Mr Carse speaks about the regulatory framework of e-banking

Keynote Speech by Mr David Carse, Deputy Chief Executive of the Hong Kong Monetary Authority, at the "Symposium on Applied R&D: Enhancing Global Competitiveness in the Next Millennium" on 8 October 1999.

* * *

Introduction

There is no doubt that technology is now the single biggest strategic issue in banking. In particular, bankers like other businessmen are, or should be, urgently reviewing the opportunities provided by the internet. Although it is tempting to dismiss much of what is said about the internet as media hype, I do believe that it is true to say that we are living in the "Age of the Internet", and businesses that do not adapt to the opportunities and challenges which this presents, will have a limited future.

Obviously this also creates challenges for regulators such as the HKMA, not least because the current regulatory framework is still largely based on the more traditional physical frame of reference. As a bank regulator, the HKMA's primary responsibility in this regard is to ensure that the regulatory framework continues to evolve and keep pace with technological developments. At the same time, the HKMA recognises that technological innovations such as e-banking services and electronic money products are desirable advances that should not be impeded.

Development of e-banking in Hong Kong

Before I talk about the regulatory framework, it will be useful to take stock of the present state of development of e-banking in Hong Kong. A regulatory framework is clearly needed only if the present situation, or the outlook, requires it.

E-banking is a rather generic term and we need to be clear what we are talking about. In the HKMA, we tend to separate e-banking into two streams: electronic money products, mainly in the form of stored value cards, and electronic delivery channel products.

As regards electronic money, I think that it is fair to say that the progress so far has been somewhat disappointing as far as banks are concerned. There are two main stored value card schemes operated by banks, Mondex and Visa Cash. Both have been in the market place for some time now. However, it seems that these products have not yet gained wide acceptance. This is not unique to Hong Kong. In fact, the reaction to these products around the world has been lukewarm so far. It appears that the product is, for the present time at least, ahead of customer demand. This may change when the electronic purse function provided by a stored value card is integrated into a chip card and combined with credit and debit card functions.

The other route to success is to link the electronic purse function more specifically to a particular type of purchase which people have to make in their everyday lives. That has been demonstrated in Hong Kong by the success of the Octopus card. As at end-September, 5.6 million Octopus cards have been issued, recording 3.8 million transactions per day. At this level, Octopus must be one of the largest stored value card systems in the world.

As regards electronic delivery channels, five banks have already launched transactional websites in Hong Kong, and a further twelve have told us that they are at the planning and development stage. Mobile phone banking is also very much a live issue. Once Y2K is out of the way, I think that we will see a spate of further activity in this area. This reflects the fact that banks are increasingly becoming aware of the need to supply the e-banking product while Hong Kong has a population very ready and willing to accept new technology. Moreover, with 200,000 km of fibre optic cabling, linked to more

than 1,500 buildings, Hong Kong has one of the finest telecommunications infrastructures in Asia. The financial infrastructure is also one of the most advanced. On the legal front, the Government has already introduced a draft Bill into the Legislative Council to facilitate electronic commerce by granting legal recognition to digital signatures and by establishing a licensing system for certification authorities. Hong Kong Post is establishing a public key infrastructure for Hong Kong and will launch its Certificate Authority service before the end of this year. The HKMA welcomes and fully supports these initiatives.

Implications for banks

The prospects for e-banking in Hong Kong are therefore favourable. However, there are also risks to be managed, and I shall be looking at these more closely. Banks are of course already used to dealing with at least some of the issues that crop up in an electronic banking environment, and so have built up experience and expertise to deal with these. However, I do believe that the internet, because of its low cost, global reach and versatility raises the stakes for the banks – both in terms of the opportunities it presents as well as the risks.

Strategic risk

In talking about these risks, let me start at the top – with the issue of strategic risk. In other words, will the bank get it right? Will it make the right choices when it comes to investing in e-banking or will it waste money by going down a technological blind alley? Should it attempt to take the lead in new technology ahead of its competitors, or should it be a follower and adopt a "wait and see" approach? The latter may be the safer course of action for smaller banks, though it does create the risk of being left behind.

The advantages of e-banking, and internet banking in particular, are quite clear – the ability, for example, to disseminate information widely and instantaneously at low cost and to cross-sell products in a much more effective way. But there are also strategic threats. The cheapness and global reach of the internet opens up the threat of increased competition from new entrants who will no longer need a branch network to operate effectively in any given market. This competition can be launched across national frontiers. In the meantime, existing players are faced with the problem of what they do with the branch networks they have so painstakingly built up over the years. Unless they can give the right incentives to existing customers to migrate to the new electronic delivery channels, and scale back their branch networks accordingly, the promised cost-savings from the internet may not be realised.

Moreover, one of the key distinguishing characteristics of the internet is the ability which it gives customers to access and compare the offers of many different retailers, including banks. This greatly increases the power to "shop around". This will increasingly be done with the help of automatic shopping agents that will travel the net looking for the best deal on behalf of customers or through the use of intermediaries who will offer consolidated product information and price quotes. This will drive down margins, particularly on commodity-type products, and erode customer loyalty. As has often been said, the Internet Age is all about customer empowerment.

What in this situation is a traditional bank to do? Is it simply a matter of waiting to be overtaken by a trendy new virtual bank with a catchy name? Luckily, for the existing players it is not as simple as that. Banking is not simply about cheap delivery, although that will become more and more important. Running a bank is not like selling books or CDs: there is a whole range of other types of risk – credit, liquidity, interest rate risk and market risk – that need to be taken into account. Moreover, while the internet does indeed lower the barriers to entry, its anonymity and the vast range of choices also increase the importance of brand name. Depositors in particular will feel more comfortable with a name that they know and trust, and perhaps one whose name they see everyday in the street on signs above physical bricks and mortar.

So banks with an existing brand name still have some advantage, but it is not something that can be wholly taken for granted. The banks will have to work hard to maintain and build their brand image,

and to offer products which differentiate themselves from their competitors. This is a tough challenge, but it is one which the boards and senior management of banks in Hong Kong will have to confront.

Operational risk

Operational risk, including security risk, is of course one of the more frequently mentioned risks in connection with electronic banking. Security is not a new risk. We are all familiar with the various security issues that banks are facing on a day-to-day basis, e.g. robberies, thefts of ATM machines, frauds. However, banking transactions over the internet do pose new issues.

A major concern about the internet is its open nature. In relation to banking on the internet, this translates into increased risk of unauthorised access to, and alteration of, information. Accordingly, the fundamental objectives that internet security arrangements should try to achieve are to:

- restrict access to the system to those users who are authorised;
- authenticate the identity and authority of the parties concerned to ensure the enforceability of transactions conducted through the internet;
- maintain the secrecy of information while it is in passage over the communications network;
- ensure that the data has not been modified either accidentally or fraudulently while in passage over the network; and
- prevent unauthorised access to the bank's central computer system and database.

The security of transactions over the internet was one of the issues that was considered by a Study Group on Electronic Banking formed by the HKMA in July 1997. The results of this exercise were published as an article in our Quarterly Bulletin in November of the same year. Based on the work of the Study Group, the HKMA takes the view that developments in internet security technology have generally reached a point where adequate security for banking transactions is obtainable in a commercially viable manner. The use of sophisticated cryptographic techniques, firewalls and other security tools can provide security that is comparable to that offered in physical transactions. However, as with a physical transaction, the effectiveness of such measures is largely dependent on their proper implementation and the establishment of a set of comprehensive policies and procedures that are rigorously enforced.

However, it should be noted that this is only a temporary assessment. Continuing developments in security technology are required to maintain the effectiveness of security measures on an ongoing basis as new threats to existing systems arise over time. Banks should accordingly be responsible for ensuring that they keep up with such developments on a continuing basis. Unless they do this, their existing security measures can quickly become obsolete. If security breaches arise from this, it would not only expose the banks to risk of loss, but also more generally undermine the confidence of their customers in the use of the internet for banking purposes. All the evidence suggests that security is very much at the forefront of customers' minds in deciding whether to use this new medium.

Legal risk

In this connection, legal risk becomes an important issue in internet banking, and one aspect of this is how any losses from security breaches should be apportioned between banks and their customers. In this regard, the views of the HKMA are quite clear and have been communicated to the banks. Our position, put simply, is that we do not believe that customers should be responsible for any security breach or system problem that is not due to negligence on their part, and we have requested that this should be reflected in the contractual agreements for internet banking services.

Reputational risk

Risk of damage to the bank's reputation goes along with the other risks I have mentioned. It can arise, for example, from operational risk even if customers suffer no actual damage. If a hacker successfully

breaks into a bank's website and makes alterations, the bank concerned can suffer substantial damage to its reputation although customers' balances are safe and the hacker has not obtained any financial benefit. This does not only affect the individual bank concerned but may also undermine confidence in the security of e-banking more generally and therefore slow down development in this area. Systems breakdown, even if only temporary, is another example of how banks may be affected by bad publicity. Given the fact that the element of trust is so fundamental to banks' business, banks will find it increasingly important to adopt measures to manage reputational risk and incorporate public relations strategies into their overall risk management framework.

Banking risks

As I have already mentioned, an internet-based bank is faced with the same types of banking risk as its traditional counterparties. In some ways, the internet may heighten these risks. For example, the ability to transfer funds between different bank accounts may increase deposit volatility and could, in extreme situations, lead to "virtual bank runs". Banks will need to build this possibility into their liquidity management policies. Similarly, it is possible that credit risks could increase in the future if the relationship with customers becomes more distant and more transitory, and if the banks relax credit standards because of competitive pressures. On the other hand, banks will be better placed to obtain and organise information about their customers in an electronic banking environment, and this could help to improve credit evaluation techniques as well as to assist marketing. It all depends how much information each bank has about a given customer. If the customer spreads his financial affairs across a large number of internet-based banks, each one will have only one piece of the overall customer profile.

Regulatory Framework

So how do we regulators address these various kinds of risk? The first point to make is that our approach to the regulation and supervision of e-banking is still at an early stage, like the product itself, and is still evolving. We recognise that we have a lot of work to do in keeping abreast of, and monitoring, developments. This is part of our general approach of trying to improve our ability to determine that banks have in place adequate systems to measure, identify and control the various types of risk with which they are faced. In the case of electronic banking, this will require us to recruit more bank examiners with specialist knowledge in information technology.

As already indicated, our existing regulatory framework is split into two parts, e-money in the form of stored value cards and electronic delivery channels.

As regards the first of these, Hong Kong is one of the jurisdictions around the world that has chosen to put in place a specific legal framework to deal with the issue of stored value cards. This is contained in the Banking Ordinance. The thinking behind the legislation was that the issue of multi-purpose stored value cards such as Mondex and Visa Cash is an activity akin to the taking of deposits or the issue of banknotes, and should be confined to licensed banks. On the other hand, we wanted to allow flexibility for non-banks to issue limited purpose cards which would have a distinct core use, such as payment for transport services, but could also be used for a restricted range of ancillary or incidental purposes. There is provision for the issuers of such cards to be licensed as a special type of deposit-taking company under the Banking Ordinance. If the range of non-core uses is very limited, it can be exempted altogether. The Octopus card presently falls into this latter category, although the issuer has stated publicly its intention to broaden the range of permitted usages and to apply for DTC status. Although there are no candidates at present, it would be open to other non-bank issuers to go down the same route – in which case, if we received an application, we would want to be sure that the issuer was financially sound and that the card scheme itself is sound in terms of chip security and risk management policies and procedures surrounding it.

When it comes to electronic banking channels, our regulatory approach is, at this stage, less specific in nature. The first step is to know what the banks are actually up to in areas such as internet banking. We therefore issued a letter to authorised institutions in 1997 saying that while banks do not need to

seek formal approval from the HKMA to offer their services through the internet, they should discuss with us in advance their plans to do so. This is to enable the HKMA to assess whether the institution's proposed internet banking system is sound and the service provided through the internet will have adequate security. Note that we are not looking for absolute security. This does not exist in either the electronic or physical world of banking. However, the level of security should be "fit for purpose", i.e. appropriate to the type of transactions to be conducted. The important thing is for the banks to undertake a rigorous analysis of what their security needs are in the context of the particular service that they are planning to offer. The HKMA therefore expects that the security aspects of the system will have been reviewed by qualified independent experts and that the risk management systems and internal controls will be reviewed and evaluated on a regular basis e.g. by external or internal auditors. We also discuss with the banks their approach to the other types of risk described earlier, with particular focus on how the risks from the internet banking service are shared between the bank and its customers.

Apart from these general considerations, a number of specific issues arise in relation to internet banking. The first is how we would treat the pure internet bank, i.e. a "virtual bank" that delivers its services entirely over the internet. If such a bank wished to be authorised to take deposits in Hong Kong, it could not be allowed to exist wholly in cyberspace. It would need to have a physical establishment here, either as a locally incorporated bank or as a branch of a foreign bank. This would be necessary to provide a point of contact with the bank in Hong Kong for both customers and the HKMA. In particular, we would require books and records to be held in Hong Kong which we could inspect. Also, like any other bank, a virtual bank would have a balance sheet and would need to hold capital and liquidity against the risks in that balance sheet. Parentage would also be important – it would be highly desirable from our point of view that an internet bank was itself majority-owned by another well-established bank that could provide guidance and financial support if necessary. In general, we would need to be assured that the virtual bank has "substance", and is not simply a "concept", taking advantage of the popularity of the internet. On this basis, our authorisation and supervisory regime for virtual banks would be similar to that for conventional banks.

However, an offshore internet bank, whether wholly "virtual" or not, might not attempt to take deposits in Hong Kong in the strict legal sense – in other words, the deposit contract might not necessarily be created in Hong Kong. Instead, the offshore internet bank might invite potential customers to send their money to a location abroad, where the deposit would be legally created. In this case, the bank would be taking deposits outside Hong Kong and would not require authorisation under the Banking Ordinance to carry on a deposit-taking business here.

But that is not the end of the story. It is also an offence to advertise for deposits in Hong Kong, even if they are to be taken outside the territory, unless the disclosure requirements of the Fifth Schedule of the Banking Ordinance are adhered to. An advertisement would include one contained on a website. The problem is how to determine whether a particular offshore website is targeted at Hong Kong. Here, we would have to look at the circumstances of each case – whether, for example, the offshore internet bank advertised its services in the local Hong Kong press or accepted Hong Kong dollar deposits or refused to take deposits from a number of specified jurisdictions, but did not include Hong Kong among these. If we come across such cases of illegal advertisements targeted at Hong Kong, how would we deal with them? The easiest case would be where the bank itself is respectable and is based in an overseas location which is properly supervised. We could then write to the bank itself and to its supervisors to notify them of the advertising rules in Hong Kong, and request the bank either to comply with these rules or to add Hong Kong to the list of the jurisdictions from which it was not prepared to take deposits. If necessary, we would seek the cooperation of the home supervisor to enforce this request. It might also be necessary to supplement this with a reminder to local Internet Service Providers about the advertising rules in the Banking Ordinance and to seek their cooperation to block offending websites. The problem with this, however, is that the website in question may not actually be posted on the local ISP's server – in which case, there may be little that the ISP can do.

If the bank concerned is not respectable and it is based in an uncooperative jurisdiction, the situation would be more difficult to handle. This reinforces the point that the public in Hong Kong should be very careful about sending money to any bank which advertises on the internet and which is based in a

jurisdiction where the degree of regulation is in doubt. In the final analysis, no form of regulation can replace individuals taking care in selecting the party with whom they do business. Again, this reinforces the importance of brand name and reputation in the internet banking context.

Conclusion

To conclude, I think that e-banking is the way forward for the banking industry, and banks in Hong Kong are well-placed to capitalise upon this. E-banking does bring new challenges and perhaps additional risks for banks, consumers and regulators. But it also brings new opportunities to improve the efficiency of the payment system and the quality of banking service. There is no question of avoiding the changes. The question is how to manage them. This is mainly an issue for the banks. But the HKMA can help by providing a regulatory environment in which the risks of such changes are minimised, and the potential benefits can be safely realised. This is an on-going task which has only just begun. We have already made a reasonable start and I hope we will see encouraging developments in the next few years to come.