ELECTRONIC COMMERCE:

WHO CARRIES THE RISK OF FRAUD?

Nicholas Bohm, *Solicitor*
Ian Brown, *University College, London*
Brian Gladman, *Information Security Consultant*

The authors gratefully acknowledge the help they have received from
Ross Anderson, Richard Clayton, Gilead Cooper, Alex Hamilton and Peter Landrock
in comments on earlier drafts.

This article was published on 31st October 2000 by
The Journal of Information, Law & Technology
http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/

Foundation for Information Policy Research

February 2000

ELECTRONIC COMMERCE: WHO CARRIES THE RISK OF FRAUD?

Introduction

1 Much debate about the risk of fraud in electronic commerce takes place without any clear understanding about who bears the corresponding risk in conventional commercial transactions. This paper examines risk in the banking transactions which underpin much of commerce, whether electronic or conventional. We compare traditional transactions such as payments by cheque or credit card with the use of newer remote voice and data systems. We then analyse who bears the risk of fraud, and explore measures used or needed to reduce it. We argue that the approach taken by banks is unfair to their customers in some cases, fails to encourage the development of adequate security measures, and prevents the banking system from playing its proper part in the development of electronic commerce in the United Kingdom. Our analysis is based on English law except where otherwise stated: the law of other jurisdictions may not be the same.

2 Electronic commerce includes electronic transactions between commercial and industrial companies, often using structured data, and not necessarily involving payments. Although the analysis in this paper can be applied to electronic commerce of that kind, we are concerned primarily with the two main other kinds of electronic commerce: electronic shopping with credit and debit cards, and online banking.

Forged cheques

3 If your bank debits your account with payment of a cheque that you did not sign, it has no authority for the debit it has applied and must credit your account with the amount charged. The quality of the forgery and care taken by the bank are irrelevant: a cheque is a bill of exchange, and under section 24 of the Bills of Exchange Act 1882,

> "... where a signature on a bill is forged ... , the forged ... signature is wholly inoperative, and no right to retain the bill or to give a discharge therefor or to enforce payment thereof against any party thereto can be acquired through or under that signature, unless the party against whom it is sought to retain or enforce payment of the bill is precluded from setting up the forgery ... . "

4 The Bills of Exchange Act 1882 did not introduce new law. It codified the contemporary common law, and reflected the more general rule which still prevails in English law. This rule is that if someone wishes to enforce a document against you on the basis that you are bound by it because you signed it, and if you deny that you signed it, then it for them to prove that the signature it bears was made or authorised by you, and not for you to prove that it was not. (The reference in section 24 to a party being "precluded from setting up the forgery" is a reference to

circumstances where someone who did not in fact make a signature is nevertheless bound by it under the doctrine of estoppel. An example is a case where a customer fails to protest that his signature has been forged on a cheque, because it was forged by a member of his family, for example: he will not be allowed to reject a later cheque where his signature has been forged by the same person, as his conduct has led the bank to believe that the signature is genuine.)

5 Banks might wish to offer current account services on the basis that they would take reasonable care to verify their customers' signatures, but that the customer would carry the risk of clever forgeries. In some legal systems that alternative rule may apply, but in England and Wales it is precluded by the plain terms of section 24 of the Bills of Exchange Act.

6 An obvious advantage of the existing rule is that the bank can decide for itself (at its own risk) what level of care to apply to signature verification. Items of small value will not usually be checked at all, but unusual or very large items may be checked not only by careful inspection of the signature and comparison with a specimen card, but also by alternative means such as a telephone call to the customer.

7 If the bank rejects a cheque presented for payment by the forger, nobody suffers an unfair loss. But if the forged cheque is presented by a merchant who has accepted it from the forger in exchange for goods or services, the merchant suffers the loss despite having had no means of attempting to verify the genuineness of the signature. For many years, merchants either accepted that risk or declined to take cheques. Cheque fraud led more and more merchants to refuse to take cheques, which annoyed bank customers and cut into the banks' fee income. The banks therefore introduced the use of cheque guarantee cards covering cheques up to a modest limit (£50 when introduced in 1965 and now more usually £100 or £250). The effect was to transfer the risk of small forgeries from the merchant to the bank: the banks could be seen as delegating to the merchant the signature verification process (using the signature on the card for comparison) in relation to smaller amounts (where they might themselves already apply little or no care to verification checks).

8 Although the rule that the bank bears the risk of forgery is plain, it does not follow that customers can easily reject any debit to their account based on a cheque simply by claiming that it is a forgery. Although some forgeries are crude enough to be obvious to anyone, others are considerably more skilful. If the bank produces a cheque bearing a signature which even on close inspection is indistinguishable from the customer's signature, perhaps supported by the evidence of a professional document examiner, then the customer cannot expect to succeed by mere

unsupported denial. The customer will in effect have to rebut the evidence produced by the bank, and may in some cases be unsuccessful in doing so even though the signature is indeed a forgery.

9 To make this point does not amount to exposing some fundamental flaw in procedures that rely on signatures: it merely shows, as is evident to common sense, that those procedures are not perfect. Controlled trials show that professional document examiners misattribute 6.5% of documents while untrained persons of comparable educational attainment perform much worse with a mismatch rate of 38.3% [Kam97, Kam98]. Indeed, examiners assert that forged signatures are almost always easy to distinguish from genuine ones on close examination, however convincing they may be on casual inspection [Harrison58].

10 Forensic examination is not limited to naked eye examination of the image of the signature. It may be enlarged, examined using optical, electron and ion microscopes, and subjected to a variety of chemical analyses. These may detect retouching or even identify the manufacturer and batch number of the ink. But genuine conflicts of experts do still occur, and the sources of error in the document examining art are a continuing topic of research and dispute within that profession. A recent study suggests that examiners' mistakes are largely psychological; people are liable to see what they want to, and even experts may subconsciously select specimens of handwriting from a criminal suspect which match a given handwriting sample [Beck95].

11 It is worth noting that no prospective forger occupies a privileged position: anyone with access to specimens of a customer's signature is well placed to produce a forgery. The bank will always have such specimens, but signatures are not secret: even where a customer uses a distinctive signature for cheques, any recipient of a cheque will thereby obtain a specimen. This proposition does not hold for other cases considered below.

12 Because banks cannot practicably examine all signatures closely enough to detect forgeries which may nevertheless be evident on close examination, and because a minority of forgeries are so good that they cannot be detected at all, we conclude that they run real risks (and indeed incur real costs) from forgery of cheques and other written instructions. Acceptance of these risks and costs has not proved a major impediment to UK current account banking as a business. We suggest that this conclusion should be used as a point of comparison for the acceptability of the corresponding risks in other forms of banking and payment transactions discussed below.

Credit and debit card liability rules

13 Credit and debit cards came into common use in the United States in the late 1950s, and were introduced in the UK by Barclays Bank in 1966. Their use expanded very rapidly in the 1980s, perhaps stimulated by the growing disparity between the amounts for which cards could be used and the more modest amounts covered by cheque guarantee cards.

14 Card transactions do not involve cheques, with the result that section 24 of the Bills of Exchange Act 1882 does not apply. Card issuers (referred to here for convenience as banks) are therefore free to apply different rules from those governing the risk of forgery of cheques, and the rules embodied in the terms and conditions on which they issue credit and debit cards are indeed different. (In some circumstances the voucher signed by the customer might in law be a cheque, with the result that section 24 of the Act would override the contractual rules; but we are not aware of any case where this has been argued.)

15 Although banks' terms vary in their details, the general rule is that the customer is responsible for (a) all transactions carried out by the use of the card with the customer's authority, and (b) for all other (i.e. fraudulent) transactions carried out by the use of the card, up to a limit of £50. This limited liability for fraudulent transactions ceases when the customer informs the bank that the card has been lost or stolen. These rules reflect the provisions of sections 84 and 171 of the Consumer Credit Act 1974 and the regulations made under it relating to credit cards.

16 By comparison with the case of cheque forgery, this régime transfers to the customer a limited part of the risk of fraudulent use of the customer's card. Such use of the card depends on physical possession of the card, however, and the customer can reduce the risk by taking good care of the card and by promptly reporting its loss. Taking care of articles like cards or keys is largely a matter of common sense (to be contrasted with the precautions required to protect electronic systems, as discussed below). The £50 exposure can be seen as providing an incentive to the customer to take care of the card and report its loss promptly.

17 The balance of the risk that is not carried by the customer is borne by the bank or the merchant. The terms governing the relationship between the merchant and the bank determine this allocation. Where the cardholder is present at the transaction, and where the merchant has not been plainly careless in accepting a non-conforming signature, and has complied with limits on the amount of an individual transaction and other applicable rules, the bank normally carries the risk. Merchants therefore have an incentive to take appropriate care in accepting card transactions, but are

guaranteed payment by the bank if proper care has been taken, just as if they had accepted a cheque with a cheque guarantee card (and with the advantage that much higher amounts can be covered).

18 This analysis deliberately ignores the rôle of banks acting as card transaction acquirers, who function as financial intermediaries between the merchant and the card issuing bank, because in considering where risk falls as between customer, merchant and the banking system, it is immaterial which component of the banking system is involved.

19 It is clear from this discussion that possession of the relevant card plays a substantial role in authenticating a card transaction, and that signature verification is much less significant than in the case of cheques. This conclusion is supported by the fact that in the UK signatures are usually made on multi-part forms, with the customer retaining the top copy. In any subsequent dispute, the copy or copies of any voucher available for expert examination will bear only "carbon" copies of the customer's (or alleged customer's) signature. Forgeries are an order of magnitude more difficult to detect from carbon copies.

20 Cards may also be used in transactions where the cardholder and the merchant do not meet, and no voucher may be signed. Examples are the use of a card for mail orders, by telephone, by electronic mail or through a web page. (Such transactions are classified as "cardholder not present" or sometimes as "MO/TO", meaning "mail order or telephone order". We refer to them for simplicity as remote card transactions.) The incidence of risk in remote card transactions is quite different from that where the card is presented by the customer to the merchant.

21 In a remote card transaction, the customer provides the merchant with information apparent from the face of the card: its type (typically Visa or Mastercard), its number, its expiry date and the name of the cardholder. (Except in the case of mail order, the customer provides no signature; and in mail order the merchant cannot compare the signature with that on the card.) The ability of the customer to provide the card information does not depend on possession of the card: it is available to anyone through whose hands the card has passed in the course of earlier transactions, perhaps to the cardholder's family and friends, and to anyone who may have received or intercepted the information as it was transmitted by telephone or through the Internet. (It would not be difficult to establish a website purely for the purpose of obtaining cardholder information, by offering transactions at favourable prices which the site owner has no intention of concluding.)

22 Where the purpose of a remote card transaction is to order goods for delivery, the merchant may be able to check the address of the cardholder through the bank, and can decline to deliver the goods except to that address. Where available this procedure provides some protection from fraudulently placed orders (except for goods ordered as third party gifts, like flowers, where this procedure cannot be followed; but such cases are usually of comparatively small value). Where the order is for online services, however, such as the downloading of software or the provision of access to online databases, no such precaution can be taken. In these cases there is very little impediment to fraud (either by the customer falsely repudiating a genuine transaction, or by an imposter using the customer's card details without authority). (We have disregarded the process of "authorisation", where a merchant complies with a requirement to check with the bank whether a transaction may proceed. The reason is that while this process enables the bank to check that the customer has not reported the card stolen or is not exceeding a credit limit, for example, it does not enable the bank to check that the card information is being used by the customer rather than an imposter. It does not guarantee payment where the customer is not present at the transaction, and therefore does not alter the balance of the risks under discussion.)

23 The liability régime is simple, although its implications do not seem to be widely understood. If the cardholder denies having entered into a remote card transaction in which the relevant card information was provided, and there is no evidence of delivery of goods to the customer or voucher signed by the customer, the bank has no basis on which to debit the customer's account. The mere use of the card information is not enough to show that the customer authorised the transaction, because of the wide class of other persons to whom the information is available. Merchants are of course members of that wide class, possessing card information in abundance: for the merchant, "forgery" of a remote card transaction is a trivial task. Faced with apparently unmanageable risks of this kind, the banks have adopted the simple approach of requiring the merchants to carry the risk. If a cardholder repudiates a remote card transaction for which there is no evidence of delivery of goods to the customer, or voucher signed by the customer, the bank makes a "chargeback", i.e. obtains reimbursement from the merchant of anything paid to the merchant in respect of the transaction (and may also make an administrative charge). The merchant is in practice unable to transfer this risk to anyone else, since he is unlikely to be able to prove who initiated the relevant transaction.

24 The banks naturally appreciate the perilous position in which this régime places the merchants. They are sometimes unhelpful to cardholders who repudiate remote transactions, by refusing to reverse the repudiated debit and responding that the cardholder must resolve the dispute with the merchant; but they are aware that this

stance is unsustainable where the cardholder denies having participated in any transaction with the merchant, and in the face of persistence by the cardholder they will accept that the transaction must be reversed. (This is not to say that customers face no problems: in some cases they have required considerable persistence in the face of evasions, and faced long delays; in others they have suffered foreign exchange losses where debit and credit of the same amount in foreign currency has left them with a shortfall.)

25 The greatest risk to the merchant obviously arises from the provision of online services. Although this is not a new risk, the merchant's risk from fraud has therefore been highlighted by the growth in commerce carried out over the Internet. Although online services can be provided in response to a telephone card transaction (by the supply of information, for example), the range of services which can be provided online has expanded greatly with the commercialisation of the Internet. The problem of managing the resulting risks for merchants may well prove to be a growing impediment to the growth of electronic commerce in online services.

26 For transactions carried out by the cardholder using a web browser to connect to a supplier's web page, it is possible to establish a secure connection so that the card information is delivered in encrypted form (using protocols such as TLS or SSL [Dierks99]). This procedure is widely followed, and provides some welcome protection against interception of the card information in transit. It cannot affect the wide availability of card information from other sources, and since the procedure cannot provide evidence that the supplier of the card information is authorised by the cardholder to conclude the transaction, it does not materially reduce the merchant's risk.

27 Visa and Mastercard have promulgated a standard for Secure Electronic Transactions, referred to as "SET" [SET99]. It would enable the merchant to check that the bank will accept the cardholder's authority as genuine, and would thereby presumably remove the risk from the merchant, or at least reduce it. The SET standard has not gained acceptance, perhaps because it is over elaborate and its implementation would be burdensome and expensive. The SET specifications do not deal with the legal régime covering relations between the bank, the merchant and the customer, presumably because this is a matter for individual banks and because the existing régime is expected to continue to apply. If the merchant's risk of chargeback is to be removed or reduced by treating the customer as present in a SET transaction, it therefore seems probable that the customer will be precluded from repudiating a SET transaction which appears to have been authorised by that customer. But the risk to the customer of losing control of the means of authorising SET transactions

(which consists of information stored in electronic form) is very different from the risk of losing a plastic card, as we explain below.

28 With the spread of availability of strong cryptographic products and services outside the United States, and the possibility of a single market in the European Union in such products and services, the banks will need to revisit these liability and security issues. Small and medium sized enterprises are among those which can derive the greatest benefit from access to selling over the Internet, but can least afford exposure to the risks which remote card transactions place on merchants. Provision of online services is one of the most effective uses of the Internet for electronic commerce, and is a valuable sector for just such enterprises, but when payment is made through existing card systems it attracts the greatest risk to merchants.

29 As electronic commerce grows, and merchants experience increasing levels of chargeback from the use of conventional card information in the new electronic medium, it is likely that there will be growing pressure from merchants for the adoption of procedures to lessen their exposure. But for the reasons explored below, any temptation for the banks to use the adoption of new technical security procedures to transfer those risks from the merchant to the customer should be sternly resisted, not only in the interest of the customers but in the wider interest of public confidence in electronic commerce.

30 Some card transactions in the United Kingdom have the benefit of section 74 of the Consumer Credit Act 1975, with the result that if the merchant defaults on his obligations to the customer, the bank is jointly liable for the default with the merchant. This is an extremely important protection for the consumer, especially given the difficulty for the consumer of knowing who he or she is dealing with on the Internet. Its extension to all card transactions, and the removal of doubts about its applicability to transactions with overseas merchants, where the Government and the banks have expressed opposite views, would do much to give consumers justified confidence in electronic commerce. But merchant default of this kind is not fraud in the sense under discussion in this paper.

Cash dispensers and telephone or online banking

31 We began by examining how the risk of cheque forgery is shared as between bank and customer, and proceeded to show that in card transactions a limited part of the corresponding risk is carried by the customer, with the balance being carried by either the bank or the merchant, depending whether the customer is present in the transaction. We now apply the same analysis to banking transactions carried out through a cash dispenser (often called an "ATM", from "Automated Teller

Machine"), by telephone or by electronic access to the banking system (either by dialling directly into the bank's system, usually called "PC banking", or through a web page or other form of access over the Internet, called "Internet banking").

32 The cost to a bank of carrying out a transaction varies very greatly, depending on how the customer gives the necessary instructions. This is shown in the following table, which is based on a 1996 Booz-Allen & Hamilton survey of North American financial institutions with Web sites, quoted in *The Emerging Digital Economy* published in 1998 by the U.S. Department of Commerce:

Branch	$1.07
Telephone	$0.52
Automated Teller Machine	$0.27
PC banking	$0.015
Internet banking	$0.01

The trend of these figures is unsurprising, although their relative disparity is nevertheless striking, and may well have increased since 1996. They help to explain the prevalence of telephone banking and foreshadow the probable growth in online banking (by which we mean both PC banking and Internet banking). There are signs that market pressures are causing the banks to share with their customers at least some of the cost savings involved, as evidenced by the higher interest rates available on some accounts which are accessible only by online electronic means. But neither consumers nor the media have yet paid much attention to the changes in the allocation of fraud risks between bank and customer which have in some cases accompanied the shift to telephone and online banking, with their different procedures for authorising transactions.

33 In the case of a cheque, the signature is the primary means of verifying that the transaction is authorised by the customer. In the case of a card transaction where the customer is present, signature has a less important rôle, and may be thought to have become secondary to possession of the card. In the case of cash dispensers and telephone and online banking, however, conventional signatures play no part at all, and there is no merchant to take the risk because the transaction is directly between the customer and the bank. The banks have responded with the introduction of alternative security procedures and a different approach to the allocation of risks between themselves and their customers.

Cash dispensers

34 Cash dispensers are typically operated by cards authenticated by a four digit personal identification number ("PIN"). A card and its related PIN are sent to the customer by post on separate occasions. The customer can usually alter the number to one of choice. The banks adopt a variety of technical and procedural methods to limit the number of bank staff who can obtain undetected access to a customer's PIN; but in order for the bank's system to respond correctly to the customer's use of the PIN in a dispenser, it must in principle be able to distinguish a correct PIN from an incorrect one, and so the bank must know the PIN or some value derived from it.

35 Although different banks' terms vary in their details, the general rule for the use of cards in cash dispensers is the same as the rule for card transactions when the customer is present, namely that the customer is responsible for (a) all transactions carried out by the use of the card with the customer's authority, and (b) for all other (i.e. fraudulent) transactions carried out by the use of the card, up to a limit of £50. This limited liability for fraudulent transactions ceases when the customer informs the bank that the card has been lost or stolen. These rules reflect the provisions of the Consumer Credit Act 1974 relating to credit cards, and also the policy of *The Banking Code* adopted in its current form in September 2000 by the British Bankers' Association, the Building Societies' Association and the Association of Payment Clearing Services.

36 However, the limitation of the customer's liability for fraudulent transactions to £50 typically does not apply where the customer has been "grossly negligent". This expression does not have a standard legal meaning, and is defined in the banks' individual terms. The wider the definition, the more easily the customer can lose the benefit of the £50 limit. Cases where the customer will be regarded as grossly negligent are normally defined as including:

- failing to take all available steps to keep the card and the PIN safe at all times
- writing the PIN on the card or anything usually kept with it
- writing the PIN down without disguising it
- not destroying the PIN notification receipt.

37 Interestingly, the latest revision of *The Banking Code* is in some respects less favourable to the customer than its immediate predecessor published in 1998. It omits the words "without disguising it", so as to prohibit any writing down of a PIN

or other security information, a prohibition rendered impracticable by some bank procedures described below. And the expression "gross negligence" has been replaced by "without reasonable care", which could have the effect of making it easier for the bank to blame the customer for a third party's fraud. It would be unfortunate if banks began making similar revisions to their terms. But the new revision is helpful in acknowledging for the first time that where a customer's card details are used fraudulently but where the card has not been lost or stolen, the customer is not liable for any part of the loss arising from the misuse.

38 The liability régime for cash machines looks very similar to the régime for card transactions where the cardholder is present, but the risks are rather different. The reason is that fraudulent use of a customer's card in a card transaction where the cardholder is present depends on the card having ceased to be in the cardholder's possession, a circumstance which the cardholder can in principle discover and use to terminate risk exposure by notifying the bank. Fraudulent cash dispenser withdrawals which appear to have used the cardholder's card (and cannot be distinguished by the bank from genuine transactions) can be made despite the fact that the card has at all times remained in the cardholder's possession without the cardholder having any reason to notify the bank of its loss.

39 Such withdrawals are possible because the genuineness of the transaction at the cash dispenser can be verified only by technical means, and the implementation of technical methods of verification has often been flawed by technical and procedural weaknesses. These weaknesses have been discussed in some detail by Ross Anderson of Cambridge University Computer Laboratory in *Why Cryptosystems Fail* and *Liability and Computer Security: Nine Principles* [Anderson93, Anderson94].

40 The unwillingness of the banks to admit the existence of technical weaknesses (including the possibility of a card itself being forged) has the practical effect of depriving the customer of the benefit of the £50 limit. The banks have tended to take the view that all disputed transactions except those which formed part of a series later acknowledged as fraudulent (e.g. after the arrest of a criminal) must have been carried out with the card and PIN issued to the customer, and so must have been due either to fraudulent collusion or to gross negligence.

41 In an otherwise unreported case described in *Liability and Computer Security: Nine Principles* a bank customer, who happened to be a police constable, complained about phantom ATM withdrawals from his account and demanded a refund of the amounts he claimed were wrongly debited to his account. The bank denied that anyone other than he could have made the withdrawals, and he was charged with making fraudulent claims for a refund. He was subsequently tried and convicted of

attempted fraud despite evidence that the bank's accounting system did not meet acceptable security standards in either design or operation. During the trial it emerged that the bank had no security management or quality assurance functions and that the software operating the bank's ATM system was routinely changed as often as twice a week with no independent checking or auditing of such changes or their effect. No proper efforts appeared to have been made by the bank to investigate these or other alleged phantom withdrawals.

42 The police constable customer was suspended as a result of the conviction. He was later reinstated after the conviction was overturned on appeal when the bank refused to provide the defence team with evidence about the operation of their computer systems. Although he was eventually cleared of any wrongdoing, the trauma was obviously severe. This case shows that even where the risks of fraud appear to be carried by the banks, they will sometimes seek to transfer the risk to their customer, with serious consequences for the customer involved.

43 The sums at risk in cases of fraudulent withdrawal are constrained by the limits placed on the customer's individual withdrawal transactions and daily total withdrawals, which has helped to reduce the sums at stake in disputes of this kind. This may be one of the reasons why the appropriateness of the underlying liability régime itself seems to have remained unquestioned. The basis of the régime is considered in greater detail below, following an examination of the treatment of telephone and online banking.

Telephone banking

44 By "telephone banking" we mean a service which the customer can use to give instructions and get information by speaking to bank staff by telephone. (We deal separately with services accessible through the telephone network using a computer.)

45 In one sense, telephone banking is as old as the widespread use of the telephone: some banks have always been willing to accept instructions by telephone from trusted customers well known to them, as part of their ordinary branch banking service. By a gradual process, customers came to be asked "security questions" designed to elicit knowledge likely to be possessed only by the customer, as a means of verifying that the telephone caller was the customer and not an imposter. The content of such questions would be derived from the customer information in the bank's possession, and their scope would not be subject to prior agreement. A customer might be asked the date when the account had been opened, or the customer's previous address or telephone number, or spouse's second forename, for

example. As a further check, banks might also return the customer's call to a telephone number already known to the bank to belong to the customer.

46 With the introduction of telephone banking as a distinct service not tied to a relationship between the customer and an ordinary branch of the bank, practice crystallised into technical and procedural mechanisms, and a distinct liability régime. Customer and bank now usually agree at the outset of the relationship a small category of "security information" to be used to verify the customer's authority to give telephone instructions. This will usually include a password chosen by the customer.

47 The attraction of modern telephone banking to the bank is that it saves the cost of maintaining a branch. One of the attractions to the customer is the availability of the service twenty four hours a day. The inevitable result is that the customer will rarely if ever be known to the individual member of the bank staff who takes the customer's call. Security procedures cannot be based on personal knowledge or derived by common sense from a general body of customer information. Instead, the bank's system may select the security information to be used to verify the session from the previously agreed items provided by the customer, and prompt the staff member with the appropriate questions and the answers to be treated as correct. So the customer may be asked to provide the third, sixth and seventh characters from the agreed password, followed by the make of the customer's first car.

48 These procedures are designed to ensure that most bank staff do not know more than a fragmentary part of the customer's security information, and have something in common with the procedures designed to preserve the secrecy of a customer's PIN for a cash dispenser card. The bank taken as a whole must nevertheless know the customer's security information in order to use it for verification.

49 The procedure for limiting the spread of knowledge of the customer's security information within the bank has the inevitable side effect of encouraging the customer to write that information down. Even people who can remember their password reliably will find difficulty in supplying specific characters chosen at random from its sequence; and an effort to avoid using publicly available information (like a mother's maiden name, found in birth certificates available to all) can lead to the use of esoteric information liable to be forgotten.

50 Also, while it limits the opportunity for fraud by bank staff who deal with customers, it may not eliminate the possibility entirely since there will be situations where a customer may wish to deal with a particular member of the bank's staff for a series of telephone transactions. This is a natural human desire on the part of a customer, and

banks may not wish to frustrate it. But it means that the opportunity then exists for a particular staff member to accumulate a full set of security information for the customer, which could be used to impersonate the customer. Customers are given no information about how this risk is managed.

51 Just as technical and procedural security mechanisms have become formalised on the arrival of telephone banking as a distinct service, so risk allocation has been documented. The terms currently in use tend to cover both telephone banking and online banking where access is provided by computer (whose special characteristics are discussed below). Two distinct trends are emerging.

52 Some banks are using terms closely based on those used for card transactions, so that the customer is bound by fraudulent instructions but liability is limited to £50. Among those adopting this approach are the Co-operative Bank and Lloyds TSB. (The terms of the "first-e" service of the Banque d'Escompte do not make it clear that the customer is bound by fraudulent instructions, but in any event the customer is said to be insured against loss from such instructions, so its service may be considered to fall into the same group.) The terms of the "marbles" service of HFC Bank are of particular interest in limiting the customer's liability to £50 generally, but reducing that limit to zero where fraudulent use occurs over the Internet (so that in this case the bank carries the whole of the risk). The telephone and online terms of First Direct, the telephone banking division of HSBC Bank, provide in clear terms for the bank to carry the whole of the risk of fraudulent use unless the bank can prove that the customer acted fraudulently or with gross negligence (not defined) or failed to observe the required precautions against disclosure of security information. The terms of the Woolwich online service limit the customer's liability for fraudulent use to £50, but among the cases where this limit does not apply is the case where the customer has failed to comply with the terms. One of the terms is that the customer must not keep a written record of the security information used to authenticate transactions. We comment below on the customer's dilemma in the face of such provisions.

53 But other banks provide for the customer to be bound by fraudulent instructions, and provide no limit on the resulting liability. Among those in this group are Prudential Banking plc, the Halifax and the Bank of Scotland. (The banks named are mentioned purely by way of example; and it should be made clear that a customer's liability exposure always ceases once the bank is notified of a compromise of the password or other security information.)

54 A typical unlimited liability approach is found in the published *Banking General Terms and Conditions* of the Egg service provided by Prudential Banking plc, which

are commendable for their lucid and straightforward language. Condition 3 deals with security, and the material terms are as follows (with emphasis added to terms relevant for risk allocation):

> 3.1 We may establish security procedures with you either by post, telephone or Internet (when available). You must keep your security details and password secret. If you make written records of any security details or password, you must disguise them so that they cannot easily be understood by anyone else.
>
> 3.2 You must tell us as soon as possible if:
>
> you think that someone else knows your security details or password;
>
> you have forgotten your security details or password;
>
> you think that someone else (other than a joint account holder or authorised person) is trying to use your account.
>
> *Until you tell us, you will be responsible for any instruction in writing or by telephone or Internet which we receive and act on, even if it was not given by you.* Normally we will pay back into your account the amount of any payments we make after you have told us. But, if we can show that you have acted fraudulently or have been grossly negligent or have not kept your security details and password secret you will be responsible for all payments we make and all losses on your account. We will have no other liability to you.
>
> …
>
> 3.5 We will do all that we reasonably can to prevent unauthorised access to our Internet banking service and make sure that it is secure.
>
> …
>
> 3.8 You will tell us as soon as you can if you find any failure, delay or error in our Internet banking service, especially in the sending or receiving of instructions. *Our records of your Internet instructions will be conclusive unless there is a clear mistake.*

Condition 5, dealing with "taking money out of your accounts", is also relevant (it is again shown with emphasis added to the risk allocation language):

5.1 We can make payments and account transfers on instructions you give us:

by using any card we have provided on your account;

on documents you or an authorised person have signed (but not copies or facsimiles);

by telephone and Internet (when available), subject to our withdrawal limits, as long as we have checked your identity from the security information and passwords *and even if the order was given by someone else using your security information and passwords.*

55 Like the cash dispenser liability régime, this looks rather similar to the card transaction régime. But once again the balance of risk has shifted towards the customer. The most striking difference is that there is no £50 limit. As is clear from Egg clause 3.2, the customer's whole available balance (up to the amount of any applicable withdrawal limits) is at risk. And the customer's protection rests wholly on the secrecy of the security information, without any physical indication (such as loss of a card) to alert the customer to any compromise of the secrecy.

The insecurity of security information

56 For a number of reasons, security information is difficult to protect. Given a requirement for the customer to provide specific characters from a password, it must in practice be written down. If the customer has several accounts with different providers of services, each protected by a password, this presents a further dilemma: if the same password is used in each case, it will be easier to write it down in a form that disguises what it is, while leaving it still usable; but this solution has the drawback that each service provider knows a password that gives access not only to its own services but also to many others. This is very undesirable in security terms, and may be prohibited by some service providers' contractual terms; but the alternative is to choose a different password for each service. Each must be written down in disguised form (if writing is even permitted), but in a form which still leaves the user able to know which service each password relates to. There is a very real risk that the conflict between these opposing requirements will be impossible for many users to reconcile successfully.

57 The problems are multiplied by the need to provide secondary security information, preferably unique for the purposes of each service for which it is required, and preferably not publicly available or generally known to the user's family and friends. It is obvious enough that mother's maiden name, wedding anniversary or names of

the user's children are unsuitable for these purposes; but it is notorious that such information is commonly used for exactly this purpose. Some banks' terms explicitly prohibit the use of vulnerable information of this kind, and require further precautions, such as regular changes of password (which can cause users to choose easy-to-remember but insecure passwords, or to write them down). Such requirements are no doubt well intentioned, but they place an impossible burden of management on the customer who uses a multiplicity of password protected services; and if the consequence of a failure to observe them satisfactorily is the customer's loss of the protection of the £50 limit, as provided in the terms of Lloyds Bank TSB and the Woolwich, the result of a mistake could be extremely harsh.

58 An interesting example of a term which could prove troublesome for customers is found in the card terms of First Direct, the telephone banking division of HSBC Bank. Clause 4.1 of the terms provides that the card may be used:

> …
>
> - to pay for goods and services through the Internet using the "secure session" features, which are included in the current versions of Netscapes and Microsoft browsers enabling you to send card details in encrypted form. The use of the Internet to place orders or make payments with your card is otherwise not permitted.

Although it does not seem that the customer loses the protection of the £50 limit by disregarding this term, customers who take the trouble to read the small print may not find it easy to know whether they are compliant. Many will not know how to detect whether they are in fact using the secure session features of their browser, and unless only the latest versions of the browsers are regarded as "current", it seems difficult to be sure which versions are current for this purpose.

Verification procedures

59 Before we proceed to consider online banking, it may be helpful to highlight the contrast between the use of signatures on cheques or other conventional written documents for verifying the authenticity of banking instructions, and the use of some combination of card, PIN and password or other security information for the same purpose.

60 The procedure for verifying the authenticity of banking instructions by using a PIN, password or other security information falls into the class of procedures based on a shared secret. When the customer uses a PIN, the bank uses its knowledge of the

PIN to check that it is genuine. (The PIN can be obscured from casual observation within banks by encrypting it immediately after input, and this is standard procedure. But the value of this and related techniques is severely constrained by the limited security available in the 10,000 combinations provided by 4 digit PINs.) Such procedures may be contrasted with signature verification, which relies instead on the physiological property that a person can easily make his own signature but cannot easily make another person's signature well enough for a forgery to pass careful examination.

61 People cannot give away their physiological properties, but either of the parties to a shared secret can reveal it to facilitate fraudulent use. Where two parties share a secret whose misuse can cause loss, it might seem remarkable that they should agree that one of them should assume sole responsibility for the loss of the secret. But that is in effect what the banks have expected of their customers: both the bank and customer must know the PIN, the customer to use it and the bank to check it. Both could reveal it to a third party who could misuse it.

62 Banks are of course regulated bodies required to be managed by persons fit and proper for the purpose, and (with occasional spectacular exceptions) do not pursue financial crime as a corporate purpose. But technical security measures are very difficult to design and implement successfully. One of the more notorious weaknesses of commerce and industry in Britain has been its inability to obtain the full potential benefit of information technology through failure to integrate it with other parts of a business. The computer department, even when called the information technology department, is rarely on the career path to the boardroom. Computer specialists, even when employed by banks, are rarely either managers or integrated into the ethos of management. They can easily become impatient of mainstream managers' failure to understand the potential of information technology. Although no less honest than other professional people, computer specialists in banks are particularly vulnerable to the stresses of cultural isolation, low esteem, and the temptation to prove they can outwit the system. These considerations militate against any claim that the culpable disclosure of security information must necessarily be more likely to originate with the customer than with the bank.

63 The use of biometric information to authenticate customer transactions through cash dispensers is seen as an answer to the problem of reliance on shared secrets. Iris recognition is now being tested by the Nationwide Building Society as an alternative to PINs [Hawkes98]. A cash dispenser compares various properties of a card user's iris with a stored record, making it extremely difficult for anyone but the card owner to withdraw money using it. Their system is said to make only one error in 131,000 cases if the probabilities of falsely accepting or rejecting an individual are set equal.

Even this might be an unacceptably high error rate if very large numbers of false attempts were feasible, which is of course not the case where the user must be personally present and the system is operated in the presence of attendants.

64 The risks are different in unattended or remote operation, where a photograph or video of the user's iris might be presented to the camera; and the risks are liable to increase significantly if use becomes widespread in a variety of applications and many businesses come to have databases of customer personal identification and linked iris codes. And it remains the case that anyone with sufficient access to a bank's financial systems may still be able to create false transactions linked to a customer. No doubt banks have procedural mechanisms to limit such risks, but there is no independent evidence by which customers can judge for themselves the effectiveness of such procedures, despite the fact that customers may be expected to rely on them by carrying the risk of fraud.

65 Where the risk to the customer is effectively limited to £50, and where that limited risk can reliably be terminated by notification of the loss of a card, with the bank carrying the balance of the risk of fraudulent transactions, the outcome of the liability régime may seem reasonable enough. But where there is no financial limit, or where fraud can occur without the loss of the card to alert the customer, the outcome seems to us to be decidedly unreasonable.

Security issues

66 We now consider security issues in the context of online banking. Although the liability régime adopted for online banking seems to be based on that for telephone banking, and in most cases the same terms and conditions govern both, the security implications are not the same. The discussion above has drawn attention to the use of a shared secret (usually several shared secrets) for use by the bank to authenticate instructions purporting to come from the customer. It might reasonably be thought that authentication essentially depends on using either biometrics (like handwriting, voice recognition, fingerprints, retinal scans, etc) or shared secrets. This was indeed true until the publication in 1976 of *New Directions in Cryptography* by Martin Hellman & Whitfield Diffie [Diffie76]. That paper, which laid the foundations of public key cryptography, showed that it was possible to establish a procedure by which (transposing it into the context of this paper) customers can control unique, secret "signature" keys for which they can provide related non-secret information that can be used by a bank to verify that instructions issued by them have been signed using these keys. (We refer to this verification information below as a "verification key".) Provided that this scheme is soundly implemented, and that owners keep their signature keys secret and under their own control, transactions

signed with them can be attributed to their owners with a high degree of confidence. In such schemes there is no shared secret since the bank does not know the value of the signature key and cannot discover it from the information it is given.

67 Implementations of public key cryptography depend on calculations with very large numbers, and are in practice dependant on the use of quite powerful computers. But they have been comfortably within the capabilities of ordinary desktop computers for some years, and are both readily available and in widespread use. Versions are available with user interfaces no more difficult to use than most general purpose home or office software.

68 It might be thought that with the customer in sole control of a signature key, the problems of liability could acceptably be solved by requiring the customer to accept responsibility without limit for all use of the signature key (at least until the bank is notified of a compromise). But that conclusion would involve considerable dangers, which we explain below after reviewing some other security issues in telephone and online banking.

69 The security of telephone banking faces the threat of interception of the telephone call and of the security information conveyed during it. The use of techniques described above in which only a part of the security information is used in any session will reduce the risk that any small number of intercepts can provide the interceptor with the means to impersonate the customer in future transactions, although the transaction information from the sessions will be obtained.

70 The telephone network requires some skill for outsiders to intercept, and the criminal character of unauthorised interception makes the task risky, especially given the limited value of intercepts. (Authorised intercepts can be disregarded as a threat to the transaction information, since the authorities can obtain the information more satisfactorily from the bank. The risk of authorised interception being abused to facilitate customer impersonation by the authorities is beyond useful discussion: those who believe it could happen cannot be reassured by discussion, and those who believe it could not happen do not require reassurance.)

71 In some cases there may be a real risk of interception between the telephone handset and the public network, either through the use of telephone extensions in homes or very small offices, or through office switchboards (especially where telephone monitoring is practised). There is also the risk of simple eavesdropping, or the planting of surveillance devices for the same purpose. Warnings given by the banks about maintaining the secrecy of security information do not draw attention to these risks. If the banks carry a substantial part of the risk of fraud, this is largely a matter

for them; but if they do not, the omission raises a further question about the appropriateness of the liability régime.

72 PC banking, in which a direct connection is established over the telephone network between the customer's PC and the bank's system, faces a different mix of risks from telephone banking by voice. Intercepting the content of traffic between modems is much more difficult than with voice calls; and if the bank and the customer have established their systems correctly, the content of the session passing between the PC and the bank's system can be made highly secure from interception. This depends on the origin and quality of the software being used by both the bank and the customer. This software must be able to protect data exchanged during an on-line banking session by negotiating session keys that are (1) unique to the session, (2) discarded once the session is complete, (3) used with widely respected algorithms and (4) of sufficient length to prevent decryption without access to keys. Software for this purpose will generally employ one of several available secure network protocols such as the Secure Sockets Layer using algorithms such as RC4 or Triple DES and key lengths typically in excess of 100 bits. (But making the session confidential does not deal with the authentication problem, which must be solved by either shared secrets, one way functions or the use of public key cryptography.)

73 If a customer gains access to a bank account through a local network, such as one operated by their employer, additional interception risks may be involved. Many companies will operate a "firewall" to protect their internal computer systems from external attacks. These will often prevent security protocols from operating "end to end" between the bank's system and the PC on the customer's desk. This may prevent the customer from gaining on-line access to the bank account or may require that access is gained indirectly using other computer facilities. In that case the additional computer and network connections involved may introduce further interception risks. The result could be access by other employees to information passing between the customer and the bank, such as passwords and other security information. This risk could be reduced by systems adopting a "challenge/response" approach, rather like that used in telephone banking, where any session passes only a fragment of the security information.

Internet banking

74 Internet banking, in which the connection between the customer's PC and the bank's system is established over the Internet, faces essentially the same risks as PC banking, with the added risk of the insecurities of the Internet. The techniques available for encrypting the session to protect its contents are available in the same way as for PC banking. The principal added risk is that the customer is deceived

into making contact not with the intended system, the bank's, but with a fraudulent imitation. In PC banking the customer dials the telephone number of the bank's system, and it would be very difficult for an outsider to divert the call to an imitation system; but the Internet has a much more complex system of addresses than the telephone network, and is much more vulnerable to diversion by a variety of methods. The consequence would be a denial of service (since the fraudulent site would not provide the service required by the customer) and the discovery by the owner of the fraudulent site of whatever transaction and security information the customer revealed.

75 Since, as discussed earlier, the bank and the customer can use public key cryptography techniques to establish a confidential channel between them, if they each have a secret that they have made known to the other, they can prove their identity by passing this secret across the secure link. It is notable that although the banks have made considerable efforts to establish "shared secret" procedures to enable them to check the authenticity of instructions given to them by customers, none appear to provide any corresponding means by which their customers can check that they are really dealing with the bank and not an imposter. To achieve this by shared secrets would present difficulties, as the banks would have to devise separate passwords to present to each customer, giving rise to significant additional password management problems for banks and customers.

76 But public key signatures provide an alternative: if both the client and the bank have signature keys, and each has the other's verification key, each can sign an initial message and thus enable the other to check that the signature belongs to the right person. This process can be automated, so that if the check fails, the parties are warned and no connection is established. Whichever technique is used, the essential condition is that it should enable the bank and the customer to verify the other's authenticity.

77 Where customer and bank have a pre-existing conventional banking relationship, appropriate channels must already exist for the exchange of the necessary authentication data. The bank knows the customer's normal signature, and the customer can call at a known branch of the bank. Mutual authentication will only be difficult in situations where a customer and a bank wish to establish a new online relationship that is not built on a pre-existing "real world" relationship. Good banking practice has always required banks to take care in checking that a new customer is who he or she claims to be (in part to prevent accounts being opened in false names to collect the proceeds of stolen cheques); and more recently banks have become legally obliged (by the Money Laundering Regulations 1993, SI 1993 no. 1933) to make suitable checks for this purpose.

78 An approach widely proposed to meet such needs is the use of Certification Authorities (CAs). The function of a CA is to affirm that a signature verification key belongs to a particular individual or organisation. The affirmation is made by the CA signing the verification key with their own digital signature. CAs thus provide a means for entirely new relationships to be established in cyberspace without the need for a conventional relationship as a starting point, at least if both parties to the proposed relationship already know the signature of the CA. (A discussion of the complex procedures required to fulfil that condition in any reliable way is outside the scope of this paper.)

79 The use of a CA for customer authentication is clearly irrelevant between a bank and an existing customer, as they already know one another. For a bank to use a CA to verify the details of a prospective new online customer would amount to delegating to a third party the duties falling on the bank under existing banking practice and the money laundering regulations. It seems unlikely that these relatively sensitive aspects of banking business will prove suitable for outsourcing.

The security of banking computer systems

80 While it is possible to establish a confidential channel between a bank and a customer, this does not eliminate the possible impact of security vulnerabilities in the computer systems used by banks and customers for on-line transactions.

81 Although UK banks have denied that weaknesses in their computer systems are responsible for alleged fraudulent transaction, the evidence discussed above and in Ross Anderson's papers [Anderson93, Anderson94] highlights failings in such systems which can have a serious impact on customers. The banks have been unwilling to allow independent experts to examine their systems, justifying this stance by claiming that they need to keep the design and operation of their systems secret in order to protect them from attack.

82 This approach, known in security circles as "security through obscurity", is now widely discredited, because any advantages provided by secrecy are offset by the fact that this secrecy allows serious faults to exist in systems for long periods without being discovered. The consequences are well illustrated by the ATM phantom withdrawal problem, where the banks have been asserting for years that the design of their systems make such events impossible in the face of steadily growing evidence that they must be wrong. As cases have come to court, defence expert witnesses have gained steadily more access to the details of banking computer systems, and have discovered that banking computer systems do not exhibit the invulnerability that the banks claim for them.

83 If banks carried the whole risk involved in on-line banking, the vulnerabilities of bank computer systems would be of lesser public concern, but the prosecution of a customer for demanding repayment of sums he claimed were wrongly debited to his account shows the serious consequences of a bank's attempt to transfer the risk to a customer.

84 It follows that customers' interests are not adequately protected even by an acceptance in principle by the banks that they will themselves carry all the risks of fraud in online banking. In practice the banks will employ mechanisms to prevent fraud, and where these mechanisms fail the banks will sometimes wrongly seek to transfer the consequences to their customers. While at first sight account security measures such as PINs, passwords and digital signatures may seem to protect customer interests, their weaknesses will sometimes be used by banks to explain failures that are in reality the result of internal problems with their own systems. In this sense, therefore, it can be argued that security based on the secrecy of the mechanisms employed by the bank operates more in the interests of the bank than of its customers.

85 The security of online banking systems from a customer perspective is therefore not very satisfactory. Although there is no doubt that the vast majority of customers will not experience problems, for the small number that find themselves victims of security failures in banking computer systems the consequences can easily be very serious. Customers who are thinking of moving to online banking should seek a bank that offers better security than that provided by PINs and passwords alone, and one that has allowed independent experts to audit and publish the results of security reviews of the computer systems it uses to provide online services. They may be in for a long search; in the meanwhile, they might do well to place limits on the amounts which can be transferred from their accounts on the basis of electronic instructions.

Client PC security

86 But even if banking computer systems were perfect, the majority of the computers used by customers for on-line banking will be home PCs that are most unlikely to meet any serious security requirements.

87 The difficulties that users have in managing PINs and passwords have already been discussed, but a number of further problems arise from the use of PCs. People tend to be very trusting of others and can often be persuaded to reveal their PINs and passwords when they should not do so. Many people have difficulty installing software on their PCs and find an "expert" neighbour or friend to help. It is not

unusual to find that the helper will be given the codes needed to operate the service being installed, in order to check that it is working and to demonstrate its use to the real customer. Undoubtedly most helpers are honest but inevitably a few will use such knowledge for fraudulent personal gain.

88 A further concern is that typical PCs do not provide much real protection for PINs and passwords unless careful control is maintained over access to the PC as well as control over the software that is installed. PCs used for home banking will often be used by several family members for a wide range of different pursuits. It is not difficult for anyone who has ongoing access to install software that will capture sensitive account and password data entered by users for later collection. This could easily be achieved by another family member or by someone called in to maintain the machine.

89 Such attacks can be even easier to mount if the software used for online transactions is not very carefully designed. Most modern PC operating systems can appear to run several applications at once. They do this by temporarily moving applications and the data they are using from memory on to files on disc called swap files. Such files will often hold sensitive data such as passwords or security keys themselves, and they can be read with utilities that are widely available. A knowledgeable programmer could easily write software that searches the swap file to find the information. Recent research has shown that some security information has characteristics that are easy to detect unless it has been deliberately disguised, and this makes such attacks all the easier to design. A computer maintainer armed with software of this kind could easily recover such information as a matter of routine.

90 Although these forms of attack are probably rare at present, this is not the result of any inherent technical difficulty but because the gains are limited while online banking is not yet widespread.

91 In addition to attacks requiring physical access, PCs used on the Internet are vulnerable to attacks in which software is remotely installed to capture and transmit a user's keyboard data to a remote locations. Since users are routinely asked to install "add-ons" such as applets and active controls, most users accept this as routine and will not understand how easy it is for a fraudulent site to install an applet that appears to offer one service but in reality captures and transmits security data back to the site in question. It would also be perfectly feasible to modify and redistribute an honest applet from a reputable company to do this. A number of cases have been reported recently in which commercial software has been found to provide its supplier with information about its user's activities, without the user having been made aware of the fact.

92 An even more potent attack would be one based on a computer virus (software designed to transfer itself from one computer to another unknown to their users, either on diskettes or over the Internet, and capable of affecting the working of any computer it reaches). Current viruses exhibit a range of behaviours from benign (or even beneficial) effects through to those of a highly malicious character, designed to inflict substantial damage on a victim's PC or the data it contains. But it is straightforward to write a virus that, once installed, looks for and captures PINs, passwords, account details and other sensitive data for transmission back to the virus writer when the victim next goes on line. By making such a virus covert – that is, as silent as possible, so that a PC user is unaware of its presence – it could easily do its job over months or even years without being detected.

93 Although we are not aware of such viruses having been written or released, the steady growth of online banking and electronic commerce will make the possibility a virtual certainty in the not too distant future. It is a threat against which many PCs have little defence. The BBC provided a vivid illustration of this type of attack on 22nd November 1999 in a programme in its *Crime Squad* series. A remote user was shown using the Internet to monitor a session in which a customer used an online banking service. The remote user was able to capture the security information necessary to carry out a successful subsequent transaction on the customer's account. The basis of this attack was not explained in detail, but it could easily have been mounted by installing a special program (in this case probably not a spreading virus) using a macro contained in a document attached to an email message (like the Melissa virus but less visible in its effect). Such possibilities must be regarded as far from remote.

94 To counter attacks of these types, Microsoft has introduced a capability for software to be signed with a digital signature so that its origin can be checked. Such signatures allow the operating system to verify the signature on a piece of code before it is allowed to run. In an ideal world this would offer a meaningful improvement in security if customers were willing and able to use it; but even if all suppliers of software could be persuaded to offer signatures, the operating system has to be trusted to carry out reliable checking of the signatures involved, and this is not as easy as it might seem.

95 The inherent difficulties involved in computer security are discussed in *The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments*, a paper by scientists from the US National Security Agency [Loscocco98]. That agency is responsible for the security of US Government communications and for monitoring and deciphering foreign communications for intelligence purposes. Any paper by the NSA on computer system security carries

very high weight indeed. The thrust of this paper's argument is that it is unrealistic to expect that security mechanisms can be implemented in software without computer operating systems that offer effective security features of a kind that do not exist in current products.

96 Although purely software based PC banking procedures seem acceptable now, for reasons such as those discussed it is hard to believe they will continue to be seen as a robust online banking solution for the longer term. Although the use of signature keys based on public key cryptography can greatly reduce the risks presented by the use of PINs, passwords and other shared secrets, even then the customer is dependant on keeping the private key secret despite the need to use it in a PC. In such an environment the customer is exposed to risks of the private key being compromised without having any means of detecting the compromise until fraudulent use comes to light. A sophisticated attack might leave no evidence of how it occurred, and the customer is therefore weakly placed to resist an assertion by the bank that the transaction must have been authorised.

Hardware based solutions

97 The unavoidable security limitations of software have led many to look for hardware solutions, such as those based on smart cards. Although software is easy to modify and hence subvert, this is less true of hardware, which makes it attractive for implementing security critical features. While hardware solutions offer better security assurance than software, they are also more expensive. As a result such solutions are likely to be advocated not just for online banking but in the wider context of online electronic commerce. The discussion that follows will therefore consider this wider context.

98 If secret data can be held in hardware, for example in smart cards, it is much less vulnerable to being discovered by an attacker. Smart cards are vulnerable to a number of forms of attack, but much less so than software since the expertise required is more specialised and the tools needed are less commonly available. But expertise in microelectronics is not rare, and many laboratories will have the necessary equipment. Several techniques have been developed to discover the internal secrets of smart cards, and some of these have been shown to be very successful for particular cards [Kömmerling99].

99 Such attacks have already become a serious problem for the purveyors of pay-per-view TV. At one point, Sky TV reckoned that smartcard forgery was costing in excess of 5% of its turnover. Once they are widely introduced, banking smartcards will clearly present an even more attractive target. Some attacks on cash

dispenser cards have involved sophisticated and expensive techniques to deceive customers into giving their PIN to a fake machine, and recent research has shown that many smartcards are vulnerable to a fake machine extracting their secrets by observing the power they consume while calculating a digital signature. Organised crime will certainly be able to obtain the means to attack smart cards when the rewards justify the effort.

100 Moreover, the undoubted advantages of smart cards when compared with security mechanisms based on software are not as easy to harness as they seem. First, where smart cards are used to hold secret information, it makes little sense to transfer this information into a PC for use, since this will remove the very protection that the smart card is intended to provide. So in order to maintain the security of the information, it has to be used on the card itself, and this is likely to require the card to have very powerful processing capability of its own. There are obvious cost implications. Secondly, at a practical level, almost no mass market PCs come with smart card readers, and this seems unlikely to change unless the need is widely recognised and the costs involved are small.

101 Thirdly, a PIN or a password will be used to activate the card in order to guard against the fraudulent use of lost or stolen cards. If this is entered through the PC's keyboard it will be vulnerable to all the attacks discussed earlier. In this case it can be argued that the loss of the PIN is not so serious since fraud will require both the card and the PIN. Although this is true, if an attack has been mounted on a PC through a virus as described earlier, it would not be hard to extend the virus to use captured password data with the smart card the next time it is inserted by the user.

102 These points are not made in order to deny the value of smart cards, but simply to point out that while they will offer big improvements when compared purely with software, they are not a perfect solution.

103 In order to overcome one of these vulnerabilities, at least one smart card manufacturer is now offering a secure smart card reader with a small keypad for the entry of the PIN. This avoids the use of the PC for PIN entry, but it remains vulnerable to an attack in which a fraudulent application running on the PC (or a point of sale terminal) displays one transaction to the user while asking the inserted smart card to authorise a completely different one. For example, a personal signature card used to sign credit card transactions is vulnerable to an attacker who presents a point of sale terminal to the user which purports to perform a genuine transaction but simultaneously authorises another transaction that is seriously to the user's detriment – examples might range from another credit card transaction for a large amount up to a re-mortgage of the user's home.

104 Smart cards are often seen as the perfect answer for implementing digital signatures, because signature keys kept on such cards can in principle have values not even known by their owners. This can prevent an owner from repudiating a genuine signature by publishing the key and claiming it to have been compromised before the transaction.

105 But providing a useful identity based signature which cannot be repudiated by this means remains very difficult, because (1) in order to ensure that the signature key is secret it must be generated on the card; (2) for the same reason it must never leave the card, and this requires that the transaction or document to be signed must be imported on to the card, with the signature process be performed by the card; and (3) the card has to export a verification key that allows the signature to be verified and associated with a person authorised to perform the transaction.

106 As already indicated, meeting requirements (1) and (2) currently requires relatively expensive "state of the art" hardware solutions, while meeting requirement (3) turns out to be difficult because it raises social and legal issues about how a person can be identified in a unique way.

107 A person's name alone is clearly not sufficient since names are not unique; but neither are names with birthdays or names with addresses (which can in any case change frequently). The use of verifiable biometric data – for example, fingerprints, iris or retinal scans or DNA data – offers a more robust solution but will be expensive. Use of such data also raises a number of ethical and privacy concerns such as those that come to the fore when identity cards are mooted: there are many circumstances where an individual may legitimately wish to use a pseudonym which has no link to any other name the individual uses. Moreover, while the costs might be contemplated for use with cash dispensers or point of sale terminals, it is less obvious that the cost of secure biometric data collection devices will soon become low enough for them to become "commodity" peripherals for home PCs. For this reason their value in the foreseeable future for online banking and electronic commerce by consumers is somewhat uncertain.

108 It is worth noting that major computer and software suppliers are aware of the need to improve the security of current PCs to meet electronic commerce and related needs. This was illustrated in October last year with the announcement of the formation of the Trusted Computing Platform Alliance in the following terms:

> "Compaq, Hewlett Packard, IBM, Intel, and Microsoft today announced the formation of the Trusted Computing Platform Alliance (TCPA), an industry group focused on building confidence and trust

> of computing platforms in e-business transactions by creating an industry standard for security technologies in personal computing environments."

109 In many respects typical PCs offer far more performance than is necessary for controlling the transactions involved in online banking and electronic commerce. They are designed for high levels of functional performance, but their resulting complexity makes the achievement of security objectives much more difficult. In many respects the ideal vehicle for online banking and electronic commerce is a small self-contained computer system such as a palmtop with a small keyboard, a screen and (possibly) an infrared port to enable it to communicate with a home PC, a bank's or a merchant's computer system, or a point of sale terminal. By keeping this device simple, and by having a keyboard, a screen, a processor and secure storage in one small self-contained unit, it would be possible to have a highly assured capability for signing transactions without being dependent on other devices such as PCs or point of sale terminals.

110 Still further security could be achieved by having the secure storage for such a device implemented on a plug-in smart card. It is possible to envisage a secure device with an integral keypad, screen, smart card reader, PC interface and biometric input such as a fingerprint reader. If such a device could be manufactured at reasonable cost it could serve both as a point of sale terminal in a merchant environment and as a PC peripheral at home. In practice the merchant terminal would have to be more robust physically, but the two devices could share much of their security design in common. We think that one essential element in achieving public confidence in such a design will be its openness to scrutiny by independent experts, and the abandonment of "security through obscurity".

111 Devices of this kind will nevertheless be expensive. We do not think they will come into widespread use without being subsidised by banks and others who benefit from the growth of electronic commerce and have the skills to collaborate in their design. The most certain way to ensure that the banks have the necessary incentive to pursue this programme is to ensure that they carry the risks of the fraud that the programme would help to prevent. Such a programme is not without precedent: the spread of mobile telephony depends on large subsidies by network service providers to reduce the cost to users of buying mobile telephones.

Perceptions of insecurity and their misuse by Government

112 It is a common observation that electronic commerce is being held back by the perceived insecurity of the Internet. Consumers' reluctance to supply card details

over the Internet is frequently cited. This reluctance is frequently derided as irrational, on the grounds that consumers supply the same details readily to strangers in person or by telephone. Unfortunately, both those who are reluctant and those who deride their reluctance have missed the point, explained above, that most of the risks of misuse of card information over the Internet fall not on the consumer but on the merchant.

113 Electronic commerce is much more likely to be held back by the justified unwillingness of merchants to take the risk of card transactions at which the customer is not present, than by the unjustified anxiety of consumers. (Consumers could of course be reassured by publicity about their freedom from this particular risk, but the banks and the merchant may not be enthusiastic to educate customers about these particular rights.)

114 The SET standard having failed to gain ready acceptance, as mentioned above, many in Government and industry have seen a solution in building trust in digital certificates linking a user's name with a verification key. We have explained above why proposals of this kind are irrelevant to online banking. The Government's proposals were originally devised to kill several birds with one stone: by promoting the importance of digital identity certificates obtained from approved providers, the Government hoped to increase confidence in electronic commerce, to introduce citizens' identity cards without incurring the resulting cost or political hostility, and to provide an inducement to consumers to deposit copies of their confidentiality keys with the approved providers (as a means, called "key escrow", for maintaining access by the intelligence and law enforcement agencies to intercepted communications). The proposals were perhaps too clever by half, and the stone did a good deal more harm to the Government than to any of the birds.

115 The proposals provoked damaging controversy and considerable mistrust of Government objectives. Indeed the Government's continuing but misguided conviction of the central importance to electronic commerce of digital name certificates for consumers can only intelligibly be explained by the fact that to abandon that conviction would involve the unpalatable admission that the Government's "consumer protection" justification for its digital certificate policy was a bogus cover for its key escrow objective.

116 All-purpose digital name certificates are of very doubtful utility, among other reasons because names do not adequately distinguish people in large populations. They are also irrelevant to many transactions (what the merchant needs to know is that a card number is given by the person authorised to give it, whatever their name may be), where they needlessly reduce legitimate privacy. Their widespread use would

depend on a complex hierarchical infrastructure of mutual recognition of different certificate issuers' certificates, and on achieving practical solutions to many unsolved problems connected with expiry and revocation of certificates. And the suspicion inevitably remains that Government's continuing enthusiasm for these castles in the air derives mainly from its hope that from among them may emerge (free from cost or blame to Government) a citizen's identity card. Convenient for Government as such a development would be (because Government typically needs to assign a unique identifier to each citizen to avoid multiple claims for social security benefits or tax reliefs, for example), Government's wish to portray the solution to its own problems as being promoted for the benefit of electronic commerce as a whole continues to be profoundly counter-productive.

Misperceptions of security: legislative bungling

117 We have concluded that there will be no early technical fix for the problems of safeguarding a user's signature key, and that users should therefore not be burdened with proving that what seems to be their signature was in fact not made by them. In this section we review the legislative initiatives being pursued in the European Union and the United Kingdom in the light of this conclusion.

118 The European Union's Signature Directive ("Directive 1999/93/EC ... on a Community framework for electronic signatures") came into force on 19th January 2000. Its primary objective is to discourage divergence between the various member states' treatment of electronic signatures, and in particular the creation of barriers to free trade within the EU, and it is undoubtedly valuable for these purposes.

119 The Directive distinguishes between electronic signatures in general and "advanced electronic signatures", the definitions being as follows:

> (1) "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
>
> (2) "advanced electronic signature" means an electronic signature which meets the following requirements:
>
> > (a) it is uniquely linked to the signatory;
> > (b) it is capable of identifying the signatory;
> > (c) it is created using means that the signatory can maintain under his sole control; and

> > (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

We have concluded that neither PCs nor smartcards nor biometrics nor any methods currently available or likely to be available in the near future can enable a user to keep a signature key secure; and it follows in our view that condition 2(c) cannot be fulfilled, and that no advanced electronic signatures can be made.

120 It is of course no fatal reproach to the Directive that it should thus deliver thunder with no lightning; and it could be excused on the basis that the law will for once be ahead of events. But the existence of a legislative régime that seems to assume the existence of advanced electronic signatures may mislead users into believing that they do indeed exist. This assumption appears from the ensuing series of definitions:

> (3) "signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;
>
> (4) "signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;
>
> (5) "signature-creation device" means configured software or hardware used to implement the signature-creation data;
>
> (6) "secure-signature-creation device" means a signature-creation device which meets the requirements laid down in Annex III

121 The requirements laid down in Annex III are as follows:

> 1. Secure-signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
>
> > (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
> >
> > (b) the signature creation data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

> (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
>
> 2. Secure signature creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

These requirements represent an admirable wish list, and indeed reflect an awareness of many of the threats discussed above. But they seem to reflect an assumption that "currently available technology" does in fact provide adequate means of protection against forgery, and in our view this is dangerously misleading.

122 Article 3 of the Directive provides that:

> 4. The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated. A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.

The law can no more make an insecure system secure than it can determine the value of *pi*. There appears to be no mechanism for public scrutiny of determinations of conformity under the Directive, and no opportunity for challenge. Some member states with well established smartcard industries may appoint bodies which prove unable to resist the temptation to promote the interests of their national industries by finding that their products conform to Annex III. The resulting determination must be recognised throughout the EU.

123 Even a justified determination would be of limited value to the user. Recital 15 to the Directive makes it explicit that "Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate." The result is that despite the requirement of Annex III that "Secure signature creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process," the possibility remains that PCs or point of sale terminals to which such devices are presented may (without any nonconformity with Annex III) allow a signature key to sign a document of which the signatory is unaware.

124 If an electronic signature is taken to be an advanced electronic signature (justifiably or otherwise), this raises the question of what legal consequences follow. The point is addressed, up to a point, by Article 5 of the Directive, which provides as follows:

> 1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
>
> (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
>
> (b) are admissible as evidence in legal proceedings.
>
> 2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
>
> – in electronic form, or
> – not based upon a qualified certificate, or
> – not based upon a qualified certificate issued by an accredited certification-service-provider, or
> – not created by a secure signature-creation device.

(We disregard the matter of qualified certificates, which are irrelevant to this discussion.)

125 English law on signatures lays down no formal requirements. The impression of a rubber stamp can be a signature, as can a facsimile of a handwritten signature sent by fax machine, as can a faint piece of handwriting made using a pencil. Anything which benefits from paragraph 2 of Article 5 has nothing to gain from paragraph 1. Subject to possible future changes in English law discussed below, therefore, it is immaterial whether an electronic signature is an advanced electronic signature. Any greater security enjoyed by an advanced electronic signature (whether real or illusory) has no legal effect in England.

126 In particular, it is important to note that the Directive does not require an advanced electronic signature to be accorded any special status. Indeed, by requiring it to satisfy legal requirements "in the same manner as a handwritten signature", it may well prevent it from being given any special status. We have argued that there is no technical justification for treating an electronic signature which wrongly appears to

have been made by a particular signatory as nevertheless binding on that signatory; and likewise no technical justification for putting on to the apparent signatory the burden of proving that he or she did not make the signature. To do so would be to depart from the existing English law rule that it is the relying party, and not the apparent maker, who bears the burden of proving the genuineness of a signature. The Directive clearly does not require a departure from this rule, and arguably prohibits such a departure. Whether intended or not, we think that this is a highly desirable result.

127 Just as the Directive is approaching the end of its legislative journey, the United Kingdom's much debated Electronic Communications Bill has begun its passage through Parliament. As introduced it is consistent with the Directive, providing for electronic signatures (similarly defined) to be admissible, and establishing machinery for treating statutory requirements for writing to be satisfied by electronic data. It makes no distinction between one kind of electronic signature and another. In the event of a dispute about the genuineness of an electronic signature, the issue would have to be decided on the basis of expert evidence about the method used.

128 There remains one cloud in this serene sky, however. Clause 8 of the Bill, which provides the machinery for amending legislation to enable the use of electronic writing, gives the following powers:

> (4) ... the power to make an order under this section shall include power to make an order containing any of the following provisions—
>
> > (g) provision, in relation to cases in which the use of electronic communications or electronic storage is ... authorised, for the determination of any of the matters mentioned in subsection (5), or as to the manner in which they may be proved in legal proceedings
>
> (5) The matters referred to in subsection (4)(g) are—
>
> > (d) the person by whom such a thing was done.

An order under the clause could therefore provide that if a signature can be proved to have been made by a particular private key, it is to be treated as made by the owner of that key unless the contrary is proved by the owner (and perhaps even then). This is precisely the approach that we argue to be unjustified, and indeed contrary to the EU Signature Directive. Unfortunately, that Directive, with its references to secure signature devices which the UK would be obliged to "recognise", might encourage just this use of the clause 8 powers.

129 When Australia considered these issues, the Commonwealth Attorney-General appointed an Electronic Commerce Experts Group to produce a report; and one of its conclusions was that there should be no reversal of the ordinary rule that the relying party must prove the genuineness of a signature. That conclusion was accepted, and the resulting Australian legislation provides accordingly. We think that UK legislation should similarly deny Ministers any power to alter this rule. We would therefore support an amendment to clause 8 (already published by the Foundation for Information Policy Research) to introduce the following limitation:

> (9) No order under this section shall make any provision inconsistent with the following provisions of this section.
>
> (10) Unless otherwise agreed between the purported sender and the recipient of an electronic communication, the purported sender of the electronic communication is bound by that communication only if the communication was sent by the purported sender or with the authority of the purported sender.
>
> (11) Unless otherwise agreed between the purported maker of an electronic signature and any person relying on it (or any person through or under whom the person relying on it claims), the purported maker of the electronic signature is bound by that signature only if the signature was made by the purported maker or with the authority of the purported maker.
>
> (12) Subsections (10) and (11) are not intended to affect the operation of a law (whether written or unwritten) that makes provision for:
>
> > (a) conduct engaged in by a person within the scope of the person's actual or apparent authority to be attributed to another person; or
> >
> > (b) a person to be bound by conduct engaged in by another person within the scope of the other person's actual or apparent authority.

Unfortunately the Government at present remains unwilling to accept such an amendment.

Solving the merchant's problem without unfair contract terms

130 To solve the merchant's problem, the banks need to invent an electronic equivalent of the cheque guarantee card, but without the features of the SET scheme which

have hindered its adoption. An example of a possible approach is that the bank should certify a signature key for use by the customer for each account which the customer is authorised to use. The certificate would be signed by the bank with a signature key which the merchant could verify. The merchant would know from the certificate the value up to which the bank was thereby guaranteeing the customer's account signature. The merchant could also be required to check that the bank had not revoked or suspended its certificate by checking the equivalent of a "hot card" list. (The bank could suspend its certificate if funds or facilities were exceeded, to deal with the risk of a stolen signature key being used in a huge number of transactions.) The procedures for verifying the bank's signature on the certificate, and for checking the fact that the certificate had not been revoked or suspended, could be made entirely automatic.

131 The appropriate liability régime for such an approach is equally simple. The bank must be bound to pay the merchant if the merchant has correctly verified the customer's signature and the bank's certificate for it. In the case where the customer claims that the signature was forged, the bank must carry all the risk (or all the risk above £50) unless it can prove the contrary. For this purpose, "proving the contrary" must require positive evidence of the customer's responsibility, not mere assertion that in the absence of any acceptable explanation discovered by the bank, the customer must be in the wrong.

132 Such an approach is open to the objection that it is easy for us to give away the banks' money in this way. The answer to that objection is that taking this risk is what the banks earn their commission for. It is the central core of the function of banks in trade finance to bridge the risk between merchant and customer, and through bills of exchange and letters of credit it is exactly what they have been doing with great success for several centuries, despite the risks of forgery to which such documents are prone. Electronic commerce is a fresh opportunity for them to deploy their traditional skills in a new environment.

133 There is also a practical justification for this allocation of risks. Neither the merchants nor the customers can provide the technical infrastructure for electronic payments: only the banks can do so. Those who provide the technical infrastructure should carry the risks of its deficiencies: just as the banks decide how small an amount justifies checking the signature on a cheque, because they carry the risk of the decision, so the banks should carry the risk of forgery of electronic signatures. And in due course, if it is worth their while, the banks can subsidise the emergence of genuinely secure signature devices whose design can command enough public confidence to justify a modification of the liability régime. Among the essential requirements for public confidence is the abandonment of "security through

obscurity" and its replacement by an open and transparent approach; a further requirement is that the legal régime must be defined at the same time as the engineering approach that is claimed to justify it.

134 There is finally a legal reason why banks should not seek to allocate to consumers the risk of fraudulent use of their accounts. Regulation 5 (1) of the Unfair Terms in Consumer Contracts Regulations 1999 (SI 1999 No. 2083) provides as follows:

> A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.

We began by drawing attention to the fact that the bank and not the customer carries the risk of forgery of a cheque. That allocation of risk provides a benchmark against which to assess any alternative. Both where customer authentication relies on shared secrets, and where signature keys can be stored or used only in insecure systems, allocating more than a very small risk of fraud to the customer seems inescapably (in the words of the Regulations) to cause "a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."

135 Regulation 8(1) provides that "an unfair term in a contract concluded with a consumer by a seller or supplier shall not be binding on the consumer." The Director General of Fair Trading is responsible for the enforcement of the Regulations, and has power to apply for an injunction to restrain the use of an unfair term. A copy of this paper has been supplied to him.

136 We also draw attention to the impact on such contractual terms of the Unfair Contract Terms Act 1977. The terms we have described are such that they attempt to place on the customer the risk of having his or her account debited with fraudulent transactions carried out by others, who may include bank staff or other persons who have gained access through the bank's carelessness in the design or implementation of banking systems. These terms seek to permit the bank to escape responsibility for its own carelessness or even fraud, and are therefore treated as exclusion clauses for the purpose of the 1977 Act. The Act renders such clauses unenforceable unless they satisfy the "requirement of reasonableness" as defined in the Act. And in permitting the bank to debit a customer's account with unauthorised payments, such terms are arguably also rendered unenforceable on the ground that they permit the bank to render a performance substantially different

from what was reasonably expected. We have explained above why we think these terms are unreasonable.

137 Where a term to which the Act applies fails to satisfy the test of reasonableness, for example because it would exclude the bank's liability for its own carelessness, the term is unenforceable in all circumstances (whether or not the customer can prove that the bank was careless in the particular case). We think that a customer faced with a bank relying on such a term will have very strong arguments under the 1977 Act; and we take comfort from the similar views on this subject expressed by the learned editor of the 11th edition of *Paget on Banking*.

Nomenclature

138 We conclude with a few observations about the use of the term "non-repudiation", which is often used in discussions of the issues addressed here, although we have not used it in this paper.

139 It is often (although not invariably) a desirable objective of a system to provide a non-repudiation service, either to prevent a signatory from falsely repudiating a genuine signature or to prevent the recipient of a message from falsely denying its receipt. Whether a particular system provides such a service, and the degree of its reliability, are matters for technical assessment.

140 If a system is believed to provide a reliable non-repudiation service, and is used in circumstances where legal consequences may follow the signing or receipt of a message, the contractual terms which establish the legal framework for the operation of the system may provide that what the system recognises as a valid signature shall bind the apparent maker, whether the apparent maker made the signature in fact or not; or that where the system records a message as having been received, the apparent recipient shall be treated as having received it, whether the apparent recipient received it in fact or not. Such terms may be described as providing for the non-repudiation of signatures or receipt of messages.

141 A technical assessment may prove that it is highly probable that a signature was made by its apparent maker. A legal assessment may hold that the apparent maker of a signature is bound by it whether the apparent maker made it or not. These two conclusions seem similar, but operate in different realms of thought. Debate about non-repudiation sometimes overlooks the distinction, to the evident frustration of the lawyers and engineers whose arguments pass through one another like angry ghosts. One object of this paper has been to bring about a fruitful conjunction of the legal and technical considerations involved.

References

[Anderson93] R. Anderson. Why Cryptosystems Fail. Proceedings of 1st Conference on Computer and Communications Security '93, Fairfax, Virginia, USA, November 1993.

[Anderson94] R. Anderson. Liability and Computer Security: Nine Principles. Proceedings of European Symposium on Research in Computer Security, Brighton, UK, November 1994.

[Beck95] J. Beck. Sources of Error in Forensic Handwriting Examination. Journal of Forensic Science 40 pp.78-87, 1995.

[Dierks99] T. Dierks and C. Allen. The TLS Protocol Version 1.0. RFC 2246, January 1999.

[Diffie76] W. Diffie and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22(6) pp.644-654, November 1976.

[Harrison58] W. Harrison. Suspect Documents pp.373-426. New York: Praeger Publishers, 1958.

[Hawkes98] Nigel Hawkes. Machines will pay up in the blink of an eye. The Times [http://www.cl.cam.ac.uk/users/jgd1000/atm.jpg], April 1998.

[Kam97] M. Kam, G. Fielding and R. Conn. Writer Identification by Professional Document Examiners. Journal of Forensic Sciences 42 pp.778-786, 1997.

[Kam98] M. Kam, G. Fielding and R. Conn. Effects of Monetary Incentives on Performance of Nonprofessionals in Document-Examination Proficiency Tests. Journal of Forensic Sciences 43 pp.1000-1004, 1998.

[Kömmerling99] O. Kömmerling and M. Kuhn. Design Principles for Tamper-Resistant Smartcard Processors. Proceedings of USENIX Workshop on Smartcard Technology, Chicago, USA, May 1999.

[Loscocco98] P. Loscocco, S. Smalley, P. Muckelbauer, R. Taylor, S. Turner and J. Farrell. The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environment. Proceedings of the 21st National Information Systems Security Conference [http://csrc.nist.gov/nissc/1998/proceedings/paperF1.pdf], October 1998.

[SET99] SET Secure Electronic Transaction LLC. The SET Specification. [http://www.setco.org/set_specifications.html] 1999.