IMPLICATIONS OF E-COMMERCE FOR THE BANKING AND MONETARY SYSTEM[1]

This article discusses various issues arising out of the growth of electronic commerce and electronic banking. It also examines the implications for monetary policy of electronic money.

Introduction

The Internet has quite suddenly multiplied by a remarkable degree the number of potential suppliers and customers with whom we can do business, and the number of avenues through which we can perform financial transactions. This opens up all sorts of opportunities, but it also attracts all sorts of warnings - about needing to know the identity of those with whom we are dealing; about needing somehow to satisfy ourselves, remotely, as to the quality of the products or services on offer; about needing to be sure of the financial standing of counterparties, be it their ability to pay or to provide credit which concerns us; and so on.

From the point of view of maintaining the stability and integrity of the financial system, the Internet sparks two particular concerns: consumer protection, with worries about scams, transparency, security, accountability, legal recourse, and so on; and systemic stability, with questions as to whether the financial system might become more vulnerable to crisis as a result, for example, of a major technical failure or of a massive herd movement of money in a particular direction.

Electronic Money on the Internet

There are two types of electronic money: that which is held on the Internet and that which is held in stored-value cards. Multi-purpose stored-value card schemes have been slow to become established, despite quite lengthy pilot projects in a number of countries. Hong Kong was nevertheless one of the first places to introduce regulations governing the issuance of such cards. Meanwhile, limited-purpose cards have proved more successful; we have a particular example in Hong Kong with the Octopus card[2], used to pay mainly for public transport, which is hugely popular.

Many people speak of the arrival of the Internet era as a revolution in business practice. From the particular viewpoint of making payments, it is regarded as a step along an evolutionary path rather than as something revolutionary. Our distant forefathers were skeptical about the introduction of banknotes in place of metallic tokens and coins; and our more recent forefathers were worried as to the reliability of cheques as a substitute for cash when they first appeared. There were also initial resistance by some to credit cards and debit cards on suspicions about the security of the arrangements, as well as opposition to direct debit schemes for fear of granting to a third party too general an authority to debit one's bank account.

But each of these innovations has, in the event, been assimilated and has taken its place in the range of accepted payment instruments. E-banking is expected to follow suit, as just another step along the evolutionary path. But it is perhaps worth pausing to consider whether there is anything intrinsically different about e-banking which demands special attention from the central bank.

Characteristics Requiring Vigilance

One area for attention is the technical security of access and messaging. This is a matter of accuracy, safety and secrecy. If we use the Internet to move our money, or to hold our money, we expect messages to arrive at their destination without error or interception; we expect the system to be safe from fraudulent or unauthorised access; and we expect to enjoy the

1 This article is adapted from a speech by Tony Latter, Deputy Chief Executive of the Hong Kong Monetary Authority, at the Conference on *China in the New Millennium: WTO, Entrepreneurs, and New Technology for Global Trade* in Nansha, Guangdong Province on 24 March 2000.

2 The Octopus card becomes a multi-purpose card on 25 April 2000 following the authorisation of its issuer, Creative Star Limited, as a deposit-taking company.

same degree of customer confidentiality as with conventional banking arrangements. We want to be assured not only that the execution process is reliable and secure, but also that there are adequate controls on any "read only" access facilities.

How can these assurances be obtained? Inevitably users are dependent on the experts. They have devised sophisticated methods of electronic signatures, encryption, certification, firewalls and the like. One way or another, by obtaining appropriate professional advice, by applying rigorous standards of compliance and computer audit, and so on, those within an organisation should be able to deliver the necessary assurances to customers, and the regulatory or supervisory authorities will need to satisfy themselves as to the dependability of such assurances. The financial authorities within countries, and on a collective basis internationally, may also have a role to play in developing recognised common standards in these arenas of technology and security.

A second characteristic deserving special attention is the nature of the person or company which is offering banking or payment services over the Internet. If we are merely using electronic services provided by our usual bank, which we know to be sound and to be supervised by an acknowledged regulator in a known jurisdiction, then we should be in no more danger of losing our money than we would be by banking with the same bank in the conventional manner, provided of course that both the bank and the regulator have kept pace with the requirements of Internet banking, such as in respect of the security aspects discussed already.

But it is quite a different story if we are tempted to part with money to some organisation masquerading as a bank, or which actually is a bank but is registered in a jurisdiction with lower supervisory standards than those to which we are accustomed. In Hong Kong, in order to protect the public, there already exists legislation governing usage of the word "bank", and governing the advertising for deposits within our boundaries by anyone not authorised to take deposits in Hong Kong. But the government cannot protect people from the possible consequences of clicking onto a website in a far-off place which is luring them to part with their money. The message is clear: make sure that you know and trust your banker.

In Hong Kong there has been some talk of new banks being established for the sole purpose of conducting internet banking. In deciding whether to authorise such a bank, the Monetary Authority would expect to apply very much the same criteria as for a conventional bank, but would need to pay particular attention to the business plan in order to ensure that it reflected realistic assumptions and prudent banking principles. The Authority intends in the near future to issue guidelines for any such applications[3].

As the supervisory body for existing banks, the Hong Kong Monetary Authority needs to take account of any particular risks that pertain to Internet banking and to be sure that banks who conduct such business do themselves properly appreciate and allow for such risks. Banks should pay attention in particular the strategic risk, in that venturing into a new business arena may not always be assured of success; the operational risk, of dependence on IT networks, and the associated security considerations to which this article has already discussed; and any additional banking risks which may arise if Internet transactions are deemed to be potentially more volatile or unpredictable, or customers less reliable, than in normal banking business.

The need to be confident about the financial intermediaries is also very relevant when we examine schemes for so-called digital cash or a cyberpurse. There have been some false starts and business failures in this field, but some potentially more durable systems are now emerging in a number of countries, albeit still mostly in only embryonic form. The concept is of a storage location - or account - somewhere in cyberspace, into which we transfer funds from our bank account or credit card, just as we would draw cash from the bank and store it in our wallet.

3 The "Guideline on Authorisation of Virtual Banks" was subsequently issued on 5 May 2000.

The schemes are designed essentially for the cyber retail shopper, who can then make payments from the purse for items purchased over the Internet: the purse operator responds to our instructions by transferring funds from our purse to an account of the seller.

One may wonder what the advantage of such schemes is supposed to be. Why not simply pay for each transaction by an electronic instruction to a bank or, more typically in the case of most retail internet purchases, by credit card? Digital cash purports to offer three advantages. First, it may be cheaper than other means for a series of relatively low value retail transactions. Second, it can be used by those who cannot or do not have a credit card - for instance teenagers. Third, it offers a degree of anonymity and perhaps a stronger feeling of security, in comparison to using a bank account or credit card, since account-related personal data need not be passed on to the individual sellers of the goods or services.

However, people should exercise some caution before utilising such cyberpurse facilities. Regardless of how the system may be presented, the purse operator is in effect acting very much as a bank, in particular by holding its client's money in a sort of deposit. Even if we initially acquired the digital cash or credit for free (through a loyalty or bonus point scheme, for example), the accumulated "savings" represent value which we would doubtless wish to protect. Customers will want to be assured that the money or credit points are in safe hands. Regulators, too, may desire to verify that no banking activity is taking place that is unlawful, although they will first need to ascertain the location of this virtual operation (a task which is itself almost a contradiction in terms) so as to identify what is the applicable jurisdiction. Although in most of these schemes the maximum sum which anyone may hold in a purse may, for the moment, be quite modest, and so the scale of potential losses limited, we need to establish the foundations of prudent behaviour and regulation in preparation for the time when the sums may be much larger.

Implications for Monetary Policy

Central banks or their government shareholders enjoy a steady stream of profit from the issue of currency in the form of notes and coin - the so-called seignorage. It is noteworthy that the public's demand for currency has been much less affected over the years than one might have expected by the emergence of successive new forms of non-cash payment such as cheques and cards. It is also doubtful whether the development of cyberpurses, cybercash and cyberpayments would have much impact on cash in circulation, at any rate in the near term. However, if there is a complete revolution such that cybercash, including electronic stored-value cards, substantially displaces physical currency within a few years. How should central banks react?

In such circumstances, central banks would lose an important source of income and would have to find ways of replacing it. Perhaps some central banks would lose their financial independence and become dependent - or more so than hitherto - on subvention from the government budget. But in a broader sense they should welcome the development because it would be evidence that the economy as a whole was enjoying a more efficient and less expensive means of money holding and transmission.

With regard to operational aspects of monetary policy in pursuit of the general macroeconomic objective of stability in the value of the currency, the advent of this new means of payment would, if it caught on to a significant extent, have some impact on the public's allocation of money holdings as between physical currency, various forms of deposit and, now, electronic forms. This in turn might affect the monetary statistics and their interpretation. However, any changes would only occur gradually. Besides, nowadays there are scarcely any central banks which rely single-mindedly and exclusively upon measures of money supply to guide their monetary policy decisions. Therefore it is believed that there is nothing much to worry about on this front.

Next, it has been suggested that Internet banking in its various manifestations could introduce additional and unpredictable volatility into world financial markets by enabling millions of people to switch funds between investments or between currencies at the click of a mouse. In general such worries are skeptical. Global financial markets have

already been exploiting the IT age with its immediacy of information and electronic dealing for some years. Capital is already hugely mobile in both scale and speed. It is doubtful whether the inclusion of new players at the retail level would have much of an additional impact.

In particular cases where monetary policy is supported by capital controls, however, Internet banking may make enforcement of such controls more difficult, since it would be operationally easier for those wishing to evade regulations to maintain offshore bank accounts. Of course, every bank in reputable jurisdictions has in place rigorous procedures to combat money-laundering, but these procedures do not normally result in customers being turned away if they are merely trying to escape capital controls or the tax regime in their home countries.

Similar considerations lead some observers to enquire whether the Internet might encourage substitution out of the national currency, resulting in dollarisation and also perhaps weakening the central bank's influence over domestic monetary conditions. If Internet facilities enable or encourage people either to economise on the usage of money (for example by netting payments due among two or more parties or by practising barter) or to reduce the frequency of movements of money (for example by leaving export receipts in an Internet account in order to pay for imports, rather than repatriating them first), then there may be a prospect of a general reduction in transactions traffic in all currencies. The usage of some may fall more than others. However, there is nothing particularly sinister in such developments, except to the extent that the Internet might facilitate avoidance of rules on remittances. The survival of the national currency and its acceptability to the public will continue to depend on the central bank carrying out a responsible monetary policy which protects the value of the currency. Discharge of this duty should not be materially affected or impeded by technological developments in payment methods. The central bank's ability to influence interest rates or the exchange rate through its market operations will not be diminished.

Conclusion

All in all, there are few concerns for the central bank in its monetary policy role that arise from the development of e-commerce; where there is an impact it is likely to be gradual and central banks should be able to adapt to it as readily as they have to other structural changes in the financial sector over the years. For the reasons discussed earlier, however, the challenge to the banking regulatory side of the central bank is likely to be rather greater.