

**REPORT ON
SECURITIES ACTIVITY ON THE INTERNET III**

ANNEX 1 – MEETING MINUTES ROUND TABLES

Table of Contents

Asian Roundtable Meeting , June 24-25 2002.....	3
Session 1 Minutes: Research and Industry Trends	3
Session 2 Minutes: Emerging Risk Profile	5
Session 3 Minutes: Cross-Border Issues	8
Session 4 Minutes : Investor Education Issues	10
Session 5 Minutes: Enforcement Issues	13
Americas Roundtable Meeting, November 25-26, 2002.....	17
Session 1 Minutes: Research and Industry Trends	17
Session 2 Minutes: Emerging Risk Profile	19
Session 3 Minutes: Cross-Border Issues	21
Session 4 Minutes: Investor Education	24
Session 5 Minutes: Enforcement Issues	28
European Roundtable Meeting, Amsterdam, March 3-4, 2003.....	31
Session 1 Minutes: Research and Industry Trends	31
Session 2 Minutes: Emerging Risk Profile	32
Session 3 Minutes: Investor Education	35
Session 4 Minutes: Cross-Border Issues	37
Session 5 Minutes: Enforcement Issues	39

Meeting Minutes Roundtables

Meeting Minutes of the IOSCO Internet Project Team's Asian Roundtable Meeting , June 24-25 2002

Session 1 Minutes: Research and Industry Trends

Summary of panel presentations

First panelist

Digital information is growing exponentially but it is difficult to get relevant information. Data mining technology will help to solve the problem.

New technology within the next 5 years that may impact on internet include: voice recognition across devices, each device becomes certificate authority, online language translation, instantaneous settlement, on demand network application and intelligent broker liquidity finder. Technology will solve most if not all of the key issues relating to effective control, investor confidence and efficiency. With regard to next generation of e-business model, Financial Services Network Hub and Utility Services Delivery Model will emerge integrating the financial value chain.

The key to industry growth still lies in the underlying market infrastructure and big environment. Focus on compliance and regulation will continue.

There will be a convergence of T+1 and Straight Through Processing ("STP").

Second Panelist

The panelist indicates that there is little or no solid research source available. Most of the research sources coming from conferences, regulators, consultants, global custodians and competitors are outdated. They can only be used as a support mechanism for building business plan.

Year 2002 is a year of closure or consolidation for internet-only brokers. There is a decline of 42% in average online activity, as shown by Deloitte's survey on online securities trading 2001.

Cross-border online transactions, mainly the rest of the world to US, decline significantly following the tech bust and market downturn. The introduction of new US IRS tax code and the cost of institutional custodian fees discourage retail investors to trade in US market.

The only cross-border trading which shows a growing prospect in the next 3 years for retail investor is Exchange Traded Fund ("ETF") because it is cheap, easy to access with home country money and it needs no in-depth research in underlying securities.

For B2B, global diversification is still underway and there is growth in electronic order placement by institutional investors and alternative investments managers or hedge fund manager.

As to the future, Exchanges will become major aggregators of global investments. Connectivity among exchanges will enable the emergence of a global pool of liquidity. ASX WorldLink model will be a norm. Global clearing and settlement system will provide settlement and custodian services to retail investors with FX offset.

Third Panelist

The panelist says that online trading in Japan grew fast after liberalisation of stock commission in October 1999. However, on-line brokers in Japan also showed a consolidation and closure trend in recent years.

There is a trend for online firms to move into margin transactions more heavily because of higher profitability.

Innovative services provided by online brokers do not prosper while price competition is crucial. Major foreign firms and online investment banks do not profit from their online business.

There are very little sources of research information. JSDA publishes amounts of online transactions twice a year and only 3 listed Internet brokers publish financial accounts. No real time information is available.

Group discussion

The trend of online trading moves towards margin trading in Japan is peculiar to that particular market. In other markets, speed and easy to access appear to be keys.

E-exchange is technically viable and has actually been built but was now extinct because it cannot attract sufficient liquidity. One of the major problems is price discovery.

Within the next three years, Internet will be more pervasive in different types of devices. This will lead to the development of financial service network hub that supports different types of front-end devices. Digital scrip will emerge and scripless trading becomes possible. Voice recognition and online language translation will make Internet more user-friendly.

Another trend IBM believed is that 2 years from now, security problem will largely be solved from the technological point of view. However, the industry suggests that practicality is the key.

In order to have a long-term sustainable Internet trading business, the business must deliver security, convenience and efficiency to customers. Future online trading business model has to work on low volume. As more than 80% of the value of a trade is in settlement and clearing, ability to provide a low cost clearing and settlement system is critical. This entails development of industry standard which will help lowering the cost of transaction and facilitating efficient STP. Low value services may be out source to utilities network providers. Online brokers have to provide service that can differentiate it from others such as investment advising.

Lots of cost inefficiencies in online trading are due to the non-existence of STP and the lack of common clearing and settlement and regulatory standards. This hurts retail investors by increasing online trading cost, which, in turn, reduces market liquidity. Although STP is good for the security industry, brokers, particularly the small ones, are sluggish to its development. The reasons are STP will deprived brokers the opportunity to profit from idle fund pending for clearing and brokers are not willing to spend significant amount to upgrade their system.

Horizontal integrations, especially those among clearing houses and using same trading platforms for different products, are more useful than vertical integrations between exchanges and clearing houses. It minimizes cost by standardizing the trading, settlement period and clearing process of different products. It also enables STP. However, horizontal integration happens infrequently because inertia exists for investors to move to a new system, for brokers to invest in a new system and for utilities to change their system.

There is a trend for exchanges becoming major aggregators by aggregating liquidity from members for trading in non-domestic products. The driving forces being exchanges' desire to increase the range of products that they can offer to their members, the brand name effect that an exchange can command and the clearing and settlement function that can be performed by the exchange.

The industry believes that most of the barriers embedded in regulations against internet trading are vanished already but political barriers still exist which hinder horizontal integration and cross border trading. More consultation between regulators and industry will benefit both parties in that regulators can make better regulations with better understanding of the development of internet and the industry and industrial practitioners can have a better understanding of the thinking and important elements of the regulation.

Questions

Please identify research sources which you utilize to keep informed of new Internet related financial products/services or emerging trends in the financial services industry?

There are little or no solid, real-time research sources available. Most sources come from conferences, regulators, consultants, global custodians, competitors and financial accounts of listed online brokers and they are mostly outdated. The information usually is not very reliable, except those from regulators.

How do you view the role of research and statistical data in your business? (e.g. How does research and statistical data influence how you allocate resources in your business?)

Since most of the research data are outdated, they are mainly used as a support mechanism in putting together a business plan. The data may help in minimising but not eliminating risk because they are not solid enough.

For information obtained from Technology Research projections, they are usually not very reliable because most of them do not realise.

What new Internet related developments have you identified as relevant to your business through the use of financial research and statistical data?

Identification of a new viable online trading business model that works under low volume is currently underway because there is a decreasing trend in the use of online trading almost everywhere. Strategies like STP and out sourcing low value services to utility providers and focusing on high value services such as research and investment advising are among the considerations.

What is the prospect of a pure Internet-only securities provider, and how does this translate to the entity's motivation to access multiple jurisdictions to reap the benefits of scale and scope?

The prospect of a pure Internet-only securities provider is not good in the near future because of the tech bust and downturn of the economy. There are lots of consolidation/closure in the industry because online brokers are unable to reach the scale and scope necessary to recoup the investment cost. New cost such as the US IRS new tax code hinders cross border trading and entity's motivation to access multiple jurisdictions. The prospect of pure Internet-only securities providers lies on its ability to operate under low business volume. Development of open standard on clearing and settlement and STP will help to lower transaction cost and facilitate cross border trading.

Do you expect significant growth in cross-border securities services in the next 3 years?

Not for retail investors but there will be growth for B2B.

Which areas of securities services that leverage on the Internet are likely to see higher cross-border growth? Are the patterns of growth different for the B2C and the B2B segments?

Different dynamics exist for B2B and B2C segments. For B2B, global diversification is still underway and there is growth in electronic order placement by institutional investors and alternative investments manager. More exchanges become aggregators in trading of non-domestic products and the trend of convergence to STP will help cross-border growth.

For B2C, many consolidations/closures occur in the industry because of the overall decrease in online trading activities. Other costs such as compliance with new US tax codes and custodian fees also discourage cross-border trading. The only potential increase in cross-border trades is the trading of ETF because ETF provides cheap, easy to access with home country money and no in-depth research in underlying securities for investing in foreign securities.

What are the key critical success factors or preconditions for cross border securities services using the Internet (e.g. high Internet penetration rate, conducive regulatory regime providing for certainty or clarity, suitability of the services)?

The services must deliver security, convenience and cost efficiency to customers. Efficient STP in line with global standards, development of open global standard on clearing and settlement, harmonisation of settlement period for different products, horizontal integration of markets, research and custodian services are critical success factors.

Session 2 Minutes: Emerging Risk Profile

Summary of Panel Presentations:

First panelist

The first panelist (risk management) highlighted risk management issues within the Asian on-line securities market. Among the risk management issues the panelist discussed were the current state of Asian on-line securities trading in 2002 and future trends, technology and risk considerations, risk management, and industry standards and regulation.

The current state of on-line trading in Asia varies considerably by country. In Hong Kong, two types of on-line trading firms have emerged; deep discount firms and full-service firms. Both types of firms are currently

focusing on increasing the number of services they provide, and improving their call centers and providing rapid response technical support to minimize the wait time for customers during system outages.

The panelist stressed the need for on-line trading firms to develop and refine their business processes, develop sound technology strategy, and mitigate the increasing security risks. In regards to industry standards, a dual approach of obtaining website certification, through an industry standard such as WebTrust, and verifying that certification through independent attestation, using SAS 70 or BS7799/ISO17799, would ensure a baseline standard for financial websites, and bolster consumer confidence in utilizing financial websites.

Second panelist

The second panelist (banking supervision) discussed the current state of e-finance/e-banking, traditional threats and emerging risks in these sectors. In Asia most local banks in developed economies offer Internet banking, and customer acceptance is growing gradually. There are few internet-only banks, and few traditional banks offering account aggregation, however. Customer demand is very low. This is in stark contrast to the growth of on-line banking in Hong Kong where 30% of Internet users, or 9% of the population, are on-line banking users.

In addition to offering on-line banking to traditional customers, banks in Hong Kong are expanding their Internet banking services to corporate customers by offering electronic trade finance and payment services. Some of the traditional operational risks faced by the e-finance/e-banking community are hacking activities and system failures (e.g. denial of service attacks, network outages, systems outages), poorly administrated networks, reliance on outside service providers, and lack of continuous security monitoring or intrusion detection mechanisms. The top three emerging risks in Asia are increased frequencies of virus attacks, cyber attacks, and a hybrid of both of these techniques.

Third panelist

The third panelist, (research) discussed Internet trading in Japan, risks and issues in building systems, risks intrinsic to the Internet, and emerging risks.

The number of Internet trading accounts in Japan continues to expand each year. In light of the consistent growth of on-line trading in Japan, on-line brokerages face issues relating to capacity planning, scalability, creating adequate duplication and backup centers for account information, and guarding against software failures and ensuring individual application failures don't spread to the entire system.

Risks intrinsic to the Internet include the time gap between the arrival of an order at the market and display on the client's screen, the time gap between the execution of the order and display on the client's screen, double entries of a single order, risks caused by no information or wrong information and the spread of rumors, with or without malicious intent.

Emerging risks have been identified in the areas of account aggregation (who has the right to IDs and passwords) and the authenticity of content (outdated information or misinformation, can a financial service provider guarantee the content of a site). The panelist concluded his presentation by stating that the Internet has not brought new risks into existence, it has simply augmented existing risks or brought those risks to the surface.

Group Discussion

The participants stressed the importance of choosing an objective 3rd party, such as an IT security-consulting firms, to audit a firms IT systems. However, the participants were reluctant to endorse the use of in-house auditing teams, as they may not have the requisite experience and objectivity. In order to overcome the hurdle of untrained or inexperienced auditors, participants recommended selecting auditors who had completed a certification program for IT auditing.

The participants agreed that the creation of international regulatory guidelines would be useful to create a baseline for operators of on-line brokerages and banks.

A discussion was held on the current trend of outsourcing operations to 3rd party vendors. It was generally agreed that outsourcing, while not a widespread practice in Asia, was beneficial to the industry as long as the outsourcee was highly qualified. Outsourcing enables rapid scalability in a firm's operations, and thus allows firms to react rapidly to changing markets. One of the most critical areas for a firm in the outsourcing process is to set forth the outsourcees obligations, including regulatory obligations, in the contract, and monitor the work continuously.

However, there were also concerns raised about the process of outsourcing. Since there are no uniform standards for outsourcees, the quality of outsourcees varies greatly. In some cases, even the outsourcees outsource work, which results in the firms not knowing who is actually completing the work. The regulatory

response to outsourcing varies greatly. However, some countries, such as Australia and Hong Kong (Hong Kong Monetary Authority), have issued guidelines to assist firms in creating a baseline for outsourcing operations.

Questions:

What are the major forms of Internet related operational risks, which firms and consumers feel they face?

Among the major operational risks faced today are: increased risk of hacking activities and system failures (such as denial of service attacks, network and systems outages), poorly administrated networks, reliance on outside service providers (outsourcing), lack of continuous security monitoring or intrusion detection mechanisms, outdated anti-virus software.

How do firms satisfy themselves that they have properly identified and are adequately addressing these risks?

Many of the larger firms contract with independent IT security consulting firms to run systems checks. However, since there are no legal requirements (in the jurisdictions we spoke with) for these types of external/independent audits, many of the poorly capitalized firms are unable or unwilling to invest the time and money necessary to conduct these assessments.

How do firms establish a realistic balance between standards of security, usability and cost, and what role should regulators play in this regard?

The cost/benefit analysis performed by firms is largely dependent on the size and reputation of the firm. A large global firm is more likely to utilize state of the art systems in conjunction with external audits given that it is dealing with sophisticated clients who demand security and accessibility. Regulators should issue guidelines, but not regulations, to set an industry standard.

What risks have firms identified in respect of web-dependent new services (aggregation, portals, digital certificates etc.)?

Some of the risks which have emerged as a result of web-dependent services include the following: account aggregation risks (who has the right to Ids and Passwords, the financial institution or user, is the displayed information current or out of date, concerns about the authenticity of the information), data privacy and customer protection (risk of sensitive or confidential data being stolen by hackers, use of sensitive or confidential information collected by aggregation service or portal).

In cases where such services are not currently subject to securities regulation, what would be the advantages and disadvantages of extending the scope of regulation to cover new services?

The advantages to extending the scope of regulation to these new services is that regulators can ensure they have jurisdiction over all parties involved in a particular transaction. The disadvantages are that many of the transactions take place in a cross-border context, and since there is no global regulator, extending the scope of regulation may not solve the problem because jurisdiction stops at national boundaries. Another disadvantage is that since many services are outsourced to companies outside of the scope of the jurisdiction of securities regulators, broadening the legislative framework would serve no purpose unless regulators also had jurisdiction over these companies.

Is there a clear definition of security 'incidents'? Can you give examples of disruptions or other market integrity issues where the internet-character of securities activities led to unforeseen disruptions?

There was no clear or definitive definition of security incidents. One example of a disruption was shortly after the September 11th attacks. In that case a virus (the I love you virus) was sent to systems throughout the world. However, as a result of September 11th, many countries had set up crisis management and command centers, which, once alerted to the virus, were able to successfully combat the virus. After the crisis was handled, a post response review was conducted, and it was determined that if the crisis management and command centers had not been in place, the damage caused by the virus could have been devastating.

What priorities for regulation in the area of IT security are set in your region and how are they determined?

There are no set regulations in the area of IT security (for the countries represented at the roundtable); however, some regulators have published guidelines to assist firms in this area. Hong Kong in particular has published guidelines in the area of IT security, which are not a legal obligation upon firms, but provide invaluable guidance for firms.

In your opinion, does the Internet enhance the possibility for the securities industry to comply with regulatory requirements such as the "know your customer" rule?

The Internet enhances the opportunity for the securities industry to comply with "know your client" rules. Properly drafted questionnaires should be able to cover all the necessary areas, and it should simplify record keeping.

What are the most important IT security risks that you can identify? How are regulators addressing them in your jurisdiction, how effective is such regulation?

See response to question i.

Session 3 Minutes: Cross-Border Issues

Summary of presentations

The Moderator reported that IOSCO members were making good progress in clarifying and even amending their legislation to adapt their regulatory approaches to the Internet age. In the cross-border context, there remained key areas where regulators were currently focusing their attention. These include key issues such as jurisdiction, consumer protection, exercising effective regulatory oversight over a remote intermediary, enhancing regulatory cooperation.

Technologies would continue to improve and evolve, regulators would have to keep an open mind and a watchful eye for new developments, and react swiftly but sensibly.

Going forward, greater regulatory transparency and clarity would be pertinent. Further, regulatory collaborations to promote level playing fields and international best practices were helpful in facilitating cross-border services.

First panelist

The first presentation highlighted the legal and regulatory issues in a cross-border context. These included licensing considerations, requirements and restrictions concerning the marketing of services and products, market conduct requirements and jurisdiction/territoriality issues. Different requirements in different markets might result in higher compliance costs. A "light touch" approach was suggested for intermediaries operating in "approved jurisdictions" (i.e. jurisdictions where the host regulator is comfortable with the standards of the foreign regulator).

Second panelist

The second panelist provided data indicating that the Internet had fuelled the growth of cross-border investing. Intermediaries recognised that while technology was an enabler for cross-border operations, it came with sizeable up-front costs. Regulation had a significant role to play in either enabling, or creating barriers to cross-border provision of securities services.

For regulators, concerns arising from cross-border activities would include investor protection and market integrity issues. They would have to be satisfied that they have sufficient mechanisms in place to ensure adequate and proper regulatory oversight of intermediaries who offer securities services from overseas jurisdictions. Different regulatory standards and requirements could impact significantly on the operating costs for intermediaries operating in multiple jurisdictions.

Group discussion

Participants cited the following elements as being necessary for the success of the EU passport approach, to facilitate the provision of cross-border services:

- Similar regulatory standards across jurisdictions
- Common institutions and legal framework
- Good enforcement regime, with high degree of cooperation, and strong sense of trust among regulators

There was, however, still scope for the regulation of cross-border activities to be streamlined so as to give rise to more effective supervision, and lower the regulatory costs for the intermediaries. One such area was the regulation of business conduct practices. The Committee of European Securities Regulators (CESR) has finalised a categorisation regime for investors, which would pave the way for intermediaries' business conduct practices to be subject to the oversight of their respective home regulators.

Within the Asia-Pacific region, the varied stages of market developments and structures were significant considerations for regional harmonisation.

Some participants suggested that the “Home-Host” regulator concept in banking could also be applied in the securities markets. Securities regulators could explore the feasibility of apportioning the regulatory responsibility amongst the relevant regulators, similar to the “Home-Host” concept. This would have to be weighed against a regulator’s responsibility to protect investors in its own market. Domestic investors would still hold their regulators responsible for any wrongdoings by foreign intermediaries.

Where regulatory practices and standards were not harmonised, one suggestion was for intermediaries to comply with the most onerous set of requirements. Such intermediaries could then be deemed to be in compliance with the requirements in relevant jurisdictions. However, in many instances, regulatory requirements might just be different rather than more or less onerous. Furthermore, customised approaches might be appropriate in order to tailor to the local climate in different jurisdictions.

At a high-level, there was already a significant degree of commonality between regulatory regimes. Regulators could consider moving towards harmonisation of regulatory standards and practices by first agreeing on the regulatory areas in which there are significant commonalities.

In Asia, efforts are underway to lay the groundwork for future cooperation. The IOSCO Asia-Pacific Regional Committee had commenced fact-finding studies to enhance members’ understanding of each other’s regulatory regimes. For a start, the members were focusing on two key areas: investors’ rights and remedies and regulation of remote terminals.

Questions

How do regulators co-operate in identifying regulatory gaps and ensuring consistent regulatory treatment when service providers offer their services in multiple jurisdictions? Please provide some examples on measures that were found to be effective.

The EU passport approach was mentioned as being effective in facilitating the provision of cross-border financial services in Europe.

In order to lay the groundwork for future cooperation, the IOSCO Asia-Pacific Regional Committee has taken measures to enhance members’ understanding of each other’s regulatory regimes. This would be the first step towards future harmonisation.

Are there any risks (IT, privacy, regulatory, market integrity or fragmentation) that will become more pressing in a cross-border environment? If such risks are identified, what are the developments and factors contributing to each of these risks?

Most of the risk and concerns cited related to uncertainties and unfamiliarity with differences in the legal and regulatory regimes in different jurisdictions. Issues of jurisdiction/territoriality for example, are not always clear. Liability issues would also vary from one jurisdiction to another.

What is your assessment of the efforts by the securities industry, IT industry and regulators in meeting these risks?

In the area of regulations, greater bilateral and multilateral co-operation to enhance enforcement of securities laws and regulations. The promotion of international best practices by IOSCO would also reduce regulatory gaps and arbitrage.

What do you see as the major impediments (e.g. consumers’ interest, cultural, regulatory, legal, lack of familiarity with foreign market, protectionism etc) that limit the provision of cross-border securities services?

Major impediments include:

- The high cost of IT infrastructure required for cross-border services.
- The cost associated with having to acquire a good understanding of the legal framework and regulatory regimes of the foreign markets, so as to mitigate legal and regulatory risks.
- The compliance cost associated with having to observe the regulatory requirements in multiple markets (e.g. multiple licensing fees, different disclosure requirements, etc.)

Is there a role for regulators and/or government to co-operate and facilitate innovation in Internet securities services and provision of cross-border securities services? If yes, what is your expectation?

Going forward, greater clarity and transparency in regulatory regimes in various jurisdictions is useful in facilitating compliance by market participants. A more open and consultative approach would allow the industry to work in partnership with the regulators to facilitate the formulation of regulatory regimes that are responsive and relevant.

Session 4 Minutes : Investor Education Issues

First panelist (consumer council)

The presentation mainly focused on the need for investor education and protection in terms of 3 areas:

- recognizing basic consumer rights;
- providing realistic dispute resolution mechanism; and
- strategies for global co-operation.

In order for electronic commerce (EC) to be successful, whether in the trading of securities or goods, consumer confidence is of utmost importance and critical. Several reports and guidelines have been released by worldwide organizations such as OECD and Consumer International dealing with issues in relation to online trading and consumer data protection and privacy. Apart from that, Hong Kong has a range of laws to protect consumers and investors in the market place. There is also a need to address the issue as to the extent to which local consumer protection laws can be enforced across different jurisdictions particularly in relation to EC disputes.

Self-regulation is one way to enhance consumer protection. In this respect, mechanisms such as trust marks are used to boost investor confidence and protection by providing a certain degree of credibility to persons or merchants who possess such certification. In addition, there is a need to ensure that there are online dispute mechanisms put in place to allow disputes to be settled electronically particularly with regards to electronically concluded trades. Codes of conduct and codes of practice are equally important in a self-regulatory environment in enhancing consumer protection.

Global cooperation is another crucial ingredient in consumer protection. In order to achieve this, there must be balanced participation by the government, industry and consumers worldwide. In addition, there should be a single forum or organization that is dedicated towards addressing issues or problems faced by government, industry and consumers and to develop a harmonized and standard approach in dealing with these issues.

Second panelist (financial portal)

The presentation mainly dealt with the business and services of a financial portal that offers financial services and products to the investing public by empowering investors in Hong Kong and China with a variety of financial tools, information and advice to assist them in making an informed investment decision and to manage their own investments.

The contents and information that is posted on the portal are checked to ensure that the information is reliable and not misleading. There is an internal person in the firm who constantly monitors the website to ensure that the quality of the information is maintained. Only persons licensed by the relevant regulatory authorities will be allowed to post information on the website and products that are offered on the website are only those that have been approved by the relevant regulatory authorities.

With respect to investor education, the firm aims to educate investors about the broadest principle of wealth management, how it can assist investors in realizing high returns at the lowest volatility and risk whilst securing satisfactory return. As for the role of the regulators, it was recommended that:

- the relevant authorities constantly monitor the contents, information and products offered on financial websites;
- financial websites must hyperlink to the relevant regulatory authorities website; and
- other jurisdiction recognizes any financial websites that have been approved by another jurisdiction.

Group discussion

A concern was raised that should financial websites be required to hyperlink to the regulator's website, there is the danger that it may give the impression that the regulator has endorsed the website. It was felt that this should not be a concern particularly if the financial website operator is licensed by the regulator and therefore subject to the relevant rules and regulations in respect of activities carried out by the financial website. However, there is a need to monitor financial websites that are not licensed. A suggestion was put forward in response to the endorsement concern that appropriate disclaimers be displayed stating that the regulators do not endorse the financial website.

Financial websites should be required to provide a checklist for investors so as to alert and remind them of the steps/measures that need to be taken before making an investment decision. For example, alerts should be displayed reminding investors to, among others, validate any information or research material obtained via the Internet, to seek professional advice before making an investment decision etc.

There is a general practice in Hong Kong that if a person intends to hyperlink to a website, permission to do so will first be obtained. The general policy in the HKSF is that if a licensed person seeks permission to hyperlink to the HKSF's website, the permission will normally be granted. However, with regards to the HKSF's eIRC website, hyperlinks to the website are not allowed by selected licensed persons as not all of the licensed persons have websites. In addition, the public may query as to why there are hyperlinks by certain licensed persons and not the rest. It was viewed that allowing hyperlinks by selected licensed persons could amount to endorsement by the HKSF.

If codes of conduct are developed in response to the need for self-regulation, an industry committee/board should be established to monitor compliance with the code and to handle any complaints from consumers/investors. Such committee/board should also be given the power to impose appropriate penalty for non-compliance such as revoking membership to the association. The decision of the committee/board should be binding on its members and the complainant.

With respect to trust marks, it was viewed that a separate entity be responsible for providing the trust mark accreditation. However, before a trust mark certification can be given, certain criteria should be fulfilled which could include the inclusion of contractual terms, protection of consumer right or providing for online redress mechanisms. It is also equally important that consumers themselves should take measures to protect their own interest and should not rely solely on the trust mark certificate when soliciting online services.

Currently, the greatest threat for online investors in Hong Kong is the risk of relying on information which may be false or misleading. Relying on such information when making an investment decision could result in losses.

Codes of practice in a self-regulatory environment should not be limited to codes or guidelines issued by regulators. Industry and consumer associations should also play a role in ensuring that issues relating to investor protection and investors' rights are addressed in these codes of conduct and complied with by the relevant parties. It was felt that protecting investors should not be the sole responsibility of the regulators.

Internet penetration in most Asian jurisdiction is still low, hence there is a need to educate the public on online trading through traditional means of communication such as television, radio, magazines, newspaper etc. rather than solely relying on electronic means to provide such education. Also it was found that the most effective way to educate investors was through the traditional mode rather than through online means. It was concluded that the use of both the traditional and electronic mode be used to complement each other in the area of investor education.

With regards to the privacy and use of consumer data, it is critical that industry have privacy policies put in place when dealing with consumer data. As to the use of the consumer data, if a consumer restricts the use of such information to certain purposes, industry should not exploit the information for other purposes unless authorized by the consumer.

There was concern as to whether the ISO was the appropriate body to issue an international code of practice for trust mark schemes. It was viewed that there is no one appropriate entity to deal with such issues and that there is a need for government, industry and consumers worldwide to get together to decide on the appropriate standard or benchmark for trust mark schemes.

The use of trust marks is not popular as it is costly coupled with the fact that there is a need to re-certify the trust mark after a certain period. Due to this, companies are reluctant to obtain such certification on an on-going basis. Furthermore, if companies fail to renew their trust mark certification, there is the possibility that consumers/investors will presume that the company has failed to meet the criteria to be re-certified thereby making these companies not trustworthy.

Industry and regulators have an important role to play in educating investors. Intermediaries generally educate investors as to how to maneuver through their website such as how to place an order, how to cancel an order etc. and to provide sufficient information to investors so as to assist them in making an investment decision. Such information is usually related to the product and the market. As for the role of the

regulators, industry was of the view that basic fundamental investing principles, the risks involved in investing, how investors protect their interest, investors rights and remedy under the law and how to deal with licensed intermediaries should be conducted by the regulators. Also it was suggested that constant dialogues between regulators and industry should be held to discuss issues faced by industry with respect to providing information to investors and how to further enhance investor education.

Eventhough online trading has shifted the responsibility for decision making of investment to the investor, the issues confronting investors in the online environment is not any different from that faced in the traditional market place. Even with the increase of online trading, it was felt that investor education should not be made a mandatory requirement before allowing investors to trade securities online. Furthermore, this could be a deterrent from trading online to take off.

It was suggested that school curriculum should include investing and investment issues to ensure that the investing public are trained from young as to the prudent way to invest. However, to implement this suggestion, it should be a government initiative rather than the regulators.

Regulators should encourage licensed intermediaries to cooperate with colleges or learning institutions to have online investment education courses available through the licensed intermediaries website.

Questions

How do we attempt to ensure that investors who make their own decisions and execute trades on-line are educated enough to be acting as their own financial advisers?

Intermediaries should be encouraged to cooperate with colleges or learning institutions to have online investment education courses on licensed intermediaries website. Also in order to inculcate prudent investors from young, the school curriculum should include investing and investment issues.

Should investor education requirements for do-it-yourself investors be mandated?

It was felt that there should not be a mandatory requirement that investors attend investor education programmes before allowing them to trade online. Furthermore, this could be a deterrent to potential online investors.

What role should industry play to ensure investors are receiving the information they require to make informed investment decisions?

Alerts, checklists or reminders should be displayed to reminder investor of the measures to be taken before making an informed investment decision. In addition, industry must ensure that any information provided to the investor through their websites is accurate and not misleading. There should be constant monitoring of the contents of the information on these websites by industry and regulators alike.

Is there a need for the development of independent investors' groups? Why aren't these groups developing?

There are local and worldwide consumer associations and independent organizations that look at the protection of consumers rights which include investors in the stock market. For example OECD issued guidelines for online trading while Consumer International had released a paper on data protection and privacy.

How do we educate investors that free online research does not necessarily equal good, unbiased research?

One way is through requiring that investment and investing be made part of the school curriculum to educate investors from young. Also tie-up with colleges and learning institutions to provide online investment courses should be looked into in further detail.

Is investor education resources from industry sources inherently a conflict of interest and biased?

For example, in Quamnet whenever there is a potential conflict of interest arising with its brokerage arm, there are blackout periods where certain securities or products cannot be discussed on the website. Quamnet also ensures that the information provided on their website is free from any conflict of interest.

How can investors determine the quality of online research sources, including investor education resources?

Investors can play a part in protecting themselves by validating any information or researches obtained from the Internet with licensed intermediaries.

How can we ensure that investors are educated about the fact that everything they read on the Internet needs to be backed up and verified?

Investor education in the form of the risks involved in relying on information obtained from the Internet should be conducted through channels of communication that has the widest scope of circulation such as newspaper, magazine, radio and television. Apart from that online education should also be used for the benefit of Internet savvy investors.

How can we help investors validate information they get on the Internet?

Licensed intermediaries and regulators should constantly monitor the information and contents posted on the websites of these licensed intermediaries to ensure that it is not false and misleading. Also alerts and reminders should be given to investors to validate information obtained from the Internet with approved licensed intermediaries before making an investment decision.

How much do investors need to be educated about the rules and regulations in place to protect them from electronic communication?

Regulators should educate investors in relation to the broad principles of investing, their rights and remedy under the law and the risks involved when investing, whether in the traditional or online environment.

Session 5 Minutes: Enforcement Issues

Summary of panel presentations

First panelist

The first panelist (Technology Crime Division, Government of Hong Kong SAR) gave a presentation on the challenges his office faces when conducting an Internet-related investigation.

The first issue he raised regarded computers where the use was incidental to the crime.

The ISPs cooperation was the next topic of the presentation, describing the incentives and disincentives for them to provide information to enforcement authorities.

And finally, the panelist raised the issue of the extra-territoriality of the Internet, and the difficulties encountered when conducting an investigation when a foreign ISP is concerned.

Second panelist

The second panelist (Internet Services Provider Association), presented the views of the ISPs regarding enforcement issues. He stated that the ISPs are a conveyor of information, which does not belong to them but to their clients. The panelist then stressed the technological limits regarding issues such as the possible due diligence ISPs can accomplish (for instance on spam e-mail), or on the cooperation with authorities when providing information.

Third panelist

Finally, the third panelist (telephone industry in Japan), presented the situation in Japan where, thanks to mobile phone and I-mode, 33 million Japanese have access to the Internet. He first pointed out the importance of maintaining the integrity of Internet services, especially due to the large number of spam e-mail. He also gave examples of the use of technology to address unwanted or spam e-mail. Finally, he pointed out the need for legal solutions to address misuse of the Internet.

Group Discussion

The first topic that was discussed regarded the necessity for enforcement authorities to create a relationship with ISPs based on trust: enforcement authorities need to know if the information given by an ISP is valid and if an ISP is trust worthy. For instance, it appears that some ISPs have a "contractual" obligation to contact their client when being investigated by an authority.

The second issue regards the means for an authority to obtain data from an ISP: since the information will only be provided after a warrant is issued, the enforcement agencies have to be precise in their demands, and cannot try "fishing" exercises to obtain the relevant data.

On the question regarding the traffic data that are kept by ISPs, the industry explained that only information needed for accounting purposes were stored for a limited amount of time (three months). The data are log in / log out time and client ID

It was stated that there is currently no legislation in Asia regarding data preservation.

On the spam e-mail issue, it appears that most ISPs in Hong Kong abide by a specific code of conduct and try to filter spam e-mail (but within the possibilities granted by technology) in order to still be able to provide a good quality of services to their customers. It was also explained that in most cases, spam e-mail originated from foreign ISPs, who do not follow such a code of conduct.

Moving on to the topic of subscriber data, the ISP industry explained that the basic information asked for individual is their ID card number. For a corporation, it is a registration number. These data are kept for a longer time than traffic information, in some cases for as long as a year after a customer has cancelled his subscription. ISPs may also have access to banking information when available, i.e. when the customers are charged for using ISPs' services. Finally, it was stated that the accuracy of the information given by the client to the ISPs was not checked: therefore in some cases the information can be completely false, especially for individual customers, but this is less of a risk for corporations.

Enforcement authorities then explained that a 6 months preservation for traffic data would greatly help investigations. A shorter period raises problems in cases of late discovery by the authority. The main difficulty of such a length of time for data preservation is caused by small ISPs, who do not preserve data because it is too costly.

On the question of filtering e-mail in order to limit spam, ISPs stated that they never look into content data. Due to ethical reasons in the first place, but also because of privacy-related legislation. Since the content data belong to the client and not to the ISP, it could therefore be considered that the ISP is acting as a hacker.

The issue of the preservation of the client caller phone number (CLI) as a traffic data was then discussed. It was stated that since the telephone is no longer the only means of accessing the Internet, this information would only provide adequate identification 80% of the time. Furthermore, it is not standardized. This raised the issue of the need for legislation or a code of conduct to be technology neutral.

The discussion moved on the very specific topic of disclosure of information by the ISPs to securities regulators. While it does not raise any problem in Hong Kong, Japanese FSA explained the difficulties they encounter: even if they can have a legal access to any information, the ISPs on the other side have a legal obligation not to disclose traffic information to any third party.

ISPs explained that if they can cooperate on a voluntary basis, they will need official documents to give information regarding their consumers.

The group then discussed the issue that was recently raised in Australia regarding e-mails: Is it possible to seize a hard disk containing unread e-mails? The law is not clear in this regard and a very conservative interpretation of the law has been taken, leading to the situation where ASIC cannot gain access the content of e-mails held by third parties.

Finally, the form of the cooperation between ISP and enforcement agencies was discussed: should there be a simple dialog, or is there a need for legislation. ASIC provided the group with a description of the situation in Australia. No legislation has been passed, but a discussion between law enforcement authorities and ISPs is taking place. This will lead to the creation of a code of practice. The parties are still discussing the matter and a second draft of the document has already been drafted. It is intended that the code will be an on-going document, that needs to be dynamic to take into account the technological changes, instead of the classic technology neutral approach. ISPs in Australia have stated that agency requirements have to be stated specifically, as they cannot retain all information, all the time. At the moment in Hong Kong, the relation between ISPs and Enforcement offices is based on good trust and cooperation. Even it is possible to create such a code is possible, the ISP industry would prefer to have a legislation, in order to give a firmer ground to requests and to know exactly where each player stands.

Questions

What kinds of traffic and subscriber data do ISPs retain?

The traffic data ISPs kept are mostly used for accounting purpose. They consist of log in / log out time and of the client ID.

Even if the client phone number is sometimes kept by ISPs as traffic data, the preservation of this information is not standardized since it is now possible to access the Internet without using a phone.

Subscribers information consist, for individuals, of the ID card number, and for corporations, the piece of registration.

ISPs also keep banking information regarding their customers (Credit card number, account number...), but only when they charge them for using their services.

Do ISPs verify the identities of their subscribers and, if so, how?

ISPs do not verify the accuracy of the information given. Therefore, it is frequent that information, mostly for individual clients, is false.

Do ISPs retain the content of electronic messages? Are certain types of information or certain types of account data retained while other forms are not? Are there any important types of information that ISPs retain securities regulators might overlook when requesting an ISP's assistance in an investigation?

The ISPs do not read or retain the content of electronic messages, mainly for ethical reasons but also due to privacy-related legislation.

How long do ISPs typically retain traffic, subscriber and account information?

In most cases, traffic data is kept for only three months. This seems to be too short for enforcement authorities, whom would like a length for data preservation of six months. On the other hand, subscriber information is kept for a longer period, like a year after cancellation by a client.

Are there any industry codes related to retaining certain types of information that would assist securities regulators when seeking such information?

There appears to be an SPAM code of practice, which Hong Kong ISPs abide by.

Technology and cost

Even if the question was not fully debated, it appears that costs are the main reason why ISPs, and especially small ones, do not preserve data for a longer period of time.

Share record with Securities regulators

Even if ISPs are willing to cooperate and to share information with securities regulators, they also have to comply with privacy related legislation that sometimes forbid them to share any information regarding their client to any third party except legal authorities.

Also, it seems that the content of e-mails falls under privacy and mail protection related legislation and, therefore, can not be shared with any regulator.

Forms of request

The ISPs are willing to cooperate on a voluntary basis but, in most case and due to privacy related legislation, they need to receive a formal request before disclosing information regarding their clients.

Customer notification

It appears that some ISPs have a "contractual" obligation to notify their customers when they have to provide information to an enforcement authority. This does not seem to be a global practice of the industry, but only the case for some small ISPs.

Emergencies

It seems possible that, if asked by a securities regulator from a different country, an ISP will preserve the data in order to identify the author of an on-going scam. The ISP will then wait for a formal request by its securities regulator to share the information, whom will then forward the information accordingly to the other regulator.

ISP surveillance

For ethics reasons and also in order to comply with privacy related legislation, ISPs do not look into the content of the information exchanged. Content information is the property of the client, and therefore it could be considered that the ISP is hacking itself.

Most ISPs try to filter spam e-mails but, due to technological limits, a full surveillance is not possible because it will deteriorate the quality of the service provided to their clients.

Regarding spam, most ISPs follow a code of conduct. However, it seems that spammers are located in countries where this code is not respected or are using ISPs who do not follow this code.

Meeting Minutes of the IOSCO Internet Project Team's Americas Roundtable Meeting, November 25-26, 2002

Session 1 Minutes: Research and Industry Trends

Summary of panel presentations

First panelist

This panelist identified the following facts as driving changes in the industry: the amount of data (need for data management), drive to real-time processing, and need to manage and collaborate with content. He described the following workflow issues: no ability to access information and instructions where the processes reside, local control of content and instructions production, regulators look for historical processes, and key transaction elements not linked electronically.

He believes that regulators are following technology development rather than looking for innovative solutions. Data linkage is the key to future developments. With data linkage the credit ring becomes irrelevant and there could be disintermediation of stock exchanges. Customers need to be linked at the pre-trade (information), trade (transaction) and post-trade (credit ring) steps.

The following success criteria were identified: cost savings, advantage of sharing information, integrity of system and users, geometric search reach and ability to work with current business models. Going forward there is a need to look at the industry infrastructure, standardization and out-sourcing of business processors.

Second panelist

This panelist described the "Home Broker" internet connection to BOVESPA. BOVESPA provides 3000 workstations for trading and data to 30,000 workstations. The brokers choose the technology providers; however, the exchange sets the requirements regarding what has to be provided. The intermediaries choose the technology providers. There is a Home Broker stamp, which indicates which brokers have been approved by BOVESPA. They also offer investor education through information and self-testing. As a result of the Home Broker network there has been an increase of 30% in trades and 15% in volume in the year 2000.

Third panelist

End users want direct access to the liquidity pool. Technology is weakening the role of the broker/dealer as gatekeeper. Advantages of the Internet include: breadth of reach of services to clients who do not generate enough revenue for higher-end trading; low cost of electronic access and trade settlement; ability to monitor activity and transparency. The panelist noted that it's getting harder to measure execution quality due to splitting of orders and linkages. The information is only complete for small orders. She reviewed the introduction of electronic trading of index future products. The advantages of trading E-minis were anonymity, speed, price discovery, transparency, better audit trails, low costs, and the breadth and reach of services. Issues include a longer wait for customers, need to code rules into devices, and all products and all things in a single box.

The impact of technology on the role of the dealer has been a) the dealer has become more of a transfer agent and b) dealers are less able to monitor what is going on. So, there are more errors in trading and more triggering of program trades. She suggested that an area for regulators to get involved in was the disclosure of trading policy rules. Institutions are more likely to want proprietary networks, while the retail customers are more interested in the internet.

In the future there would be more linking of research and trading to other services. There is also a need for research on order flow and quality of execution.

Discussion

The group discussion considered where the industry will be in a few years. Comments were made that there would be more involvement by institutional customers who would want more control of the trading process. A statement was made that there is a need for more international best practices and guidelines, transparency of rules, monitoring and enforcement. Regulators should monitor methodologies rather than establish rules. There would be a shift from transactions to the nature of relationships. A question was raised if there is the necessary infrastructure in place to allow the changes being discussed. There appears to be a large amount of demand for trading cost information and analysis.

In response to the questions on new business cases, there would be increasing demand for aggregation and integration of services. For example aggregation of financial data across accounts and relationships. A more robust financial management function will be needed. The major regulatory issue will be who owns the data. There may be a shift from intermediaries who control the data and access to data to making data available to investors to use how they choose. New models will arise from the data issue.

It was also noted that there appears to be a convergence between exchanges and brokers. Exchanges are moving to the areas beyond transaction execution such as data and other services; while brokers are looking like exchanges. There will also be new types of transactions markets: providing securities for credit on an auction basis, investors wanting to get paid for data, loyalty programs.

A global infrastructure may be required to facilitate the developing business models. In particular, global infrastructure for settlement and custody would be important. Protocols and standards may be needed to be established. Although a concern was raised that protocols can be dangerous because they freeze technology and thereby freeze innovation.

Questions

What new Internet-related developments with respect to securities trading have you identified as relevant to your business through the use of financial research and statistical data?

No one identified any particular third party research or statistical data that has been used. Some parties are doing their own research through consultation and observation of new activities of other parties.

How may technology be used in the future for securities trading purposes?

Technology will be used to provide access to information, linkage of information to analysis and transaction execution, and linkage of customers. It was also suggested that technology will be used to evaluate execution quality and costs. There will be new types of transaction market such as markets for margin. New models will change who owns and gets paid for data. Loyalty programs may also develop. In some areas such as clearing, there may be less transparency.

What is the prospect of Internet-only securities trading provider, and how does this translate to the entity motivation to access multiple jurisdictions to reap the benefits of scale and scope?

Relevance of physical location diminished. Most firms have global networks and ability to route orders to easiest access markets with the least regulatory burdens.

Do you expect significant growth in cross border securities trading services in the next three years?

Clients want access to services and products in other jurisdictions and can't understand why they are not available. Institutional customers will put pressure on intermediaries to make cross-border services including analysis and control available. Markets want access to greater liquidity and will act as another driver for greater cross-border access.

Which areas in securities trading services that leverage the Internet are likely to see higher cross-border growth? Are the patterns of growth different for the B2C and the B2B segments.

Institutional traders are more likely to use dedicated networks while retail customers are more likely to use the Internet.

What are the key critical success factors or pre-conditions for securities trading services using the Internet (E.G. high Internet penetration rate, regulatory regime providing for certainty or clarity, suitability of the services) What type of services will grow in the future?

Discussion from participants identified the need for infrastructure available at a reasonable cost. One participant suggested there is a need for a global approach to settlement, custody, service levels and data integrity. There were suggestions that there is a need for standardization and international best practices. It would be useful to have a global agreement on what are the important protocol issues from a processing perspective. However, there was concern expressed that protocols can be dangerous because they freeze technology and create barriers to innovation. One participant cautioned that the regulator should focus on performance standards rather than technology standards. Agreeing on data standards including ways to identify quality of data is very important. Investor education was also seen as an important success factor.

Session 2 Minutes: Emerging Risk Profile

Introduction by Moderator

The Moderator noted that the events of September 11 brought to light issues regarding whether securities activities over the Internet involve differences in degree or differences in kind vis-à-vis traditional securities trading activity.

Summary of panel presentations

First panelist

This panelist started the panel discussion with a description of the Internet-related aspects of the Chicago Mercantile Exchange. He noted that the velocity of trading in general has increased dramatically, with implications for regulation. Transactions that once were completed in tenths of a second are now completed in milliseconds.

In addition, he noted that the CME has changed from a closed-membership model to an open-membership model. Anyone who wishes to trade can now do so, leading to a convergence of Internet-style securities issues with those of general securities trading.

He continued by noting the increasing nature of technological operational risk. Every technological improvement has increased transaction speed. Every increase in transaction speed means less time to mitigate risk. This becomes an issue because of various interdependencies becoming built into the system. Automatic trading and arbitrage systems now mean that even a momentary glitch in the system (a mis-keyed order, for instance) has a ripple effect through the market as computers take advantage of the trading opportunity.

Possible solutions to these risks (implemented at the CME) include placing size limits on orders, price banding, and time-order cancellations (which automatically cancel orders after a set time).

A separate risk area is connectivity. There is a risk of relying on only 1 to 3 carriers, particularly in a post-Worldcom era. In this area, the Internet is actually a solution to technology risk, by offering a backup to regular systems. Customers are given a wide array of connectivity choices, through various ISPs, direct electronic connections, telephones, etc.

The increasing number of customers also means new customer demographics. Customers are now pushing broker-dealers to circumvent broker-dealer safety requirements because they slow down the speed of trades (for example, a credit check that takes 1/10th of a second costs an enormous amount of money in a world in which trades are executed in 1/1000ths of a second). This is becoming an important regulatory issue.

Many market participants also value anonymity, both for privacy concerns and other reasons.

Many exchanges have instituted Internet Disaster Recovery Linkages. These include back-up sites more than 300 miles away from the exchange. In response to the Critical Infrastructure Protection Executive Order in October 2001, the CME worked with customers, the Federal Reserve, the CFTC and the Secret Service to secure these systems.

Nonetheless, he noted that he much prefers the US Commodity Future Trading Commission's looser regulatory approach to that taken by the US Securities and Exchange Commission. The exchanges themselves have a vested interest in mitigating Internet-related risks, and excessive regulation in this area is unlikely to resolve risks as efficiently as the exchanges themselves, while the regulations proposed may be costly and ineffective.

Second panelist

This panelist addressed the Roundtable by observing that he prefers the term "business resilience" to "operational resilience" because the latter is too technology-focused. This past year has seen a series of extraordinary events, beginning with September 11, following through with the anthrax scares (where mail was delayed for long periods), and including new money-laundering patterns (including terrorist financing). On top of that are governance issues such as rogue traders, and new regulatory issues such as Basel II, new anti-money laundering legislation, US Federal Reserve/Comptroller of the Currency/SEC proposals on operational resiliency, and the UK FSA's CP142 on Operational Risk. Yet perhaps the most significant recent event has been the economic downturn.

Among the issues the securities industry should consider is disaster recovery, particularly business processes and organizational communications. One important lesson from 9-11 was that the critical transaction processing systems were very resilient. The problems came from the organizational side, because while the systems survived, the individuals involved were unable to get to work. Resiliency, therefore, is not just a CIO issue — it is an issue for the broader business.

According to the panelist, the key issues for securities activity on the Internet are: fraud and money laundering, ID management and ID theft, privacy in an era of more disclosure, and trust.

A key issue for money laundering is the existence of legacy systems. These systems are good because they work and new systems need time to become integrated and effective. However, there is no common logical tools that will work across multiple systems to detect money laundering.

Privacy and disclosure have become conflicting demands. Institutions often do not want firm-wide access to customer information because of jurisdictional issues. The technology exists, but firms do not want it.

Third panelist

This panelist devoted his presentation to a discussion of the IOSCO Internet II Report.

He stated that the issues raised in the Internet II Report are the same issues facing all firms, not just those dealing with the Internet. It is important for good regulation to cover all risks, and the risks posed by the Internet are not unique. However, recent reports by the UK FSA, the HK FSA and the US SEC (as well as the IOSCO Internet II Report) all consider the Internet to be somehow unique, despite explicit statements in each of these agreeing in principle that the nature of the risk has not changed.

Viewing Internet issues as distinct from the risks all securities firms face is not optimal. Internet discussion sites are a perfect example: posting market-manipulating information on an Internet discussion site is no different than posting this information on a physical bulletin board, yet is treated as conceptually different. Likewise, the computer hacking is not conceptually different than the case in the San Francisco area in which thieves in white jeeps formerly owned by the Postal Service drove around stealing personal information from people's mailboxes.

Another example is the suggestion in the Internet II Report that websites have warning statements “on the risks of online investing.” This is important, but is better addressed by investor education. There are, after all, risks to non-online investing. Why don't we require a telephone broker-dealer list off all the possibly nasty things that can go wrong with traditional investing—such as mis-keyed orders by the broker-dealer, misunderstanding the customer's requests, etc.? These are easily as likely to happen as any problems unique to the Internet.

He continued by noting that the Internet II Report also discusses day trading. However, the warnings suggested in the Report regarding day trading are “silly” — in particular, the warnings that day trading can lead to excessive trading by investors (and the repeated transaction charges these numerous trades entail). Essentially, the Report argues investors should be warned that the low cost and efficiency of online day trading are bad because this low cost and efficiency could lead you to make repeated trades. The suitability reviews, also suggested in the Report, would undermine active trading strategies employed by many investors.

He returned to the issue of Internet discussion sites by noting that, although regulators should be concerned about market manipulation, the appropriate way to address these concerns is for regulators to focus on the fraudsters. Proposals floated that would require discussion sites to monitor for market manipulators are unworkable. ISPs everywhere would have to hire teams of investment bankers in order to recognize cases of market manipulation. They would then have to report cases to regulators. Complicating matters is that the ISP would have to identify the poster, despite the use of Internet aliases and even an EU directive specifically allowing individuals to use aliases as an Internet ID. Furthermore, ISPs would have to continually archive these postings. This could apply to all Internet discussion sites because there is always the possibility that someone on a sports discussion site will go off on the main products of a company and this could be interpreted to be investment advice.

He concluded by saying that the end result is that the Report is “strongly oblivious” to the practicalities of the Internet. The Internet offers speed and efficiency and meets the needs of customers, and it would be a shame if those needs are not taken into consideration with new regulations or legislation.

Discussion

One participant opened the discussion session by saying that 40 years ago we would have had 85% of the same issues raised regarding the Internet with the advent of broker-dealers using the telephone, particularly with boiler-rooms and cold calls from other jurisdictions. Offline brokers should only face the same scrutiny as online brokers. Regulators should break down Internet-related issues into three categories — issues to be regulated, issues to educate investors about, and issues to facilitate.

Another participant noted that extreme volatility is part of securities markets today, not just because of the Internet, but because of automated trading software. It is important to note that the two largest securities frauds in Canada over the past year had nothing to do with the Internet.

One participant noted the inherent conflict between customer identification requirements related to anti-money laundering regulations and concerns about privacy. These regulatory areas are heading for a collision.

Another participant noted that all of the Internet-related issues discussed today are really issues of distributing risk. Where should regulators come in? Citing just customer authentication as an example, the participant argued that regulations should be principle-based, not specific rules, leaving the details to be handled by industry on a contractual or other basis. Otherwise, as has been the case with regulators unwilling to accept innovative disclosure delivery methods, these rules create expensive obligations that do not help investors. For example, securities disclosures could be made via an interactive “talking head” program such as used by Turbo Tax software. Such a system would be more effective than a paper disclosure, but is currently not permitted by securities regulations.

One participant noted the enforcement issues that arise in an environment where transferring information is frictionless. Although little information on the Internet was not already publicly available before the advent of the Internet, the Internet permits this information to be gathered quickly and with little cost. Before, one would have to seek out such information at a variety of locations, requiring physical travel and time (i.e., friction). However, the information can now be gathered quickly and at little cost, creating problems for identify theft. The problem is made worse by automated computer systems in place at banks and securities firms. In the “old days,” a teller might know the customer and notice if someone was withdrawing funds from a grandmother’s account in a suspicious fashion. However, now, provided the thief had the proper passwords and ID information, this theft might not be noticed because the human element has been removed.

However, another participant countered that in the “old days,” detecting this theft might well be dependent on a specific teller knowing the customer? What if that teller were on vacation or sick that day? Today’s software systems can detect fraudulent transaction patterns that no human could detect and do not require a human (who might be sick or absent at critical times) to be involved. The system today is actually safer.

Another participant suggested that although many of the problems cited by the Internet II Report are arguably not new, what is new is the combination of rapid technological change, borders open to capital flows, and extremely competitive environments for securities and banking firms. In the past, with few competitors and protected commission structures, banks and securities firms could invest individuals and technology to protect their trading systems. Today, under intense competition, there is a fear that firms will skimp on security, particularly in a booming market. Therefore, regulators are necessary in order to set a floor for standards—we can’t always rely on firms to do it themselves.

Another participant argued that firms do take fraud seriously and that there is no worry of a race to the bottom.

Session 3 Minutes: Cross-Border Issues

Summary of Panel Presentations

First panelist

Electronic communication networks (ECNs) currently comprise approximately 26% of the dollar volume on Nasdaq. The advantages are reduced transaction costs, more price information, faster transactions and anonymity. The negative effects of ECNs are that they may permit fragmentation in liquidity and thereby create opaque markets or permit transactions at differential prices. Typically, in electronic markets there are no dealers to provide liquidity to investors. Direct buyers provide liquidity but there may not be sufficient

continuous order flow. The traditional way to provide price continuity is to funnel trades through a dealer so trades are concentrated. Price discovery also is difficult at the opening on ECNs. If, however, markets are located in multiple jurisdictions, it is possible that prices could be kept in appropriate relationships electronically more efficiently than through regular arbitrage.

E-brokers are regulated in Canada if their websites are accessible to Canadians, in which case, they must be registered. Otherwise their conduct contravenes the law and is regarded as contrary to the public interest. Why is this so--because the presumption is that investors need protection. However, in the context of the Internet regulatory protection needs to be flexible so as not to constrict the medium unduly. Regulators should consider the extent to which cross-border service providers themselves limit direct access and thereby provide needed investor protection. Further, Internet investors may be more sophisticated and require less protection than those reached by other methods such as cold calls.

The traditional regulatory methods are outdated; a new approach should be risk-based. The regulator should look at the qualities of the customer, the type of product, and where the securities or margin are held in deciding how to apply the regulatory framework. "Suitability" requirements also should be re-examined in light of the sophisticated Internet user. Many Internet users are bypassing advice because they don't need it or can search out primary information on the Internet.

Harmonization will be difficult to achieve. International harmonization cannot take place until there is national harmonization. In Canada there is no single national voice and this may be a pre-requisite to comprehensive international cooperation. Further, harmonization of secondary markets is meaningless without parity in how the primary equity markets are regulated in various jurisdictions.

One alleged concern of a passport system is that it can encourage a race to the bottom in regulation. It is said that to attract brokers or participants, jurisdictions may adopt less stringent standards and markets may move to establish in less regulated places. Studies have not found this to be true, however. Market forces are requiring more disclosure not less. In Canada, the reluctance to endorse a passport system has not been for regulatory reasons but may be based on cost or competitive issues.

Second panelist

The industry should view the regulator as a friend. The regulator creates a safe harbor by providing a road map of what can and cannot be done. Also, it can limit competition since only highly capitalized firms can demonstrate the ability to address regulatory requirements.

The cross-border issues for institutional customers are not different because of the Internet, only more profound because of the speed of transacting and because of the risk of error where there is direct electronic access. All large clients now insist on having 24-hour access meaning that there is never an end to the day.

As a general rule, in order to solicit and/or service clients an entity must be registered in some capacity where the clients are located. That is the premise the current regulatory system is built on. But there are exceptions, and it is the exceptions to the regulations that cause problems. This is because the exceptions differ from jurisdiction to jurisdiction. The rules also are often different for different products-- there is no consistency. For example: futures and securities in the US and financial products vs. non-financial products in Germany and Japan. For many institutional clients there may be no requirement for the broker to establish a presence, but the definition of an institutional client is not uniform. This is a huge problem for global firms. Firms deal with this problem by taking the most conservative position in the first instance. It is a race to the top, not the bottom, in regulatory compliance.

The firm also has to decide whom to permit to have client access and reconsiders only if the client pushes. In terms of the Internet the firm takes a conservative approach. Should access be openly available or limited? The answer is both. Originally intermediaries and markets tried to provide the firms with their own proprietary connection arrangements -- but demand today is for open architecture. WWW access is made generally available to intermediaries, however, only approved customers can gain direct electronic access after they have disclosed their jurisdiction and then only approved persons can have direct access or access research that may have regulatory implications.

Recommendations in the context of cross-border registration would be (1) to create a safe harbor for the dissemination of general information, and (2) to defer to the home country's registration when a broker is soliciting non-home country institutional clients regardless of the product. Regulators also should try to create common definitions, in particular, for what is an institutional customer. Rules should be clear and

consistently applied. For example, in some jurisdictions it is unclear whether it is prohibited or permitted for non-local firms to electronically link their order routing systems with the local exchanges.

Additionally, there is a disproportionate reaction to adverse local developments. Although politics may demand a reaction to regulatory failures, regulators should try to react to misconduct or fraud through enforcement actions not through additional regulations. Finally, there should not be an attempt to regulate prescriptively because the technology is changing too rapidly. Instead, regulators should seek to adopt uniform global guidelines or "best practices".

Third panelist

Today there is a huge opportunity for the retail investor. In the US retail is between 9-12% of dollar volume in the market. Online transaction penetration is 88% in the US and 67% in Canada. The risks associated with online investing are not new. They are really the same as when using a telephone to place orders or meeting customers face-to-face. Technology facilitates an increase however in access and an increase in transaction speed. This can be a benefit to investors by: improving the selection of a product, making trading price information more accessible and more timely, reducing transaction costs, and increasing competition.

In terms of cross-border issues, the world has become a single networked market place. The sophistication and reach of communications networks permits easy global access and the increasing ease of electronic channels has rendered territorial borders obsolete. Investing has become a 24/7 activity. This challenges securities regulators.

Securities regulation traditionally has been based on the concept of "residency". The broker and customer are territorially co-located which permitted strict control over qualifications and supervision of activities. The focus always has been on investor protection, from the perspective of the seller and from the perspective of the buyer. Barriers to cross-border services were initially technology-related such as restrictions on encryption export. Now the barriers to such services are regulatory restrictions and protectionist initiatives along with cultural biases.

Risks associated with cross-border activities include: (i) market integrity concerns that develop when there are jurisdictional regulatory gaps in market conduct; (ii) money laundering; and (iii) misleading or insufficient disclosure. In reality, most market conduct breaches such as fraud, insider trading and manipulation have not involved cross-border participants.

Recommendations: reassess the "residency" approach to regulation; consider developing a "primary" regulator concept with regulatory cooperation to address jurisdictional interdependencies, and encourage proper disclosure.

Questions

How do regulators cooperate in identifying regulatory gaps and ensuring consistent regulatory treatment when service providers offer their services in multiple jurisdictions? Please provide examples on measures that were found to be effective.

Regulators begin by trying to harmonize their domestic policies. When there is a single national voice, then efforts at harmonization can be expanded cross-border. Otherwise, substituted compliance works in some jurisdictions--where the home regulator recognizes compliance with the licensing regime in the other jurisdiction subject to some additional customer protections for the customers being serviced in their jurisdiction, such as additional disclosure. A passport system is only a viable possibility where there is reasonable equivalence in the rules in the jurisdictions in which a firm is licensed and that into which it is being passported. Whatever structural analysis is adopted, there needs to be a reassessment of the residency approach to regulation. A "primary" regulator concept with regulatory cooperation to address jurisdictional interdependencies may be the desired approach.

Are there any risks (IT, privacy, regulatory market integrity or fragmentation) that will become more pressing in a cross-border environment? If such risks are identified, what are the developments and factors contributing to each of these risks?

Market fragmentation is a risk found in electronic markets because it is easy to establish electronic markets. These electronic markets can duplicate other markets or fill small niches and therefore have limited liquidity. Liquidity mechanisms, however, can be explored for providing continuous liquidity in electronic markets. Regulators should undertake further consideration of what is appropriate. Regulators may also consider whether multiple markets for the same product can result in more opaque rather than transparent prices and

what the appropriate regulatory response to this situation is—requiring best execution; forcing consolidation; approving new liquidity mechanisms, or having competition resolve the matter.

What is your assessment of the efforts by the securities industry, IT industry and regulators in meeting these risks?

Regulators are promoting more consolidation of electronic networks. Some believe, however, that how the market develops should be a process of competition not of regulatory intervention.

What do you see as the major impediments (e.g. consumers' interest, cultural, regulatory, legal, lack of familiarity with foreign market, protectionism, etc.) that limit the provision of cross-border securities services?

The impediments to cross-border activity are not new because of the Internet. They are the same impediments just magnified because access is 24 hours a day and transactions occur more rapidly. Lack of common regulatory definitions creates problems in cross-border activities; for example, "institutional customer" and "sophisticated customer" mean different things in different jurisdictions and therefore providers of services are subject to substantial costs when offering the same services to the same class of customers in different jurisdictions. Also, harmonizing primary market regulation may be a prerequisite to opening access further to secondary markets.

Is there a role for regulators and/or governments to cooperate and facilitate innovation in Internet securities services and provision of cross-border securities services? If yes, what is your expectation?

Yes, on a broad level the Internet forces regulators to re-examine the structure of securities laws as a whole. The regulator should create a safe harbor by charting what can and cannot be done and making requirements as transparent as possible. In particular more thinking should be done about the regulatory interest in specific issues and how those interests relate to oversight and broker oversight markets. If possible non-prescriptive approaches should be used so they can be more flexibly applied and more readily adapted to changes in technology. Common definitions (as sought in Europe) should be a goal so that all jurisdictions have a base-line view of who is a sophisticated investor. Of course, with cultural, legal and developmental differences among markets, this result may be difficult to achieve. In the meantime, it appears that those markets and intermediaries which want the broadest access must comply with the most stringent requirements not the least. The Europeans, Australians, the CFTC and the Canadians are coming up with new means of competing across regulatory borders that should be studied.

Session 4 Minutes: Investor Education

Opening Remarks from the Moderator

Investors are increasingly turning to the Internet for investment information and execution services. The global nature of the Internet means that consumers are able to access the websites of providers in foreign countries where product disclosure and risk warnings are unfamiliar to them. Where investors turn to the Internet to execute trades, they may be doing so without proper advice. Numerous enforcement proceedings have resulted from stock manipulation on Internet chat lines.

These facts evidence the need for more investor education; for example, investors need to be educated on how to conduct and validate research and other information found on the Internet. Investor education is a strong tool to achieve investor protection and mitigate threats posed by the Internet.

The greatest challenges lay in developing content, resources and safeguards to meet the needs of a differentiated audience. Investors accessing services via the Internet may find themselves investing in stocks having had "no culture of investing in equities."

Summary of Panel Presentations

First panelist

The National Association of Investors Corp. ("NIAC") was established in 1951 as a non-profit association, NIAC is a coalition of investment clubs. More than 350,000 count themselves among its US membership. Members, who are distributed across 30,000+ clubs, control \$125 billion in investments with another \$200 million new equity pouring into markets every month.

The organization's aim is to provide increasingly sophisticated education and support for its members. For example, a nationwide volunteer network will deliver over 2,000 seminars and conferences in 2002. It also publishes a magazine, which reaches 400,000 people.

NIAC's program is built around four principles:

- i. Invest regularly
- ii. Discover/own leadership growth companies
- iii. Reinvest capital gains and current income
- iv. Prudently diversify.

The importance of research is emphasized ("We tell them if you can't understand the company or how the company is going to grow, don't invest in it").

NIAC has joined with 21 countries in the World Federation of Investors. Its counterpart organization in Canada is the Canadian Shareowners Association.

The Internet...

- o Challenges

Investors need help to be able to use online resources effectively. Indeed, NIAC has developed a course on how to use the Internet effectively. The course is delivered through regional Chapters.

- o Opportunities

Opportunities include: member communications; access to research (for \$25.00/year members are able to access CompuStat Data from S&P); and distance learning. Traffic to NIAC's website (www.better-investing.org) reached 4 million impressions per month as at November 30, 2002.

- o Observations

Consumers are often ambivalent about pursuing investor education.

< When asked if they'd like to know more about equities and bonds, most will indicate that they would. When asked if they'll devote five hours per week to learn more about investing, most will flatly refuse.

They may also be reluctant to disclose gaps in their personal knowledge.

< When asked if they know the interest rate paid on their savings account, most will answer "yes." When prompted to state the rate, most will admit that they "don't know."

The most difficult challenge for groups concerned with investor education is to motivate individuals to take the time to become educated. Once they realize they should be spending time on investor education, it may be too late.

Second panelist

In Brazil, 15 million people have access to the Internet making it one of the top ten users worldwide and the largest in Latin America. Even so less than 10% of Brazil's population (160 million) is online.

In the financial sector, 75% of Brazil's 215 financial institutions offer Internet services. Among residents with bank accounts (40 million), 3.5 million – or less than 1% -- utilize those services. Why? In all likelihood, investment illiteracy is the cause.

In response, the Brazil Mercantile & Futures ("BM&F") promotes investor education through the Internet. The Distance Learning Centre on the BM&F website (www.bmf.com.br) is a virtual classroom that attracts 225,000 visitors per month and registers 2 million page hits in the same period. Twenty-five per cent of visitors are non-residents of Brazil. The panelist commented that visitors use the site for price discovery and other disclosure.

With respect to content development early considerations were:

- < relevance of the site itself;
- < appropriate level of education (beginner vs. advanced)?
- < relevance of subject matter (golden rules vs. how to rebuff boiler room tactics)?

- o Site Design

The site avoids being too childish or playful while remaining flexible and expandable. Multiple learning solutions are offered – users can “learn by driving.” Remote access is next.

- Target Audience

No one size fits all. There are features for new investors as well as programs for the more sophisticated or professional audiences. For example, online courses are available to employees of financial institutions at their workplace. Learning programs are layered. Additional value has been created by integrating BM&F courses into programs of study for MBA and other university students.

- Subject Matter

BM&F has taken the view that “we offer [investors] the markets and [should] teach them how to profit.” One of its courses is a step-by-step approach illustrating how to use options/futures.

The panelist touched on suitability and other investor protection matters vis-a-vis the Internet. Noting differences in knowledge and sophistication among users, he commented on the benefits of a virtual gatekeeper and suggested that regulators and SROs move to validate investor education content and certify programs or courses. He felt that regulators also have a role to play in monitoring (but not endorsing) chat rooms et al.

Third panelist

The panelist mentioned his prior work and good standing with securities regulators, SROs and industry associations in the US in the field of investor education; for example in the development of www.investingonline.org (for the North America Securities Administrators Association) and www.investorprotection.org (for the Investor Protection Trust). He then highlighted common mistakes that undermine regulators’ efforts to effectively use the Internet to deliver investor education. Solutions were also identified.

- Dusty Brochure Syndrome

Regulators are mistaken to think that popular videos or brochures will reach a wider audience by posting it on the Internet without a promotional strategy or consideration given to reformatting the content to make the most of the medium.

Solution

Re-purpose the content to take advantage of the technology, and adopt a marketing plan to bring the resource to the public’s attention through maximum exposure.

- Lack of Point of Sale Strategy

Solution

Make an effort to reach investors at the point where they are making decisions. For example, online brokerages link to www.onlineinvesting.org – bringing the information and tools to investors when and where they are needed. During the planning and development stages of any web project, consult with the industry to create high and sustained impact at launch and over time.

- Invisibility

For investors beginning their search, regulators must remember that it is critical for their material to be picked-up by popular search engines in the first 1-2 pages of search results. Otherwise it will not come to the attention of most browsers.

Solution

Embed and highlight frequently used search terms within your site. Update these quarterly.

- ‘Plain Wrapper’

Sites designed by regulators often go ‘low-tech/no gloss’ on the assumption that they are not in competition for the investor’s attention. Wrong. Attractive and interactive sites are most frequently used.

Solution

Consider how people approach the web. Incorporate graphically appealing elements that engage and teach.

- Multiple Drill-Downs

You may have great investor education content but it will go untapped if it’s more than two clicks away.

Solution

Break-out your content so it becomes immediately accessible.

Group Discussion and questions

Should investor education requirements for do-it-yourself investors be mandated?

In response, an industry practitioner noted that forcing people to become educated would disenfranchise a whole group of investors.

Is investor education from industry sources inherently a conflict of interest and biased?

Industry practitioners who focus on their clients' broad-spectrum needs and use the commercial relationship to provide education can distinguish themselves. Picking-up on one participant's observation that education delivered at the point-of-sale has the best chance of making an impression, practitioners were exhorted to create a "race to the top" to offer quality education focused on the advisor-client relationship and how those relationships are regulated. The OSC's Fair Dealing Model (found on www.osc.gov.on.ca) was brought to the assembly's attention. A practical application of this approach would be to educate investors about differences in market structure between various regulatory regimes. For example, in Canada investors are clamoring to learn how the NASDAQ works.

A related question drew attention to the efficacy of educational initiatives provided by regulators. Where large investment firms are associated with the wealthy (and not having the interests of the individual investor at heart), securities regulators may be seen as part of a larger bureaucracy that stifles opportunity. In the US con artists take advantage of these sentiments.

Panelists agreed that the disenfranchised were more clearly at risk. This was seen as a reason to redouble educational efforts not only in ways that resonate with the end-user but by engaging the media and other knowledge multipliers. Regarding scams and frauds, www.investingonline.org deals with these as educational content through a 'pump-and-dump' simulation. Creating public awareness about the availability of information on scams and frauds also plays a part in reducing their incidence.

Another thought was to create a system where pop-up windows with 'buyer beware' messages accompanied all investment opportunities offered through the Internet.

Taking this one step further regulators together with consumer groups, might be encouraged to establish guidelines or a validation structure but this would need to be explored in detail. When called into question, it was admitted that the idea was wishful thinking. Caveat emptor is more realistic and conveys that investors carry some of the responsibility for the soundness of their investment decisions.

How can we help investors validate information they get on the Internet?

NIAC tells its members to buy a good magnifying glass and read the small print. Look for warning signs. Check third-party research.

The Consumers Council of Canada recently completed a survey that revealed a real crisis in consumer confidence following the telecom bubble, Enron et al.¹ Even though the Council accepts the notion that consumers shoulder the responsibility for verifying investment information that comes to them via the Internet, third-party validation has real potential to boost confidence. Another commentator observed that ISPs have a vested interest. Public confidence in them will erode where ISPs were found to host websites that have defrauded individual investors. There was disagreement from another participant regarding this view. In his view the real losers are legitimate companies whose reputations are harmed. This is one reason why the industry needs to be involved in raising the bar on investor education on the Internet.

The Consumers Council of Canada also commented that having a better understanding of the certification process practiced by regulators/SROs could help restore confidence. Others agreed. For example, in the US, most FOREX fraud is perpetrated by unlicensed individuals. If investors restrict their dealings to licensees they will reduce their exposure to investment fraud.

Also in that country, the SEC found that lay-people have difficulty understanding rules and regulations as they are presently written. This has resulted in numerous complaints – underscoring the need to apply plain language principles to rulemaking. In its experience, where people are given basic information they will actually read it.

An industry practitioner observed that plain language does not remove the complexity from financial and investment concepts – how many clients will ever understand beta? When clients come through the door they want advice not a 25-page document intended to educate them. Similarly, when consumers take their car to a garage for maintenance, they don't want a course in auto mechanics. There are also situations where more education erodes investor confidence because consumers realize the full extent of what they don't know. More typically, investors resist 'learning' about the risk/reward relationship stressing that they want zero risk and a 25% return.

¹ Another participant countered that educated investors are using the downturn as a buying opportunity. He sees this as a key difference between an educated investor and the less well informed. This is not being reported.

One participant noted that conventional educational methods need to be rethought – especially where the Internet is the delivery medium. Taking people from ‘A’ to ‘Z’ may be the wrong process. We need to examine how people use the web; for example, information needs to be shortened and to the point, topics must be readily accessible from homepage, regulators’ sites should encourage others to link to them, etc (See: Alliance for Investor Education). “Manageable” information that people can master helps build confidence.

Panelists were asked for evidence that educational initiatives resulted in consumers investing more sensibly – particularly where the audience is diffuse.

NIAC

Member clubs file a statement of their investment philosophy. The degree to which a club’s investment portfolio matches its profile is one measure of success. Of clubs sampled by NIAC, most hold investments that are congruent with their profiles. In terms of performance, 51% of clubs beat the S&P 500. This result is three times better than the track record of professional portfolio managers. On the downside, about 2% got caught by Enron. “Investor education is getting some traction or we would be seeing other results.”

Generally

Budgetary and other resource restrictions have meant that little backend analysis has occurred. In the United States, the Securities Investor Protection Corporation is underway with a two year initiative to dispel public misconceptions about investing following which it will evaluate the impact of the campaign. In Brazil, regulators and SROs have focused on identifying opinion leaders and “knowledge multipliers” (e.g. media) and educating these people to report accurately in ways that will help educate consumers. This prompted the observation that many advisers are as equally uninformed as their clients (viz basic concepts as well as more esoteric products such as derivatives).

Session 5 Minutes: Enforcement Issues

Summary of panel presentations

First panelist

This panelist provided an overview of some of the challenges that his firm faces in dealing with law enforcement in an Internet-related investigation. He commented on the obligations of ISPs to law enforcement agencies and the need to work together. In light of increased activity, there has been an increase in the number of requests by law enforcement agencies and it is equally important that law enforcement and regulatory agencies work together as well. One of the significant concerns ISPs have is the need to maintain client confidentiality and privacy policies. He then addressed some of the questions in the Enforcement questionnaire and how his firm has dealt with these issues (see responses in section below).

Second panelist

This panelist provided an overview of his self-regulatory organization and some of the cases the organization has seen recently. In light of the fact that the organization is a self-regulatory organization for securities dealers only, many internet-related schemes may fall outside their jurisdiction and are referred to the appropriate agency (e.g. SEC). Many of the recent cases involve pre-IPO (initial public offering) schemes that solicit investors to buy shares before the company goes public. Other violations include trade reporting violations, non-disclosure to clients and advertising rules.

Third panelist

This panelist reviewed the main types of ISPs and the services they provide. He then went on to discuss the types of information that law enforcement request from ISPs and what ISP firms want from law enforcement agencies. He added that ISPs are most likely to be supportive and cooperative in spam investigations. Many terrorist investigations and criminal cases have been solved using hot.mail and e-mail account activity.

He raised concerns about the different standards for retention of data in different countries. For example, in Europe, there is a requirement to dispense of personally identifiable information as soon as it is no longer needed for business purposes. On the other hand, requiring mandatory retention of data will create massive databases of private information and excessive costs to ISPs.

Group discussion

An industry participant raised questions about the lack of regulatory requirements in Canada in this area, especially data retention. ISPs are concerned about civil liability especially in light of current privacy laws. Vague regulations with no defined periods will not provide the guidance required by ISPs. There needs to be

significant cooperation between ISPs, law enforcement and securities regulators to discuss exactly what is needed by enforcement agencies. He commented that education and cooperation is essential.

In the U.S., data retention by ISPs is not a requirement. However when law enforcement needs this information, they are able to ask the ISP to preserve it under the Electronic Communications Privacy Act (ECPA). Typically, the information is preserved for 90 days. However, law enforcement needs to be very specific in their request for information. The comment was made that this has worked well so far.

In response to a question relating to spam, it was estimated that 30-40% of e-mail is spam. It was added that only a very small percentage is securities fraud related.

Turning to the costs relating to storing and managing requests from law enforcement agencies, the most significant cost is compliance staff. This can range from 5-8 employees to a maximum of 20 employees in the largest ISP firms. Storage of data is very expensive especially if the ISP must keep the data for six years. An industry participant added that the industry is relatively new and the current equipment does not have data retention capabilities. This would be a huge cost for firms, and most firms (approximately 80%) are small operations with less than 20 employees.

In reply to a question relating to an appropriate time period for keeping records, it was noted that the U.S. regulators require e-mails to be maintained in readily accessible form for three years. These standards also apply to telephone records.

With respect to the concerns about privacy legislation and the ISP's contractual obligation to clients, some firms post their privacy policy on their websites. Clients must agree to this as a condition of service. However, there are "carve out" provisions that allow the information to be provided where it is required by law, and allow for non-identifiable information to be provided to vendors.

In response to the question whether the ISPs can take any action against securities fraud, a participant commented that ISPs do not get involved in what is discussed in chat rooms. However an important step towards enforcement would be to ensure that securities fraud and criminal laws apply to the Internet world and not just the paper world.

The group then discussed whether this is an area that securities regulators should push for international standards and regulation of this industry. There were concerns raised that the ISP is merely a conduit to the Internet. Strict regulations would drive the costs of business very high and create barriers to entry. Others added that law enforcement in this area includes child pornography, terrorism and securities fraud. Therefore, the primary focus will be on criminal activities and securities fraud is seen as a lesser concern. Finally, it was noted that more emphasis should be added on consumer education, as this would be a better approach to pursue.

In response to a question about how compliance reviews have changed, a participant commented that there has been an increased focus on monitoring of the Internet and the retention of e-mail and electronic records.

A question was raised about whether there is any regulation of discussion group operators. Typically these firms have very thin operations and content is not edited. It is very difficult to regulate content providers, as they will go to another country if they do not like the regulatory requirements of a particular country.

Finally, the discussion turned to whether there was a need to regulate in this area. It is a problem, especially in the areas of thinly traded securities and promoters in chat rooms and message boards. Others noted that the SEC statistics seem to indicate that Internet offences have increased exponentially. On another note, an industry participant added that these issues have been discussed by ISPs for years and it must be remembered that a number of good things are happening in chat rooms. Although regulation is the easy solution, investor education is important.

Questions

What kinds of traffic and subscriber data do ISPs retain?

Although this will vary with ISP, the ISP will typically maintain: session logs, which include the IP address; user ID; and the length of time online. This will also depend on the service provided. For example, caller ID can be maintained with dial-up phone service but is not possible with cable service. Typically, e-mail will be maintained on the server for 30 days. ISPs do not follow where subscribers go on the Internet.

Do ISPs verify the identities of their subscribers and, if so, how?

ISPs do some verification when client signs up for service but this is limited to what the clients tell the firm. For example, credit checks will be performed if a credit card is provided. Although an ISP can identify the subscriber, it is not always possible to identify who is using the PC if s/he passed the security test.

How long do ISPs typically retain traffic, subscriber and account information?

E-mails are maintained on the server for 30 days. Customer billing and accounting records are kept for 7 years and session logs are kept indefinitely. Session log information is most useful to law enforcement investigations.

Are there any industry codes related to retaining certain types of information that would assist securities regulators when seeking such information?

The Authority to Share Records Retained by ISPs

Can ISPs voluntarily cooperate with law enforcement authorities by providing information?

There are a number of rules in the U.S. relating to what can be provided to law enforcement. There is a real concern about privacy policies; ECPA sets out the legal process that law enforcement must follow before a firm provides this information. The three levels of due process range from a subpoena (to get name, address, manner of billing, service provided) to search warrant (to get session logs) to a Title III order. A Title III order provides the most powers however it is difficult to get. For example, to get e-mail that is less than 180 days, a search warrant is normally required. If more than 180 days, a subpoena is required however law enforcement must notify the customer.

What kinds of information can be provided to securities regulators on a voluntary basis?

Generally will not provide individually identifiable information without legal process. However, ISPs can help in other areas such as training to law enforcement and providing useful advice on evidence gathering.

What kinds of information do ISPs provide private third parties (such as vendors, customers, etc.) and under what conditions?

Generally, the ISP will not provide individually identifiable information about customers except to vendors in certain circumstances and in accordance with contractual terms and conditions. Non-disclosure agreements with other providers state that information must be kept confidential.

Should regulators issue guidelines to ISPs regarding the establishment of baseline standards for retention of information (subscriber, traffic, content) and timelines for that preservation?

Currently, Canada and the U.S. do not have data retention requirements for ISPs. Concerns were raised about the need for clear guidance, as vague regulations would cause ISPs to "keep everything". Other concerns raised were the enormous costs to store large amounts of data and the need to replace equipment as current equipment does not have this capability.

How do firms establish a realistic balance between the length of preservation time and storage of records, particularly where there is a high volume of traffic?

Surveillance.

Are there any measures that securities authorities can take to assist ISPs in deterring securities fraud?

Firstly, authorities should know what to ask for. The more information provided, the better able the ISP will be able to respond to the request. Secondly, there must be inter-agency cooperation so that each agency knows who is investigating what. This should also include a centralized reporting framework to ensure that there is communication with all agencies involved. Finally, there should be criminal laws to fight spam. Civil enforcement is not adequate. The industry cannot fight this alone; the securities industry needs to work with law enforcement to establish anti-spam laws with civil and criminal penalties.

Other comments include that the ISP industry should not have mandated requirements, but should work with law enforcement to decide what data should be kept. Otherwise, this will require ISPs to have massive storage database about subscribers.

Meeting Minutes of the IOSCO Internet Project Team's European Roundtable Meeting, Amsterdam, March 3-4, 2003

Session 1 Minutes: Research and Industry Trends

First panelist

This panelist described the role of technology in enhancing internet trading, in terms of turning data into information, orders and transactions. This is because the internet adds transparency to each element of the value chain, from the data to the execution of the transaction: most data is free and is easier to access to external reports; investors can check their position more frequently; security lending and margin trading is facilitated; operational costs and commissions continue to fall; self - service trading is more and more convenient; post trading service has improved throughout online access. Information technology provides the private investors via the internet with tools previously solely used by the professional investor. The volume of data available has increased exponentially, and it is necessary to develop new methods for looking at it. So the panelist argued that, for the investment firms, this is the key to differentiate their service.

The second point touched by the panelist relates to the use of technology in building up a pan-European capital market, developing a (as yet unavailable) system of comparable financial information on all listed companies across Europe. IBM is working to create such a system, aimed at harmonizing national information sources and offering comparable accounting information based on IAS.

The panelist then discussed the level of security in online financial services: technology offers a variety of solutions, such as digital certificates, tokens, smart cards and biometrics readings more advanced than the existing levels, based only on PIN, password and personal data.

Finally, new technologies are emerging enabling things like online language translation, instantaneous settlement and intelligent agents for liquidity aggregation.

Second panelist

This panelist (representing a major French internet-broker) described the new technology that will become a strategic subject for the coming years: the BANDWIDTH, based on fiber networks, in which information and speed are allied.

In the past years the WAP technology was not a success, because screens were small and it didn't allow fast operation. The arrival of the new mobile phones generation (multimedia) and of GPRS and 3G represents one of the key developments for the future.

Another factor that will enhance cross border trading will be the use of the ISIN code: a company will be represented by a security code, the same in every exchange all around Europe.

Third panelist

This panelist (representing an Italian bank) described the Italian scenario from the point of view of a local online broker. The growth of online finance in Italy has leveraged on the infrastructure, with a widespread PC adoption and a very high number of mobile phone users. Other key success drivers have been the market conditions in year 2000 and the competitive pricing structure. Banca Fineco is a domestic player. Cross border activity is not developed because of the differences still existing in Europe in terms of languages and cultures, legislative and fiscal systems and clearing methods.

Fourth Panelist

This panelist described the activity carried out by the largest market specialist in Germany. This specialist, that operates with institutional traders, banks and discount brokers, runs 40.000 different order books and can guarantee to the retail client (operating through a professional) the best price, made with reference to the Xetra price. Competition between markets is regarded as a positive factor, and it is foreseeable that in Germany only three markets will survive. The panelist discussed three major factors responsible for having created a level playing field for retail and professional investors:

- o the retail investor can have access to the same information available for the institutional investor, due to the information technology;
- o the private investor is able to sell his shares within seconds, while institutional investors don't have the possibility to execute a trade immediately with a click;

- for the retail investor the cost of execution has been reduced dramatically, while the institutional investor pays a percentage (expressed in terms of basis points) of the transaction's value.

Due to the reduction of revenues, banks and brokers are trying to internalize the transactions, in order to reduce settlement and clearing costs that represent a great percentage of the transaction costs, up to 85% of the total costs. So the panelist argued that technology should be used to reduce the costs of settlement and clearing.

Discussion

The group discussion considered the advantages of competition between markets, which brings efficiency and gives to the private investors the opportunity to choose where to route their orders. Comments were made that regulators should help to improve the transparency of information but let the market do its work in growing competition. It was also noted that common standards may be required to facilitate the dissemination of information and the cross - border trading.

Questions

What new Internet-related developments with respect to securities trading have you identified as relevant to your business through the use of financial research and statistical data?

No one identified any particular third party research or statistical data that has been used. Some parties are doing their own research through consultation and observation of new activities of other parties.

How may technology be used in the future for securities trading purposes?

Technology will be used to provide access to information, linkage of information to analysis and transaction execution, and linkage of customers. There will be new types of transaction market such as markets for margin.

What is the prospect of Internet-only securities trading provider, and how does this translate to the entity motivation to access multiple jurisdictions to reap the benefits of scale and scope?

This topic was not discussed as such, even if the business model presented during the session was described as click and mortar environment, combining pervasive computing with traditional customer coverage.

Do you expect significant growth in cross border securities trading services in the next three years?

There are still significant differences between countries, that represent obstacles to the growth of cross border trading.

Which areas in securities trading services that leverage the Internet are likely to see higher cross-border growth? Are the patterns of growth different for the B2C and the B2B segments?

Institutional traders are more likely to use dedicated networks while retail customers are more likely to use the Internet.

What are the key critical success factors or pre-conditions for securities trading services using the Internet (E.G. high Internet penetration rate, regulatory regime providing for certainty or clarity, suitability of the services)? What type of services will grow in the future?

Discussion from participants identified the need for infrastructure available at a reasonable cost. One participant suggested there is a need for a global approach to settlement, custody, service levels and data integrity. There were suggestions that there is a need for standardization and international best practices. It would be useful to have a global agreement on what are the important protocol issues from a processing perspective.

Session 2 Minutes: Emerging Risk Profile

Summary of panel presentations

The moderator opened the session with an introduction to the speakers. He highlighted that a major issue of the Emerging Risk Profile is outsourcing of specific services.

First panellist

The first panellist (representing a major bank in Portugal) stated that trading via the Internet is not more risky than trading through other channels. He claimed that rather the contrary is the case due to less human

intervention, which reduces the risks of human errors; more control, since everything is based on Straight Through Processes (STP); and automated procedure, i.e. automatically coverage of open positions or decisions on settlement risks. STP is very controlling with regard to in-house frauds, which cause more damages than external frauds; IT-bugs (the panellist admitted that a 100 % security does not exist but the chance of detection would be higher); Interface breakdowns, while reconciliation of information is a problem; and clusters/redundancy.

One of the inherent risks is a product of one of the advantages of the Internet: information and trading are carried on in real time, which allows less or no time for the correction of mistakes. For that reason the operator of such a system has to make sure that it works properly.

As regards STP-risks and responsibilities for an operator, there is a need for software with different levels of edition and authorisation. Furthermore, it must be assured that the participants can rely on real-time automated information (quotes). A third party information control is therefore necessary - which is difficult to check, if the information is supposed to be delivered in real-time to the customer. A constant research has to be done to monitor existing and occurring risks and needs. Of great importance is also the awareness of the "Know your customer"-demands. And finally, the price of the information has to be taken into account.

The panellist closed his presentation with the résumé that with the use of the Internet business models have changed and information has a new role. Important for online-customers, who are in particular very demanding, is speed, easy access and cost. Trading is one of the activities where the Internet makes a difference: new investors are attracted (i.e. senior citizens) and new patterns of trading have been established (fast, direct and/or heavy trading).

Second panellist

The second panellist (representing an international law firm) gave an overview about the regulatory issues arising from outsourcing. He started with the requirement to have an accurate organisational structure as it is laid down in the EC-Investment Service Directive (ISD) and in many national rules. This issue is generally not purely Internet-related but the use of the Internet constitutes a specific scenario due to the delocalisation and the unrestrainable number of clients.

He went on with a description of the legal situation in Spain and the United Kingdom and the relevant insufficiencies. In Spain investment firms are subject to specific regulation to cover security, confidentiality, liability and capacity in order to combat money laundering and monitor the compliance with the rules of conduct. In the UK high level principles for all FSA-regulated firms are in place; banks have to obey special regulations for the outsourcing of material functions (i.e. the contract must be produced to the FSA); further regulation is currently drafted ('Integrated Prudential Sourcebook').

The main problem occurs if the 'insourcing' companies are not financial service providers and as such not subject to securities supervision. This leads to limitations on areas which can, or respectively cannot, be outsourced since the responsibility for business activities shall not be given away with their outsourcing. Additionally, it is essential to establish appropriate control mechanisms.

It might be recommendable to establish **standards for the outsourcing** of business activities. Besides the general question, if such standards are suitable or not, the following issues have to be taken into account:

- Insourcer's level of understanding of the business,
- Guarantee of Confidentiality (external and internal),
- Training of staff,
- Flexibility towards changing market conditions,
- Ability to change to another insourcer,
- Contractual terms and conditions,
- Continuity.

The panellist proposed also to establish **standards on Audit and IT Security**. Different levels of security are possible, which depends on the nature of the information processed. He proposes the appointment of a compliance officer for IT Security and an audit of the system at least every two years. Such standards would lead to the practical implications that although they are only applicable to personal information, particularly in Spain, the securities measures would be implemented for all processed information. They would also apply not only to controllers but also to processors.

With regard to the supervision of outsourcing the responsibility for the relevant activity stays with the investment services providers. They must have an organisational structure, with a level of responsibility on top level (Board of Directors or CEO). The responsibility of the regulator may include a direct access to the insourcer relating to the outsourced business parts, an ad-hoc regulation in place, the certification of standards and an adequate treatment for extraterritoriality.

The panellist ended his speech with the remark that in Spain the lack of the relevant regulation has had a visible effect because an 'outsourcing-culture', in the sense that the investment firms are aware of their responsibility for the outsourced activity, has not been created. He also high-lighted the problem of confidentiality when insourcers deliver the same services to several investment firms which are competing in the financial market.

Third panellist

The third panellist (a risk management consultant of an international accountancy/consulting firm) gave a presentation about Online-Security and Privacy and pointed out the critical online risks: unauthorised trading, reliance on incorrect financial information, online fraud, unavailability/trading chain dependencies, privacy breaches and disputed trades.

Generic requirements are the identification and authentication of information, persons and systems, the authorisation, data integrity, confidentiality (company and privacy sensitive), non-repudiation and the possibility to control and audit these obligations. These issues were addressed in several sets of regulations, i.e. EC-directives and national legislation.

The panellist emphasized the need for a business oriented approach to regulation. Risk and security management should be top down.

Specific security areas are authentication, encryption and electronic signatures. Means for authentication are – with different security levels – tokens (smart cards etc.), ID/password, encryption between two entities and digital certificates. Electronic signatures have a high security standard since they require a face-to-face registration and a certificate validation. It would be important for the market to provide a cross-recognition for electronic signatures, but remarkably over 50% of the relevant entities have not even thought about such a Public Key Infrastructure of electronic signatures. Only 10 % have fully implemented it.

Discussion

An industry representative indicated that outsourcing was an easier alternative than joint ventures. The Approved Person Regime in the UK was strict and good; there were clear rules for the accountability, i.e. for outsourcing of risk assessment functions the specific risk management is monitored.

One participant stated that it would be difficult to establish common standards since there are – even on European level - many differences in languages, definitions and in particular cultures. It was added that specifically small companies could for financial reasons not easily comply with strict obligations asking for complex organisational structures. The reply was given that due to the cost factor especially small companies were tempted to outsource material functions. Regulators and clients should therefore be more worried about the way risk management and data protection were handled in such cases.

The opinion was confirmed that the establishment of standards for technical systems would not be practicable because it was not possible to identify a single system as the best solution for all purposes. On the contrary, such standards would rather be to the detriment of further development of new and better systems. Technical standards might also lead to a breakdown of the market since smaller entities might not be able to afford a necessary technical conversion to comply with these standards.

An useful approach for outsourcing would be a Service Level Agreement in the contract between out- and insourcer where all conditions are laid down, including the transfer of know-how and skills. From the point of the industry it could be seen as sufficiently supervised if the regulators had access to examine such arrangements.

As regards computer security, the statement was made that this would not be a question of technology but of economics. The main issue was that the investment firms would be trying to dump the risk on their customers in their terms and conditions and therefore had no interest in fixing mal-functioning parts of their web-sites.

With regard to the reliance on electronic information, it was emphasised that besides the issue of security of published information the customer has equally to bear responsibility: sophisticated online-customers would look for certificates on websites and for information about the responsible persons or entities. The customers should be educated that the Internet can be secure but they need to undertake own efforts to get the respective assurance. It was admitted that there were firms whose standards of data-protection were inadequate, but that generally speaking from the industry's point of view this was not the main problem. One participant added that the goal should be to make it as easy as possible for the customers to make good investments.

Serious problems could be created by spoof e-mails and the fraudulent copying of websites of legitimate investment firms, which happened very often. To combat such actions the managers of an attacked company would have to find a reasonable balance between the potential risk, the likely benefits of a successful fraud and the costs of essential counteractive measures.

Session 3 Minutes: Investor Education

First panelist

The first panelist represented a major Italian online broker. Currently trading online in Italy represents by far the most important channel: in 2001 the online segment represented 70% of the trades (against 29% in 2000). In the beginning of 2000 there were 351.000 online accounts, at the end of 2001 there were 1.549.000. There are two main profiles of the online investor :

- 1) customers with a low portfolio (less than 20 trades a year). This group (the majority) does not only want a trading possibility but a larger range of investing possibilities and information. They need to be educated, informed and advised via a variety of channels, e.g. they also want the possibility to speak directly with an advisor.
- 2) customers with a high portfolio turnover (in 2001 4% of the Italian online investors) with more than 7 trades per month. This group is autonomous and self-confident; it only needs quotes, trading access (speed, performance, dedicated platforms).

The firm of the panelist has several solutions for the needs of the mass affluent customers: advanced technologies; multi channel services; decision support tools for financial advisors; management and reporting tools for financial advisors and customers. The video conference advisor is a key application for the future. In general one of the main goals of this broker is in this respect to give the customer the maximum level of information on the website in order to prevent them from having to leave the site to look elsewhere for the information they need.

More than half of the customers consider their financial experience as just sufficient or even less: they need information, education and advice, one-to-one if possible. However, they prefer trading via the internet, which will remain the main channel. The winning strategy consists in combining an efficient internet channel for trading online and direct access to personal financial advisors. The firm of this panelist can now offer low cost consulting services via web and telephone (asset allocation, risk return analysis, a "trading recommendation centre" both through the platform and the advisors, advice on real estate, retirement etc).

Second panelist

The second panelist represented a non-profit organisation for investor education, which was set up in may 1997 by a major European exchange. The purpose of this organisation, which today has trained 40,000 'pupils', is to introduce the stock market to the general public. The institution has several programs: from introduction level to derivatives, technical and financial analysis. In general there are three categories of investors: the individual shareholders, participants to shareholder clubs and employee shareholders. Important success factors for investor education are:

- Objectivity (no product to sell)
 - Adapted to 'new' investors: basic rules and simple tools which enable them to make their own decisions.

The characteristics of the new investor are: young, from a large range of socio professional categories, and with little or no initial training in economic and finances. To become aware of the quality of research sources, there is a need for basic education (market rules, accountancy).

Due to the internet, the retail investor has access to a large range of information and a large number of sophisticated tools. However, the retail investor is not educated enough to understand and to appropriate all the information.

The panelist concluded by stating that investment education must be controlled, supervised and labelled.

Third panelist

The third panelist argued that the approach which financial regulators should take is simple: abstain from giving guidelines about what is right or wrong when it comes to issues relating to the predictability of financial markets and research relating to what makes up a good security. What is important is the relation between risk and return; in this area there is a role for regulators. Most of the financial scandals and problems that have occurred, on the Internet or otherwise, can all be related to the fact that investors did not understand the risks (financial or other) involved or the information they got was biased. The main objective

for regulators with respect to Investor Education is in the view of the second panelist: *assure that private investors are aware of the risks (of all kinds) involved*. Regulators should continuously ask themselves whether the risks are obvious for investors and whether all parties do offer insight in the risks involved, regardless, whether we deal with the Internet or other sources of information. If not, regulators should act immediately.

One of the basic concepts in finance is the diversification principle, which Markowitz showed in 1952. In the opinion of the panelist any financial institution should at least INFORM investors of this principle and regulators should take appropriate action if financial institutions develop products that do not use this principle (like for instance many financial products that use financial leverage). The second objective for regulators is: *assure that financial institutions measure risk tolerance of their clients in a proper way*.

The panelist is sceptical when it comes to regulating Information and Investor Education. In this respect he does not see any new problems that didn't already exist with other media. He is more positive about the advantages that internet has over the other media. In his opinion the focus of regulators should lie in forcing parties involved to inform investors about risks involved and in assuring that financial institutions pay more attention to adequately measuring risk tolerance of their investors.

Fourth panelist

The fourth panelist (representing an online broker) stated that the current online investor is 1) educated and self-confident; 2) wants to invest by himself and is able to do so 3) but wants the same tools as the 'advised' customer and the professional investor. The panelist discerned two categories of market players:

- *advisory only*, a diversified and scattered group with, in principle, no knowledge of client's portfolio and which is in most situations non regulated. In his opinion every advice should be accompanied by an explicit warning that the advice is a generic advice and that it may or may not be in the best interest of the investor to follow up the advice. Also the method employed, the type of risks involved and the investment horizon must be made clear. The preference of the panelist is that market players should give up generic advice.
- *advisory plus execution*. This group has, in principle, a good knowledge of client's profile and portfolio, and is closely regulated.

The opinion of the panelist on research is that banks/brokers must report conflicting interests and should publish an historical overview of their recommendations. Concerning risk market players should concentrate on risk instead of return.

The opinion of the panelist's firm is that there should be a "financial driving licence". This licence should at minimum include: a well thought-out risk profile, investment objectives and investment experience. This "driving licence" should be compulsory, with ground rules laid out by the authorities, and maintained by a periodic re-examination in close co-operation with the industry. At this moment the firm of the panelist gives 'road service' in different levels:

- level 1: no service (access without any support; unfiltered external information; orders are only checked against 'available balance' and clients takes full responsibility (within the law).
- Level 2: service on request (more support, orders are checked against risk profile; certain instruments can be blocked (only if the customer desires) and unfiltered (but with the firm's approved) external information
- Level 3: continuous service (before ordering a client can ask the computer for instructions or explanation; some orders/products are blocked; filtered external information).

Group discussion

The main themes of the group discussion were as follows:

Is investor education a task for the industry or for the regulator?

It was agreed that the industry has an important role in training/education, but the educational activities of the industry usually have a commercial background. For this reason investor education from non-commercial organisations should be preferable to organisations with a clear commercial interest. The fourth panelist, who strongly advocated the "financial driver license", had a clear preference for a major role of the regulator in case of exams for such a licence. In general there was a consensus for a kind of regulation/supervision of investor education activities.

On investment advice: some participants made a clear statement that an investment advice should always be accompanied by disclosure of the interests of the firm/advisor in the specific chair. One panelist stated that rules on Chinese walls alone are not sufficient. Further disclosure is therefore needed.

The role of financial portals in investor education (positioned between broker and customer): one panelist made a clear statement that financial portals should not give investment advice because they do not know the specific customer, his portfolio and the risk involved.

One intervention was made by a panelist of the session on enforcement. He stated 1) that a risk indicator is difficult to implement because there are several 'lumps' of money with different attitudes of risk ;2) there are several internet scams: The regulators seem to do nothing to prevent this practices.

Session 4 Minutes: Cross-Border Issues

First panelist

The panelist, representing a major international bank based in the Netherlands, draws the regulatory landscape of the EU where the mutual recognition principle serves as a cornerstone of the Internal Market. The mutual recognition principle is built on and requires a certain level of harmonization of rules as well as mutual trust among regulators. He finds that in general it works well. However, there are still some gaps to close by a higher level of harmonization (e.g. conduct of business rules) and increased trust among regulators. According to the panelist the EU Legislation is making excellent progress with the proposed new Investment Services Directive and the Prospectus Directive which promote clear country of origin control respectively mutual recognition as well as harmonisation of conduct of business rules.

Nevertheless, some difficulties have to be overcome to make it work really well in practice. These difficulties include the implementation of the regulations in the member states, language barriers, dispute settlement mechanisms and the cooperation between regulators. The protection of national markets and national interests are forces that still hinder the common market. The application of local business conduct and consumer protection rules have often been used in this sense. However, the panelist acknowledges the impressive progress achieved by the Committee of European Securities Commissions (CESR) regarding the close cooperation of national regulators and the establishment of sound procedures for joint interpretations and consultation.

The panelist concludes that while in the EU the Financial Services Action Plan and the E-Commerce Directive contribute to the ability to deliver online cross border services he would welcome IOSCO to promote the mutual recognition principle and trust among regulators globally.

Second Panelist

In general, the panelist (representing a major international bank, based in Switzerland) sees a lot of barriers and road-blocks at the border for cross border financial services. He presents a comparison of the regulatory approaches in the US and in the EU regarding cross border financial services, especially online financial services.

The US approach appears to be highly restrictive and complicated as any offering of financial services into the US triggers licensing requirements. Already access to a website containing financial market information or quotes is deemed to constitute "solicitation" and a US offering and thus triggers licensing requirements. Exemptions from licensing requirements appear to be very limited and narrow. According to the panelist, the US approach constitutes a huge risk for any investment services provider offering online services.

In the EU, licensing issues for EU-firms are generally resolved either by the application of the Banking or Investment Services Directive Passport. Nevertheless, for non-EU financial services firms the situation seems to be quite restrictive too, but according to the panelist's opinion the approach adopted by the EU member states in general provides more flexibility.

The panelist then compares the situation of a non-EU services firm in the main EU-countries. He thinks that the absence of an international passport system or similar reciprocity procedures unduly restricts the development of internet services in the financial market. He also points at possible restraints for multi-channel customer services due to current licensing issues.

Third panelist

The panelist (from the European Commission) presents the strategy of the European Commission (EC) to create the environment for an EU-wide internal market in financial services including online cross border business.

The approach adopted by the EC is based on two pillars: a high level of harmonization and mutual recognition. While these pillars have previously been seen as antagonists nowadays they are tightly tied together and complementary.

The provision of cross border securities services in the EU is governed mainly by three EU-directives: the E-Commerce Directive, the Distance Marketing Directive and the Investment Services Directive (ISD). While the E-Commerce Directive fundamentally endorses the country of origin principle some derogations had to be conceded, e.g. regarding consumer contracts.

However, these derogations bear the danger of being abused for protectionist measures. The Distance Marketing Directive – not online-business specific – is not based on the same philosophy of country of origin / home country control principle as the E-Commerce Directive but it aims at a maximum harmonization of standards. The Investment Services Directive – currently in the process of being revised – puts a strong emphasis on investor protection and investor confidence.

The ISD endorses both the home country control principle, the principle of mutual recognition as the principle of a high level of harmonization. Regarding its implementation and application, the Committee of European Securities Regulators (CESR) has a key role for as much harmonization as possible among the EU-Member states.

Nevertheless, even after the implementation of the revised ISD there still remains the issue of consumer contracts that continue to be governed by the law of the consumer's country. Therefore the EU started the process to review this concept as well. Concerning alternative dispute resolution mechanisms for cross border financial business the EU established FIN-NET two years ago in order to boost investor confidence. FIN-NET is based on existing ombudsman-schemes in every member-state.

Fourth panelist

The panelist (representing an international data provider/news service) emphasises the importance of cross border services for multinational or global financial services providers. Unfortunately, in many countries a lot of barriers are unnecessarily blocking cross border online financial services.

Nevertheless, the panelist sees quite a few encouraging signs for the cross border trade in financial services. He considers the EU to be an outstanding pioneer by enacting the E-Commerce Directive and promoting the mutual recognition principle / country of origin principle also for financial services. This is based on equivalent regulation in the member-states. However, all too often regulators seem to look for identical rather than equivalent regulation.

Regarding the possible creation of a transatlantic securities market, the panelists explicitly mentions EC-Commissioner Frits Bolkestein's speech of February 24, 2003, in which he calls for mutual recognition between the EU and the US based on equivalent – but not identical- regulation. In the same context, reference is made to the report by Benn Steil in cooperation with ISMA ("Building a Transatlantic Securities Market").

Another encouraging sign for a more realistic and favourable approach towards the cross border trade in financial services is the Australian Securities & Investment Commission's (ASIC) papers on cross border business and its goal to avoid an unnecessary duplication of regulatory regimes on wholesale services. ASIC's approach builds on mutual recognition in the case of equivalent regulation.

Group Discussion

For the EU it is of very great importance to build a common market for financial services in order to foster economical growth. To achieve this, regulation has to be harmonized in all the member states. However, the problem the EU has been confronted with is that if the EU-Regulation is not sufficiently detailed the national implementation rules in the member states tend to get too divergent. The EU had to issue interpretive guidelines in order to solve some of the problems which arose from this unwanted divergence. According to the so-called Lamfalussy-Procedures the detailed guidelines are developed by groups of senior experts from the national regulators. These procedures also include a robust a transparent consultation process. However, these consultation procedures in general lead to even more detailed guidelines than initially proposed. On the other hand, market participants complain about too detailed rules. Industry representatives welcomed the adopted procedures.

Nevertheless, under the current regulation even within the EU the cross border trade in financial services is still rather burdensome as e.g. local conduct of business rules have to be respected which can significantly differ from country to country. In addition, the issue of the applicable law governing the contracts as well as the issue of the competent court remain unsolved. Therefore, industry participants pointed out that any harmonization in these areas, especially in the area of conduct of business rules as proposed in the revised ISD, would make cross border business easier.

The promotion of the mutual recognition principle based on mutual recognition of equivalent regulation is welcomed as a very encouraging development the financial industry. Therefore many participants praise ASIC's approach even if it currently applies to the wholesale business only. While industry representatives welcome the initiatives to open markets for financial services between the EU and the US, they expressed their opinion that the EU should not only focus its attempts on the huge but most restrictive and complicated US market but rather look to other significant and less restrictive markets. Regarding the issue of equivalence of regulations, industry participants point out that too often authorities require a similar regulation rather than an equivalent one, an approach that is hardly considered realistic. Therefore they

would appreciate IOSCO to strongly promote the mutual recognition principle ideally based on a an approach taking into account several levels of regulatory equivalence.

Session 5 Minutes: Enforcement Issues

Summary of panel presentations

During his introduction, the moderator reminded the audience that the regulators obtained only a few criminal convictions in cases of market manipulation and insider dealing, mainly due to the difficulties of obtaining evidence that met the standard of proof beyond reasonable doubt.

He also stated that there is a real public interest in combatting such wrong-doing, and this could therefore justify the intrusion into an individual's private life in order to get relevant and important evidence. It is the responsibility of the regulators to consider whether there are alternative sources for obtaining the information that is needed. Regulators, therefore, need to make a realistic judgement regarding the type and amount of data ISPs should be asked to retain, and the length of time for such retention. Regulators must determine what data would be convenient to have, and what data is really necessary for the prevention, detection or prosecution of criminal offences. Regulators are too often guilty of undertaking very wide fishing expeditions, and in the area of the Internet have to be extremely careful that such an approach might dredge up a lot of personal data.

The moderator explained how hard it is to have an idea on the size of the problem securities regulators are facing on the Internet, even with the existence of international surfdays or pilot programs to gather data and statistics on the issue. Therefore, it seems very hard to analyse the costs and benefits, both financial and in terms of private rights versus common interests.

Finally, he explained that most regulators lack knowledge of the type of data created when someone goes on the Internet, and invited the industry participants and the panellists to provide some information on this specific topic.

First panellist

The first panellist (a consultant internet expert representing an international ISP) gave the view of an ISP on the questions raised in the Status Update document.

After a brief overview on the information ISPs have about their customers and on the various type of communication data they retain, he insisted that ISPs are more and more concerned about the confidentiality they owe to their customers. Complying with current EU directives, they only retain communication data as long as it is needed for business purposes, which means one to three months. They are willing to help regulators and to provide information, as long as the requests comply with data protection regulation.

Regarding surveillance, he explained that access to content is interception, and therefore can only be authorized in very few and specific cases. As far as real-time access to traffic data is concerned, it will be extremely expensive and therefore unlikely to be proportionate.

Finally, the panellist stated that other authorities have already considered such issues, and that securities regulators should work closely with these authorities. He also reminded people that, since such technical data is easily forgeable, regulators will only obtain 'intelligence', not 'evidence'. This means that the regulators must know exactly what they can request from ISPs and, more important, what it means: therefore he insisted on the need for regulators to invest in training.

Second panellist

The second panellist (representing a major international financial internet site (market leader in Spain)) gave a presentation on the cooperation between his company and the various national securities regulators where his financial information website is available.

From the experience of this portal, of the many services provided - contents, services, personalization, e-commerce and community - only the last of these poses a conflicting issue with the regulator because of the possibility of circulation of confidential information, insider trading etc. on message boards.

Like ISPs, the information they have about their clients is often inaccurate, since they have no obligation nor possibility to perform verification, except for billing account information when a payable service is concerned. They also cooperate with securities regulators, providing traffic data and account information, as long as they received formal request to do so.

However he reminded delegates that such financial websites are not regulated by securities regulators, and only have to comply with media related laws, even if they are a new type of medium. Therefore, they sometimes have to set up their own code of conduct, like for instance for message boards, which are currently unregulated. He also stated there is a request for regulation on these very specific aspects of their activities, which are not covered by current legislation.

However, he reminded that regulation has to be compatible with

- Data protection issues
- Respect for freedom of speech
- Respect for the obligations of ISPs and portals towards the users
- Penalties must have a sense of proportionality
- The cost of measures for ISPs and portal must be taken into consideration

Group Discussion

The discussion started with the presentation by the first panellist of an example of spam email he created, in order to illustrate how difficult it was to track a fraudster. His email, sent to a UK resident, was promoting a US OTC stock, allegedly on the verge of skyrocketing. Two hypertext links were available, pointing to websites with addresses counterfeiting the names of famous UK banking firms.

The representative from the ISP which was supposed to be providing the email address of the sender, explained that, if formally requested, they would have been able to indicate if the sender account was valid or not. If the sender account was a valid one, the securities regulator would have to request the US ISP, to which the email address belonged.

It was also explained that only the credit card number is checked when subscribing to the ISP's services, in order to make sure the card is authorized. However, the card could have been stolen but not already deauthorized. Another industry participant reported that as long as the service offered is free, it is not possible to verify the information provided by their client.

Even if they also offer free services, the second panellist reported that, in the three cases the securities regulator solicited information, the account information was accurate. He also indicated that even though message boards are not regulated, the community regulates itself: therefore, participants need to build a solid reputation among their peers. Should such a message be posted on a board instead of being sent by email, the advice would be unlikely to be followed, and the message would almost certainly be reported to the webmaster.

The ISP also invited the regulator to check the email header in order to make sure the email really originated from one of its customers, and that the address was not forged. The first panellist explained that the analysis of the header showed that the message had been sent using a standard spamming service to disseminate large amount of emails. The IP used to send the three copies of the email the regulator has received respectively belonged to a primary school in Korea, to an ADSL Italian provider, and to a dentist website located in Peru.

Moving on to the hypertext links, the representative from the bank whose name was used explained that they were frequently confronted with such fake emails or websites, and that they were dealt with as an intellectual property issue. After getting an injunction, they can ask the ISP to pull the spoof website from the Internet. Identifying the author will be the task of the regulator, but they will report the case only if someone has been disadvantaged.

However the panellist explained that website addresses were bought from a US provider for 10\$ a month, using an online payment service. He also explained that the main difficulty for fraudsters is not to know how to conduct such a fraud but to launder the money they then obtain. Unfortunately, it seems fraudsters have been very innovative in finding new ways to launder the money, using the same online payment service, either by quickly moving the money to other accounts, or by using it to pay online for services or products.

After this example, a participant explained the Single Point Of Contact (SPOCs) approach used by UK police forces to request ISPs: instead of having police officers requesting directly the ISPs, their request is channelled to the SPOC, who will be able to request the correct ISP for the correct information.

The need to improve international cooperation between regulators was also stressed, since, as the example has shown, the Internet knows no border. Even if police forces are looking at solutions that operate in other countries, they may face reluctance from governments. This means also that, if international cooperation is not conducted on a global level, once fraudsters realize that having their spoof website hosted in a specific country will help them not to get caught, they will start to choose countries with no Internet related legal framework to host their site. Currently the choice is only cost-driven.

Finally, the ISPs representatives explained that both storage and retrieval are costly when data retention is concerned. Figures were given by one ISP to show the amount of data they process each day, and therefore to imagine the size of systems needed to retain so much information.

Questions

What kinds of traffic and subscriber data do ISPs retain?

The information retained by the ISPs will depend on the type of service they offer: e.g. incoming phone number is not available for broadband access. Most ISPs will retain data of connectivity (IP address, date, duration) and email services (to, from, size), in order to settle disputes, to track spammers or to debug systems.

In terms of subscriber data, ISPs also retain banking information when they charge their customers for the service they offer.

Do ISPs verify the identities of their subscribers and, if so, how?

According to some regulation, ISPs have to verify the identity of their clients, which is achieved by sending a letter to the subscriber. However it seems that most ISPs do not have to perform such verification, and only check if the credit card is authorized when they offer a paid service.

Do ISPs retain the content of electronic messages? Are certain types of information or certain types of account data retained while other forms are not? Are there any important types of information that ISPs retain that securities regulators might overlook when requesting an ISP's assistance in an investigation?

Email is considered as private and it would therefore be illegal to retain their contents.

How long do ISPs typically retain traffic, subscriber and account information?

According to EU regulation, ISPs have to delete information as soon as it is no longer needed for business purposes or billing. Therefore traffic data is in most cases retained for one to three months.

Can ISPs voluntarily cooperate with law enforcement authorities by providing information?

ISPs are more and more concerned about the confidentiality they owe to their customers, and will in most cases need a formal request from the authority prior any information.

=0=