issued in February 2002.

Are any special license or permits required for E-Finance business?

- Any e-finance organisation that intends to carry on banking business in Hong Kong must be authorized under the Banking Ordinance, as for other AIs. The main principle is that the HKMA will not object to the authorization of such e-

[1] Hereinafter refer to as Hong Kong

finance organisations in Hong Kong provided that they can satisfy the same prudential criteria applicable to conventional banks.

- For existing AIs that intend to introduce e-finance business, they do not need to apply special license or permits from the HKMA. However, they should discuss their plans and the relevant risk management measures (e.g., in the security measures as well as consumer protection arrangements) with the HKMA in advance.
- The new *Securities and Futures Ordinance* introduces a licensing regime, which is administered by the SFC, to cater for companies providing automated trading services. Where the automated trading services resemble stockbroking, the licensing regime will apply; and where they are more reminiscent of a stock exchange, a separate authorisation regime will apply.

What types of internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- The Office of the Telecommunications Authority launched an anti-spamming program jointly with the Hong Kong Internet Service Providers Association (HKISPA) and the Office of the Privacy Commission for Personal Data (PCO) in February 2000. An Internet Services Providers Industry Code of Practice for tackling spamming on the Internet was also introduced at the same time.
- Hong Kong has an effective legislative framework to tackle the issue of cyber security. Illegal activities on the Internet are prohibited by the relevant provisions in, amongst others, the Crimes Ordinance, Theft Ordinance and Telecommunications Ordinance.
- Overseas e-finance organisations (including virtual banks) intending to solicit offshore deposits from members of the public in Hong Kong would not be required to be authorized. However, the advertising materials for deposits must comply with the statutory disclosure requirements in the Fifth Schedule of the Banking Ordinance. The HKMA will issue a guideline to specify the factors the HKMA takes into account in determining whether an advertising material for deposits issued over the Internet or other electronic channels is an advertising material that must comply with this Fifth Schedule.
- In accordance with this Fifth Schedule, the advertising materials for deposits should include, among other information, certain specified information about the deposit-taker and the deposit product being advertised as well as a prominent warning to the effect that the deposit-taker is not subject to the supervision of the HKMA. The objective is to ensure that material facts are available in the advertising materials to enable prospective depositors in Hong Kong to make their own judgement about placing a deposit with the deposit-taker.

1.2 Laws and regulations related to Cross-Border transactions

- There are no specific laws addressing cross-border transactions.
- As mentioned above, a foreign e-finance organisation intending to carry on banking business in Hong Kong must be authorized under the Banking Ordinance.

However, foreign e-finance organisations that intend to solicit offshore deposits from members of the public in Hong Kong would not be required to be authorized.

- The SFC has indicated that, as a general principle, it will not seek to regulate dealing, commodity futures trading, and leveraged foreign exchange trading that are conducted from outside Hong Kong and over the Internet, provided such activities are not detrimental to the investing public in Hong Kong.
  However, for the purpose of registration as a dealer, trader or adviser in Hong Kong, an entity is required to have a physical presence in Hong Kong.

1.3 Laws and regulations for consumer protection in E-Finance

- Currently the HKMA has no formal powers to deal with consumer protection issues relating to the banking sector. Nevertheless, the HKMA and two banking industry associations have been promoting good business practices and transparency of banking services including e-banking services among AIs through the Code of Banking Practice issued by the industry associations. In particular, one chapter of the Code of Banking Practice specifically deals with e-banking services, such as in relation to disclosure, complaint handling and allocation of liabilities for unauthorized e-banking transactions.
- A major issue relating to consumer protection in e-finance is how to safeguard the personal data privacy. Data privacy in Hong Kong is protected by law under the Personal Data (Privacy) Ordinance overseen by the Office of the Privacy Commissioner for Personal Data (PCO). The Ordinance regulates the collection, storage, use, accuracy, security and retention of the personal data relating to individuals, from which it is reasonably practicable to identify the individuals. The Personal Data (Privacy) Ordinance provides that organisations based in Hong Kong must provide individuals with the right to have their personal data collected in a lawful and fair manner and to be informed of the purposes for which the data are to be used; to have personal data kept accurate, up-to-date, secure and for no longer than necessary. Data should only be used for the purpose for which they were collected and unless consent to a change of use of the data has been given by the data subject. Personal data must also be protected against unauthorized or accidental access and use. If information is to be generally available, the provider must ascertain a data user's personal data policy and practices. Individuals have the right to obtain a copy of their personal data held by a data user and to require correction of any inaccuracy.
- Failure to observe any of these requirements is not automatically an offence, but the PCO may serve an enforcement notice, and non-compliance may lead to a fine or imprisonment.
- With regard to data protection on the Internet, the PCO has issued guidelines on the protection of personal data privacy on the Internet, providing guidance to individuals and organisations. 'A Guide for Data Users' aims to assist data users in complying with some of the more commonly applicable requirements of the Ordinance when they are collecting, displaying or transmitting personal data over the Internet.
- The PCO has also released a guideline 'Preparing an on-line Personal Information Collection (PIC) Statement and Privacy Policy Statement (PPS)' to assist data users. Details of these guidelines can be obtained from http://www.pco.org.hk.

- In 2001 the PCO launched a series of E-Privacy management handbooks. The first title released was "A Policy Approach to Building Trust and Confidence in E-Business". The handbook proposes that on-line businesses formulate and disseminate an E-Privacy policy framework. In addition, it offers practical guidelines for developing such a framework with a view to protecting the personal data privacy of the individual and thereby enhancing trust and confidence in E-transactions.

Are there any laws and regulations related with data protection (particularly private information)

- See above

2. Self-regulation and Codes of Practice

2.1 Codes of Practice

- As mentioned above, one chapter of the Code of Banking Practice issued by the banking industry associations specifically includes guidelines about proper banking practices in relation to e-banking services, such as about disclosure, complaint handling and allocation of liabilities for unauthorized e-banking transactions. All AIs must follow the Code of Banking Practice.
- The PCO released a guideline 'Preparing an on-line Personal Information Collection (PIC) Statement and Privacy Policy Statement (PPS)' to assist data users. It is likely that some industry associations have adopted these guidelines.

2.2 Trust Mark/Seal of Assurance Schemes

- The Hong Kong Society of Accountants (HKSA) has started to license Certified Public Accountants firms to provide theWebTrust service, which is an e-commerce assurance service. WebTrust (www.webtrust.org) is developed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).
- The Better Business Bureau has a trust mark.

2.3 Dispute Resolution

- The HKSA and Hong Kong International Arbitration Centre (HKIAC) has also launched the HKIAC Electronic Transaction Arbitration Rules (Rules) as a third-party arbitration framework for use and adoption by on-line merchants in Hong Kong to handle consumer disputes.
- In relation to personal data privacy, the PCO has the power to take steps to liaise between the complainant and the supplier, to initiate mediation, to carry out formal investigation, and to issue an enforcement notice.

- Contravention of an enforcement notice may result in a fine or imprisonment.
- At any time an individual has the right to take civil proceedings.
- Individual consumers who have a right of action under various consumer protection ordinances can be assisted in their private actions with funds from the Consumer Legal Action Fund. The Fund was established with a government grant and administered by the Consumer Council.
- Mediation services provided by the Consumer Council may also be one way of resolving disputes.

3. Enforcement

- The HKMA enforces its regulatory framework of e-banking through on-site examinations and off-site reviews of e-banking controls and initiatives of AIs. The HKMA also monitors whether AIs have complied with the Code of Banking Practice, through independent compliance checks performed by AIs' internal auditors.

4. Cases

4.1 Consumer Education

- Under the Code of Banking Practice and the HKMA's guidance notes on e-banking, AIs have responsibilities in consumer education related to e-banking. In particular, AIs should make clear and prominent disclosure covering consumers' liability for unauthorized transactions, consumers' obligations in relation to security for e-banking services and security precautions related to e-banking.
- The Consumer Council undertakes consumer education and information dissemination of consumer protection matters – including e-commerce and e-finance.

4.2 Cold Calling Cases

- Hong Kong's role in the Thai based cold calling cases has been described elsewhere. Most of the money transferred in the boiler room case went through Hong Kong bank accounts. It has proven difficult for investors to recover their money so far, suggesting that cross-border enforcement remains a problem.

4.3 International Cooperation

- The HKMA participates in the work of the Electronic Banking Group (EBG) of the Basel Committee on Banking Supervision in developing a paper on risk management and supervision of cross-border e-banking activities.

Indonesia: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- In Indonesia, the e-commerce market is fairly small and undeveloped. Its difficulties are readily apparent and may have more to do with traditional ways of conducting business than with legal barriers. Arguably, nothing legally prevents businesses or individuals from engaging in e-commerce. There is no special regulation for e-banking/on-line securities activities. Consequently there is a widespread lack of trust and confidence in the security, integrity, reliability, and enforceability of electronic transactions.
- An Information Technology Law is in preparation to provide jurisdictions and umbrella provisioning for IT implementations in Indonesia. The law will cover all aspects on IT implementations such as: Privacy protection, Electronic Commerce, Competition, Consumer protection, Taxation, IPR, Intellectual Property Right http://www.itu.int/asean2001/documents/pdf/Document-21.pdf
- A number of draft laws relating to Information Technology are also underway. Two universities (University of Indonesia and Padjajaran University) specializing in cyber law research have presented draft laws on Information Technology, and Digital Signature and E-commerce. Recently, the draft laws were presented to the IT community for in-depth discussion before being submitted to the House of Representatives. These laws are expected to provide legal guidelines for the emerging electronic means of transactions. One of the draft laws focuses on B- to-B transactions. (http://www.hhp.co.id/news/nw20011024_1.html) (Nov 2001)
- The Indonesian government will not complete drafting a law on cyber crime until 2004 because of the lack of information technology experts in the country, according to State Minister of Communications and Information Syamsul Mu'arif. (http://www.totaltele.com/vprint.asp?txtID=43779) (Sep 2001)

Are any special license or permits required for E-Finance business?

- Banks using the System Information Technology should report their planning, implementation, modification, abuse and audit of their system information technology to the Central Bank of Indonesia.

1.2 Laws and regulations related to Cross-Border transactions

- Indonesia says it has difficulties to control transactions offered by offshore providers.

1.3 Special laws and regulations for consumer protections on E-Finance

- Until the enactment of the Law on Consumer Protection (LCP) on 20 April 1999, there was no comprehensive legislation providing a framework for consumer

protection in Indonesia. The LCP came into effect on 21 April 2000. The scope of the LCP is broad: it covers all kinds of goods and all kinds of services. (Art.1 no.5) (http://www.ciroap.org/apc1/countries/indonesia_overview.html)

- There is no special consumer protection law which regulates e-banking activity other than general consumer protection law
- There is no special regulation for e-banking/on-line securities activities, and in the event a dispute occurs existing *Civil Law* will be used.

What types of internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- None since no law in place.

2. Self-regulation

Dispute Resolution

- Bank Indonesia considers that bilateral or multilateral agreement between countries regarding payment system to protect consumers across countries is essential in the cross border payment system.
- The LCP established an independent body, the National Consumer Protection Agency, to regulate consumer protection and a dispute settlement body, the Consumer Dispute Settlement Agency, in each regency to function as a small claims court for resolving conflicts between vendors and consumers. Reportedly, supplementary regulation to implement the law is still being prepared. It is not clear if the law will extend the same level of protection to Internet consumers and monitor Internet advertising activities.

3. Cases

- No cases have been found for Indonesia. At this stage there is rather little activity in e-finance and the regulatory structure is not yet developed to deal with problems.

Japan: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- No special legal framework concerning e-finance, but existing *Banking Law, Securities and Exchange Law,* and *Insurance Law* are applied to e-finance activities. There are some specific laws on electronic transactions, shown below, which have implications for e-finance. The Financial Reconstruction Commission and the FSA have responded to the establishment of new forms of banks (including internet only banks, by formulating "Measures for Licensing for and Supervision of New Types of Banks including Entry into Banking Business by Non-financial Entities (Operational Guidelines)" in August 2000. Also, the "Law Partially Amending the Banking Law, etc." that is being submitted to the Diet further adapts to the entry of non-financial entities into the banking business by regulating major shareholders of banks.
- The *Law Concerning Exceptions of the Civil Code Related to Electronic Consumer Contracts and Electronic Notice of Acceptance* (*Denshi shohisha keiyaku oyobi denshi shodaku tsuchi ni kansuru minpo no tokurei ni kansuru horitsu*, Law No 95 of 2001) came into effect from December 25 2001. Under this new Law, contract formation occurs when the notice of acceptance arrives (rather than when it is sent) if it has been dispatched electronically. In addition, *The Law Concerning Electronic Signatures and Certification Services* (*Denshi shomei oyobi ninsho gyomu ni kansuru horitsu*, Law No 102 of 2000) has been in effect from April 1 of 2001 clarifying the legal status of e-signatures and certification services. It has close parallels to those enacted recently around the world (summary at http://www.meti.go.jp/english/report/data/gesignline.html). It defines an electronic signature as confirming that its user has created the information and that the information has not been altered (art 2 para 1), and provides an accreditation scheme for providers of electronic certification services (defined Art 2(2)). The Japan Quality Assurance Organisation (http://www.jqa.or.jp/j/index_e.html) has been designated as the body to conduct such assessments. There is also provision for simplified accreditation of foreign service providers accredited outside Japan.
- Study Group within the FSA has issued Electronic Sales of Financial Services and Supervisory Policy, followed by FSA's administrative action to allow electronic delivery of information to fulfill certain legal requirements (disclosure, etc.) (http://www.fsa.go.jp/p_fsa/news/newsj/f-20000418-1a.html)
- The Law on Sales of Financial Products came into effect in April 2001 to protect users of financial services, by measures such as (a) requiring financial service providers to provide customers with certain important information, and (b) explaining the liability of financial service providers for any damages caused by their failure to follow such requirements, as a special case of the Civil Code. The Law on Sales of Financial Products applies equally to products delivered by electronic means. (http://www.fsa.go.jp/syouhi/syouhi.html)

Are any special license or permits required for E-Finance business?

- The FSA issued operational guidelines in 2000 concerning licensing and ongoing supervision of e-banking activities including that of internet banks.
- According to the Banking Law, there is no explicit prohibition on web-based deposit taking services targeting Japanese residents other than the regular banking license that is required for any banks operating in Japan.

1.2 Laws and Regulations related to Cross-Border transactions

- Under the Law on Foreign Securities Firms, a foreign broker-dealer is not allowed to engage in securities businesses with residents in Japan unless it registers its main physical branch in Japan. However, broker-dealer can be exempt from FSA's regulation if applicable to the Article 2 of the Cabinet Order for Enforcement of the Law on Foreign Securities Firms.

1.3 Special laws and regulations for consumer protections on E-Finance

- Basic consumer protection is covered by *The Consumer Protection Fundamental Act 1968, The Consumer Contract Act* and *The Law on sales of Financial Products.*

Are there any laws and regulations related with data protection? (particularly personal information)

- Currently *The Law on Protecting Personal Information*, which establishes basic and common rules covering any sectors, is under discussion in the Diet.
- For financial institutions, there is no specific regulations for data protection, however it is considered that they have duties of confidentiality concerning personal data learned through their business.
- MITI (now METI) has Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector since 1999. METI has provided advice to business organizations including the Japan Consumer Credit Industry Association to establish or revise guidelines for each industry sector.
- JISC (Japanese Industrial Standards Committee) established the JIS (Japanese Industrial Standard) entitled "Requirements for Compliance Program on Personal Information Protection" in March 1999 to standardize the level of protection of personal data in companies.
- *Interim Report on Protection and Utilization of Consumer Credit Data* was published in July 1999 by the working group jointly organized by the Financial System Council, the Industrial Structure Council, and the Credit Sales Council.

2. Self Regulation and Codes of Practice

2.1 Codes of Practice /Guidelines

- Japan Banking Associations (JBA) and Japan Securities Dealers Association (JSDA) has issued Guidelines of Internet financial services, which point out concerning points such as system risk, consumer relations through Internet, etc.

2.2 Trust Mark/Seal of Assurance Schemes

- The "Online Trust Mark" system, which indicates the reliability of the companies' websites, was started by The Japan Direct Marketing Association and The Japan Chamber of Commerce and Industry in June 2000. Admission to the system requires businesses to display 1) Name of the online shop, (2) Geographical address,(3) Telephone number(s),(4) Sales price , (5) Other cost including delivery charge, etc.,(6) Method and conditions of payment, (7) Delivery date,(8) Return policy,(9) Name of the person in charge. They must also comply with all the relevant laws and regulations such as the Specified Commercial Transactions Law and the Act against Unjustifiable Premiums and Misleading Representations and meet a number of other conditions.
- The "Privacy Marks Award System", has been operated by Japan Information Processing Development Center (JIPDEC) since 1998. Companies and designated organisations can display the mark, including on websites, to show they are adequately handling personal data based on the METI guidelines. This system helps consumers to easily distinguish the companies' level of protection of personal data. Efforts are underway to facilitate reciprocal recognition of privacy marks with BBB Online (US), Commerce Trust (Singapore) and KAIT (Korea).

2.3 Dispute Resolution

- There are a number of organisations which provide advice on consumer problems with a focus on internet issues:
    - National Consumer Affairs Center and Local Consumer Centers – advisory and counselling services for consumers, consumer information/education http://www.kokusen.go.jp/ (National Consumer Affairs Center)
    - Lawyers for Internet Consumers Problem - advisory service for consumers, advocacy on consumer issues, consumer information / education http://www1.neweb.ne.jp/wb/licp/
    - Committee on Consumer Problems, Japan Federation of Bar Associations - advocacy on consumer issues, consumer information / education http://www.nichibenren.or.jp/index.htm

  For dispute resolutions for financial institutions, please also see 3. Enforcement.
- ECOM Working Group on Consumer Protection is undertaking a study of how ADR (Alternative Dispute Resolution) should be used in Japan. The target is to

find out appropriate ADR in the e-commerce in Japan through assessing ADR needs for consumers and businesses ad verifying the validity of ADR mechanism (consultation/conciliation, mediation, arbitration). From past November, on-line ADR systems (including cross-border transaction with USA and Korea) in operation.

3. Enforcement

- ADR systems are brought to financial industries associations such as JBA and JSDA, Japan Asset management Association, etc. However, there are no specific regulations and schemes for covering disputes of cross-border financial transactions.

4. Cases

4.1 Cold Call

- Some unauthorised foreign investment companies tried to raise funds from Japanese investors through their Web sites. FSA introduced a new guideline that they must register to the FSA in 2000. Since then, the number of such activities has significantly decreased.
- FSA provides on its web site various information useful for consumers in making e-finance transactions, including a list of registered or licensed financial service providers. (http://www.fsa.go.jp/densi/densi.html)
- It also provides a list of overseas securities firms known to be offering services to Japanese clients but not having registered in Japan's jurisdiction.(http://www.fsa.go.jp/densi/densi.html)

4.2 International Cooperation

- FSA is actively participating in various activities of international fora, such as the EBG of the BCBS, the Internet Task Force of the IOSCO, and the IAIS.
- Japan participates in the International Marketing Supervision Network (IMSN) and, more specifically, in eConsumer, http://www.econsumer.gov which is a pilot project run by the IMSN. eConsumer focuses on cross-border e-commerce B2C transactions, and provides an online portal for consumers to obtain information about the approaches to enforcement of consumer protection law within the participating countries, and to make a complaint online. Consumers consent to this information being viewed and used by the law enforcement agencies which participate in eConsumer. The consumer web page is supported by a secure database accessible only by participating agencies. The project is intended to facilitate dialogue between agencies and to streamline investigations of complaints with an international dimension.

4.3 Consumer Education

- FSA provides on its web site various information useful for consumers in making e-finance transactions, including a list of registered or licensed financial service providers. (http://www.fsa.go.jp/densi/densi_menu.html)
- It also provides a list of overseas securities firms known to be offering services to Japanese clients but not having registered in Japan's jurisdiction. (http://www.fsa.go.jp/densi/densi_menu.html)

Korea: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- *Framework Act on Electronic Transaction*, (the E-Commerce act) came into force on Dec 1, 2001. Covers only electronic banking. E-securities and e-insurance are excluded. There is no mention of electronic finance in the *Banking Act.*
- *Act on Electronic Financial Transactions*: the bill is under discussion at present and may be presented to the National Assembly early in 2002. This bill would define electronic payment methods, and take measures to step up inspection and supervision of information technology and enhance security and privacy in electronic financial transactions. According to one of the drafters if it goes ahead, this would be the first law of its kind, internationally. Proposed provisions include rights and responsibilities of the financial institutions involved in electronic transactions; and regulations of electronic payment products (e-money, smart cards etc).
- *Electronic Signature Act* is in place.
- *Regulation on Supervision of Electronic Financial Transactions by Financial Institutions* became effective in 2001, providing security and soundness of e-finance.
- *Act on Utilization and Protection of Credit Information*

Are any special licenses or permits required for E-Finance business?

- *There are no Internet-only banks in Korea. The basic regulatory rule in electronic banking has been compliance with the same rules as applied to bricks-and-mortar operations: commercial presence, licence/registration, compliance with regulations.*

1.2 Laws and regulations related to Cross-Border transactions

- There is no explicit provision for cross-border transactions in the draft law on electronic finance.
- Some sections of the existing legislation (Framework Act on Electronic Transactions, Act on Real Name Financial Transactions and Protection of Confidentiality; Act on Utilization and Protection of Credit Information; Regulation on Supervision of Electronic Financial Transactions by Financial Institutions) contain coverage of the cross-border issues.

1.3 Special laws and regulations for consumer protections in E-Finance

- Korea now has a Data Protection law in place (see below).
- General consumer protection is provided by the *Consumer Protection Act* (1980). It sets out the obligations of business and government and the role of the Korea Consumer Protection Board (KCPB). There are a number of other bodies with responsibility for consumer protection in specific areas of e-commerce (MOFE, FTC,MOCIE, MIC, MOJ) – see eConsumer.gov for details.

- *Act on Real Name Financial Transactions and Protection of Confidentiality* sets out in detail the obligations of financial institutions to carry out business on the basis of the real names of customers and to protect the privacy of transactions details except in specified circumstances where information is require by a prescribed authority for a legal purpose.
- *Act on Utilization and Protection of Credit Information.* Under the authority granted by the Ministry of Finance and Economy and provided for in the Act Korean Federation of Banks (KFB) serves as the credit information centre and manages credit information of individuals and businesses from financial institutions in Korea. This information is intended to help banks avoid bad loans.
- *Regulation on Supervision of Electronic Financial Transactions by Financial Institutions* covers issues on consumer protection since 2001.
- The Ministry of Finance and Economy has come up with strengthened regulations for on-line transactions in order to protect customers. The new rules, which came into effect in late 2001, include compensation clauses. MFE is also working on measures to protect consumers from possible losses arising from on-line fraud and illegal electronic transactions. (October 17&24, 2001, http://www.korea.net)
- Recently there has been a political commitment to proceed with a series of policies to enhance consumer rights in the era of digital economy. (http://www.korea.net, Dec. 5, 2001)

Are there any laws and regulations related to data protection?

- The Personal Data Protection Act, which was based on the OECD Guideline, has covered data protection in the public sector since 1994.
- In 2000, the MIC announced the 'Personal Data Protection Guideline', and publicised them through public hearings in the private sector. The guidelines covered information service providers, website operators, internet shopping malls, and off-line service provider such as travel agencies, airlines, hotels, etc.
- The Act Concerning the Protection of Personal Data on Information and Communication Network followed in January 2001 (the Data Protection Act). The Act follows the OECD guidelines and requires that personal data be collected only with permission and subjects should be advised of the purpose of the data collection, and their rights (including access to personal data). Disclosure to third parties without permission is restricted. The act also establishes the Korea Information Security Agency (KISA).

What types of internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- The Act on Promotion of Information and Communication Network Utilisation & Data Protection prohibits advertising (spam) data or e-mail for commercial purpose. Messages should not be sent without consent and must contain prescribed information content (sender's detail and purpose of mail), except when they include provision for senders to reject mail.

2. Self-regulation and Codes of Practice

2.1 Codes of Practice

- Korea Federation of Banks says it annually informs the public of information under its management, the kind of information, the purpose of pooling and sharing information, the list of organizations with access to the pooled data, and the protection of privacy rights in accordance with the Act on Utilization and Protection of Credit Information. (www.kfb.or.kr).
- KFB also has a set of General Terms and Conditions of Electronic Financial Transactions that set out a model for e-finance transactions. They spell out methods of handling errors and the obligations of banks to maintain and provide records of transactions.
- Consumer World (consumer information website) Http://www.consumer.go.kr provides a variety of information inlcuding Cyber Consumer Council
- A code of practice is maintained by the Korea Information and Contents Business Association http://www.kiba.or.kr but details are not available in English.
- Direct marketing guidelines (Korea Direct Marketing Association) http://www.kodma.or.kr (not available in English).
- Self-regulation on marketing practices of securities companies (Korea Securities Dealers Association) http://www.ksda.or.kr

2.2 Trust Mark/Seal of Assurance Schemes

- In early 2002, the Korea Information and Communication Industrial Association (KICIA) and the Ministry of Information and Communication (MIC) introduced the 'ePrivacy Marks' system which shows that businesses handle personal data on internet and electronic transactions according to the law and guidelines. (www.privacymark.or.kr)
- The 'I-Safe' mark system was also activated and is a more stringent system requiring a higher level of security and privacy protection. (36 companies acquired as of January 2002) However, at present it does not cover e-finance

2.3 Dispute Resolution

- The Cyber Consumer Centre (CCC), which was established in July 2000 as an affiliate body of the Korean Consumer Protection Board (KCPB) (http://www.cpb.or.kr), explores consumer issues and develops policy instruments for improving consumers' rights in cyber space. The CCC focuses on elaborating solutions for consumer matters. (http://www.econsumer.or.kr)
- The KCPB operates the consumer-counseling site (http://www.sobinet.cpb.or.kr) which provides advice on on-line consumer issues.
- The 36 I-Safe shopping mall help desks and the 50 eTrust shopping mall help desks provide advisory service at any cases in e-commerce consumer problems but do not cover e-finance.
- The Korea Information Security Agency (KISA) operates the Personal Data Protection Centre under the new Data Protection Act, and the Personal Data Mediation Committee from July 2001.

- Under the Data Protection Act, the Dispute Mediation Committee for Personal Data, consisting of 15 committee expert members appointed by the MIC, was established in December 2001.
- There are other public and private organisations which provide advice and solutions to consumer problems about e-commerce transaction issues.

3. Enforcement System

- Under the Consumer Protection Act consumers may request complaint redress and remedy for damages caused by use of goods or utilization of services to the Korea Consumer Protection Board (KCPB) with the procedure prescribed by Consumer Protection Act. This also covers e-commerce transactions. KCPB may recommend both the parties to agree on compensation for damages. If an agreement is not reached within 30days after receiving a complaint, it will be immediately referred to the Consumer Disputes Settlement Commission of KCPB. Consumer Disputes Settlement Commission, which has quasi-judicial power, will mediate and make a decision about the complaint. If both parties accept the verdict made by Consumer Disputes Settlement Commission, the verdict has the same legal effect as a judicial settlement in the court. If the company does not accept it, the KCPB will help the consumer by filing a civil suit. Consumer complaint redress and dispute resolution services are free of charge. The government budget bears the expense.
- The Ministry of Finance and Economy (MFE) introduced the regulation to protect consumers and to prevent improper electronic transaction and dispute. (established on December 1985, revised on December 2000)The MFE can issue orders to cancel improper contracts, to refund money for exaggerated advertisements, and compensate consumers' losses; it can order service providers to take necessary corrective measures and impose a fine for negligence. The MIC can also impose a fine or penal sentence for sending adult spam mail to under age people.
- The Internet Crime Investigation Center (ICIC) in the Supreme Public Prosecutor's Office is established to cope with the different characteristics of Internet and computer crimes. ICIC monitors recent trends about new types of crimes that include crimes in electronic commerce. ICIC also cooperates with domestic agencies such as Korean Information Security Agency and Information Communication Ethics Committee and maintains contact with foreign agencies to handle cross-country crimes.

4. Cases

4.1 Consumer Education

- The Ministry of Finance and Economy, in co-operation with the Korea Consumer Protection Board, has carried out a Consumer Protection Week in 2001 to start a campaign to organize seminars on protection for uses of the Internet and electronic commerce.

- 43 Electronic Commerce Resource Centers (ECRCs were established by Ministry of Commerce, Industry and Energy in 1997 to be involved in educating, training and consulting related to e-commerce. It is not clear whether they have special expertise in e-finance or consumer protection.

4.2 International Co-operation

- The Personal Data Mediation Committee is said to play a role in international co-operation.
- In February 2002, the KICIA exchanged an MOU with Japan (METI) to mutually admit their marks.
- Korea has taken an active role in developing the International Trustmark Network (ITN) which is a non-profit network organization consisting of members of internet trustmark awarding organizations. This includes trustmark schemes which cover personal information protection and consumer protection. The ITN is engaged in information sharing on the worldwide trustmarks program and mutual co-operation between members for resolution of consumer complaint on e-commerce. Korea hosted several early meetings of ITN to develop the structure and policies and will hold the position of the first Chair until the first half of year 2002. The initial participating organizations are IDA, CNSG of Singapore, PwC, ePublic of U.S.A, and KIEC, KAIT of Korea. Japanese organisations are considering whether to join.

4.3 Spam Email

- There are a number of organisations which provide their websites for reporting and solving the spam e-mail problem: The Information Communication Ethics Committee (www.icec.or.kr), The Personal Data Protection Center (www.cyberprivacy.or.kr), The Internet Crime Inspection Center of the Supreme Public Procurator's Office (www.icic.sppo.go.kr), The Police Cyber Center (www.police.go.kr).

Malaysia: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- *Banking and Financial Institutions Act 1989*
- With regards to the Malaysian capital market, the Securities Commission (SC) aims to ensure that all existing securities regulations is technology neutral and to undertake such reforms necessary to achieve this by way of legislative amendments, rule changes or policy statements to clarify the SC's views on capital market activities using technology platforms. Existing securities regulations encompasses the *Securities Commission Act 1993, Securities Industry Act 1983, Futures Industry Act 1993, Securities Industry (Central Depositories) Act 1991* as well as all subsidiary legislation and rules made thereunder.
- *The Evidence Act 1950*: this Act was amended in 1993 to enable computer-generated records and information to be admissible as evidence.
- *Interpretation Act 1948* and *1967* and *Companies Act 1965*: these Acts have also been amended, recognizing electronic storage of data and information as well as electronic submission of statutory forms and documents to the Registrar of Companies.
- *Computer Crimes Act 1997 (brought into effect 1 June 2000)*
  "This Act provides for a framework to counter computer offences such as unauthorised access to computer material, crimes of fraud and dishonesty through the computer, unauthorised modification of contents of a computer and so on. The Act is not limited by jurisdiction. It has effect outside as well as inside Malaysia. Where a computer crime is committed outside Malaysia in respect of computers or data in Malaysia or that which may be connected to or used in Malaysia, the crime may be treated as a crime within Malaysia and the perpetrator may be dealt with under the provisions of this Act." (Wong Sau Ngan)
- The *Digital Signatures Act 1997* (http://www.cca.gov.my/legislation.html): this Act became effective on October 1, 1998, and it provides for, and regulates the use of, digital signatures and other related matters concerning digital signatures. The related regulations are *Digital Signatures Regulations 1998*. http://www.cca.gov.my/legislation.html
- In a commentary on this act a specialist in legal & regulatory policy says the Act provides for the treatment of document signed with a digital signature created in accordance with this Act to be treated as legally binding as if the document was signed with a handwritten signature.
- The Bank Examination Department (of the Central Bank) has established the Information Systems Supervision Unit to -
  i) Monitor the soundness of the information and communication technology infrastructure of the financial institutions;
  ii) Advocate the implementation of internationally accepted best practices for ICT management; and
  iii) Assess the state of technology risk management within the financial sector with a view to its potential impact upon financial stability.

- Also the Government is reported to be in the process of drafting the personal data protection law, which was expected to be tabled by the end of 2001. The proposed law will regulate the collection, use and disclosure of personal data collected according to certain prescribed principles. (http://www.msc.com.my/mdc/infrastructure/cyberlaws.asp)

Are special licenses or permits required for E-finance business?

- Banking and Financial Institutions Act 1989 requires a person commencing to operate an electronic funds transfer system to obtain Bank Negara Malaysia's approval in advance.
- Bank Negara Malaysia has issued Minimum Guidelines on the Provision of Internet Banking Services by Licensed Banking Institutions that all licensed banking institutions should observe in providing Internet banking.
- Persons that fall within the definition of dealing in securities regardless of the chosen medium (electronic or otherwise) are required to be licensed under the Securities Industry Act 1983 and Futures Industry Act 1993.
- The SC is proposing to issue Guidelines on Electronic Prospectuses and Internet Securities Application. Some of the features of the Guidelines include security aspects, enhancements that can be made to an electronic prospectus, advertisements, notices that should be displayed, issuance, circulation or distribution of electronic prospectuses and electronic application forms and provisions for Internet securities application.
- "Guidelines on the Establishment of Electronic Access Facilities by a Universal Broker", issued by Securities Commission on August 29, 2001, provide guidance to universal brokers wishing to establish electronic access facilities, commonly referred to as Internet kiosks, investment centres, booths or terminals, for use by their clients.

1.2 Laws and regulations related to Cross-Border transactions

- Research to date has not revealed any special laws or regulations relating to cross-border transactions of banks, other than those related to foreign exchange.
- The SC had released a policy statement on *"Primary Offers of Securities via the Internet"* in August 1999. This policy statement deals with the position of securities that are offered by offerors based overseas via the Internet. The SC is of the view that an offering over the Internet that is accessible by persons in Malaysia will be caught under section 32 of the *Securities Commission Act 1993* which deals with proposals/offers that will require the prior approval of the SC. There are certain aspects that the SC will take into consideration in assessing whether approval is required under section 32. The policy statement also sets out several recommended practical steps/measures, (which are not exhaustive) that may be taken so that such offer will not be caught under the said section.
- Surveillance efforts in relation to the Internet or other forms of technology are preliminary, and there is no formalized system in place.

1.3 Laws and regulations for consumer protection in E-finance

- Bank Negara Malaysia issued Guidelines on Consumer Protection on Electronic Fund Transfer in 1989 which requires financial institutions providing any type of electronic fund transfer to have standard terms and conditions, which shall include the consumer's liability for any unauthorized electronic fund transfer, the consumer's right to stop payment of a pre-authorized electronic fund transfer and the consumer's right to receive relevant documents in relation to electronic fund transfers.
- A new piece of legislation on Personal Data Protection is in the process of drafting which aims to regulate the collection, possession, processing and the use of personal data by any person or organization. This Act, now in the final stages of drafting, will also introduce penalties including fines and imprisonment for those who abuse cyber-information.
- The SC's approach to ensuring consumer protection in E-finance is to ensure that investors are well-informed and educated so that they are able to self-police. This provides the best form of defence against any contravention of securities laws particularly those perpetrated over the Internet. To this end, the Securities Industry Development Centre (SIDC), the education and training arm of the SC had recently launched the Malaysian Investor (MIN) website (www.min.com.my) to educate investors on the capital market. The website covers the basics of investing, types of investment instruments as well as investor protection measures. In addition, the SC has, since end of 2000, posted a list of licensed intermediaries on the SC's website to enable investors to ascertain if whether they are dealing with persons who have been duly licensed by the SC.

2. Self-Regulation and Codes of Practice

2.1 Codes of Practice

- The *Code on Electronic Client-Ordering System (ECOS Code)* issued by the Kuala Lumpur Stock Exchange sets out requirements to be complied by stockbroking companies intending to provide for an electronic client ordering system to the general public. The Code deals with issues in relation to the role and responsibilities of the stockbroking companies and the system, connectivity and security requirements of the ordering system.

2.2 Trust Mark/Seal of Assurance Schemes

- A trust mark scheme was launched in Malaysia in January 2002. The ProTrust seal "provides Internet users with business information pertaining to site authentication, financial verification, front-end e-business details, privacy verification, as well as, back-end e-business process and integrity verification." (http://www.mybizaid.net/news_inhouse005.htm)

2.3 Dispute Resolution

- In relation to dispute resolution, Malaysia is a signatory to the Convention on the Settlement of Investment Disputes established under the auspices of the International Bank for Reconstruction and development that establishes facilities for international conciliation or arbitration.
- Further to this, the Kuala Lumpur Regional Centre for Arbitration was established in 1978 with the objective of providing a system for the settlement of disputes for the benefit of parties engaged in trade, commerce and investments with and within the Asian and Pacific region (http://www.klrca.org/main.html)
- On January 2002, Bank Negara advised that all commercial banks and finance companies have set up a dedicated Complaints Unit. The Unit is a focal point for managing complaints received by the banking institutions. Complaints lodged will be processed and responded within two weeks of its. In the event that the cases remains unresolved, banking institutions are required to explain in writing the reason for which the complaint could not be resolved. Complainants may then forward their complaint to the Banking Mediation Bureau (BMB).

3. Enforcement System

- The research at this stage has not revealed any specific regulations for dispute resolution and enforcement systems on E-Finance.
- With respect to cross-border transactions, in relation to securities in particular:
  - The SC is a member of global enforce.net, a web-based global discussion forum for securities regulators.
  - The SC is represented on the IOSCO Internet Task Force, which provides guidance on the use of the Internet by the securities industry and securities regulators.
  - The SC participated in the Internet Surveillance Training Program organized by IOSCO.

4. Cases

4.1 Consumer Education

- The Policy Statement on "Primary Offers of Securities via the Internet" was put to the test when the SC became aware of an unapproved fund, i.e. the Capitalshare Fund (Fund), soliciting investments from persons in Malaysia.A press warning on an unapproved fund taking the form of Capitalshare The Fund, is an offshore open-ended mutual fund consisting of 6 mutual funds which are traded on-line offered by an investment management company registered in the Cayman Islands.
- In deciding whether the Fund required the approval of the SC under the Malaysian securities law, consideration was taken with respect to the determining factors and practical steps highlighted in the SC's earlier policy statement on "Primary Offers Of Securities Via The Internet". It was decided that the Fund required the

approval of the SC since it was accessible to persons in Malaysia. Despite concluding that the Fund fell within the regulatory jurisdiction of the SC, the cross-border nature of the offer hampered any attempts at enforcement by the SC. The SC therefore decided that educating potential investors would be the best course of action in this circumstance. A press warning was therefore issued where public investors were warned of the danger in investing in such unapproved schemes and that they should be wary of such schemes that may be disseminated through the Internet, fax, brochures and other form of medium.

4.2 International Cooperation

- The SC has also forged closer ties and strengthened cross border co-operation with other international regulatory counterparts, such as the Hong Kong Securities and Futures Commission (SFC) and Thailand Securities and Exchange Commission (TSEC) on issues related to electronic enforcement. In this respect the SC had alerted the TSEC in relation to a non-licensed scheme in Malaysia ran by a company with a correspondence address in Thailand.

Mexico: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- The *E-Commerce Act* entered into force on June 7, 2000. This new legislation is based on the UNCITRAL model law. Areas covered include consumer protection, privacy**,** digital signatures and electronic documents.
- *The Credit Information Companies Act* (Ley para Regular las Sociedades de Información Crediticia) has recently been enacted, covering Habeas Data (Data protection) in financial and banking records. Until recently, credit rating agencies in Mexico, were regulated only by corporations rules. Consumers were not allowed to obtain a copy of their credit reports. Sections 42 to 44 of the new Act create a legal basis to allow consumers to obtain a copy of their credit reports and make a complaint**s** regarding inaccuracy of the credit data. Provisions of the *Credit Information Companies Act* allow consumer's access to their personal credit information fall short of e.g. the US *Fair Credit Reporting Act*.
- A new article has been included in the Consumers Protection Act empowering the government "to provide an effective protection to consumers of electronic transactions or transactions concluded by any other means, and the adequate use of data provided by the consumer" (Art. 1 - VIII); and to co-ordinate the use of an Ethics Code by financial services providers including the principles of this law.
- A new chapter in the Consumers Protection Act has been added, entitled "Rights of Consumers in electronic transactions and transactions by any other means." The new Article 76 bis, Section I, provides: "This article applies to relations between providers and consumers in transactions conducted by electronic means. The main principles stipulated by the Act are: a) Financial services providers shall use in a confidential manner, the information provided by the consumers and shall not be able to transfer it to third parties, unless the consumer express its consent to or exist a formal requirement from a public authority; b) Financial services providers must use technical measures to provide security and confidentiality to the information submitted by consumers, and notify the consumer, the characteristics of the system; before the transaction is made, c) Financial services providers must respect consumer decisions when they refuse to receive commercial solicitations.
- In principle there is an agreement on issuance of digital certificates for e-commerce transactions. The digital certificates system is based on a Public Key Infrastructure (PKI).
- A legislative draft for the *Electronic Bill Payment Act* is expected to be sent to Congress by March 2002 to its discussion and in its case approval. The Act will establish a legal basis for electronic bill presentment and payment system by the banking institutions.

Are there any special licenses or permits required for E-Finance business?

- E-finance business can be conducted by the registered and licensed financial institutions with physical presence in Mexico.

1.2 Laws and Regulations related to Cross-Border transactions

- Cross-border electronic transactions by consumers from individual accounts are not allowed. Foreign banks (branches or subsidiaries) have to establish a commercial presence in Mexico, be registered and licensed, and comply with the applicable regulations. There are no Internet-only banks in Mexico. Government agencies (e.g. "CONDUCEF") (e.g. The National Commission for the Protection and Defence of Financial Services Consumers "CONDUCEF") does not offer any protection to the consumers of overseas banking services. Certain cross-border electronic transactions/payments also escape the jurisdiction of CONDUCEF, e.g. Western Union, store cards and Centros Cambiarios. The Federal Consumer Protection Agency (PROFECO) has developed a legal framework for handling consumers' complaints, and refers financial cases for consideration by CONDUCEF.
- Unusual, suspicious or worrysome transactions, as well as transactions in excess of US $10,000 have to be reported to the Evaluating Committee of each bank before the National Banking and Securities Commission evaluates them. The Commission may forward the case to the Ministry of Finance which evaluates if a legal action proceeds regarding money laundering/ illicit activities.
- There is no special law applicable to cross-border transactions, due to the virtual impracticability of such a law.

1.3 Special laws and regulations for consumer protections on E-Finance

- No specific e-finance law has been developed to date. Provisions for electronic banking are covered within existing legislation, supported by the second-tier regulations/ guidelines by the Ministry of Finance, the Central Bank and the National Banking and Securities Commission, as well as the other National Commissions.

What types of internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- The Criminal Code was amended in 1999 to incorporate as a criminal offence the unauthorized access to computer systems (hacking). Activities to amend, destroy or cause the loss of information are criminal offences according to the new Criminal Code.
- No regulations/legislation in place concerning access of minors to restricted sites including pornography; unauthorised gathering of information from the Web sites ("spydering"); deceiving use of electronic information.
- The National Banking and Securities Commission will intervene to prevent offerings from the offshore banks to the Mexican residents, if the soliciting Web site is hosted in Mexico, or an advertisement is placed in a traditional media.

Are there any laws and regulations related to data protection? (particularly private information)

- The 1917 Mexican Constitution has long-standing protection of persons.
- Article 76 bis of the Federal Consumer Protection Act is formulated according to the seventh principle contained in the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (approved on December 9, 1999). It defines permissible uses of personal information, and requires consumer's authorization for the release of information to third parties.
- Article 214 of the Penal Code protects against the disclosure of personal information held by government agencies.
- Chapter 6 of Mexico's Postal Code, in effect since 1888, recognizes the inviolability of correspondence and guarantees the privacy of correspondence. In 1981, the Penal Code was amended to include the interception of telephone calls by third persons.
- The Law Against Organized Crime of 1996 allows electronic surveillance with a judicial order. Electronic surveillance in cases of electoral, civil, commercial, labor, or administrative matters is prohibited. Protection from unauthorized surveillance is extended to cover all private means of communications.
- The Ministry of Economy implemented strict measures, including introduction of electronic signatures, to protect consumer privacy and prevent Internet fraud and illegal e-commerce activities (October 2000).
- Public consultations will be initiated by the Ministry of Economy (Secretaría de Economía) and the Consumer Protection Agency (PROFECO), to discuss implementation of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

2. Self-regulation and Codes of Practice

2.1 Codes of Practice

- Article 24 Section IX bis of the Federal Consumer Protection Act requires the Federal Consumer Agency (PROFECO) in coordination with the Ministry of Economy to promote the use of ethics codes among businesses engaged in electronic commerce.
- The Mexican E-Commerce Association (AMECE) and the National Association of Public Brokers disseminate information to consumers.

2.2 Trust Mark/Seal of Assurance Schemes

- No special Mexico-based trust mark schemes have been identified.

2.3 Dispute Resolution

- Dispute Resolution Policy was developed by the Network Information Centre (NIC).

- The Federal Consumer Protection Agency, PROFECO is putting up a proposal to the Attorney General to develop an on-line ADR procedure.

3. Enforcement System

- Mexico is observing and analyzing the experience of e-banking development in other countries, and the papers and recommendations that have been published by international organizations such as Basel Committee on Banking Supervision, the OECD and within the scope of the NAFTA agreement.
- Mexican officials have co-operated with International Internet Sweep Days organised by IOSCO.
- The National Banking and Securities Commission has co-operative arrangements with the US Federal Reserve Board and the Bank of Spain.

4. Cases

4.1 Cold Calling Cases

- A fraudulent retirement plan operated by the foreign financial body was offered to the Mexican nationals resident in California, US. The dispute was resolved through the Ministry for Foreign Affairs, using consular and diplomatic channels. There are no successful examples of legal action against foreign providers in cross-border disputes. (Related to this issue we will like to know the source of this information)

4.2 International Co-operation

- Mexico participates in the www.econsumer.gov initiative which currently involves the US Federal Trade Commission, OECD and 14 individual OECD economies and has been operational since April 2001. The public Web site offers on-line lodging of complaints related to cross-border electronic commerce. There is also a restricted access law enforcement site, for the use of participating regulators and enforcement agencies.
- Mexico is a member of the International Marketing Supervision Network (IMSN) since 1994. It also serves as a gateway for disseminating the OECD information in Latin American countries, providing translation of the relevant documents into Spanish. Mexico participates in the International Internet Sweep days, targeting cross-border violations in e-commerce and internet securities trading.

New Zealand: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to e-finance

- There are no specific laws on electronic finance but a new law on electronic transactions (still in draft) has implications for e-finance. Existing commercial and securities laws apply to e-commerce generally.
- New Zealand statutes are available online (unconsolidated, so amendments need to be searched for separately) (http://www.knowledge-basket.co.nz/tkbgp/welcome.html)
- All banks operating in New Zealand must be registered with the Reserve Bank, are subject to supervisory requirements and are required by law to disclose their financial condition each quarter. In addition, non-bank financial institutions that fund from retail sources are required under the Securities Act to issue a prospectus, in which they are required to disclose their financial statements and related information. The Securities Act also requires any entity (including banks) that offers investment products to the public to issue disclosures in relation to the terms and conditions of the investment product and a summary of the risks associated with the investment. The Fair Trading Act and Consumer Guarantees Act also provide general protection for consumers of services, including financial services, particularly in relation to the service being "fit for purpose".
- Electronic securities trading systems are approved by the New Zealand Government through an Order in Council. Offers of securities can be made electronically under the Securities Act 1978. The Securities Commission is the entity responsible for monitoring and enforcing securities law disclosure. The Securities Markets and Institutions Bill, due to be enacted early 2003, will give the Commission additional enforcement and investigative powers and resources to investigate primary and secondary market breaches of securities law. This would be a significant strengthening of its enforcement powers and would apply to electronic transactions of securities.
- For securities business disclosure provisions are monitored and enforced by the Securities Commission. The Securities Commission has a range of powers to enable it to take action where an issuer of securities to the public is in breach of securities law, including the disclosure requirements.
- The *Electronic Transactions Bill* (based on UNCITRAL's Model Law on E-Commerce) is before Parliament. The Bill will reduce the uncertainty concerning the legal effect of electronic information and will provide default rules for the time and place of dispatch and receipt of electronic communications. The Bill will also allow certain paper-based legal requirements to be met by using electronic technology. The provisions are expected to come into effect later this year. The Bill will give legal effect to electronic records and signatures, and will be applicable to all acts and regulations requiring writing, signatures, or retention of records unless specifically excluded. See www.med.govt.nz for more information.
- The Crimes Amendment Bill has been introduced to deal with cyber crime issues.

- Policy work on a comprehensive reform of New Zealand's evidence law is well advanced and this will clarify issues to do with electronic evidence.
- The Minister of Consumer Affairs is considering changes to consumer credit laws. The reforms would replace the Credit Contracts Act 1981 and the Hire Purchase Act 1971 by a single Consumer Credit Bill. A key element of the Act would be to give the Commerce Commission authority and resources to investigate the activities of lenders and take action if necessary. This would be a significant strengthening of its enforcement powers and would apply equally to e-finance credit contracts. The Bill will allow credit transactions to be completed electronically, provided the debtor consents and other standards are met (such as the requirement that electronic documents be usable for subsequent reference).

Are any special licenses or permits required for e-finance business?

- There are no specific regulations for e-banking or online securities trading. However, electronic securities transfer systems require approval. Approval is given by the Government on the recommendation of the Securities Commission.

1.2 Laws and regulations related to cross-border transactions

- New Zealand has relatively few controls on foreign exchange transactions and foreign investment. However, a few specific restrictions exist. These relate to: United Nations sanctions, foreign investment rules (certain direct foreign investments may need approval from the Overseas Investment Commission) and terrorism (the New Zealand government has in place various measures to deal with the prevention and suppression of terrorist financing).
- New Zealand Criminal Law is considered to apply to domestic business that deals with foreign consumers.
- Almost all registered banks in New Zealand are foreign owned. Currently only two banks are owned by domestic interests and neither of these banks has a significant market share of the total banking market.
- Overseas persons may offer securities to New Zealand investors provided that, where New Zealand investors have been targeted, the investment disclosures meet the New Zealand requirements.
- There are no restrictions on non-registered offshore banks offering services through the Internet, unless the institution concerned uses 'bank' in its name and carries on business in New Zealand or has an office in New Zealand.
- Residents may deal with foreign banks in foreign jurisdictions.
- There are no laws in New Zealand that require the registration of intermediaries, dealers or advisors. Sharebrokers and futures dealers are treated differently.
- Overseas persons may offer securities to New Zealand investors provided that, where New Zealand investors have been targeted, the investment disclosures meet the New Zealand requirements. The Securities Markets and Institutions Bill (due to be enacted in early 2003) will implement a mechanism for mutual/unilateral recognition of other jurisdictions' offering documents. If recognition arrangements are developed with other countries, investment disclosures from those countries will not have to meet New Zealand standards. Currently, the

Securities Commission provides exemptions to New Zealand disclosure requirements for certain jurisdictions.

1.3 Laws and regulations for consumer protection in e-finance

- Existing consumer protection laws apply to all business activities irrespective of the channel used ("technology neutral" so it applies to e-commerce). The consumer protection legislation covers, among other activities, unfair trading practices, pyramid selling, door-to-door selling and consumer guarantees of quality in sales of both goods and services (so this would apply to e-finance). The Ministry of Consumer Affairs has broad responsibility for consumer protection regulation *(*http://www.consumer-ministry.govt.nz*)*.
- The *Model Code for Consumer Protection in Electronic Commerce* was issued by the Ministry of Consumer Affairs in October 2000 to support the development of industry codes for consumer protection in e-commerce transactions. The Model Code is an amalgam of key regulatory requirements (including fair trading, consumer guarantees, and privacy laws) and international guidelines. It is intended to provide guidance on the components of an effective self-regulatory framework that adequately protects consumers so they may have confidence in transacting online. While the Model Code is not legally binding or enforced by the Ministry, it sits against a regulatory backdrop and is complemented by enforcement mechanisms which give consumers access to remedies outside self-regulatory schemes. (http://www.consumer-ministry.govt.nz/Model_Code.html)

Are there any laws and regulations related to data protection (particularly private information)?

- New Zealand's Privacy Act 1993 applies to the handling of all personal information collected or held by agencies, whether in the public or private sectors. Personal information includes any information about an identifiable living person, whether it is on a computer, in a paper file or stored in other forms. The Act has twelve information privacy principles. The principles are technology neutral, which allows them to operate in a number of contexts and also means they will not date as new technologies come into existence. The principles are not prescriptive but set a number of standards and allow agencies to meet them in their own way. They recognise that different kinds of agencies will have different purposes for having information. (http://www.e-commerce.govt.nz/privacy/index.html). The Privacy Act has undergone several amendments from 1993 onwards. (http://www.privacy.org.nz/people/fact3-0.html)
- Common law in New Zealand also places strict duties on banks with respect to the confidentiality of client information.

What types of Internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- As in Australia, the Privacy Act 1993 limits the opportunities for spamming, by requiring businesses to advise consumers of the purpose for which information is collected, and by limiting the purposes for which information may be used and disclosed. This limits the on-selling of mailing lists.

2. Self-Regulation and Codes of Practice

2.1 Codes of Practice

- The Ministry of Consumer Affairs encourages individual businesses and trade associations to adapt and adopt the *Model Code for Consumer Protection in Electronic Commerce* to help ensure that their practices meet consumers' interests. (http://www.consumer-ministry.govt.nz/Model_Code.html) and offers the Guideline for Developing a Code of Practice (http://www.consumer-ministry.govt.nz/discussion_papers/dp_codes_of_practice.html)
- The Ministry of Consumer Affairs monitors industry self-regulation including codes - eg, Insurance, Banking and Direct Selling codes of practice.
- The Consumers' Institute is an NGO which is self-funding and provides lobbying and advocacy on consumer issues. It maintains web-based consumer information on contract to the Ministry of Consumer Affairs (http://www.consumer.org.nz)
- There are codes of practice under the Privacy Act 1993 which have the status of legislation. (http://www.privacy.org.nz)
- Electronic Transactions Bill (http://www.med.govt.nz/irdev/elecom/transactions/index.html)

2.2 Trust mark/seal of assurance schemes

- The Direct Marketing Association (http://www.dma.co.nz) and the Advertising Standards Authority (http://www.asa.co.nz) have developed an Electronic Marketing Standards Authority (http://www.emsa.co.nz) which will operate a trustmark and dispute resolution process for consumers who have experienced problems with online advertisers or marketers.

2.3 Dispute resolution

- The Disputes Tribunal is part of the courts system and provides a low cost, informal alternative to court proceedings. *(*http://www.courts.govt.nz*).*
- It is not clear whether there are any pure online alternative dispute resolution providers based in New Zealand. However, there is a large number of ADR practitioners based in New Zealand, and we understand that ADR practitioners do conduct dispute resolution at a distance, using telephone, fax, and email communications.
- New Zealand law also enables the parties to a contract to agree on their own dispute resolution processes, and this is frequently done by way of contractual agreement between parties in a wide range of contracts.
- In addition, the Arbitration Act makes provision for parties in dispute to appoint an arbitrator to mediate between the parties and to assist in reaching a solution.
- In the banking industry, the Banking Ombudsman scheme also provides a process for contracting parties to resolve their disputes with a bank, where the parties

request the Banking Ombudsman to assess the dispute and to impose a binding solution on the disputing parties.

3. Enforcement System

- The Commerce Commission is responsible for enforcement of fair trading and competition legislation (http://www.comcom.govt.nz). The Commission can bring civil or criminal actions in the courts, which can impose fines and grant a variety of remedies.
- The Privacy Commissioner is responsible for enforcing the Privacy Act 1993 (http://www.privacy.org.nz). Most privacy-related consumer complaints are resolved through conciliation by the Privacy Commissioner, who is required by statute to attempt to conciliate complaints.
- The Securities Commission is responsible for enforcement of securities legislation (http://www.sec-com.govt.nz). The Commission can make a range of orders in relation to breaches of securities law and will be able to take civil actions in the Courts for breaches of securities trading law under the Securities Markets and Institutions Bill.

4. Cases

4.1 Consumer Education

- Public and private consumer organisations periodically publish consumer awareness reports and, where necessary, consumer alerts.
- The Securities Commission maintains, on its website a list of warnings it has issued (see http://www.sec-com.govt.nz). It currently is posting warnings from the Serious Fraud Office about Advance Fee frauds such as the infamous Nigerian letters. These letters are not uncommon in New Zealand. The would-be victim is offered the opportunity to access multi-million dollar funds said to have been generated by government or quasi government contracts by the payment of certain monies to Nigeria (or to bank accounts set up by the Nigerian fraudsters). The Serious Fraud Office considers that an educated investing populace is the best deterrent to thwarting would-be fraudsters but it is not clear that criminal prosecutions would be possible since the originators would be outside its jurisdiction.
- The Ministry of Consumer Affairs operates Scam Watch, a web based information resource which warns consumers of scams circulating in New Zealand. The types of scams listed include: unauthorised prize and lottery schemes, Nigerian letter advanced fee fraud, pyramid selling schemes and unregulated investments. It also includes information on Internet based offers of investments and suggests several measures to deal with spam mail.

4.2 Cold calling cases

- The Securities Commission cooperated with Hong Kong authorities to contact New Zealanders who had sent money to bank accounts in Hong Kong for investments as a result of cold-calling from Manila and Bangkok.
- The Securities Commission maintains a warning list on its website (www.sec-com.govt.nz) of overseas brokers who offer securities to New Zealand consumers, mainly through cold-calling.

4.3 Criminal prosecutions

- The SFO has a court case pending against an individual facing charges alleging involvement in a "Prime Bank Instrument" scam and has successfully convicted an investment advisor on a similar charge. The Prime Bank Instrument fraud is a sophisticated method of Advance Fee fraud that developed in the 1980's in the USA and in Europe. It is premised on the so-called existence of a secret market within which the world's prime banks are said to trade financial instruments on a daily basis in billion dollar volumes and at huge, irreversible and perpetual profits. In the New Zealand case it is not clear whether the approaches were made over the Internet or by direct calls.

-

4.4 International Cooperation

- The Securities Commission is a member of IOSCO and co-operation with home authorities of foreign banks
- New Zealand (through the Ministry of Consumer Affairs) is a member of the international Marketing Supervision Network (http://www.imsnricc.org) MSN and econsumer.gov, (http://www.econsumer.gov) which provides a portal for consumers to make complaints about cross-border electronic transactions which have gone wrong. Consumers can also access information on the approaches to enforcement of consumer protection law by participating countries.
- EMEAP, an organisation of Asian-Pacific central banks, also provides a framework for sharing information and perspectives on issues relating to payment systems and electronic finance systems.

Singapore: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws relating to E-finance

- Monetary Authority of Singapore (MAS), the principal regulator and supervisor of financial institutions in Singapore, has issued a number of MAS *Guidelines and Policy Statements* that relate to the provision of financial services via the internet. These include *Policy Statement on Internet Banking (19 July 2000), Internet Websites Circular (January 2000) and Internet Guidelines (14 February 2000).*
- Singapore has introduced a number of general e-commerce policy initiatives and laws which also affect e-finance. The *E-commerce Hotbed Programme* was introduced in 1996 to develop the e-commerce legal and technical infrastructure, and e-commerce services. In 1998, the *Electronic Commerce Master Plan* was published. This aims to bring in e-commerce to develop Singapore as an international e-commerce hub (building upon its established strengths in international trade, international financial services, telecommunications and IT systems). It also aims to create an e-commerce services sector, and to harmonise cross-border e-commerce laws and policies.
- The *Electronic Transactions Act* 1998 ("ETA") was enacted in1998 (based on the UNCITRAL Model Law on E-Commerce). The ACT aims to facilitate e-commerce by affording legal recognition to electronic and digital signatures; by establishing the legal framework which provides for the setting up of a Public Key Infrastructure; by affording legal sanction to electronic records, files and documents; and by allowing public institutions and government departments to accept filing and issue licences and permits in electronic form. The Act also clarifies the network service providers' liability for third party content.

What types of internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- The *Computer Misuse Act* (Chapter 50A Part II) contains a list of offences. For details of the *Computer Misuse Act*, see http://agcvldb4.agc.gov.sg/

Are any special licenses or permits required for E-Finance business?

- Under MAS's Policy Statement on Internet Banking, the admission criteria for internet-only banks will be the same as for traditional banks except for the lower minimum paid-up capital requirement for subsidiaries of Singapore-incorporated banking groups. Singapore currently has at least one licensed internet-only bank.

1.2 Laws and Regulations related to Cross-Border transactions

- The current regime of import and export regulations and procedures applies to e-commerce. TDB's website has more information: http://www.tdb.gov.sg/ieinfo/importexport.shtml

- The Monetary Authority of Singapore (MAS) requires entities transacting in banking business and offering banking services in Singapore, including via electronic means, to be licensed.
- MAS's licensing framework does not draw a distinction between traditional banks and non-traditional banks such as e-banks.

1.3 Special laws and regulations for consumer protections on E-Finance

- There is no comprehensive consumer protection legislation in Singapore to-date. Any action brought for damage caused by defective products will be primarily premised on the law of tort or contract.
- Section 47(3) of the *Banking Act* gives the legislative foundation for banking secrecy. It provides that no person may reveal any information whatsoever regarding the money in or other relevant particulars of accounts. Section 47(3) is subject to certain exceptions, most notably, where the customer consents to the release of such information. Other than Section 47(3) above, there are numerous statutory provisions providing for confidentiality of data (including personal data) in specific instances, e.g. the *Computer Misuse Act* (Chapter 50A) contains provisions which protects data stored in computers from unauthorized access and tampering; and the Telecom Competition Code which requires all telecom service providers licensed by the Infocomm Development Authority (IDA) to protect end user service information. Singapore also has a strong common law tradition, e.g. common law remedies for breach of confidence; copyright; defamation; negligence.
- The *Evidence Act* was amended in 1997 to allow the use of electronic records as evidence in the courts.
- The *Computer Misuse Act* defines a class of critical computer systems and provides them with greater protection. To deal with new potential abuses of computer systems, the *Computer Misuse (Amendment) Bill* came into force on 1 Aug 98. The amended act takes a more sophisticated approach to provide for enhanced penalties proportionate to the different levels of potential and actual harm caused. It also addresses new potential computer abuses such as denial or interruption of computer services and unauthorised disclosure of access codes.

Are there any laws and regulations related to data protection? (particularly private information)

- As stated above, there are numerous statutory provisions dealing with various aspects of data protection, the most common being the use and disclosure aspects of data protection. The Government established a set of Public Sector Data Protection Principles in Nov 2001 to govern the use, retention, sharing and protection of personal data of the public among the government agencies. There is, however, no general and comprehensive data protection or privacy legislation in Singapore. The common law of confidence also provides civil remedies against the unauthorised disclosure of confidential information imparted in circumstances that impart an obligation of confidence and that result in detriment to the party communicating it.
- The Infocomm Development Authority of Singapore (IDA), on behalf of the National IT Committee, released a set of guidelines on January 6, 2000 to

safeguard public interests when Internet Access Service Providers (IASPs) conduct preventive security scanning exercises.

- The Computer Misuse Act 1993 ("CMA") prohibits the unauthorised interception of computer communications. However, the CMA provides the police with additional powers of investigation. allowing the police lawful access to data and encrypted material in their investigation of offences under the CMA
- The Electronic Transactions Act 1998 ("ETA") imposes a duty of confidentiality on electronic records, books, registers, correspondence, information, documents or other material obtained under the Act.
- The Telecom Competition Code imposes a duty on telecom service providers licensed by the IDA to protect end user service information. This includes, but is not limited to, information regarding the end user's calling patterns; the services or equipment used by the end user; the end user's telephone number and network configuration; and the end user's billing name, address and credit history.
- The Banking Act Chapter 19 provides for secrecy of bank accounts.
- MAS is working with the industry to set up the Singapore Consumer Credit Bureau, an industry-led project, which will be launched in September 2002.

2. Self-regulation and Codes of Practice

2.1 Codes of Practice

- In 1999, the National Internet Advisory Committee (NIAC) released a voluntary industry *E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce ("the E-Commerce Code")* with the aim of establishing public confidence in e-commerce transactions over the Internet. It was adopted by CaseTrust and incorporated into its Code of Practice as part of an accreditation scheme promoting good business practices among store-based and web-based retailers. CaseTrust is an accreditation programme, developed by the Consumers Association of Singapore (CASE), which recognises good business practices among store-based and web-based business establishments.
- However, the drafting of the E-Commerce Code did not take into account the 1998 EU Directive which prohibits the transfer of personal data by EU countries to a country which does not have an adequate data protection regime. The Legal Sub-committee of the NIAC subsequently prepared a more comprehensive Model Data Protection Code for the Private Sector ("the Code"), which was released in February 2002, for industry self-regulation in Singapore. The data protection provisions in the E-Commerce Code have since been superseded by the more detailed Code.
- The Code seeks to be applied to data processing activities across all sectors (in the private sector), and serves two key purposes:
    a) It establishes minimum acceptable standards for electronic data protection; and
    b) It promotes the harmonisation of electronic data protection principles among the various sectors, rendering the future establishment of any data protection regime an easier task.

- The Code is modelled on internationally-recognised standards, in particular the *1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*; the *1995 EU Directive*; and the *1996 Canadian Standards Association (CSA)'s Model Code for the Protection of Personal Information*.
- The Code is worded in general terms as it is intended to be applied by a wide range of industry sectors. As such, the framework has to be broad and flexible enough to take into account sectoral differences, variations in individual cases, even the development of new technologies.
- The Code establishes 11 "Data Protection Principles" which, it is intended, will serve as national benchmarks for the fair handling of personal data. They are:
    1) Accountability
    2) Identifying purposes
    3) Consent
    4) Limiting collection
    5) Limiting use, disclosure and retention
    6) Accuracy
    7) Safeguards
    8) Openness
    9) Individual access
    10) Challenging compliance
    11) Transborder data flows (optional)
- The Code is voluntary and is not law.
- The Code has since been passed on to the National Trust Council (NTC) for adoption. The intent of the Code is in line with the NTC's charter to build confidence amongst businesses and consumers in on-line transactions so as to spur e-commerce growth. The NTC launched a public consultation exercise for the Code in February 2002 to seek wider feedback from members of the industry and the public.

2.2 Trust Mark/Seal of Assurance Schemes

- In March 2001, the NTC implemented a nationwide trust mark initiative, known as the TrustSg Programme, to recognise on-line merchants with sound e-commerce practices.
- Existing and potential trust mark providers such as trade associations, chambers of commerce and businesses are encouraged to accredit themselves under the TrustSg Programme. If their Code of Practice meet the standards set by NTC, they will be appointed as Authorised Code Owners (ACO) and be given the authority to award the TrustSg seal to the worthy on-line merchants within their industry.
- To obtain the TrustSg seal, on-line merchants have to comply with the Code of Practice set by their respective ACO.
- There are presently two ACOs for the B2C category; namely the Consumers Association of Singapore (CASE) and Commerce Trust Ltd.
- The TrustSg Programme is an important initiative which will contribute towards the development of Singapore as a trusted e-commerce hub. The benefits are two-fold. Accredited on-line merchants will be recognised as trusted and secure players by end-users both locally and globally. Consumers in return, will feel

assured to transact with a TrustSg accredited merchant, thus gaining the sense of confidence in on-line transactions.

2.3 Dispute Resolution

- Electronic Alternative Dispute Resolution mechanisms are supposed to be available through the Internet to resolve any type of dispute including those related to e-banking and on-line securities activities.
- IDA is working with the Singapore IT Dispute Resolution Advisory Committee (SITDRAC), Singapore Mediation Centre, Singapore International Arbitration Centre and e@dr to educate and raise both business and consumer awareness on the usefulness of ADR schemes that are available to them.
- e@dr is an electronic dispute resolution process offered by the Subordinate Courts in partnership with the Ministry of Law, the Singapore Mediation Centre (SMC), the Singapore International Arbitration Centre (SIAC), the Trade Development Board and the Economic Development Board. e@dr seeks to leverage on the use of technology to help resolve disputes.
- CDRI - Court Dispute Resolution International: Where the case is complex or involves a substantial claim, it will be channelled to the Court Dispute Resolution International (CDRI) service, and e.CDRI (which is the electronic version). CDRI and e.CDRI are settlement conferences co-conducted by a Singapore judge-mediator and a judge from a foreign jurisdiction. The co-mediation provides a forum in which additional judicial perspectives and views are brought to bear on disputes.
- The Singapore Mediation Centre ("SMC") is a non-profit making and non-partisan entity funded by the Government through the Ministry of Law, and guaranteed by the Singapore Academy of Law. It has the support of both the Supreme Court of Singapore and the Subordinate Courts of Singapore.
- The Singapore International Arbitration Centre (SIAC) is a non-profit organisation which aims to:
- provide facilities for international and domestic commercial arbitration,
- promote arbitration as alternatives to litigation for the settlement of commercial disputes.
- The SIAC Rules are based largely on the UNICITRAL Arbitration Rules and the Rules of the London Court of International Arbitration
- SITDRAC is an honorary advisory committee to the Singapore Mediation Centre and the Singapore International Arbitration Centre on IT matters.

3. Enforcement System

- No additional information is available on enforcement.

4. Cases

4.1 Consumer Education

- While there are no consumer education/awareness programs specifically on e-finance, IDA looks after consumer education in e-lifestyle more generally. For more information, see http://www.ecelebrations.gov.sg/main_flash.htm

4.2 International Cooperation

- Co-operation with the home supervisors of foreign banks.
- Singapore has forged bilateral agreements with several countries on collaboration on e-commerce. Memorandums of understandings have been concluded with China, India, Australia, Germany, Korea, UK, Japan and Canada.
- Singapore-Canada collaboration. On June 1998, Singapore successfully completed interoperability trials for cross-certification of Singapore's and Canada's Public-Key Infrastructures (PKIs). This cross-certification arrangement was the first in the world and it set a precedence for trusted cross-border transactions to occur using the existing infrastructure for local PKIs. With the Singapore-Canada cross-certification infrastructure in place, local businesses and consumers would eventually be able to use locally issued digital certificates to conduct secure transactions with users holding certificates issued by a Canadian CA.
- Singapore-India Collaboration. Singapore and India have embarked on several bilateral co-operative projects on e-commerce, e-learning and e-governance. Singapore is working with India in the setting up and operation of electronic clearance of trade documents. Both countries are also undertaking a joint programme to develop PKI interoperability. This involves information sharing, standards harmonisation and establishing cross certification links.
- Asia PKI Forum. Singapore, together with Japan and Korea co-founded the Asia PKI Forum, an industry-led forum with the objective to promote the use of PKI as the foundation to secure cross-border e-commerce. Other members to the forum include Australia, China, Hong Kong, Malaysia and Chinese Taipei.
- Japan-Korea-Singapore Collaboration on PKI. Singapore, Japan and Korea embarked on an experiment in June 2001 to achieve cross-border technical PKI interoperability between CAs.

Chinese Taipei: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to Finance and E-finance

- Chinese Taipei's *"Banking Law"* allows deposits to be withdrawn and transferred in a manner that a bank may agree with its customers, which can include withdrawing and transferring via the Internet.
- The government approved the *"Standard Service Agreement of PC and Internet Banking"* submitted by the Bankers Association on May 26, 1999. The Standard Agreement provides a sample copy of contract for banks intending to engage in e-banking with consumers. Banks intending to offer PC and internet banking are urged to prepare their own form of agreements in line with the spirit behind the principles set forth in this Standard Agreement. (http://www.bmck.com/ e-commerce/Banking-Financials/00.12.22Taiwan.doc)
- Ministry of Finance approved *"The Security and Management Criteria for Electronic Banking of Financial Institutions"* submitted by the Bankers Association on August 7, 2000, aiming at setting-up minimum security measures including cryptographic algorithms.
- Ministry of Finance published *"Regulations Governing Approval of the Issuance of Store-Value Card by Banks"* on Oct 8, 2001.
- *"Electronic Signatures Law"*, which gives legal validity and status to electronic documents, signatures, and media equal to paper-based transactions was passed on Oct 21, 2001, and comes into effect on 1st April 2002. (http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm).
- Ministry of Economic Affairs (http://www.moea.gov.tw) is developing an *"Action Plan on the Overhaul of E-Commerce Environment and the promotion of B to C E-Commerce"*. The aim is to improve the environment for the development of E-commerce regulations and to solve the problems incurred by E-commerce. (http://stlc1.iii.org.tw/eclaw/ec_law.htm). Ministry of Economic Affairs was also responsible for drafting of *"Electronic Signature Law"*.
- *Penal Law* and *Code of Criminal Procedure* have been amended in order to combat cyber crimes. A first draft of a specific charter on cyber crime in the *Criminal Law* has been completed. (April 01 2002 Business Times)

Are any special licenses or permits required for E-finance business?

- No virtual banks exist. Banks are required to have a physical presence.
- Banks providing E-banking service are required to apply for the approval of Ministry of Finance in advance.

1.2 Laws and regulations related to Cross-Border transactions

- Under the *Banking Law*, a foreign bank is required to have a physical presence to offer traditional banking activities or e-banking activities.

- Chinese Taipei's supervisory authorities conduct on-site examinations on foreign bank branches (foreign banks that provide cross-border services must have a physical presence in Taipei) to ensure proper Internet banking activities are provided to consumers.

1.3 Laws and Regulations for Consumer Protection in E-finance

- The protection of Internet consumers will be reinforced by "*Guideline on Consumer Protection in Electronic Commerce*", devised by Chinese Taipei's Consumer Protection Commission in November of 2001, and the pending Amendment to the existing "*Consumer Protection Law*". (http://www.cpc.gov.tw)

What types of Internet activities would be prohibited by the legislation?

- None are explicitly banned.

Are there any laws and regulations related to data protection (particularly private information)?

- In order to protect the safety of the transmission of data related to financial information, Chinese Taipei has promulgated the "*The Security and Management Criteria for Electronic Banking of Financial Institutions*" as the minimum requirement for e-banking security controls. The Criteria themselves, combined with the "*Standard Service Agreement of PC and Internet Banking*", have demonstrated government's determination to encourage banks to develop e-banking products and services, including the capital transfer to the consumer on the Internet.
- "Law Protecting Computer-Processed Personal Data" was passed in 1995. According to the LPCPD, private enterprises such as banks, financial institutions, securities houses, insurance companies, telecommunication companies, and futures commission merchants that intend to collect personal data via computers must first be approved and licensed by competent authorities. (http://www.bmck.com/ e-commerce/Banking-Financials/00.12.22Taiwan.doc) Under this law, Internet banking services may require a license for data collection.

2. Self-regulation and Codes of Practice

2.1 Codes of Practice

- Secure Online Shopping Association (http://www.sosa.org.tw)

2.2 Trust Mark/Seal of Assurance Schemes

- Institute for Information Industry has advocated "Trust Mark" in a series of reports such as "Study Report on the Mechanism to Push for Quality E-Shops" and seminars including "Taiwan e-TRUST Forum at MOEA" in May 2001. (http://www.ec.org.tw/net/ecpilot/0310.html)
- Secure Online seal programme (http://www.secureon-line.com.tw)

- Secure Online Shopping Association (http://www.sosa.org.tw)
- Net Consumers Association (http://www.net080.com.tw)

2.3 Dispute Resolution

- Secure Online Shopping Association (http://www.sosa.org.tw)
- Net Consumers Association (http://www.net080.com.tw)

3. Enforcement System

- "Bureau of Monetary Affairs" (http://www.boma.gov.tw/index.htm) under the Ministry of Finance (http://www.mof.gov.tw/), is responsible for the regulation, supervision and study of financial development and policies. BOMA is now drafting a plan to advance e-finance. (http://www.boma.gov.tw/index_dir01.htm)
- Securities and Futures Commission (http://www.sfc.gov.tw/) administers and supervises the issuing and trading of securities and futures. In promoting the project of electronic trade on securities, SFC instructs "Taiwan Stock Exchange Cooperation" and "Over-The-Counter Securities Exchange" to amend laws and regulations to guarantee the security of electronic trading and reduce the risk.
- Ministry of Justice (http://www.moj.gov.tw) has responsibility for criminal and legal issues.
- Consumer Protection Commission (http://www.cpc.gov.tw) was founded in July 1994 to study, propose, and review basic policies on consumer protection and to supervise the implementation of these policies. CPC also devised "Guideline on the Consumer Protection in Electronic Commerce" in order to ensure transaction fairness, protect consumer rights, establish consumer confidence in e-commerce, and promote the healthy development of e-commerce, as well as provide guidance to competent authorities in establishing consumer protection measures.

4. Cases

4.1 Consumer Education

- "Consumer Online Shopping Guide", posted on the website of Consumer Protection Commission, serves to enhance consumers' awareness of the risks in on-line shopping. (http://www.cpc.gov.tw/cpc2/cpc2_1_11.doc)
- Net Consumers Association (http://www.net080.com.tw/home.asp)
- Secure Online Shopping Association, Consumer's Foundation and Consumer Protection Institution of China also provide consumers with useful information when shopping and trading on-line. (http://www.sosa.org.tw, http://consumers.org.tw, http://www.e-consumer.org.tw/index.asp)

4.2 Cold Calling Cases

- No information is available about experience of cold-calling cases in Chinese Taipei.

4.3 Hacking

- So far, there is no case in Chinese Taipei of customers' accounts of an Internet Bank being hacked.

4.4 International Co-operation

- Chinese Taipei's Criminal Investigation Bureau (CIB) has reached a tentative agreement with its Chinese counterparts in Beijing and Shanghai in December of 2001 to install a hotline to exchange information on crime including all sorts of Internet-based crimes. The bureau said that over 3,500 Chinese criminals were arrested in Taipei from Jan. 1 through Oct. 31 of 2001. (Taipei Times, January 29th, 2002)
- Chinese Taipei and US signed a judicial assistance pact on Nov. 14 of 2001 that will provide communication channels for judicial officials of the two countries to jointly clamp down on drug trafficking, money laundering and other crimes, including economic and Internet offenses. (Taipei Times, January 3rd, 2002).

Thailand: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- No special legal framework for electronic financial transactions until draft laws (below) are passed.
- Banking Law and Securities Law cover any electronic financial transactions at present. Providers must be licensed. Rules and regulations regarding explanations required for sales of financial services do not vary with the types of communication used. The banking and securities laws are *Commercial Banking Act*, B.E. 2505, *Ministerial Regulation & Notification* of the Ministry of Finance, *Notifications & Circulars* of the Bank of Thailand, *Act on the Undertaking of Finance Business, Securities Business & Credit Foncier Business*, B.E. 2522.
- The *Electronic Transaction Law* was approved by the Parliamentary on October 31 in 2001 and enacted in February 2002. According to Article 3 of the *E-Transaction Bill*, the law applies to all civil and commercial transactions using electronic data, except for those that are specified in a Royal Decree.
- The *Electronic Transactions Act* defines the legal status of electronic records as being equal to paper documents, if they are properly handled. The Act also defines the scope of legal recognition of transmission and reception processes for electronic data records; time and place of occurrences of such transmission.
- The *Electronic Signature Act* defines the electronic equivalence of signature as a proof to identity of the signing party (i.e., authentication) and that the signer approves the content that is being signed. The law is neutral to the choice of technology used for electronic signature. It recognizes the well established trusted third-party system of *Certification Authority* (CA) and *public-key infrastructure* (PKI) based on encryption technology. At the same time, it also gives a freedom of choices for business parties to choose their own kind of electronic signature.
- The IT Laws Development Project as part of the National Information Technology Committee (NITC) and the National Electronics and Computer Technology Center (NETEC) is drafting six IT laws: *Personal Data Protection Bill, Computer Crime Bill, Electronic Funds Transfer Law, Universal Access Bill, Development on Information Infrastructure Bill.* As yet there is no description of these draft bills available in English.

Are any special license or permits required for E-Finance business?

- Any existing financial institutions seeking to offer their services over the internet must get the approval from the Bank of Thailand in advance.
- Bank of Thailand has issued new guidelines regarding the Usage of Internet network for undertaking of commercial banking business to cover all business transactions which are permissible by the Banking Law.
- The Securities and Exchange Commission has already issued guidelines on securities trading system for on-line brokers.

1.2 Laws and Regulations related to Cross-Border transactions

- The Bank of Thailand requires any entities offering banking services, irrespective of the channel used, to be licensed and have physical presence in Thailand.
- The foreign exchange regulations seem to permit transfers in and out of the country in both domestic and foreign currency. For residents evidence is required for the source of funds and for obligation to pay in foreign currency, which may limit the possibilities for freely using internet for these transactions. Non-residents are free to operate on domestic and foreign currency accounts held with Thai banks so they should be able to use cross-border e-finance methods more easily than residents.
- The legal basis for exchange control in Thailand is derived from the *Exchange Control Act* (B.E. 2485) and *Ministerial Regulation No. 13* (B.E. 2497) issued under the *Exchange Control Act* (B.E. 2485). Forex control is entrusted to the Bank of Thailand by the Ministry of Finance. All foreign exchange transactions are to be conducted through authorized banks. Authorized persons (money changers) can only buy foreign notes and travellers' cheques and sell foreign notes.
- Foreign currencies can be brought into Thailand without limit but any resident must deposit them with a Thai bank within 7 days. Foreign currency deposit accounts are available but there are restrictions on deposits and withdrawals requiring evidence of obligation to pay in foreign currencies to persons abroad, authorized banks, the Export and Import Bank of Thailand, or the Industrial Finance Corporation of Thailand within 3 months from the date of deposit.
- Nonresidents can open and maintain both foreign currency and baht accounts with authorized banks in Thailand. The forex accounts must be deposits of funds that originate from abroad. Balances on such accounts may be transferred without restriction.
- Capital transactions (payments for services, investments etc) are permitted for both foreigners and Thai residents, in some cases with supporting documentation, Inward foreign investments are not limited, outward transfers by Thais are permitted up to US$10 million yearly.
- Securities business license must be obtained from the Minister of Finance upon the recommendation of the SEC in order to provide securities services in Thailand. Currently, the SEC has a policy not to issue any new securities license. It gives a list of on-line securities firms under SEC's supervision in its web site.

1.3 Special laws and regulations for consumer protections in E-Finance

- There are no special laws, regulations or guidelines relating to consumer protection in e-finance.
- Existing consumer protection laws are applied to all business activities irrespective of the channel used. (further details will be provided on the features of the general consumer protection law - whether provisions on unsolicited business will be applied to internet and e-finance transactions)

What types of internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- This will not be clear until the Computer crime law is complete

Any laws and regulations related to data protection (particularly private information)

- Yes – see above Data Protection Law.

2. Self-regulation

2.1 Dispute Resolution

- Existing consumer protection laws are applied to all business activities irrespective of the channel used.
- Complaint handling processes are the same as those for traditional services.

3. Enforcement

- The SEC is a member of IOSCO. Thai SEC has MOU with eight countries to cooperate on cross-border supervision.
- The Bank of Thailand is studying recommendations that have been published by BIS and other supervisory entities on standardising approaches to cross-border supervision and enforcement.

4. Cases

4.1 Consumer Education

- No specific information.

4.2 Cold Calling and Similar Cases

- Case described below illustrates that once criminal activity was suspected (i.e. operating without a securities licence) enforcement was effective.

4.3 Criminal Prosecutions

- This same case resulted in criminal prosecutions under the normal financial sector legislation (i.e. not specific to e-finance but an example of cross-border issues) in contravention of Section 90 of the *Securities and Exchange Act* B.E. 2535 which requires that the persons must be licensed by the Minister of Finance.

4.4 International Co-operation

- In July 2001, Securities and Exchange Commission, Thailand (SEC Thailand) in Co-operation with the Royal Thai Police, the Anti-Money Laundering Office, the Immigration Bureau, the Inspection of Job Seekers Protection Division, the Australian Federal Police, and the US FBI and Customs conducted raids against several companies suspected of being unlicensed securities companies which may have engaged in fraudulent activities against foreign investors.
- These entities allegedly contacted more than 100 Australian investors. They attempted to conceal their business operations by renting a virtual office to act as switch board facilities to transfer calls to other locations where they had physical presence.
- It was discovered there were large fund transfers out of the country which raised suspicion of the involvement of an international group based outside Thailand and possible international money laundering. As a result the SEC Thailand asked for Co-operation from the Royal Thai Police, and other organisations listed above in conducting raids.
- Since the initial complaints came from investors in Australia so the successful enforcement in this case involved a response from Australian supervisory authorities, communication between Australian and Thai supervisors, Co-operation between law enforcement bodies (police forces) and supervisory bodies domestically, and Co-operation between enforcement bodies internationally.

United States of America: Consumer Protection and Enforcement in Electronic Finance

1. Regulatory Structure

1.1 Laws and regulations relating to E-finance

- The Federal Reserve Board has been given the responsibility for implementing certain laws in banking and financial activities. These laws are implemented in part through the FRB regulations, one of which applies to any electronic transfer that authorizes a financial institution to debit or credit a consumer's account, including securities and commodities transfer. It defines the liability of the consumer for unauthorised transfers, and contains general disclosure requirements.
- The Office of the Comptroller of the Currency (OCC) regulates national banks, DC banks, federal agencies and branches of foreign banks and their subsidiaries. The OCC issues guidelines to the banks, pertaining to the consumer protection in electronic transactions.
- The Securities and Exchange Commission (SEC) regulates brokerage firms, mutual funds and investment advisors. New SEC rules are designed to facilitate electronic dissemination of information, easier access to information and resulting enhanced market exposure for foreign securities.
- Antifraud provisions of the Investment Advisers Act of 1940 and the Securities Exchange Act of 1934, as well as anti-touting provision of the Securities Act of 1933, are applied for on-line securities transactions.
- The *Uniform Electronic Transactions Act* was finalised in 1999 by the National Conference of Commissioners on Uniform State Laws (NCCUSL), establishing the legal equivalence of electronic records and signatures with paper-based systems. As of July 18, 2001, 37 states have enacted UETA. *Uniform Computer Information Transactions Act* is a draft state law for contracts relating to software and other forms of computer information. As of July 24, 2001, only 3 states have enacted UCITA. *Uniform Money-Services Business Act* (UMSBA) covers, among other areas, a uniform approach to the regulations and licensing of stored value cards and other Internet payment systems, with the purpose of consumer protection.
- *Electronic Signatures in Global and National Commerce Act* ("E-SIGN Act" signed on June 30, 2000) provides a national uniform standard for electronic transactions and creates legal instrument for electronic signature, electronic contract, or electronic records. Both interstate and foreign commerce are covered by the E-SIGN Act, unless covered by the Uniform Commercial Code (other than Sections 1-107, 1-206 and Articles 2 and 2A), or governed by a State statute, regulation or law. Consumer safeguard provision requires all critical notices to be delivered on paper. The principle of technological neutrality is embedded in the Act, extending to all types of electronic transactions. Consumer consent to receive electronic records instead of paper-based material is required according to the Act. Other provisions of the Act include validity requirements for electronic signature, contract and records; retention requirement for electronic records and contracts; notarization rules, and national uniform standards applicable to banking, insurance and stock industries. Title III of the E-SIGN Act, Promotion of International

Electronic Commerce, Sec 301(2)(A) requires removal of paper-based obstacles to electronic transactions by adopting relevant principles from the Model Law on Electronic Commerce (UNCITRAL, 1996).

- *Truth in Lending Act* requires institutions to give notice of credit terms to borrowers, and *Truth in Saving Act* requires the disclosures of fees and interest rates. Both apply to on-line services.

Are any special license or permits required for E-Finance business?

- Chartering/Licensing of e-banks in the US is handled by the same governmental authorities that charter or license traditional physical depository institutions, and is largely pursuant to the same procedures used to process applications by traditional brick-and-mortar banks.
- The Internet and the National Bank Charter Office of Comptroller of Currency's Corporate Manual was produced in January 2001, to provide regulatory guidance on the creation and operation of the Internet banks. Filing for a new Internet bank charter follows mostly the same process as for any national bank charter.
- In general, record keeping requirements are same for on-line and other broker dealers.

1.2 Laws and Regulations related to Cross-Border transactions

- Foreign banks with a physical presence in the US are required to obtain authorization.
- The federal banking agencies have not imposed special requirements or restrictions on the electronic delivery of banking services by banks not licensed to do business in the US.
- Banks conducting cross-border Internet banking must comply with the Office of Foreign Assets Control's (OFAC) regulations, to restrict transactions with the countries under sanctions. Adherence to the Bank Secrecy Act and relevant cross-border risks require the banks follow stringent identification/disclosure procedures when opening Internet accounts with foreign customers.
- The Securities and Exchange Commission (SEC) requires registration if an offer is to be made to US residents. The SEC has published its views on the application of the registration obligations under the US federal securities laws to the use of Internet web sites to disseminate offering and solicitation materials for offshore sales of securities and investment services. The SEC's Offshore Release indicates that if the Internet solicitation targets US residents, registration provisions of the US securities law apply. Off-shore offers and sales escape the US registration requirements under Regulation S (Securities Act of 1933) and Rule 15a-6 (Securities Exchange Act of 1934). Regulation S indicates that if the Web site has an explicit disclaimer that the offer is valid for persons resident outside US only, and supplementary check procedures are in place (eg check for the non-US residential address of the purchaser). Rule 15a-6 applied to internet-publicized investment services allows offshore dealers to transact with certain categories of the US investors (see Statement of the SEC Regarding use of Internet Web Sites to Offer Securities, Solicit Securities Transactions or Advertise Investment Services Offshore", International Series Release No. 1125, March 23, 1998).
- *National Bank Offshore Activities Act of 2001* (H.R.2273), (pending) is designed to amend banking laws with respect to offshore activities, investments, and

affiliations of national banks. Activities of national banks are proposed to be subject to certain reporting requirements without regard to any territorial limitation. National banks should report on acquisition of a beneficial interest in an offshore company; and violations of banking, financial services, or labor laws committed by its agents, affiliates, or any other corresponding entity. The Comptroller of the Currency is proposed to be authorised to issue a cease and desist order: (1) prohibiting a national bank from further involvement with such violators; and (2) requiring the bank to dispose of ownership interests in such entity. Any foreign bank having a Federal branch or agency is to be treated as a national bank for purposes of this Act.

- The proposed *Bankruptcy Abuse Prevention and Consumer Protection Act of 2001* (Placed on the Calendar in the Senate) [H.R.333.PCS], contains Title VIII: Ancillary and Other Cross-Border Cases, Title VIII expands the scope of bankruptcy law to incorporate the Model Law on Cross-Border Insolvency, and to establish a statutory mechanism for dealing with cases of cross-border insolvency, and co-operation between U.S. courts, trustees, and debtors and their foreign counterparts. It prescribes guidelines for access of foreign representatives and creditors to Federal and State courts; recognition of a foreign proceeding and relief; and co-operation and direct communication with foreign regulators.

1.3 Special laws and regulations for consumer protections on E-Finance

- The *Fair Credit Billing Act* (FCBA) and *Electronic Fund Transfer Act* (EFTA) establish settlement procedures for disputed credit and bank account transactions, including unauthorised electronic transactions/charges. The FCBA applies to credit cards and revolving charge accounts (i.e.department store accounts; loan accounts are excluded). The maximum liability for a lost or stolen card is limited to US$ 50. The EFTA Act covers electronic fund transfers resulting in the withdrawal of cash from the bank accounts. Depending on the promptness of reporting an unauthorised transaction from the bank account, consumer liability starts from US $50 if the loss is reported within two business days, rises to US $500 if the loss is reported within 60 days upon receipt of the statement, or becomes unlimited if the consumer fails to report lost/stolen card or an unauthorised transaction within 60 days.
- The *Fair Credit Reporting Act* deals with privacy protection with respect to information distributed by the consumer reporting agencies (CRAs). According to the Act, credit bureaux and other CRAs can release personal financial information to the third parties only if they have certified that they are permitted by law to obtain a consumer's credit report, for the purpose of evaluation of application for credit, insurance, rental property, or for employment purposes. If the company that obtained a credit report plans to share information with its affiliates, the consumer has to be notified, and may opt-out.
- The *Gramm-Leach-Bliley Act* (GLB) of 1999 imposes limitations on the ability of financial companies to share financial information about their customers with certain non-affiliates, such as service providers, joint marketers, and other non-affiliates. While consumer's personal financial information, according to the GLB Act, may be provided to non-affiliated service providers and joint marketers, sharing of information with other third-party non-affiliates has to be authorized by the consumer, with the provision for opting-out. However, various consumer

groups have noted that Title V of the GLB Act contains too many legal loopholes to provide adequate privacy protection. The provisions of the Act became effective on July 1, 2001.

- *Electronic Communications Privacy Act* prohibits any unauthorized person to intentionally intercept electronic communications or conduct unauthorized access.

What types of internet activities are prohibited by the legislation (e.g. spamming, direct soliciting of deposits etc)?

- The Telemarketing Intrusive Practices Act of 2001, S.1881, was introduced December 2001 and is still pending. It directs the Federal Trade Commission to establish, maintain, and periodically update for each State a list of consumers who request not to receive telephone sales calls; and notify consumers of the establishment of the lists. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2001 (or the CAN SPAM Act of 2001), S.630, introduced in March 2001 amends Federal criminal law to subject to a fine or imprisonment the transmission of unsolicited commercial electronic mail message containing fraudulent routing information accompanied by header information that is materially or intentionally false or misleading.

Are there any laws and regulations related to data protection? (particularly private information)

- The EC Directive on Data Protection that came into effect in October 1998 prohibited transfer of personal data to non-EU nations failing to meet the European standards for privacy protection. This directive could have had a very large impact on the information flow between the US and EU, due to the light-handed and mostly self-regulatory approach to the privacy issues in the USA. A "safe harbor" framework was developed by the US Department of Commerce and the European Commission, approved by the EC in July 2000, to certify that a US company complies with the EU standards on privacy protection. The Department of Commerce maintains a list of companies which voluntarily comply with the EU privacy standards. As of March 2002, there are 156 companies on the Safe Harbor list.
- Consumer Privacy Protection Act of 2001 H.R.2135 introduced June 2001 (pending), prescribes limitations upon the disclosure by an information recipient of consumer personal and optional information, with certain exceptions.
- Privacy Commission Act of 2001, H.R.583 introduced February 2001, (pending) seeks to establish the Commission for the Comprehensive Study of Privacy Protection to study and report to Congress and the President on issues relating to protection of individual privacy.
- The Consumer's Right to Financial Privacy Act of 2001, H.R.2720, introduced August 2001 (pending), seeks to amends the Gramm-Leach-Bliley Act to revamp financial institution obligations regarding disclosures of personal information sharing.
- The Privacy Act of 2001, S.1055, introduced in Senate in June 2001 (pending) prohibits the sale and disclosure of personally identifiable information by a commercial entity to a non-affiliated third party unless prescribed procedures for notice and opportunity to restrict such disclosure have been followed.

2. Self-regulation and Codes of Practice

2.1 Codes of Practice

- American Bankers Association has adopted a set of Privacy Principles.
- The National Association of Securities Dealers (NASD), Manual & Notices to Members, CONDUCT RULES [2000-3410] contain *Standards of Commercial Honor and Principles of Trade (2110,* rules on transactions with customers, and disclosure principles.

2.2 Trust Mark/Seal of Assurance Schemes

- A number of trust mark schemes have been developed including the following.
- Better Business Bureau (BBB) BBBOnline Reliability Seal Program was established in March 2000 to assure that companies complied with their own posted privacy policy. The seal also means that the company agrees to participate in the consumer's dispute resolution system.
- TRUSTe, the first on-line privacy seal program, awards a trustmark confirming that the company complies with the privacy principles and has a consumer complaints handling system in place. Implemented at more than 1,200 Web sites in different lines of business (August 2001).
- Privacy Bot – establishes and verifies level of privacy protection offered by the site. Includes a mediation system for handling the consumer disputes.
- TruSecure – a Web Certification system to assure security of the site and information protection, supported by the International Computer Security Association (ICSA).
- WebTrust - a joint Web trust seal program between the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), to ensure compliance of the electronic business with the business practice disclosure requirements, transaction integrity, security and privacy standards adopted by AICPA/CICA.
- BetterWeb – on-line privacy seal provided by PriceWaterhouseCooper's.
- JIPDEC – a Privacy Mark developed by the Japan Information Processing Development Center.
- VeriSign (provides an electronic substitute of a sealed envelope by offering a digital ID and digital certificate).

2.3 Dispute Resolution

- Early examples of the Internet-related on-line ADR systems in North America include Cybertribunal.org (the University of Montreal, complaints about on-line software purchases and ISPs); the BBBOnline.org offering ADR in privacy-related disputes; ClickNSettle.com - on-line settling of insurance claims disputes. A variety of cases are handled by the iCoutrhouse.com that uses real juries and judges in resolving disputes.
- The Hague Conference in December 2000 was devoted to the exchange of views between consumer advocates, business sector and government regulators on the Alternative Dispute Resolution systems (ADR) and their application to cross-

border consumer protection in e-commerce. The Consumer Sentinel, a Canada-US joint venture complaint recording network, recognised that at present, most of the domestic consumers' complaints were against the domestic service providers. A report by the Consumer International, "Disputes in Cyberspace: Online Dispute Resolution for Consumers in Cross-Border Disputes", analysed 36 types of ADRs offered by private sector and consumer groups, and found ADR showed limited efficiency in handling cross-border B2C complaints. In the press release by the Office of the Press Secretary, the White House (December 20, 2000), it was stated that "businesses, consumer groups and governments should work together to educate consumers and businesses about good business practices, including ADR, as a means to ensure fair and effective implementation and enforcement, and promote consumer confidence to the fullest extent possible". The US response was driven by two European initiatives. The European Extra-judicial Network (EEJ Net), the out-of-court cross-border dispute resolution system, was established by the European Parliament in July 2001. The ADR system for handling cross-border financial services complaints, the Financial Services Network (Fin-Net) was established in January 2001. A mutual memorandum of understanding rested jurisdiction of handling the complaint in most cases with the service provider's country.

3. Enforcement System

- Since 1994, 182 Internet-related cases were brought up by the FTC against 593 defendants. More that $180 million was ordered in redress, disgorgement, and more assets were frozen for the cases that are still pending. Fraudulent Internet activities stopped by the federal district court actions would have amounted to $250 million pa.
- The Office of Internet Enforcement (OIE), a part of the SEC, was formed in 1998, to identify areas of surveillance, formulate investigative procedures, provide enforcement guidance nation-wide, and conduct Internet investigations and prosecutions. Internet "Enforcement Sweeps" are conducted on a regular basis, targeting similar types of Internet misconduct for investigation and prosecution. The fifth nation-wide Internet fraud sweep (2001) resulted in 11 enforcement actions initiated by SEC against 23 companies and individuals that used the Internet to defraud investors. The cases involved both publicly traded securities and privately held companies. The Internet was used by the perpetrators to "pump" the market capitalization of the stocks involved in the cases by more than US $300 million, and raise US $2.5 million from both domestic and overseas investors. Online means used for the frauds included "spam" emails, electronic newsletters, websites, hyperlinks, message boards and other Internet media (see http://www.sec.gov/news/press/2001-24.txt for the complete media release).
- The SEC's Office of Compliance Inspections and Examinations conducted a series of examinations of broker-dealers offering on-line trading, and provided recommendations for consumers of these services (January 2001, http://www.sec.gov/news/studies/on-line.htm).

4. Cases

4.1 Consumer Education

- Consumer organisations are very active in providing education websites. The National Consumers League's National Fraud Information (NFIC) Center is an example.
- FTC maintains a Consumer Response Center which provides education on its sites.

4.2 Cold calling cases

- The US has initiated actions in several of the cold calling cases listed elsewhere (see the descriptions for Thailand and Australia).

4.3 Prosecutions for email

- The FTC charged a major medical company with violation of the privacy policy, by sending a group email to an open list of 600 addresses of people taking one of their medical products in 2001. The case was settled in 2002.

4.4 International co-operation

- The US bank supervisors are actively supporting the efforts of the Basel Committee on Banking Supervision's Electronic Banking Group (EBG).
- The Securities and Exchange Commission, in collaboration with twenty of its regulatory counterparts, conducted an International Internet Surf Day on March 28, 2000. The effort initiated by the International Organization of Securities Commissions (IOSCO) was targeted at detection of cross-border securities violations on the Internet, and their deterrence. During the action, around 220 staff members representing twenty-one regulatory authorities jointly identified over 1,000 sites for follow-up review (of which over 250 case involved cross-border activity). SEC staff visited more than 200 sites, with 78 requiring the follow-up review by the participating regulators. Offences/violations included potential unregistered offerings, pyramid schemes, unlicensed investment advice, and high-yield investments. International co-operation of regulators has been recognized as the enforcement tool in combating illegal cross-border activity. There are over thirty formal information-sharing agreements in place between the SEC and foreign authorities responsible for protection of consumers against cross-border fraud. In fiscal year 2001, 364 requests were made to foreign authorities for enforcement assistance, and 483 requests from the foreign agencies were received by the SEC.

4.5 Private sector developments to overcome cross-border jurisdiction difficulties

- A joint venture between BBBOnline and JIPDEC, a Privacy Mark developed by the Japan Information Processing Development Center, provides mutual recognition of the privacy standards by US and Japanese companies.
- Special security measures have been introduced by private credit card companies to prevent fraudulent use of stolen credit card numbers. Visa introduced the Cardholder Information Security processing (CISP) system in 2000, followed by MasterCard's Site Data Protection Service (SDPS) in 2001.
- American Bar Association Section of Business Law works on a Global Cyberspace Jurisdiction Project, focussing on a range of issues including consumer protection. The Information Security Committee of the Electronic Commerce Division concentrates on the public key infrastructure, cryptology, risk analysis, standards, and legal aspect of secure digital commerce.
- The Worldwide E-Commerce Fraud Prevention Network, http://merchantfraudsquad.com, comprising more that 1,000 members worldwide, including financial institutions and banks. This non-profit association was formed in September 2000 by America Express, ClearCommerce, Expedia.com, and First Data Corp – a private sector initiative to overcome cross-border internet fraud issues.

*The information in the Annex B was gathered by a survey team from the Australian National University (ANU) during January – March 2002 based on the prior research and interviews with local experts on necessary basis. The followings are lists of those entities, which cooperated with the ANU for their interviews and discussions.

Australia

Consumer Protection Division and Asia-Pacific Division, Dept of Treasury

China

Department of Economics, Renmin University
China Center for Economics Research, Peking University

Hong Kong

Hong Kong Monetary Authority
Trade Practices Division, Consumer Council

Indonesia

Financial Information Technology Development Center, Ministry of Finance
Indonesia Media Law and Policy Centre & Global Internet Policy Initiative, Minister of Communications and Information
Bank Indonesia
Ciptamaya
PT Samudera Indonesia Tbk
PT Lime Intermedia Asia
PT Euronet Sigma Nusantara
PT Bonet Utama
Hadromi and Partners Attorneys at Law
MASTEL (The Indonesian Infocom Society)
ICT Adviser, Partnership for Economic Growth USAID/GOI Project
KPMG Consulting – Barents Group USAID Fiscal and ICT Project
Senior Public Finance Advisor, USAID
Economic Growth Team Leader, USAID
Bappenas/USAID/DAI Food Policy Support DAI (development Alternatives Inc)

Japan

Keio University
Institute of Asia Pacific Studies, Waseda University
Regional Office for Asia and the Pacific, IMF
Australian Embassy
Ginza Daiichi Houritsu Jimusho (Private Law Firm)

Korea

Korea University
Institute of Finance

Malaysia

Bank Negara Malaysia
National Economic Action Council, Prime Ministers Department
Securities Commission

Mexico
Commission for the Protection and Defence of Users of Financial Services
Procuraduria Federal del Consumidor
Banca Y Ahorro, Secretaria De Hacenda Y Credito Publico
Comision Nacional Bancaria y de Valores
Banca Multiple, Secretaria De Hacienda Y Credito Publico

Singapore
Monetary Authority of Singapore
Nanyang Technological University

Thailand
Bank of Thailand
Thai Telephone and Telecommunication Public Co Ltd
Seranee Holdings Co Ltd
Thailand Australia Capacity Building Facility
Senior Financial Sector Specialist, The World Bank
Allens Arthur Robinson
Australian Embassy

USA
Columbia University
National Economics Research Associates Inc
Monetary and Exchange Affairs Division, IMF
Institute of International Economics
Development Research Group, World Bank

Entities contacted during APEC SOM I ECSG

1) Ministry of Consumer Affairs, New Zealand
2) Electronic Commerce Task Force, Canada
3) Bureau of Consumer Protection, Federal Trade Commission, USA
4) Japan Information Processing Development Corporation, Japan
5) Equipment Commerce ad Information Policy Bureau, Ministry of Economy, Trade and Industry, Japan
6) National Electronics and Computer Technology Center, National Science and Technology Development Agency, Ministry of Science Technology and Environment, Thailand
7) State Ministry of Communications and Information, Indonesia
8) Faculty of Business, Economics and Policy Studies, University Brunei Darussalam, Brunei Darussalam

Glossary

Terms	Definition
Aggregators	Aggregation is a service that allows customers to view their on-line accounts and other information held with different institutions (e.g. bank, investment, credit card, frequent-flier etc) at a single location on the Internet, accessible via a single password. Aggregators are providers of such a service. This service is delivered either via direct feeds (e.g. a bank providing aggregators with a data feed containing information about client accounts under an agreement), or through clients themselves providing their on-line log-on details and passwords to aggregators which then use them to access account details and make the data available to the customer (this is known as screen-scraping).
Application Service Providers (ASPs)	ASPs are providers of IT services that deliver IT-enabled business solutions across a network via subscription-based pricing. Increasingly, ASPs have also evolved to include service bureaus that provide processing or outsourcing services (e.g. operational or middle to back-office activities).
Bandwidth	This is a terminology used to indicate the transmission or processing capacity of a system or of a specific location in a system (usually a network system) for information (text, images, video or sound). Bandwidth is usually defined in bits per second (bps) but is also described as either large or small.
Business-to-Business (B2B) Transactions	B2B transactions refer to commercial transactions enacted between two businesses in private sector.
Business-to-Consumer (B2C) Transactions	B2C transactions refer to transactions enacted between businesses in private sector and consumers.
Business-to-Government (B2G) Transactions	B2G transactions refer to transactions enacted between businesses in private sector and the government or government agencies.
Central Securities Depository (CSD)	A CSD is a facility (or an institution) for holding securities, which enables securities transactions to be processed by book entry. Physical securities may be immobilized by the depository or securities may be dematerialized (i.e. so that they exist only as electronic records). In addition to safekeeping, a central securities depository may incorporate comparison, clearing and settlement functions.

Click-and-Mortar	This refers to banks that conduct its banking activity via the Internet delivery channel as well as traditional physical channels such as branches, ATMs or kiosks. For example, giving customer access to his account both via the Internet and through a network of branches.
Consumer-to-Consumer (C2C) Transactions	C2C transactions refer to transactions between consumers via electronic means and channels.
Cross-Border Transaction	A cross-border transaction refers to a transaction between two counterparties located in two different countries.
Customer Relationship Management (CRM) System	CRM is a technology-enabled strategy to convert data-driven decisions into business actions in response to, and in anticipation of, actual customer behaviour. From a technology perspective, CRM represents the systems and infrastructure required to capture, analyze and share all facets of the customer's relationship with the enterprise. From a strategy perspective, it represents a process to measure and allocate organizational resources to those activities that have the greatest return and impact on profitable customer relationships.
Delivery versus Payment (DVP)	DVP is defined as a link between a securities transfer system and a funds transfer system that ensures that delivery occurs if, and only if, payment occurs.
Digital Certification	A Digital Certificate is an encoded document that verifies the connection between a Server's (computer) public key (known to anyone) and the server's identification. The Certification process is similar to that provided by a driver's license, which verifies the connection between the photograph and the personal identification. Cryptographic checks, including a digital signature (electronic equivalent of a person's unique writing of their own name), ensure that the information within the certificate (message) has not been tampered with during transmission.
Digital Signature	The electronic equivalent of a person's unique writing of their own name, usually performed today using public key cryptography. To create a digital signature, a hash function is performed on a message to create a unique message digest. The message digest is then encrypted using the sender's private key; the recipient decrypts the digest using the sender's public key. The recipient uses the public key of the sender to verify the authenticity of the sender, who should be the only one possessing that private key.

E-Banking	E-Banking is the provision of retail and small value banking products and services through electronic channels or means, as well as large value electronic payments and other wholesale banking services delivered electronically. It encompasses a wide range of activities from making deposits through ATMs to issuance of e-money. It is also referred to as cyber-banking, remote banking or on-line banking.
Electronic Bill Presentment and Payment (EBPP)	EBPP is a system provided by banks and third-party service providers that allows billers to electronically present a bill to a consumer so that the consumer can electronically pay the amount owed. Funds are sent either electronically or by check by the bank or third party to the biller.
E-Commerce	E-Commerce is the ability to purchase goods and services, including final payment settlement, solely with electronic transfers of financial value. It is a business environment integrating electronic transfer and automated business systems (end-user computing and computer-to-computer capabilities). It is commonly referred to as business conducted over the Internet.
Electronic Communication Networks (ECNs)	ECNs are systems that can deliver a range of services; from acting as an intermediary (e.g. collecting investors' orders and routing them), to providing trading platforms and performing a wide range of functions of an exchange. For example, it can internally match buy and sell Limit Orders, or represent the highest bids and lowest asks on the open market, thus eliminating the need for human traders. It can also facilitate after-hours trading.
Electronic Data Interchange (EDI) Systems	EDI systems provide for the electronic exchange between commercial entities (in some cases also public administrations), in a standard format, of data relating to a number of message categories, such as orders, invoices, customs documents, remittances advice and payments. EDI messages are sent through public data transmission networks or banking system channels. Any movement of funds initiated by EDI is reflected in payment instructions flowing through the banking system.
E-Finance	E-finance refers to the electronic marketing and delivery of financial services, and electronic payment and settlement of financial transactions.
Electronic Funds Transfer (EFT) Networks	EFT networks are networks set up formally (based either on private contract or statute law) with multiple membership, common rules and standardized arrangements, for the transmission and settlement of money obligations arising between the members.

E-Government	E-Government refers to the provision of and/or payment for government services through electronic channels or means.
E-Insurance	E-Insurance is the provision of insurance products and services through electronic channels or means.
E-Money	Money/monetary equivalents that can be transmitted electronically. It is largely outside established payments system of banks, checks and paper currency. Its value can be stored electronically in a device such as a chip card or a hard drive in a personal computer and reduced through purchase or transfer.
E-Payment	E-Payment is the payment for goods or services through electronic channels or means.
E-Trading	E-Trading is the trading of physical goods, financial assets (such as debentures, stocks, bonds, options, derivatives, etc.) or services through electronic channels or means.
Financial Institution	A financial institution is an institution (public or private) that collects funds (from the public or other institutions) and places them in financial assets, such as deposits, loans, and bonds, rather than tangible property.
Infocomm Technology (ICT)	ICT is a cluster of IT related and communications related technologies. Information technologies facilitate the various stages of how information is produced, captured, sensed or detected, manipulated, processed, packaged, compressed, stored, secured, presented, etc. Examples include CD ROM, LCD projectors, computer, watch media files, smart cards, biometrics, etc. Communication technologies deal with how information is transmitted, passed on via intermediaries, and received. Examples include optical networking, mobile communication networks, antennas, infrared, wireless LAN, bluetooth, USB interface, an internet access modem, an Ethernet card and telephone.
International Central Securities Depository (ICSD)	ICSD is a central securities depository that clears and settles transactions in global or international securities and cross border transactions in domestic securities.
Internet Discussion Sites (IDS)	This is an electronic space where people can go to communicate on-line usually in real-time. These sites are often organized around specific interests.

Internet-Only Banks	This refers to banks that conduct its banking activity through the Internet delivery channel only. They tend to take the form of monoline lenders, which are specialist providers of a single service or product, or full-service financial service providers, for whom cross-selling a range of products is preferred. As a norm, customers would perhaps receive better interest rates to reflect cost savings enjoyed by the bank, as it is unencumbered with physical infrastructure like branches. Also known as virtual or cyber-banks.
Internet-Primary Banks	This refers to banks that predominantly conduct its banking activity through the Internet delivery channel, but also retains limited physical presence such as mini-offices or ATMs to complement its on-line offerings and enhance customer service.
Internet Service Provider (ISP)	ISP is an entity that provides access to the Internet. Some of the more commonly used connection methods include: (1) modem and common telephone lines (2) cable lines, or (3) through direct connection using a dedicated line.
On-line Trading Platforms (OTPs)	OTPs can cover a wide spectrum of systems offering an array of products/services. These ranges from systems that enable foreign investors to access an exchange, electronic trading matching systems like electronic communication networks (ECNs), bulletin boards, automated order-routing systems, broker-run proprietary systems, and automated linkages between brokers and customers.
Over-the-Counter (OTC)	OTC refers to a method of trading that does not involve an exchange. In OTC markets, participants trade directly with each other typically through telephone or electronic links.
Payment and Settlement System	This refers to the transfer system for funds and financial assets.
Payment versus Payment (PVP)	PVP is a mechanism in a foreign exchange settlement system, which ensures that a final transfer of one currency occurs if and only if a final transfer of the other currency or currencies takes place.
Portal	A World Wide Web site or service that is a major starting site for users when users get connected to the Web or that users tend to visit as an anchor site. It offers a broad array of resources and services, such as email, forum, search engines, and on-line shopping malls. Examples of general portals include Yahoo, Excite, Netscape, Lycos, CNET, Microsoft Network, and America Online's AOL.com.

Private Key	One of two keys in public key encryption. The user keeps the private key secret and uses it to encrypt outgoing messages and/or digital signatures and to decrypt messages received.
Public Key	In encryption, a two-key (split) system in which one key, used to lock data, is made public so all can lock, and a second key, kept private, is used to unlock or decrypt (see private key) the data.
Public Key Infrastructure (PKI)	PKI is the set of security services that enable the use and management of public key cryptography and certificates, including key, digital certificate and policy management.
Real–Time Gross Settlement System (RTGS)	RTGS is a system that provides for the continuous (real-time) settlement of funds or securities transfers individually on an order-by-order basis (without netting).
Securities	Securities include debentures, stocks or bonds issued by governments and corporations, including any right or option in respect of these instruments and derivative contracts.
Straight-Through-Processing (STP)	STP refers to the capture of trade details directly from front-end trading systems and complete automated processing of confirmations and settlement instructions without the need for re-keying or re-formatting data.
S.W.I.F.T	Society for Worldwide Interbank Financial Telecommunications (SWIFT) is an industry owned cooperative supplying secure messaging services and interface software to over 7,000 financial institutions in 197 countries.
Technology Neutrality	This refers to adopting a neutral stance on how (i.e. the form of electronic delivery) e-finance is delivered but emphasizing on the completeness of content/information or effectiveness of customer protection etc.
Token	An object serving as evidence of authenticity or as a guarantee.
Trust Mark System	A system which helps consumers to identify reliable on-line business enterprises by means of a certain mark posted on the website of those enterprises that follow an agreed code of practices. Developing such trust mark systems that are internationally recognized would contribute to building more consumer confidence in cross-border transactions.
Vertical Portal	A vertical portal is a web site that provides a gateway or portal to information and resources for a particular industry.

United Nations Commission on International Trade Law (UNCITRAL)	UNCITRAL, established in 1966, has the mandate to further the progressive harmonization and unification of the law of international trade. It is the core legal body of the United Nations system in the field of international trade law.

APEC Working Group on Electronic Financial Transactions Systems

Co-chairs:

HONG KONG, CHINA

Mr. James H. LAU Jr.
Executive Director, Monetary Policy and Markets Department, Hong Kong Monetary Authority

JAPAN

Mr. Yasusuke TSUKAGOSHI
Director, International Affairs Division, Financial Services Agency
(from July 2001 until September 2002)

Mr. Masamichi KONO
Director, International Affairs Division, Financial Services Agency
(from September 2000 until June 2001)

Members:

AUSTRALIA

Ms. Brenda BERKELEY
Senior Treasury Representative, Australian Embassy, Tokyo

BRUNEI DARUSSALAM

Mr. Umar ALI ABDULLAH
Head of Computer Services, Information Technology and State Store Department, Ministry of Finance

Mr. Mahmud MOHD. DAUD
Director, Information Technology and State Store Department, Ministry of Finance

Ms. Manhani MOSHIN
Finance Officer, Financial Institutions Division, Brunei Currency Board

Ms. Yap Lye TIN
Senior System Analyst, Information Technology and State Store Department, Ministry of Finance

Mrs. Irene Tsue-lng YAP
Finance Officer, Brunei Currency Board

CANADA

Mr. Denis NORMAND
Senior Chief, Department of Finance, Ministry of Finance

Mr. Andrew RECTOR
Senior Project Leader, Financial Sector Policy Branch, Ministry of Finance

PEOPLE'S REPUBLIC OF CHINA

Ms. LIANG Jing
Coordinator, 8th APEC Finance Ministers Meeting, Ministry of Finance

Mr. XU Wensheng
Principal Staff Member, Science and Technology Department, People's Bank of China

Mr. ZHANG Ye
Deputy Director General, Information Department, China Securities Regulatory Commission

Mr. ZHAO Fuchang
Coordinator, International Department, Ministry of Finance

HONG KONG, CHINA

Ms. Ann AU
Manager, Central Moneymarkets Unit, Hong Kong Monetary Authority

Mr. Stanley CHAN
Senior Manager, Central Moneymarkets Unit, Hong Kong Monetary Authority

Mr. Andy CHING
Manager, Central Moneymarkets Unit, Hong Kong Monetary Authority

Mr. Esmond LEE
Head, Market Systems Division, Hong Kong Monetary Authority

Mr. LEE Kwok-Hung
Manager, Central Moneymarkets Unit, Hong Kong Monetary Authority

Mr. George TAM
Senior Manager, Supervision of Markets Division, Securities and Futures Commission

Mr. Stanley WONG
Deputy Secretary for Financial Services and the Treasury (Financial Services), the Government of the Hong Kong Special Administrative Region

Ms. Sylvia YIP
Manager, Central Moneymarkets Unit, Hong Kong Monetary Authority

INDONESIA

Ms. Rosmaya HADI
Head of Rupiah Settlement Division / RTGS Operations, Accounting and Payment System Department, Bank Indonesia

Ms. Pipih Dewi PURUSITAWATI
National Payment System Development Bureau, Bank Indonesia

Mr. Kunto WINDIHARTO
National Payment System Development Bureau, Bank Indonesia

JAPAN

Mr. Masatsugu ASAKAWA
Director, Office of Regional Financial Co-operation, International Bureau, Ministry of Finance

Dr. Takatoshi ITO
Deputy Vice Minister of Finance for International Affairs, Ministry of Finance

Mr. Ken IWATA
Section Chief, Regional Financial Co-operation Division, International Bureau, Ministry of Finance

Mr. Mitsutoshi KAJIKAWA
Deputy Director, Office of Regional Financial Co-operation, International Bureau, Ministry of Finance

Mr. Tadaaki KAWAMURA
Section Chief, International Affairs Division, Financial Services Agency

Mr. Satoshi KAWAZOE
Manager, Money and Capital Markets Division, Financial Markets Department, Bank of Japan

Mr. Makoto KOIKE
Official, Office of Regional Financial Co-operation, International Bureau, Ministry of Finance

Mr. Kazuo KOJIMA
Deputy Director, International Affairs Division, Financial Services Agency

Mr. Toshiyuki MIYOSHI
Deputy Director, Regional Financial Co-operation Division, International Bureau, Ministry of Finance

Mr. Hironobu NAKA
Deputy Director, International Affairs Division, Financial Services Agency

Ms. Saiko NAKAGAWA
Official, International Affairs Division, Financial Services Agency

Mr. Masashi NAKAJIMA
Manager, International Department, Bank of Japan

Mr. Satoshi OHUCHI
Consul, Consulate-General of Japan

Mr. Motoyuki OKURA
Official, Office of Regional Customs Co-operation, Customs and Tariff Bureau, Ministry of Finance

Mr. Shigenori SAKAMOTO
Section Chief, Office of Regional Customs Co-operation, Customs and Tariff Bureau, Ministry of Finance

Mr. Nobuhiko SUGIURA
Research Fellow, Communication and Policy Division, Financial Services Agency

Mr. Tomomi TSUKUDA
Official, Regional Financial Co-operation Division, International Bureau, Ministry of Finance

Mr. Hiroshi WATANABE
Deputy Director General, International Bureau, Ministry of Fina nce

Ms. Kayo YOSHIDA
Official, Planning and Coordination Division, Global Economic Research Division, International Department, Bank of Japan

THE REPUBLIC OF KOREA

Mr. Jinho BYUN
Research Fellow, Korea Securities Research Institution

Mr. Yong-Ho CHOI
Deputy Director, Banking System Division, Ministry of Finance and Economy

Mr. Chol-Hwi LEE
Consul for Finance and Economy, Korean Embassy in Tokyo

Mr. Jae-Soo YOO
Deputy Director, FinancialCooperation Bureau, Ministryof Finance and Economy

MALAYSIA

Ms. Hazeleen Syrene ABDUL RAHIM
Senior Executive Officer, Law Reform & Regulatory Policy Department, Securities Commission

Mr. Christopher FERNANDEZ
Senior Manager, Payment Systems Department, Bank Negara Malaysia

Ms. LAM May Yin
Manager, Law Reform & Regulatory Policy Department, Securities Commission

MEXICO

Mr. Manuel ACEVEDO
Deputy Director, International Banking Affairs, Ministry of Finance and Public Credit

Ms. Geraldine CABRERA SOLORZANO
Deputy Director of Foreign Financial Intermediaries, International Banking Affairs, Ministry of Finance and Public Credit

SINGAPORE

Mr. Chee Hoe CHAN
Assistant Director, Market Infrastructure & Risk Advisory Department, Monetary Authority of Singapore

Ms. CHANG Su Hoong
Director, Securities and Futures Department, Monetary Authority of Singapore

Ms. Audrey CHIA
Analyst, International Department, Monetary Authority of Singapore

Mr. Enoch CH'NG
Executive Director, Market Infrastructure & Risk Advisory Department, Monetary Authority of Singapore

Ms. Yiat-Wan LEONG
E-Government Executive (Policy), Managing for Excellence Office, Ministry of Finance

Mr. PEH Kian Heng
Lead Analyst, International Department, Monetary Authority of Singapore

CHINESE TAIPEI

Mr. Kuo-Hsing CHANG
Senior Economist, The Central Bank of China

Mr. Kuo-Ming CHANG
Assistant Director, IT Office, Bureau of Monetary Affairs, Ministry of Finance

Ms. Lifang CHENG
Officer, Bureau of Monetary Affairs, Ministry of Finance

Mr. Jack Chiang-Jye FANG
Officer, Division of Supervision of Domestic Bank, Bureau of Monetary Affairs, Ministry of Finance

Mr. Hsi-Ho HUANG
Senior Officer, Division of International Banking, Bureau of Monetary Affairs, Ministry of Finance

Mrs. TWU Chiou-Ling
Auditor, Division 2, Securities Firms Administration, Securities & Futures Commission, Ministry of Finance

THAILAND

Mr. Ronnapoom CHAIKUNA
Team Executive, Payment Systems Group, Bank of Thailand

Mr. Somchai CHOONARATANA
Team Executive, Monetary Policy Group, Bank of Thailand

Mr. Vacharakoon JIVAKANONT
Analyst, Payment Systems Group, Bank of Thailand

Mr. Sayan PARIWAT
Senior Director, Payment Systems Group, Bank of Thailand

Mr. Lt. Banpachai PUTTIBUNDIT
First Secretary, Office of Economic and Financial Affairs, Royal Thai Embassy in Tokyo

Ms. Ketsuda SUPRADIT
Senior Economist, International Economic Policy Division, Ministry of Finance

Mrs. Saowanee SUWANNACHEEP
Assistant Governor, Bank of Thailand

Ms. Sibporn THAVORNCHAN
Director, Payment Systems Group, Bank of Thailand

UNITED STATES OF AMERICA

Mr. Wilbur MONROE
Deputy Director, Office of International Banking and Securities Markets, U.S. Treasury Department

ASIAN DEVELOPMENT BANK

Mr. Yin QIAN
Senior Financial Economist, Financial Sector and Industry Division (East), Asian Development Bank