The Internet: Increasing the Complexity of the Customer-Technology Relationship

Abstract
The retail banking industry has known for many years that customer technology uptake is not a simple process. For example, phone banking and ATMs meet many customer needs, but have not replaced bank branches. The Internet adds a further complexity to the customer-technology relationship. In this paper I review the development of the Internet, and examine what success has been achieved in developing it as a commercial transaction medium given its non-commercial origins. I then examine one recent form of attack on retail Internet banking customers and consider whether the Internet’s design assists or hinders banking customers’ use of technology-based services in this case.

Introduction
Technology has transformed the way we use financial services. However, as in other areas, technology uptake in retail banking is not straightforward. Technology for banking customers, for example, isn’t necessarily adopted as expected by financial services organisations. This is shown in the 1990s calculations made regarding cost of customer transactions by retail channel (the way the customer accesses a service).

Gosling (1999) provides typically optimistic comparative figures for various channels: A financial transaction through a bank teller, $1.07; through a telephone call centre, 52 cents; via an automatic telling machine (ATM), 27 cents; over the Internet, 1 cent. These calculations led Gosling to describe the following futuristic scenario for 2009:

> The biggest shock for the time traveller walking down tomorrow’s high street [local shopping centre], though, is the absence of bank or building society branches. There is still a Post Office branch, which acts as an agent for cash transactions for the banks, but most of the bank branches have gone. Initially banks tried to exploit their branch networks by selling financial products from them. Customers soon learnt, though, that they could get better value for money by banking with supermarkets, car manufacturers and airlines than they could with the old high-street banks. All of the surviving banks had reshaped themselves dramatically over the last five years. Many had merged. These commercial changes had been dependent on important technological developments. One of these has enabled consumers to feel confident that they can make transactions over the Internet with absolute security. This has rested on the universal introduction of smart cards, which double as electronic purses -- money stored on a plastic card.

Why did this vision fail? In part it was an expectation based on ‘technological determinism’, the view that the virtues of a technology are its primary driving force for adoption, and that once released a new technology will change people’s behavior. In part it was because the way users adopt technology isn’t necessarily the way that providers expect. Call centres, phone banking through Interactive Voice Response (IVR), ATMs, and Internet banking have all been widely adopted within retail banking. At the same time, two other phenomena can be seen. First, customers as a group are not leaving pre-existing channels such as branches. Second, the number of touch points for each retail banking customer has significantly increased (so that a decline in the cost of each transaction is at least partly offset by an increase in the number of transactions).

A report on information technology in the retail banking sector (McKinsey Global Institute 2002) examined the United States experience of banking transaction costs. While the cost per transaction declined from $1.10 to $0.96 between 1985 and 1998, the average number of transactions for each household rose, from 75 to 167. As a result, the total cost of serving each household had risen from $83 to $160 over the same period. The report identifies four trends that contribute to this problem: product proliferation; channel proliferation; the willingness to retain customers ‘at all costs’; and poor information technology implementation: ‘As customers captured surplus benefits, banks’ profits were further limited.’

---

The biggest shock for the time traveller walking down tomorrow’s high street [local shopping centre], though, is the absence of bank or building society branches. There is still a Post Office branch, which acts as an agent for cash transactions for the banks, but most of the bank branches have gone. Initially banks tried to exploit their branch networks by selling financial products from them. Customers soon learnt, though, that they could get better value for money by banking with supermarkets, car manufacturers and airlines than they could with the old high-street banks. All of the surviving banks had reshaped themselves dramatically over the last five years. Many had merged. These commercial changes had been dependent on important technological developments. One of these has enabled consumers to feel confident that they can make transactions over the Internet with absolute security. This has rested on the universal introduction of smart cards, which double as electronic purses -- money stored on a plastic card.

Why did this vision fail? In part it was an expectation based on ‘technological determinism’, the view that the virtues of a technology are its primary driving force for adoption, and that once released a new technology will change people’s behavior. In part it was because the way users adopt technology isn’t necessarily the way that providers expect. Call centres, phone banking through Interactive Voice Response (IVR), ATMs, and Internet banking have all been widely adopted within retail banking. At the same time, two other phenomena can be seen. First, customers as a group are not leaving pre-existing channels such as branches. Second, the number of touch points for each retail banking customer has significantly increased (so that a decline in the cost of each transaction is at least partly offset by an increase in the number of transactions).

A report on information technology in the retail banking sector (McKinsey Global Institute 2002) examined the United States experience of banking transaction costs. While the cost per transaction declined from $1.10 to $0.96 between 1985 and 1998, the average number of transactions for each household rose, from 75 to 167. As a result, the total cost of serving each household had risen from $83 to $160 over the same period. The report identifies four trends that contribute to this problem: product proliferation; channel proliferation; the willingness to retain customers ‘at all costs’; and poor information technology implementation: ‘As customers captured surplus benefits, banks’ profits were further limited.’
These issues are understood within the retail banking industry. One experience shows just how ‘difficult’ customers can be. An early online initiative was British Internet and telephone bank Egg, launched by Prudential Insurance. In its first six months of operation the bank won 500,000 customers with £5 billion of deposits. Egg originally focused on telephone banking, but then moved its emphasis to Internet banking. The bank’s early success surprised Prudential, although it offered a preferential interest rate and emerged in a market with little initial competition. Egg floated in June 2000. At the time it had nearly a million customers, £7.3 billion in deposits and total loans of £2.5 billion. Nearly two-thirds of all transactions were over the Internet (Mackintosh 2000a). The shares floated at 160 pence and quickly rose to 190 pence before falling to as low as half that in the following year. At this point the difficulties of developing an on-line bank became clear. A mid-2000 survey showed banking industry optimism in the Internet at only 5 per cent compared to 67 per cent three months earlier (Mackintosh 2000b). Within four weeks of its float, Egg had lost 20 per cent of its stock value as customers withdrew funds in response to a cut in savings interest rates and it reported half-year losses of £80 million. Blaming the customer, chief executive officer Mike Harris said that it was mostly older, less ‘Internet savvy’ customers who were leaving, a group that the bank had not targeted (Mackintosh 2000c). By November a further similar drop had occurred, and a new strategy was now proposed: there would be a greater emphasis on telephone banking, and the bank talked about opening a network of branches (Jenkins 2000).

While all technology uptake is to some extent unpredictable, the Internet adds a new level of complexity. Technologies such as IVR and ATMs were designed from scratch to meet the stringent security and privacy requirements of banking. The Internet was not.

**Early usage and Internet architecture**

In its development up to the early 1990s, the Internet lacked a commercial imperative, reflecting its usage and funding basis. The origins of the Internet meant that at no point up to the early 1990s were its commercial or transactional capabilities critical to its progress. This is evident in its architecture, which is highly useful for communication for both commercial and non-commercial users, but poorly supports business transactional requirements. By the beginning of its commercial period in 1995 its overall use had grown beyond the capacity of orderly technological modification (Adamson 2004).

The Internet is based on packet switching, a technology invented by Paul Baran in the 1960s (Davies 2001). His object was the establishment of a fault-tolerant network based on existing infrastructure for maintaining command and control during a nuclear war. As the Internet moved out of the military-research environment in the 1980s, it took on the architecture that still defines it today. It was now meeting new requirements, and subject to wider usage and development influences. None of these new influences, however, placed commercial transactional demands on the network.

Throughout the 1980s Internet traffic rose dramatically and its funding moved to an academic basis. Much academic and research funding was based on the identification of business benefits but this was not reflected in requirements of the Internet. The benefits identified for Internet connectivity within funding proposals tended to be vaguely defined opportunity loss. In 1979 United States computer science departments not on the Internet argued that they were at a disadvantage when recruiting staff or competing for research grants (Winston 1998).

Tim Berners-Lee’s original 1989 proposal to develop the World Wide Web’s prototype shows that while commercial distribution of the World Wide Web may have become important, the requirements of commerce were absent at the beginning. Under the specification heading of ‘Non Requirements’ he listed ‘copyright enforcement and data security’ (Berners-Lee, 1989). This is in contrast to requirements of commercial data communication alternatives of the time.

The Internet’s architecture is useful to hundreds of millions of people. Nevertheless, its basic architecture of the early 1990s lacked many features required of a commercial transactional medium. IBM’s Leung (1999), for example, describes the Internet architecture’s weaknesses as follows: best effort service; security exposures; not commercial grade; and growth outrating capabilities. Here I examine five commercial transactional requirements, contrasting the Internet to other technologies that inherently support them: security of financial exchange; proof of transaction; identification of a commercial party; establishing a single meaning for a transaction; and facilitating payment.

**Security of financial exchange**

Despite its military research background, the Internet’s original protocol suite provides no security. Specifically it does not innately support any of the three core communication requirements for security of data: integrity, confidentiality or authentication. These are generally accepted requirements for secure
transactions (Ghosh 1998), which are also found in other security requirements. Not all are required for all transactions:

Integrity: Has the transaction been deliberately or accidentally altered? Has the figure on an order or cheque been changed? Because this is impossible to prevent (all electronic communication includes the possibility of error), the focus is on identifying whether a change has been made. Packets traversing the Internet infrastructure, which is owned by thousands of separate companies and organisations, will travel by an unspecified path that could include almost any country in the world, even when communicating between two users in the same city. By default all data is sent in a form that can be read and modified. A local or national telephone call or letter, in contrast, generally stays within a single country.

Confidentiality: Is the transaction visible to parties other than the intended recipient? As the Internet transmits clear (unencoded) text, confidentiality is not provided by default. This is also not universally required. For example, public documents or marketing information have no requirement for confidentiality.

Authentication: Is each party to a transaction who they claim to be? This is examined below.

These points show that the requirements for secure communication of commercial transactions are well established. The absence of support for these on the Internet reflects their absence as requirements during development of the Internet.

Proving a commercial activity occurred

Financial transactions are a central aspect of business. They form the basis of payment services. A financial transaction is a discrete event. For example, a purchase is either completed or not. A single electronic transaction may have many steps, and at any one of these steps a computer may fail or a connection may disappear. At the conclusion of the process both parties to the attempted transaction need to unambiguously agree that a purchase, offer or agreement has either been made, or not, regardless of any technological problems. These requirements can be summed up as:

• atomicity: a transaction either completely fails or completely succeeds;
• consistency: relevant parties agree on the facts of the exchange;
• isolation: transactions do not interfere with each other; and
• durability, the ability to recover to the last agreed state (Camp & Sirbu 1997).

The case of billing for services highlights the difference between the Internet and the global telecommunications network. A telecommunications company devotes a large proportion of its technical resources to ensuring it can bill customers for services provided. This includes identifying the service and providing proof that the service was used by a customer (date, time, length of call). Historically, domestic phone calls involved only one company, and only international phone calls required the division of the charge between providers. In an increasingly fragmented market, telecommunications companies must now keep track of millions of calls, and have commercial relations with other companies for the settlement of calls that use both their services. ‘Settlement’ is a process used by multiple parties involved in providing a telecommunications service to a user, such as a call between countries, or from one mobile network to another. Pre-agreed cost charging formulas determine how much needs to be paid between companies at some regular interval. In contrast to this telecommunications environment, early Internet usage was based on the data communication expectation that telecommunications lines will be leased and used as required, independent of the amount of traffic carried.

A data packet of information travelling across the Internet can traverse one or many of tens of thousands of networks. Unlike the telephone system, the amount paid to an Internet service provider (ISP) by an Internet user is not split among the networks that forward the packet. Rather it is kept by the ISP, who pays other ISPs for the amount of traffic moving between them. Statistically, the payment may eventually be shared out among the providers, but this is a random result, as ‘the Internet interconnection environment remains one where there are no soundly based models of financial settlement in widespread use today’ (Huston 1999).

The events of the transaction must leave an auditable trail. Without this a financial system would be unable to legally prove that a transaction had taken place. In this case it would be unable to enforce contracts, prove its own compliance with contracts or provide evidence of activity including governance requirements. As a result it would probably go out of business. While this may appear obvious, the case of Independent Energy in Britain illustrates the problem. The company had several dot-com characteristics, including NASDAQ stock exchange listing and co-provision of telecommunications services with a company called Future Integrated Telephony. Its 160 staff serviced 242,000 customers in a competitive energy environment. In 2000, lending banks that were owed more than £100 million refused to renew credit arrangements, and the company went
into receivership. At the time it was owed £119 million by customers, but could not provide evidence of this, and so was unable to collect these accounts (Taylor & Jones 2000).

This description of financial transactions shows that transactional architecture must be deterministic: the result of the transaction in the overwhelming majority of cases has to be what was meant, and when it is not there should be evidence of what went wrong. The design of the Internet protocol suite TCP/IP is non-deterministic. It aims to achieve overall reliability in a network, not necessarily individual reliability for each segment of that network. This concept of ‘best effort’ is core to the Internet’s design and to an understanding of the Internet’s flexibility. While the telephone network will reject an attempt to connect if the destination is unavailable (a busy signal), the Internet will send information out in the hope of success, by design (best effort). There are many methods for overcoming the limitations that this creates, including within the TCP protocol itself, but the design choice of ‘connect if a full service available’ or ‘make every effort to get any part of the message through’ remains.

**Identifying a commercial party**

The Internet by design is an anonymous network. This by itself is not a block to commercial activity. The vast majority of all commercial transactions in Australia by number (not value) are cash-based (Information Industries and Online Taskforce 1998), and therefore potentially anonymous.

The process of identifying parties to a transaction is authentication, ensuring that each party is who they present themselves to be. In a contract to supply items for a period of time under particular terms and conditions this is important. When someone walks into a shop to buy a loaf of bread, it is generally not important (an exception would be during a time of rationing). It may be partial, for example in the sale of cigarettes or alcohol, where age rather than identity is important. TCP/IP provides no mechanism to certify parties to a communication. Co-inventor Cerf (2002) identifies this as one of the key weaknesses of the protocol.

Identifying consumers is required for services that are legally or commercially limited to a geographical area, such as pharmaceutical, insurance, gambling and auction sites, and for age-limited services. Identifying a business is required for consumer protection and consumer confidence, as commercial transactions require a consumer to trust a vendor with credit card and other personal information. This makes trust and privacy necessary elements of a commercial network, elements that are not inherently provided by the Internet’s architecture.

Where an order based on a facsimile or letter will be accepted in normal commerce, there is no secure way to attach a person’s signature to an electronic document. (An image of a signature is worse than no signature, because it can be easily copied to other documents.) The solution is an ‘electronic signature’. This is a long numerical sequence which links an individual to a document. It is considered a unique electronic signature because the result is easy for the signer to produce and difficult for anyone else to forge. Apart from the difficulty of correctly using such an approach, the main limitation is the process for establishing electronic signatures. In particular, for all the digital signatures to have meaning in the Internet commercial environment there would need to be an international ‘public key authentication framework’, a means for signatures from separate organisations to be recognised by each other. This is a regulatory challenge rather than a technological one, involving issues such as national sovereignty, the right of citizens to conceal secrets (recognised in some countries but not in others), and commercial liability. By contrast the fax, which remains widely used in business, successfully identifies commercial parties in a ‘low tech’ manner. The most valuable thing about a faxed business order, in addition to its simplicity, is that it is fixed, and therefore moderately difficult to fake. The Internet by contrast is so sophisticated and versatile that anything it produces (especially a scanned personal signature) is inherently untrustworthy.

Once a transaction has successfully occurred, there remains a requirement to prove that this was the case. This is called ‘non-repudiation’, the action of ‘preventing the data recipient later denying receipt of the data or the sender denying transmission’ (Caelli, Longley & Shain 1994). A dated signature on a contract is a typical means of proving this. There are also electronic means of doing this, although proving time of electronic signature can be more difficult than proving the signature itself. The Internet by default provides no proof of time, identity or content of a communication.

**Single meaning of a transaction**

Parties to a transaction must agree on the meaning of their communication. Here the Internet’s potential flexibility places it at a disadvantage to a more structured approach, such as a paper-based order form or invoice, or the traditional electronic data interchange (EDI) approach.
The characteristics of electronic commerce have their origins in 19th century railroad developments. United States railroad companies used the (electro-mechanical rather than electronic) telegraph to forward information about the contents of trains between stations (Zinn & Takac 1989). The 1980s predecessor of current electronic business was electronic data interchange. Unlike earlier data exchange systems, EDI provided a framework for the exchange of data between separate organisations, to meet the requirement for multiple organisations to agree on the meaning of business messages. Because of this requirement for inter-organisation cooperation for the purpose of trade, EDI dissemination involved an enthusiastic band of advocates who collaborated to have cross-industry standards developed. The electronic data interchange campaigners from the late 1980s created a large body of literature identified by Sokol (1989). EDI met three key requirements: common meaning, common infrastructure, and security.

**Common meaning:** Within a single corporation, due to multiple purchasing policies, acquisitions and other reasons, by the 1980s incompatible computer systems were common. Nevertheless the possibility existed within a single organisation to resolve this, by executive instruction if all else failed. For separate organisations to communicate meaningful information to each other required a standardised method for conveying order forms, invoices and the hundreds of other forms which make up commercial transactions, in a mutually understood way.

**Common infrastructure:** Getting an EDI message between two organisations requires a common communication infrastructure. For two organisations exchanging large amounts of information a dedicated communication link is generally the most cost effective. For organisations dealing with dozens or hundreds of other partners this is impractical. So commercial value added networks (VANs) were created to act as switching points for EDI messages. While these provided reliable and guaranteed delivery of information, their cost for data transmission is several orders of magnitude higher than Internet data transmission costs. This cost can lead to a mistaken expectation of savings through a less reliable medium. While the individual cost of an Internet-based transaction may be a few cents or a fraction of a cent, in an automated process involving thousands of transactions (per week or even per second) the cost of manually correcting one transaction in error may be hundreds of dollars. This could be required by poor data quality, ambiguous business rules and user uncertainty or error. Any transmission difficulty that increases this, such as Internet congestion, may increase rather than reduce overall costs.

**Security:** This is required for two reasons. First, EDI messages contain information that may be commercially sensitive. Second, two businesses linked by EDI will want to ensure that the only information they provide is the information they want the other party to see. The individual design of most EDI solutions assisted in providing security.

During its heyday in the late 1980s electronic data interchange swept the business world. EDI and private (non-Internet) network solutions in 2006 continue to carry the vast majority of the world’s electronic commercial transactions by value. In particular the Society for Worldwide Interchange of Financial Transactions, [www.swift.com](http://www.swift.com), transfers millions of messages worth trillions of dollars per day. The total volume of privately carried transactions is vastly greater than that carried by the public Internet. While a simple examination of financial transaction channels shows this to be self-evident, this is widely misunderstood within the technology community. Many electronic business infrastructure discussions also confuse the Internet and private TCP/IP-based networks, which are similar in technology but are completely separate in operation, and do not directly connect to the Internet.
Payment mechanisms

The Internet has no standardised mechanisms for charging, in contrast to the telephone system where users can be charged a few cents or tens of cents in their local currency for services. Security for the purpose of financial exchange has been a central factor of some commercial networks since the telegraphy industry a century before the Internet. Standage (1999) describes the introduction of a secure cash transfer system for up to $US100 established by Western Union in 1872, including the following steps which resemble the functional description of modern electronic payment systems:

The system worked by dividing the company’s network into 20 districts, each of which had its own superintendent. A telegram from the sender’s office to the district superintendent confirmed that the money had been deposited; the superintendent would then send another telegram to the recipient’s office authorising the payment. Both of these messages used a code based on numbered code books. Each telegraph office had one of these books, with pages containing hundreds of words. But the numbers next to these words varied from office to office; and only the district superintendent had copies of each office’s uniquely numbered book. A running count was kept for each book, and each time a money transfer telegram was sent, the next word in its unique numerical order was sent as one of the words of the message.

The postal service, like the Internet, lacks the ability to support secure transactions (because a letter could be stolen from a letterbox, for example), so methods of payment such as postal orders and non-negotiable checks have been developed that overcome this. When the Internet is used to replace other remote purchasing channels, such as the telephone or mail-order catalogue, a non-Internet payment system will already be in place.

Still unresolved today for the Internet is a standard means for transferring payments regardless of currency or amount. There are point-based solutions such as consumer-to-business credit card payments and the currency and country limited consumer-to-consumer PayPal, www.paypal.com. However, there is no general international system equivalent to cash or local telephone billing.

Phishing

The characteristics described in the previous five sections were lacking at the time that investment began to flood into Internet electronic business from 1995. Where these deficiencies were identified, particularly in the area of security, technological approaches were developed to correct the problems. However, these have been only partly adopted. The primary effect of these limitations on the Internet as a transactional medium was not to prevent commercial investment, but to make this investment more difficult and expensive than expected. In recent years the phishing attacks on retail banking customers show that the challenge of the Internet’s architecture remains.

Phishing is a simple and elegant scam. A bank customer receives an e-mail notifying them of a security administration requirement to visit their bank’s web site and enter their name and password. The unaware customer is directed to a copy of their bank’s web site, and voluntarily provide name and password, which are then used to steal money from the customer’s account. How does the Internet’s architecture assist or hinder this? Based on information in the previous sections, particularly the difficulty of identifying a commercial party, it is easy to see that the Internet’s specific architecture adds to the difficulty of preventing such a fraud. Following are some elements of this:

The unreliability of digital evidence: While in the real world it is moderately difficult to forge company documents or letterheads, in the digital world it is trivially easy. To reproduce a company logo is simply to visit a web site and cut-and-paste. An entire website can be copied in minutes, and from a viewer’s perspective be indistinguishable from the original.

The challenge of location: One banking scam involves setting up a fake ATM to collect card details, including PIN numbers, from people attempting to use it. A similar result can be achieved by attaching a ‘skimming’ device to the front of a real ATM. To collect the results, a fraudster must return to the scene, and thereby risk capture. On the Internet, the fraud can be perpetrated from any country, and the perpetrator need never be within thousands of kilometres of either the banking customer or their bank.

The difficulty of different legal jurisdictions: In all likelihood the fraudster and the banking customer will also be in different legal jurisdictions. There may be little or no opportunity to prosecute the fraudsters even if their identity is known.
The obscuration of technology: The Internet banking customer has no way of distinguishing a reasonable administrative request. The arbitrary requirements of technology are rarely understandable, so a customer can only guess whether an e-mail requesting action is valid.

The weakness of security as an add-on: In the phishing scenario, the customers have done several things right. They have not necessarily used a weak password that could be guessed, they have not given it to anyone, they have promptly responded to a security alert (although a bogus one). Further strengthening of password, computer, or operating system security won't help in this case.

A variation of this phishing attack was launched against a major Australia bank in mid-2006. Sherriff (2006) reports that the attack caught more than 1,000 victims. It began with an e-mail claiming that the bank was bankrupt, and invited customers to a link for more information. Those who followed the link received a hostile program, which monitored the next attempt made to log on to the bank’s site. When the customer tried to log on, it launched a fake bank pop-up window that captured the customer’s details. In this case the customer’s ignorance of Internet technology is combined with susceptibility to non-technology rumors (believing that a major bank could unexpectedly fail).

Schneier (2000) describes phishing-type attacks as early as 1993 (although the specific phishing phenomenon emerged after this work was published). He classifies this type of attack on security as social engineering. The Internet’s architecture makes it very easy for someone in a distant part of the world to imitate a legitimate bank, and even in 2006 moderately difficult to get such a site closed down. This is a typical sign that security has been included after the Internet was created. It is not a core feature of the Internet’s architecture, as described earlier. The phishing attack appeared after nearly a decade of Internet security add-ons. Unlike a security fault in hardware or software, which can be rectified, this security vulnerability reflects the inherently poor support that the Internet provides to financial transactions.

Addressing these risks

While the Internet architecture described above has existed at least since the early 1980s, the rise of on-line banking has can be located in the late 1990s. Since then a significant proportion of all banking transactions have moved to the Internet. From both a customer and a bank perspective it is unrealistic to expect this trend to reverse. This creates a challenge for both parties: how to minimise risk in an inherently high risk environment.

In my research I identified three factors required for profitable investment in Internet-related services (Adamson 2004):

1. Be guided by the way users currently use the Internet.
2. Don’t try to stretch the Internet to do what its technical architecture doesn’t support.
3. In order to profit from its investments a company also needs to achieve some sustainable competitive advantage, that is, to provide a product or service that its competitors cannot easily duplicate.

In relation to security, because most banks offered on-line banking services at a similar time, there was little opportunity for any single bank to meet the third requirement for profitability, by winning customers from other banks not offering the convenience of on-line banking. Nevertheless, the two other rules are relevant to this discussion.

The first rule means that in using on-line methods to provide financial services or to encourage financial literacy, we should be using tools that the user is familiar with (such as the web browser). We should minimise the add-ons or other demands made on the user. We should even encourage the user to be an educated sceptic. For example, whenever we propose an on-line tool we should consider how such an approach could be corrupted. UK police are currently e-mailing victims of identity theft warning them that they are at risk (BBC News 2006). I suggest that this is a poor approach, as the more people come to believe them, the more difficult it will be when a new generation of phishing attacks pretends to be from positions of authority such as the police or tax office, as well as commercial organisations.

The second rule suggests that while all security presents an imposition on users, some are less helpful than others. For example, we shouldn’t expect a user to understand that when they see a ‘padlock’ on their screen they should right-mouse-click on it to determine whether communication between the user and the web site is 128-bit rather than 40-bit encrypted. We know that the average user would make no sense of this suggestion at all. This puts a burden on providers of on-line financial services or financial literacy campaigns to have a realistic expectation of the technology-customer relationship.
Conclusion

Technology continues to transform the way that customers use financial services. The nature of this transformation, however, will not necessarily match the expectation of the financial services institution. Customers have been seen to adopt lower cost channels such as phone banking and ATMs, but without giving up the higher cost branch channel.

While technology in general is an unpredictable tool for changing customer habits, the Internet adds a new level of unpredictability. In 2006, a decade after the commercialisation of the Internet, banking customers continue to be vulnerable, in this case to phishing attacks. This reflects one weakness of the Internet as a transactional medium, the inability to identify a commercial partner in a transaction. This is one of several weaknesses that the Internet displays as a transactional medium.

Any approach to address complex financial services usage challenges based on the Internet and its existing architecture will similarly have to take these limitations into account. It will also need to acknowledge the very limited success achieved by attempts to modify the Internet’s underlying architecture to make it more suitable for financial transactions over the past decade.

Finally, in designing financial services and projects to assist financial literacy, financial service organisations will need to match their activities to both the actual usage habits of on-line users, and to the technical limitations of this new and immensely popular communication medium.

Bibliography