hoped to obtain additional funding to extend the project after its close in July 2002, to appraise and add to the database collections outside academia and the national libraries. Such libraries include the Inns of Court, Government departments, the Public Record Office and major public libraries. Also, the project needs to move to a further phase envisaged by the project partner libraries: the use of the database to draw up a national collection development strategy for foreign, international and comparative law.

In addition, if funding can be obtained there are several additional databases that could be built, to aid interrogation of FLAG and foreign law research generally. First, a series of brief descriptions of the law literature of each country could be compiled, to assist users identify the types of legal material appropriate to their research needs and, second, a searchable, world list of citation abbreviations.

With the addition of these features, FLAG has the potential to become a major foreign law hub on the Internet, of value to law researchers not only in the UK but worldwide.

Peter Clinch
Project Manager, Foreign Law Guide (FLAG) Project
(Peter.Clinch@sas.ac.uk)

E-banking and authentication

by Stephen Mason

Steven Mason

As the result of the commercial use of the Internet, large numbers of commentators discuss the need to authenticate the identity of an individual or a transaction. Whilst this article will consider what is meant by authentication, the author has reached the conclusion that it will always be difficult to ascertain the true identity of a person who uses the Internet for banking.

Authentication is the process by which a person or legal entity seeks to verify the validity or genuineness of a particular piece of information. In certain circumstances, there is a need to verify the identity of an individual or legal entity. Discussions relating to authentication over the Internet have failed to grasp that a bank cannot verify the identity of an individual or legal entity over the Internet with any certainty. At best, a bank must put sufficient safeguards in place to reduce the risk of dealing with somebody other than their customer over the Internet.

AUTHENTICATION FOR A PURPOSE

It is not always necessary to establish the identity of a person or legal entity for a transaction to take place. Providing both parties to the barter are happy to buy and sell a product or service using a trusted means of exchange, both buyer and seller will part, comfortable that each has reached an amicable bargain. It may be that neither party to the trade will wish, or need, to meet again.

However, if something goes wrong with the transaction for any reason, one party may wish to pursue the other to resolve the matter. Depending on the nature of the dispute and what action the complaining party intends to take to seek a remedy, it may be necessary to establish the identity of the party causing the problem.

An everyday example: validating the means of exchange

When we deal directly with other people, the need to authenticate the identity of the other party depends on a number of factors, including the nature of the goods or services sold and any legal or regulatory requirements. Where there is no requirement or need to authenticate the identity of a person or legal entity, both the buyer and the seller assess the risk involved with the transaction. For instance, a buyer may decide to purchase a DVD on a Saturday market stall. If the buyer knows the trader from whom they intend to buy the DVD, a certain level of trust will already exist between the two. As a result, any transaction that takes place will be founded on mutual recognition and the knowledge by both parties that if something goes wrong, each knows how to contact the other to effect a remedy.

However, where the buyer is passing through a town and is unlikely to make a return visit, the potential buyer takes different factors into account than the local buyer. An outsider will use what intuition their life experience has taught them to assess whether to trust each seller in the market. In this set of circumstances, it is unlikely that the transient buyer is concerned about authenticating the identity of any of the store holders. The buyer will evaluate the physical signals they observe about the seller of DVDs. Their response, and whether to trust the seller, will be one part of the process in deciding to buy. Another consideration will be the potential loss they may suffer if they buy a DVD that does not work. If the buyer considers it is worth taking the risk, because the likely loss is negligible, then they may buy from the unknown seller if the other signals they have processed establish the seller is to be trusted.

Similarly, the seller, if they do not know the identity of the buyer, will enter the transaction if the medium of exchange is to be trusted. Whether the buyer pays in cash or by way of a cheque or credit card, the buyer is able to carry out a procedure that goes some way to establishing the authenticity of the medium of exchange.

Cash

If cash is proffered, tests of look and feel help to establish the genuineness of the notes and coins proffered. It may be the seller also uses a device to check whether paper money is legitimate or a forgery.

Cheque

Where a cheque is offered, certain formalities are required to guarantee payment of the amount written on the cheque by the issuing bank:

- the buyer writes the correct date, the amount in figures and numerals and signs the cheque with their manuscript signature in the presence of the seller, and
- the seller writes down the unique number on the reverse of the cheque (which is found on the cheque guarantee card that in turn corresponds to the bank account as printed on the face of the cheque), ensures the information written by the seller on the cheque is correct and compares the signature on the cheque guarantee card against the signature written by the buyer in the presence of the seller.

Once these formalities are satisfactorily completed, the seller can rest assured that in normal circumstances, the issuing bank will honour the cheque and cause the seller's bank account to be credited with the amount on the cheque.

Credit card

A credit card is dealt with slightly differently, in that the credit card is processed either through an electronic authentication system, or a copy of the information on the credit card is transferred to a paper record of the transaction by an impression. In both instances, a paper record is created and signed by the buyer, acknowledging receipt of goods to the value printed recorded.

The buyer is required to compare the signature on the paper record to that on the reverse of the credit card. Clearly, the method of entering a transaction by means of the electronic authentication system is safer for the seller, because they will be informed in real time if the transaction is not authorised. Where the transaction is by way of an impression of the credit card details on to paper, the seller is obliged to establish, by looking through a list of cancelled credit card numbers, whether this particular credit card has been revoked for some reason.

Whichever method of exchange is used—cash, credit card or cheque—the seller is not identifying the identity of the buyer. They are merely seeking to establish the validity of the means of exchange. The buyer is assumed, in most circumstances, to be the legitimate user of the cheque and cheque guarantee card. However, neither the cheque nor the accompanying cheque guarantee card is evidence that the person in possession of these items is the person whose name appears on the documents.

AUTHENTICATING THE CUSTOMER FOR THE FIRST TIME

Before opening a bank account for a person or legal entity, the bank demands the future customer provides a certain number of documents to authenticate their identity. The range of documentary evidence required to open an account is usually sufficient to establish the identity of the person or legal entity with some certainty. Whilst a small percentage of customers will succeed in opening an account under a false identity with intent to defraud, by constantly monitoring accounts, banks can reduce their exposure in such circumstances.

Risks with the Internet

Using the Internet is risky. The specification for the internet was simple: if a command to launch a nuclear weapon was issued, it was to reach its destination, no matter how much damage had occurred to the infrastructure. The taxpayer paid for an excellent 'open' system. However, an open system means anybody can use it, and some very clever people have used various methods to disrupt commercial activities on the Internet.

- Hackers can impersonate a legitimate customer by obtaining their account number, password, personal identification number and e-mail address by various means, including the use of a sniffer, which is a device that eavesdrops on telecommunications traffic, capturing information as it moves over the Internet.
- It is possible for a third party to direct visitors to a ghost web site, which is an exact replica of the web site the visitor thinks they have visited. A ghost web site is set up

to obtain information from visitors - from credit card details to names and addresses. The aim is to obtain sufficient information relating to the identity of an individual to use it improperly.

- Alternatively, having visited a legitimate web site, the visitor may decide to enter a contract for goods or services and pay by entering number of the their credit online. It is possible, at this point in the process, for the seller to provide information that can be intercepted by a third party as it is transmitted to the buyer.

The Financial Services Authority (FSA) have listed a number of other risks in their discussion paper 'The FSA's approach to the regulation of e-commerce', dated June 2001, at paragraph 5.5. Further discussion on this topic is also provided in the Basel Committee on Banking Supervision Electronic Banking Group White Paper 'Electronic Banking Risk Management Issues for Bank Supervisors', dated October 2000, page 17 and in an earlier White Paper 'Risk Management for electronic banking and electronic money activities', dated March 1998, 18 - 25. Given the internet is a new medium, new means of assessing the risks for both buyers and sellers must be developed to make the internet a safer place in which to conduct business. This is why the concept of authentication is considered so important in the electronic environment.

DUTIES IMPOSED ON THE ONLINE BANKS

The FSA and the Basel Committee on Banking Supervision have provided advice and guidance to banks that have an online presence. Both organisations emphasise the need to ensure the Board and Management Oversight included people that have the requisite expertise to advise and guide them concerning the proper functioning of their e-banking systems.

In the FSA's discussion paper, mentioned above, the FSA highlighted the advice offered in relation to electronic communications at paragraph 9.51, which quotes a section from the FSA Conduct of Business Sourcebook, COB 1.8.2G states that:

For any electronic communications with a customer, a firm should:

(1) have in place appropriate arrangements, including contingency plans, to ensure the secure transmission and receipt of the communication. It should also be able to verify the authenticity and integrity of the communication. The arrangements should be proportionate and take into account the different levels of risk in a firm's business;

(2) be able to demonstrate that the customer wishes to communicate using this form of media; and

(3) if entering into an agreement, make it clear to the customer that a contractual relationship is created that had legal consequences.

The Basel Committee on Banking Supervision, in its May 2001 paper 'Risk Management Principles for Electronic Banking', also raised this issue in discussing what issues are to be included in relation to Principle 4, that 'banks should take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business over the internet'. The comment to Principle 4 indicated that it is *essential* for banks to confirm that a particular communication, transaction or request for access is legitimate. The commentary goes on to state that the bank should use reliable methods to authenticate the identity and authorisation of established customers that wish to initiate transactions electronically.

Both the FSA's approach and the views of the Basel Committee on Banking Supervision seek to establish a very high duty on banks in relation to online banking. It is suggested that no system that is used by banks for online transactions can clearly identify a customer nor authenticate the authorisation of a customer. At best, a bank can use methods that help to establish the *probability* that they are dealing with a customer over the Internet, although in the normal course of events, it is possible to say with some certainty that most of the transactions entered over the Internet will be with customers of the bank.

However, there is a possibility that the bank may be dealing with somebody other than a customer. This is why it is important for an online bank to evaluate the risks and put into place sufficient safeguards to satisfy it that it can be sure that the risk of dealing with somebody other than the customer is low.

ELECTRONIC AUTHENTICATION

Various means can be used to aid the process of authentication over the Internet, but none of them will work properly unless both parties to a transaction take the same care in assessing the risks that attend their use of the Internet. Whilst there are problems with the various methods of reducing risk, providing the level of authentication is adequate for the purpose of minimising the risk, a particular method or combination of methods can be sufficient in a given set of circumstances:

- Encryption helps to ensure information is transferred without being read by a third party. However, there are serious problems with this method if the bank wishes to encourage the customer to have a means of encryption on their computer. It may be that the customer wishes to obtain access to their account from a computer other than the one on which the encryption software is based. There are a host of other technical issues that make encryption problematic, and are dealt with more fully in the author's article 'Electronic Signatures in the EU and world e-commerce: technical and legal ramifications', *Computers and Law*, December 1999/January 2000, Volume 10, Issue 5, 37 - 44; electronic version: http://www.itsecurity.com/papers/digsig.htm.

- The use of electronic signatures can verify the identity of the sender (see paragraphs 9.16 to 9.27 of the FSA Paper for a short discussion of electronic signatures), however, there are serious issues relating to electronic signatures that need to be addressed by the bank if this route is chosen. See the author's paper 'The evidential issues relating to electronic signatures', published in the April/May 2002 edition of *The Computer Law and Security Report*.
- Passwords and user identification codes can provide access to protected areas of a web site. Relying on passwords alone can be very dangerous, because hackers more easily obtain them than any other form of identification.
- Tokens and biometrics can be used on their own or in conjunction with one or more of the above methods, although biometrics (for instance, scans of the face, iris, hand and voice) is difficult to implement at present.

Each method is flawed and is susceptible to misuse and interception. Most attempts at authentication used on the Internet do not, however, verify the identity of an individual. In many cases, even when credit card numbers are encrypted, the aim is to ensure the credit card number is transferred safely over the Internet, not to link the use of the credit card number with the authorised user. Similarly, a user may be given a password to enter a web site or part of a web site, but the use of the password does not prove that the authorised user has used the password to gain entry.

OBLIGATIONS AND LIABILITIES OF THE PARTIES

The European Union has also drawn up a Commission Recommendation in relation to online banking: 97/489/EC dated 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder (*Official Journal L* 208,. 02/08/197 P 0052-0058). This Recommendation provides, in Article 8, for the liability of the online bank in e-banking transactions. Section III provides for the obligations and liabilities of the parties to a contract for online banking. The customer is required to:

- take all reasonable steps to keep the electronic payment instrument safe, together with the means (such as a personal identification number or other code) which enable it to be used
- notify the bank without delay after becoming aware of loss or theft of the electronic payment instrument or the means which enable it to be used
- inform the bank of unauthorised transactions on their online account
- inform the bank of errors or other irregularities that occur with the account.

The liability of the customer, up to the time they inform the bank of any problem, is a maximum of ECU 150, except where the customer has acted with *extreme* negligence in undertaking their duties, or they act fraudulently. That the negligent act or omission must be extreme suggests the imposition of a lower duty of care. One area in which a customer may not be considered to be negligent is where, for instance, they do not have high quality security measures in place to prevent a hacker placing a Trojan horse on their system.

By the terms of Article 6(3), the customer is not liable where the payment instrument has been used without electronic identification. Interestingly, the use of a confidential code or other similar proof of identity on its own is not deemed to impose liability on the customer.

The burden of proof falls on the bank under Article 7(2)(e) to show the transaction was accurately recorded and entered into accounts and was not affected by any technical breakdown or other deficiency. Whilst an online bank may be able to establish evidence to prove the accurate recording of transactions, and that there was no other problem, a customer may still have the upper hand. For instance, it may be that the customer can demonstrate that they could not afford (because its cost was disproportionate to the benefits) a sufficiently adequate security system to prevent hackers placing Trojan horses on their computer. If this is so, the customer (especially if a consumer), only needs to establish this lack of security on their computer to demonstrate under this same Article 7(2)(e) that the problem may be been caused by some 'other deficiency' - to whit, that they did not have sufficient security on their system to prevent a hacker placing a Trojan horse on their computer which subsequently permits the hacker to gain unauthorised access to the user's online bank account for fraudulent means.

The author suggests that, at present, online banks cannot achieve the requirements demanded by the FSA or the Basel Committee on Banking Supervision. Both institutions demand the online bank to identify the customer and authenticate the authorisation of a customer. As far as the author is aware, no online bank can achieve such certainty with the technology that is available at present. At best, online banks can assess the risks, evaluate the different types of authentication available on the market, and monitor the customer's accounts closely to identify any irregularities (such as attempts at fraud, money laundering and the like) at an early stage.

Stephen Mason

The author is a barrister specialising in e-risks, e-business, data protection, interception of communications and commercial law. To contact him, send e-mail to stephenmason@stephenmason.co.uk.

He is presently in the process of setting up a new company, Pario Communications Limited, bringing IT and the law together.