Keeping digital cash secure

Dr Ian Walden (*)

---

1. **Introduction**

Digital cash schemes are being viewed as a key payment mechanism for the future, whether for use in a traditional retail context or to engage in electronic commerce across the Internet. The main advantage of digital cash against more traditional electronic fund transfer mechanisms, such as credit card-based transactions, lies primarily in its potential for providing low, per transaction, processing costs. Another feature that is seen as being appealing to the consumer is the security and privacy that derives from the fact that personal information does not need to be communicated for such payments to be made.

Conversely, however, digital cash obviously presents significant security risks to the parties involved. The banking community will be primarily concerned with the threat of forgery leading to independent generation of money supply. Scheme operators who offer payment services, but do not act as a custodian of funds (therefore operating outside of the supervision of national banking regulators) will need to minimise their exposure to liability. While consumers will need assurance that their funds are not accessible to unauthorised persons and that unauthorised loss or destruction of the value held will not occur.

Data security is the central element in the achievement of `legally secure' digital cash, minimising the liability risks from using digital cash as a payment service. Data security is seen traditionally as an exclusively technical process. Data users protect their information assets through a range of physical, logical and operational measures designed to insulate their systems against threats arising from deliberate interference by persons or from natural and accidental events. However, users should also be aware of the complementary legal aspects of data security. Such legal issues can be distinguished under three main headings:

legal obligations to implement data security procedures

legal recognition of the use of certain security standards

legal restrictions on the use of certain forms of security mechanisms

This article considers each of these aspects from the perspective of the providers of digital cash payment services, whether PC-based (eg. Digicash) or Smart Card (eg. Mondex): banks and scheme operators.

2. **Obligation**

The law often imposes explicit or implicit obligations upon an organisation to implement data security procedures. Explicit obligations are usually designed to protect some third party such as a data subject or consumer; while an implicit obligation to implement appropriate data security may be inferred from an organisation's tortious duty of care towards third-parties, such as the need to ensure data accuracy in the provision of information.

2.1 **Legislation**

Legislative sources of data security law can be sub-divided into three general categories, embracing not only criminal law, but civil and administrative law as well:

· `sui generis' legislation which directly addresses information security issues;

· legislation regulating information technology which contain provisions directly addressing data security;

· the existing commercial legislative and regulatory framework which imposes requirements which have implications in terms of data security (eg. record-keeping requirements).

Over recent years, the increasing dependency of society on computer systems, paralleled with the growing perception of their vulnerability to external interference, has led to consideration among national legislators of the need for sui generis data security legislation. The Council of Europe, in a report on `*Computer-related crime*', has proposed that:

"The Member States could....establish a legal framework which would require manufacturers and users to observe at least a minimum of regulations relating to computer security."

The first significant statutory initiative along these lines was the US Computer Security Act 1987. The Act applies to federal government agencies and gives the National Institute of Standards and Technology (NIST) the authority to develop standards, guidelines, and associated procedures for computer systems. The potential impact of the Act is significant since the US government represents the largest user of computers in the World. To date, however, it appears to have failed to significantly improve the data security practices of government agencies.

The growth of electronic banking itself has attracted the attention of national and international legislators over recent years. The nature of such legislation has required that data security issues be explicitly addressed to some extent: eg.

· Denmark Payment Cards Act 1984, Article 10, if the Ombudsman is dissatisfied with security procedures then changes have to be negotiated with the institution. Failing that, the Ombudsman can issued an order to comply.

· In the US, Article 4A of the Uniform Commercial Code, governing `wholesale' funds transfers, states that a payment order is only effective if "the security procedure is a *commercially reasonable* method of providing security against unauthorised payment orders".

· The UNCITRAL Model Law on International Credit Transfers, at Article 5(2)(a), requires that "the authentication is in the circumstances a *commercially reasonable method of security*..".

Although such provisions tend to be framed in extremely general terms, they do indicate the possible direction of future legislative initiatives.

Data protection legislation is an example of an area of law which directly embraces aspects of data security. Data protection laws are designed to protect the subjects of data processing and have proliferated throughout Europe over the past two decades. A critical element of effective data protection is the need for data security. Article 17 of the EU data protection Directive states:

".. the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network..."

Data users are therefore expected to consider the sensitivity of the personal data they process, and implement suitable security procedures. Existing national data protection legislation also makes explicit reference to the need for data security measures, although varying in the degree of detail and intervention by the data protection authority. Some national data protection legislation has been widely drafted to cover certain types of computer misuse, in particular `unauthorised access', which may require the breach of security measures in order for an offence to be committed.

The extent to which a digital cash scheme gives rise to particular data protection issues depends on the particular manner of its operation. From the issuer's perspective, where a bank provides digital cash against deposits held on the customers account, the bank will process personal data and will need to comply with the relevant legislation. However, other systems may allow the digital cash to be generated directly from the payment of physical cash, in much the same manner that existing applications operate, such as phone cards. Such transactions should obviously not generate personal data.

In terms of the recipient of digital cash, where it is used to make payments across the Internet, although the actual transmission of value itself will not identify the payer to the payee, information related to the transaction often will. Location details for receipt of the goods or services being purchased, whether delivered in tangible form (eg. to an address) or electronically (eg. email), will often constitute personal data. However, digital cash used in a traditional retail environment should not generate personal data for which the payee has regulatory obligations.

2.2 **Regulatory supervision**

Banking sector activities are generally subject to regulatory supervision by the Central Bank. The Central Bank will inevitably be concerned with the risks associated with the provision of digital cash services. In the UK, for example, the Bank of England is empowered to prevent the authorisation of certain banking activities if they are perceived to be in breach of the criteria provided in Schedule 3 of the Banking Act 1987: eg. para. 4(7) states that:

"an institution shall not be regarded as conducting its business in a prudent manner unless it maintains ... adequate accounting and other records of its business and *adequate systems of control of its business and records.*"

With regard to this provision, the Bank of England Banking Supervision Division has issued a `Notice to Institutions' outlining the nature of such controls.

The Bank of England would therefore be able to prevent a bank from offering a digital cash service where it was of the opinion that insufficient controls were in place to prevent forgeries and fraud giving rise to liquidity risks for the individual institution, as well as the banking system as a whole. Such regulatory supervision does not extend, however, to non-banking scheme operators offering digital cash services.

2.3 **Liability**

Contractual liability for a failure to take adequate data security measures is obviously primarily an issue to be determined between the providers and their customers. The main exception to this, present in one form or another in most jurisdictions, is a duty of confidentiality imposed on banks. In the UK, this duty is an implied contractual duty. Confidentiality will therefore be a central concern in the provision of digital cash services by banks. Whilst for scheme operators confidentiality may be less of a concern.

The contractual terms and conditions under which a digital cash service is offered will obviously be determined by the provider. As such, the provider will attempt to limit their liability to the greatest possible extent. Their ability to do this will usually be subject to consumer protection laws. Industry codes of practice may also be relevant. In the UK, the banking community has adopted a code of practice, *Good Banking*, which addresses certain general issues relating to data security, primarily for the customer.

Under common law, tortious liability arises because one party has been negligent in fulfilling its responsibilities towards the other party. Liability for negligence requires three essential elements:

· The defendant must owe the plaintiff `a duty of care', because there exists a sufficiently close relationship between the two parties;

· a breach of the duty to care must have taken place, ie. the defendant must have failed to take `appropriate' and/or `adequate' precautions; and

· the plaintiff must have suffered some damage as a result of the breach.

Integrity is one of the central principles of data security. In terms of negligence, *Hedley Byrne & Co. Limited v Heller and Partners Limited* extended English common law to the negligent provision of information. Subsequently, the courts have been cautious about the extent to which information providers should owe a `duty of care', since the nature of information and its ability to be widely disseminated would open up a vast potential floodgate of litigation.

In terms of ensuring that a digital cash payment service operates within a `legally secure' environment, the second element of negligence is of key importance: what are considered to be appropriate safeguards? This is viewed by the courts as essentially a question of fact that can be objectively arrived at on a case-by-case basis. Past case law indicates that security procedures and techniques should be based on what is currently available, rather than simply following practice within a particular industry. The cost of implementation should also be considered in relation to the nature of the data being protected.

3 **Recognition**

"In our information society, more and more technical standards are used in formulating laws, regulations, decisions etc...standards are becoming more important in drafting contractual obligations and interpreting the meaning thereof, whether or not in the courtroom."

In an electronic commerce environment, the implementation of data security standards may provide the functional equivalent of traditional legal actions. Digital signatures, for example, may function to protect message integrity, as well as legally binding the user to an authenticated message. Such electronic techniques may also satisfy statutory requirements for a "signature" to be present on a particular document.

Digital cash schemes obviously require appropriate authentication from the customer in order to release the funds held. However, the nature of cash-based payments mean that an audit trail is not created for each transaction. Where a customer requests from its bank that digital cash be made available (eg. loaded onto a smart card via a telecommunications link), the issue of the customer's mandate will arise. Existing bank contracts generally state that the use of the customers card and identification code (eg. PIN) constitutes "irrevocable and unconditional authority from the customer to the bank to debit the designated account". Contracts for the provision of digital cash are likely to replicate such terminology. The legal efficacy of such terms could, however, potentially be challenged under consumer protection legislation as unfair.

In recent years, in reaction to data user fears regarding data security, there has been a movement towards the creation of national and international standards specifically addressing the security of IT products and systems. The US Department of Defence's, Trusted Computer Systems Security Evaluation Criteria (TCSEC), commonly known as the `Orange book', was the first major attempt to laid down standards regarding the level of security required within an IT environment.

In the UK, a 1989 Report on Banking Services made explicit reference to the need for security standards in electronic payment services, recommending:

"Banks should therefore adopt the principle that an EFT system must meet certain minimum standards of security in its authorisation procedures...."

The Government's White Paper in response to the report noted the Committee's concerns with regard to adequate security safeguards, but since maintenance of security was in the interests of both the banker and the customer it was merely suggested that they "may wish to include a provision in the code of banking practice to state that they will continue to maintain minimum standards of security in their present and future EFT systems".

General technical standards directly impacting on digital cash schemes are emerging, both at the hardware level, such as the EMV application standard for Smart Cards, and for the communication of payment instructions across an open network, such as SET. The international acceptance and development of such standards, incorporating appropriate security functionality, will be an important component in the growth of the market for digital cash services.

4. **Restrictions**

National laws may restrict the use of certain data security techniques. The most publicised example is the area of cryptography. The use of cryptographic techniques is fundamental to the security of existing digital cash schemes. However, the use and international transmission of cryptographic algorithms, designed to authenticate or ensure the confidentiality of electronic data, is regulated in many countries under export control legislation. Certain data security products, such as cryptographic software and hardware, are classified as `munitions' and therefore fall under the regulatory regime. Such laws exist in Europe at both Member State and European Union level.

In terms of digital cash, such regulations may:

place limits on the strength of the cryptographic mechanism that may be used by the application (eg. limiting the available key length); and

restrict the ability of customers to `legitimately' cross-borders with digital cash products.

Historically, banks have obtained special exemptions under national export control laws in order to use strong cryptography within fund transfer systems. The international communications network SWIFT, for example, has obtained permission to use DES and RSA algorithms, with 512-bit keys, in all the over 100 countries in which it has member banks.

National governments have an obvious self-interest in ensuring such inter-bank networks are extremely secure and reliable. Where banks and scheme operators use cryptography within retail digital cash applications, however, they are likely to find export restrictions continue to be applicable.

The growth of electronic commerce and associated concerns over the security of networks such as the Internet has led to significant commercial pressure being placed on governments to relax existing legislation. In the US, for example, the government has been concerned to reform the current regime to ease the regulatory framework whilst retaining certain rights to prevent the use of such techniques to facilitate criminal activities. Under the proposed "Commercial Key Escrow Regulations" organisations wanting to export cryptographic products would be required to deposit the relevant cryptographic keys with an independent "escrow agency". US government law enforcement agencies would be able to present themselves to one of these agencies and request a copy of a particular key upon presentation of an appropriate court warrant. In the UK, the Department of Trade and Industry has recently issued a consultation paper which proposes the establishment of licensed Trusted Third Parties.

5. **Conclusion**

Data security mechanisms, in particular the use of encryption, lie at the heart of the development of digital cash products. The widespread adoption of such payment techniques is likely to depend on the degree to which card issuers, whether banks or scheme operators, are able to provide adequate assurances to customers and regulators about the strength of such security. Legal recognition of such techniques will go some way towards addressing such concerns. The removal of legal restrictions on the use of certain techniques will also enable the industry to continue to enhance the security of their digital cash services.

Cybernews Volume 2, numéro 2 (printemps 1996)

(*) *Director, Computer-Related Crime Research Centre*
Queen Mary & Westfield College, University of London

© copyright 1998 Lex Electronica Tous droits réservés / All Rights Reserved ISSN 1201-7302
