

# JISC Legal Briefing Paper: Developments in e-Commerce Law



Andrew Charlesworth - 20 June 2004

This Briefing Paper discusses recent developments in the UK legislative framework applicable to e-commerce practices and related technologies, including the effect of the Consumer Protection (Distance Selling) Regulations 2000, and the Electronic Commerce (EC Directive) Regulations 2002 on the marketing and selling of goods and services, including educational services, via the Internet. It examines the status of electronic signatures in UK law, notably their role in the use of electronic invoicing for VAT purposes. It also discusses the legal implications of FE and HE institutional roll-out of smart cards and various forms of e-money.

**Please note** : this guidance has been prepared by JISC Legal for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

## Table of Contents

1.	Executive Summary .....	1
2.	Introduction .....	3
3.	e-Commerce and Distance Selling .....	4
4.	The e-Commerce Directive .....	6
5.	General Information Requirements .....	7
6.	Commercial Communications .....	8
7.	Electronic Contracting Formalities .....	8
8.	Enforcement Measures .....	9
9.	Electronic and Digital Signatures .....	9
10.	Smart Cards & e-Money .....	14
11.	Compliance Advice .....	17
12.	Acknowledgements .....	18
13.	Useful Links .....	21
14.	Articles .....	23

## 1. Executive Summary

Commerce by electronic means has seen steady growth since the early days of electronic communications, but in recent years, the development of the Internet and World Wide Web, combined with the increasing sophistication and falling price of both business and consumer technologies, has seen a dramatic expansion in the role of e-commerce in both B2B and B2C relationships, in addition to its driving influence in the newer area of C2C transactions.

The rapid growth and increasing role of e-commerce has resulted in significant activity on the part of governments and international organisations to ensure that it continues to

develop within a comprehensive and contemporary framework of legal regulation. This has often meant legislators engaging in a radical rethink of existing regulatory mechanisms in order to accommodate the unique features of new e-commerce related technologies.

This paper provides an introduction to an array of e-commerce related technologies and legislation, whilst focusing, in particular, on the effect that these may have upon FE and HE institutions in the UK. Whether an institution is providing e-commerce services for consumers (e.g. advanced distance learning courses), contracting to use e-commerce services from other businesses (e.g. online purchasing), or simply adopting e-commerce related technologies in the workplace and among student populations (e.g. [smart cards/electronic purses](#)) those involved in their adoption and provision will need to be aware of the developing legal framework.

Additionally, the adoption of e-commerce technologies will also require managers and administrators responsible for their implementation and oversight to ensure that their institution is aware of the implications of broader legislative initiatives, such as data privacy and freedom of information for any proposed uses of e-commerce technology.

This briefing paper describes:

- Recent developments in the UK legislative framework applicable to e-commerce practices and related technologies
- Issues arising from those recent developments applicable to FE and HE institutions
- Measures that may be taken to ensure compliance with the UK legislative framework

It is of interest to:

- Deputy Principals, Pro-Vice-Chancellors and other senior managers responsible for legal compliance
- Senior managers and administrators responsible for implementation and oversight of e-commerce related developments in their institutions
- Senior managers responsible for information, IT and other institutional strategies.

### **Key Issues to Note**

1. The effect of developing e-commerce legislation on the sale of goods and services via the Internet, both nationally and within the wider [European Economic Area](#) (EEA).
2. The impact of e-signatures legislation on traditional forms of verification, authentication and repudiation of contracts and other commercial documents
3. The rules imposed by e-money legislation on the issuance and use of electronic stored payment systems like smart cards and electronic purses
4. The wider legal implications of the adoption of e-commerce technologies including privacy, and freedom of information.

## 2. Introduction

e-Commerce remains a high growth area of the economy despite the collapse of the dot.com bubble. The collapse of overheated investment in IT and e-commerce stocks almost at a stroke removed the majority of the highly speculative and often poorly planned business ventures. Institutions seeking to develop the use of e-commerce services are now much more cognizant of the need for a clear, logical and coherent business plan to ensure success. An important element of that business plan has to be a broad understanding, on the part of both senior management and those tasked with implementing the necessary technical and institutional elements, of the legal environment in which the institution's e-commerce services will be operating.

Much of the UK's current legislation in the area of e-commerce has arisen as a result of the need to implement [EU Directives](#). The EU regards the effective legal regulation of the e-commerce sector as a vital element in stimulating future economic growth, promoting closer integration, and allowing the EU to play a direct role in the setting of international technical, commercial, and legal standards. As such, the EU has issued a series of key Directives over the past 8-10 years which either directly, or indirectly, have had the effect of placing e-commerce services within a tighter regulatory framework. These Directives include the [1995 Data Protection Directive](#), the [1997 Distance Contracts Directive](#), the [1999 Electronic Signatures Directive](#), the [2000 e-Commerce Directive](#), the [2000 e-Money Directive](#), and the [2002 Privacy and Electronic Communications Directive](#).

The EU's legislative initiatives in the e-commerce arena have thus put significant pressure on Member State governments to pass national measures to implement the Directives. However, EU Directives are problematic because:

- Member States are permitted significant leeway in their implementation and often implement Directives in ways which render their national implementing legislation partially incompatible with that of other Member States e.g. the 1995 Data Protection Directive may in fact have widened some differences between the Member States' national data privacy laws rather than narrowing them;
- they tend to be drafted in very general terms, rather than in the very precise terms usually found in UK Acts of Parliament;
- a considerable amount of time may pass from the initial proposal of a Directive by the European Commission to its adoption by the European Parliament and Council to its final implementation by the Member States, e.g. the 1995 Data Protection Directive was first proposed in 1990, was adopted in 1995 and finally implemented by all Member States in 2003.

Thus, in combination with the continual advances in available technologies, which have led to rapid changes in business practices and commercial opportunities, national legislation is sometimes little aid to, or even obstructive of, the development of new e-commerce services. An example of this can be seen in the development of [m-](#)

[commerce](#) where mobile phone operators found their plans to develop the use of mobile phones as electronic wallets obstructed by the nature of the UK's implementation of the [e-Money Directive](#), as money placed in prepay accounts and used to buy non-phone services, such as subscribing to a website or entering prize competitions would be held to be e-money, under UK [Financial Services Authority](#) rules, and thus required to be [held in trust](#) by the mobile networks. Given that mobile phone operators have tended to use prepay money essentially as a cash float, a requirement to place any prepayment defined as e-money in trust would severely limit their operations. This has naturally slowed the implementation of new 'm-commerce' services by the mobile phone operators.

Awareness of existing legal regulation of e-commerce and a grasp of how the law may affect the possible uses of e-commerce services in the FE and HE sectors is thus critical. Failure to adequately address the relevant legal issues may well result in costly and institutionally damaging setbacks to the implementation of e-commerce services.

### 3. e-Commerce and Distance Selling

This section will discuss the general legislative framework for e-commerce in the UK It will concentrate primarily on e-commerce issues of importance to FE and HE institutions and is not an exhaustive overview of the content of the legislation, which is wide ranging. The [Department of Trade and Industry](#) provides detailed guides to the key pieces of UK implementing legislation, the [Consumer Protection \(Distance Selling\) Regulations 2000](#), and the [Electronic Commerce \(EC Directive\) Regulations 2002](#). ***Consumer Protection (Distance Selling) Regulations 2000.***

[The EU Distance Selling Directive](#) was adopted on 20 May 1997 and was implemented in the UK by means of the [Consumer Protection \(Distance Selling\) Regulations 2000](#). These Regulations came into force on 31 October 2000. The Regulations apply only to contracts concluded in the context of organised distance sales or service-provision schemes, and apply to the sale of goods or services to [consumers](#):

- on the Internet
- on interactive digital television
- by mail order, including catalogue shopping
- by telephone
- by fax
- by advertising on television or radio, in newspapers or magazines,

The Regulations do not apply to:

- contracts relating to the supply of financial services
- B2B transactions.
- sale of land or buildings
- sale of land plus construction of buildings
- vending machines
- public pay phones

- auctions, including Internet auctions

#### *General information requirements*

The institution must provide clear and comprehensible information to enable the consumer to decide whether to buy, including:

- the institution's name and, if payment is required in advance, its address.
- a description of the goods or services
- the price including all taxes
- delivery costs where they apply
- arrangements for payment and for delivery of goods or performance of services - if no date is specified delivery or performance must be within 30 days of the order
- the right to a cooling off period during which the consumer may cancel the order for any reason, unless the sale is covered by one of the exceptions to the right to cancel
- how long the offer or the price remains valid
- the minimum duration of the contract in the case of a contract to supply goods or services continuously or recurrently
- if the supplier wants to be able to offer substitute goods or services if those ordered are no longer available, the consumer must be told of this in advance and informed that in this case the cost of returning substitute goods would be borne by the supplier.

This information can be given in any form that is appropriate to the means of distance communication being used e.g. on a website in the case of e-commerce sales.

#### *Written confirmation*

When a distance contract has been made the institution must send to the consumer confirmation of the main items of prior information. This confirmation must be provided in writing or another durable medium, such as fax or e-mail, unless it has already been provided in writing, e.g. on the institution's website. It should include details about when and how the consumer can exercise the right to cancel, a geographical address where he can contact the institution, and details of any after-sales services and guarantees.

The consumer must be informed if the contract includes a term that will require that the consumer return the goods in the event of cancellation and whether the consumer or supplier will be responsible for the cost of return. If the contract is for a service with no specified end date or for a period of more than one year details must be provided about when and how the consumer can terminate the contract. The institution must provide this written confirmation at the latest by the time that the goods are delivered or, in the case of services, before or at an early stage during the performance of the contract.

#### *Cooling off and cancellation*

The Regulations provide a cooling off period and an unconditional right to cancel during that period. The purpose of the cooling off period is to allow the consumer the opportunity he would have had in a conventional shop to examine the goods or to reflect on the nature of the service before deciding to buy. The cooling off period begins as

soon as the order has been made and ends, in the case of services, seven working days after the day the order was made or, in the case of goods, seven working days after the day of receipt of the goods. There are some exceptions to the cooling off period and the right to cancel.

The Regulations require the consumer to send a notice of cancellation in writing, including fax or e-mail. The notice may be given either to the supplier or to a person notified to the consumer by the supplier as a person to whom the consumer may send the cancellation notice. The effective date of cancellation for the purposes of the Regulations is the date on which the notice is sent. When a consumer cancels the order all money paid must be returned within 30 days of the date the notice of cancellation is given.

#### 4. The e-Commerce Directive

[The EU e-Commerce Directive](#) was adopted on 8 June 2000 and has been implemented in the UK by means of the [Electronic Commerce \(EC Directive\) Regulations 2002](#).

These Regulations came fully into force on 23 October 2002. They apply to the provision of '[information society services](#)', e.g. [B2B](#) and [B2C](#) services, including:

- services provided free of charge to the recipient (e.g. funded by advertising or sponsorship revenue)
- services allowing for online electronic transactions (e.g. interactive online shopping)
- online trade and advertising (e.g. on the Internet, by email or by mobile phone), regardless of whether the goods or services in question are themselves delivered electronically.

The Regulations do not apply to:

- the actual goods
- any off-line delivery of goods or services
- off-line elements of any transaction that began online (e.g. off-line contract negotiations after a response to a website advertisement).
- on-line activities that are not of a commercial nature.

The Regulations treat B2B and B2C services differently, with wider discretion in B2B services for businesses to opt out of some of the measures designed primarily to protect [consumers](#) using B2C services.

*Jurisdiction, 'country-of-origin rules' and choice of law*

UK law will, generally, apply to information society services provided from the UK, wherever in the [EEA](#) they are delivered. This is known as 'country-of-origin regulation'. However, the e-Commerce Directive's 'country-of-origin regulation' does not apply to certain aspects of consumer contracts, which are governed by the '[Brussels Regulation](#)'. The Brussels Regulation states that, while the Member State where an information society service provider is based has jurisdiction over civil and commercial matters

involving that provider, there are exceptions to this general principle concerning consumer contracts. Consumers within the EU are given the right to bring proceedings against information society service providers *either* in the courts of the Member State of the consumer's domicile *or* in the courts of the Member State of the entrepreneur's domicile, if:

- the contract executed between the consumer and the seller is for the sale of goods on installment credit terms, a loan repayable by installments or for any other form of credit made to finance the sale of goods; or
- the seller pursues commercial or professional activities in the Member State where the consumer lives, or directs such activities to that Member State, and the subject contract falls within the scope of such activities.

This suggests that information society service providers who enter into consumer contracts with consumers, without limiting their activities to consumers domiciled in certain Member States, may face the risk of being sued in any Member State. It is presently unclear in what circumstances the exception for activities directed at consumers in a foreign Member State might apply, or how an information society service provider might arrange its web site marketing in order to lessen its risk of being subject to a claim in a foreign Member State.

The United Kingdom Department of Trade and Industry has published a [Guidance Note](#) addressing these questions. This suggested that:

- If an information society service provider sells to consumers in other Member States and this is reflected in its web site, consumers will likely be entitled to sue in their Member States of domicile.
- A web site may be seen as being directed to other Member States if it offers, for example a choice of languages or currencies of those Member States, or gives product specifications, delivery times or prices for those Member States.
- If the information society service provider intends to sell its products or services in certain specific Member States only, and the web site in question reflects this intent, it is less likely to be sued in other Member States.

The Brussels Regulation does not affect the choice of law governing the substance of a dispute. This is governed by the '[Rome Convention](#)' of 1980, which applies to all European Economic Area countries and allows consumers the protection of the mandatory laws of their own country. This can override the law specified by an information society service provider in its contracts, thus information society service providers should ensure they are aware of the impact of the different mandatory consumer protection laws in Europe and avoid dealing with consumers in countries whose laws they do not wish to be bound by.

## 5. General Information Requirements

An institution providing an information society service must make available to a recipient of the service, in a way that is easily, directly and permanently accessible:

- the name of the institution
- the institution's address in the [EEA](#) country whose laws will generally apply to the provision of the service in question
- details about the institution, including an email address for rapid, direct and effective contact.
- where the institution is registered in a trade register available to the public, and this information is relevant to the service provided, details of that register and the institution's registration.
- where the provision of the service requires authorisation, the particulars of the relevant supervisory authority.
- where the institution undertakes an activity that is subject to VAT, the relevant identification number.

## 6. Commercial Communications

Commercial communication by an institution which constitutes or forms part of an information society service (e.g. an advertising email) must:

- be clearly identifiable as a commercial communication;
- clearly identify the person on whose behalf the commercial communication is made;
- clearly identify as such any promotional offer (including any discount, premium or gift) and ensure that any conditions that must be met to qualify for it must be easily accessible, and presented clearly and unambiguously; and
- clearly identify as such any promotional competition or game and ensure that any conditions for participation are easily accessible and presented clearly and unambiguously.

Unsolicited commercial communications sent by email must be capable of being identified as such as soon as they are received. The Directive requires senders to consult and respect opt-out registers where individuals have indicated that they do not want to receive unsolicited commercial communications. The UK Regulations do not deal with issue of opt-in/opt-out for unsolicited commercial communications as the government felt that this was already adequately addressed by UK data protection legislation.

## 7. Electronic Contracting Formalities

The Regulations do not deal with contract formation itself. This remains subject to common law, existing statutory provisions or the law of another relevant Member State. However, they do provide for specific formalities which must be observed during the contracting process. Where a contract is to be concluded online, an institution must, in advance of an order being placed, inform the recipient about:

- the different technical steps to follow to conclude the contract, so that recipients are made aware of what the process will involve and the point at which they will commit themselves;
- whether or not the concluded contract will be filed by the institution and whether it will be accessible.
- the technical means for identifying and correcting input errors prior to the placing of the order; and
- the languages offered for the conclusion of the contract.

These requirements do not apply:

- where the initial contact is made via a website but, for reasons relating to the complexity of the contract, it is actually concluded offline
- to contracts concluded exclusively by exchange of email or by equivalent individual communications.

An institution must also indicate which codes of conduct it subscribes to that are relevant to the order, and give information on how those codes can be consulted electronically. Where the institution provides terms and conditions applicable to the contract to recipients, the institution must make these available to them in a way that allows them to store and reproduce them.

Where the recipient of the service places an order through technological means, an institution must:

- acknowledge receipt of the order to the recipient without undue delay and by electronic means
- make available suitable technical means allowing the recipient to identify and correct input errors before placing the order

## 8. Enforcement Measures

The Director General of Fair Trading and other consumer-protection bodies can apply to the courts for [Stop Now Orders](#) where the continuing infringement of the Regulations by an institution harms the collective interests of consumers. The courts will also be able to order institutions to publish corrective statements with a view to eliminating the continuing effects of past infringements.

## 9. Electronic and Digital Signatures

As an increasing number of commercial transactions are carried out electronically, with no complementary paper documentation, the traditional mechanisms by which the parties to a transaction may identify themselves, demonstrate their intent to enter into a transaction, and validate the terms of that transaction, have had to be re-examined. The traditional way of performing those three tasks has often been by way of a signature (e.g. the signature on the deed for the sale of a house, or the signature on a credit card

slip authorising payment by the credit card company to the vendor on behalf of the purchaser). Written signatures may thus demonstrate that

- a transaction involving the signer has taken place (evidence)
- the signer has understood that they are entering into a contract (ceremony)
- the signer has agreed to the terms of the contract (approval).

Clearly, while a signature may represent these elements, this may be a rebuttable presumption in each case – signatures may be forged (negating evidence); the signer may not understand that they are in fact entering into a binding agreement (negating the effect of ceremony); or a vendor may misrepresent the contract terms (negating approval).

Formal requirements for legal transactions, including the need for signatures, have varied across legal systems, and with the passage of time. Today, most legal systems have reduced the need for formal requirements, such as a written contract complete with written signature, or have minimized the consequences of failure to satisfy such formal requirements, for a wide range of common commercial transactions. Nevertheless, good practice dictates that the degree of formality applicable to a particular transaction, even where such formality is not required by law, should be sufficient to assure the parties of its validity and enforceability.

The historical concept of a "signature" is extremely broad, in that legal systems may recognise as a signature any mark made with the intention of authenticating the marked document (e.g. John Smith, His Mark X). In a digital setting, today's broad legal concept of "signature" may well include markings as diverse as:

- digitized images of paper signature;
- typed notations such as "/s/ John Smith";
- or even addressing notations, such as electronic mail origination headers.

These are commonly termed [electronic signatures](#) and should be distinguished from the concept of [digital signatures](#). Unfortunately, the two terms are often wrongly perceived as interchangeable, and thus "digital signature" may be found in the literature in a context which indicates it means any form of computer-based signature.

From an information security perspective, a "digital signature" means the result of applying certain specific technical processes to specific information, in a process known as "public key cryptography". This uses an algorithm employing two different but mathematically related "keys;" one for creating a digital signature or transforming data into a seemingly unintelligible form (the "private key"), and another key for verifying a digital signature or returning the message to its original form (the "public key"). If many people need to verify the signer's digital signatures, the public key must be available or distributed to all of them, perhaps by publication in an on-line repository or directory where it is easily accessible.

Computer equipment and software utilizing two such keys are often collectively termed an "asymmetric cryptosystem." A further process often, but not always, linked with public key encryption and which can be used in the creation and verification of a digital signature is the hash function, which when applied to a particular message creates a unique number in the form of a hash value (the "message digest").

The use of a digital signature utilising the hash function can be described thus:

- Alice wishes to send Bob a document, and to ensure that the document cannot be secretly altered in transit without Bob knowing about it;
- Alice creates a key pair consisting of a "private key" and a "public key";
- Alice creates a document, and uses the "hash function" of her encryption software to generate the "message digest" for it. This message digest will be unique to the document, as any change made to the document will result in the hash function producing a different message digest
- Alice then enciphers the message digest with her private key. The enciphered message digest, which is sent to Bob with the original document, becomes Alice's digital signature for that document;
- Bob can decipher the message digest only if he uses Alice's public key, and can thus verify that Alice sent the document (assuming that the public key is in fact created by Alice). He can also verify the integrity of the document by creating his own message digest of the document and comparing it to Alice's deciphered message digest. If the two message digests are identical, Bob can be sure the document has not been altered in transit from Alice.

From a legal perspective the use of digital, as opposed to simple electronic signatures, provides two key evidentiary elements:

- because digital signatures cannot easily be forged, unless the signer loses control of his private key either accidentally or intentionally, they can provide a high level of authentication of the signer (evidence)
- digital signatures can protect the integrity of the content of a message/document when used with the hash function, as alterations to the message/document can easily be proved by reference to the message digest (authenticity)

However, the potential weakness in a PKI system can be proving who actually participated in a particular transaction, in other words, how do we know Alice is Alice? In the previous example, the "key pair" created by Alice has no automatic connection with any person; it is simply a pair of numbers. Thus, Eve, a third party wishing to interfere with Alice and Bob's communications, might place a public key on a website stating that it is Alice's public key. If she then sends a message to Bob which purports to come from Alice but is in fact signed with Eve's private key, when Bob uses the fake public key he will not know that the message/document has in fact come from Eve rather than Alice.

There are two potential solutions to this problem which permit the association of a particular identity with a key pair and, consequently, to prove beyond any doubt, the

existence of this association, the identity of the signer and the integrity of the message in order to prevent a party from denying the origin, submission or delivery of the message and the integrity of its contents (repudiation):

- Alice and Bob could arrange in advance to exchange Alice's public key and then use that to communicate. But this presupposes that Alice and Bob have had a secure communications channel over which to exchange a key - and this is generally not the case with Internet communications which often occur between parties that have not had prior dealings.
- In the absence of such a secure communications channel, non-repudiation of digital signatures can be guaranteed by the involvement of a "Trusted Third Party" (TTP). In e-commerce these are usually bodies known as "certification authorities" (CAs or CSPs). A certification authority undertakes the confirmation of the identity of the subject of a digital signature, and issues a digital certificate which links a public key explicitly to that specific identity and, depending upon the level of inquiry used to confirm the identity of the subject, the certificate provides the recipient of a message with a variable level of confidence in the authenticity and authorship of the message. Certification authorities themselves are usually authenticated by some method, to confirm the legitimacy of their certificates. Usual methods of CA authentication are by cross-authentication between CAs, or by hierarchies of CA's with a "Root CA" (such as a government agency) at the apex of the hierarchy.

The EU law concerning electronic and digital signatures takes the form of the [1999 Electronic Signatures Directive](#), whilst in UK law the relevant implementing legislation is the [Electronic Communications Act 2000](#) and [Electronic Signatures Regulations 2002](#).

The Electronic Communications Act 2000 provides:

- the government with powers to introduce a voluntary accreditation scheme for businesses which offer encryption and digital signature services.
- the government with powers to amend references to 'writing', 'signatures' and 'paper' in existing legislation to make it clear that these requirements may be met electronically.
- that e-signatures are admissible in legal proceedings, although the weight given to them will depend on the technology used.

The Electronic Signatures Regulations 2002 require:

- the Secretary of State for Trade and Industry to keep a public register of 'certification service providers' (CSPs) who purport to offer 'qualified certificates'. A certificate is defined as an electronic confirmation that a particular e-signature belongs to a named individual. A qualified certificate is one that meets certain standards set out in the Regulations. CSPs purporting to offer such certificates must adhere to both the applicable standards for these certificates and those in respect of their own conduct. The Secretary of State is obliged to publicise any failure to meet these standards which comes to her attention.

- CSPs issuing or guaranteeing qualified certificates to the public liable to anyone who suffers a loss as a result of reasonably relying on such certificates (unless the CSP can prove that it was not negligent) and provide that CSPs based in the UK can obtain only such personal data as they need to issue a certificate from the relevant data subject. They may only process this data to the extent necessary for issuing a certificate.

In practice, however, the impact of the legislation to date has been minimal. The Directive introduces a special category of 'advanced electronic signatures' (AESs), largely equivalent to digital signatures, which must be treated as the equivalent to handwritten signatures, but it appears that neither a UK- nor a Commission-endorsed AES is yet available. In any event, the UK government has chosen not to introduce specific legislation implementing the section of the Directive which provides that an AES must be treated as the equivalent of a handwritten signature as the government believes that a court would already have to give an e-signature meeting the requirements for an AES evidential weight equal to that of a handwritten signature.

The UK government has not yet exercised its powers to introduce a voluntary accreditation scheme for CSPs, as it currently considers the industry self-regulated [tScheme](#) to be sufficient, and has used its powers to amend legislation relatively rarely e.g. to permit the filing of company documents electronically and the issuing of electronic prescriptions for medicines. With regard to CSP liability, while the Directive provides that a CSP has *prima facie* liability for its qualified certificates, it also permits a CSP to limit the purposes and, in particular, the value of transactions for which its qualified certificates may be used. The UK has not implemented this right to limit liability, since the government believes that a CSP can already do so, subject to applicable laws on exclusion and limitation of liability.

However, it is clear that the EU sees the role of e-signatures continuing to grow, as demonstrated in the [2001 Invoicing Directive](#), implemented in the UK by the [Value Added Tax \(Amendment\) \(No. 6\) Regulations 2003](#) on 1 January 2004. This allows for electronic invoicing provided that:

- the customer accepts the electronic invoice;
- the authenticity of the origin and the integrity of the contents of the invoice are guaranteed either by using an advanced electronic signature, or Electronic Data Interchange (EDI);

and requires all Member States to accept these two methods whilst permitting Member States to also accept other means of e-invoicing for supplies on their territory, and not imposing the requirement of authenticity of origin and integrity of contents. In the UK, this means that, as [HM Customs and Excise](#) has allowed unsigned fax and e-mail invoices and the posting of invoices to a website for UK domestic transactions, that these practices may continue. However, if the invoice prepared by a UK company, such as an FE or HE institution, relates to a transaction in another Member State's territory (e.g. France), the French authorities must also have adopted the UK position. If French

VAT law does not allow e-mail invoicing (and it doesn't), the e-invoice prepared by the UK company will need to be compliant with the French VAT rules.

## 10. Smart Cards & e-Money

HE and FE institutions have for many years provided their staff and students with a means of identifying themselves as members of the institution; this usually takes the form of some sort of PhotoID card. Often this card has performed other functions as well e.g. the addition of a bar-code permitting the use of the card as an identifier for institutional computer systems such as library entry and borrowing systems. Most institutional cards have tended to be [dumb cards](#), with relatively simple functions based around bar-codes or magnetic strips. However, with the advent of [semi-dumb cards](#) and [smart cards](#), the ability of cards to perform more complex tasks has rapidly increased, and several institutions have trialed cards that can function as [electronic purses](#), capable of use for payment across a range of institutional services, and sometimes for third party services. A key advantage of smart cards is that they can perform functions without immediate access to a central computer system.

The use of ID cards generally raises a number of legal issues, the most obvious being those relating to privacy and security. Institutions have to be aware that the collection of data via the use of cards that can be linked to an identifiable individual, e.g. records of entry and exit from buildings on campus, will be covered by the data protection principles laid out in the data Protection Act 1998. These principles require amongst other matters that there to be a purpose for which personal data is collected and used; that the data only be used for that purpose; and, when the data is not longer required for that purpose, that it be destroyed. It is clear therefore that institutions should be aware of the nature and scope of any data collection via card systems relating to identifiable individuals; be able to justify the purpose of that collection and use; and have measures in place to ensure that the data is held in accordance with all the data protection principles, until such time as it is no longer required.

As smart cards have become decreased in cost, and become much more widely available, their use as electronic purses on an institutional basis has become theoretically feasible. An institutional smart card could thus not just be a means for access to buildings and services, but could also function as a cashless payment system for institutional services ranging from photocopying to cafeteria purchases, and additionally for purchases from selected third parties. Several Universities, including Aston, Exeter, Edinburgh, Nottingham and York Universities trialed such a system in conjunction with Mondex in the mid-to-late 1990s, all eventually abandoned the system, primarily due to the cost of running the system. However, as the Higher Education Smart Card Association (HESCA) point out,

Universities still want to deploy smart cards. This is even truer as the cost of administration continues to rise and as more and more automation is introduced for the provision of student services and facilities on and off campus. The replacement of the current high number of single function

plastic cards by one secure, long lived multi-application smart card, offers a number of measurable benefits

HESCA suggest that the potential range of applications for smart cards within the FE and HE sector include:

- Electronic purse for all payments (refectory, photocopying, vending, laundry)
- ID supported by photo or biometric information
- Physical access into rooms, dormitories
- Log-in access into PC's, documents
- Examination access control
- Student Union membership
- Society membership
- Lecture attendance recording
- Course accreditation recording
- Curricular schedule
- Car-parking
- Off Campus Learning
- Student Voting
- The recording of other rights and privileges

It is no co-incidence that electronic purses are at the head of this list. Many people believe that despite early teething problems, electronic money, or more popularly [e-money](#), has the potential to take over from cash as the primary means of making small-value payments and could make such transactions easier and cheaper for both consumers and businesses, as such considerable development continues on electronic money systems within both the financial services and telecommunications industries.

This interest has not gone unnoticed by the financial regulatory authorities. While e-money may provide considerable benefits, it also potentially poses important hazards, in terms of liability for loss, possibilities of fraud, and its potential use for money-laundering. As a result, in 2000 the European Union introduced a new directive to regulate the use of certain types of e-money - the [e-Money Directive](#). In 2002, this Directive was implemented into UK law by the [Financial Services and Markets Act 2000 \(Regulated Activities\) \(Amendment\) Order 2002](#) and the [Electronic Money \(Miscellaneous Amendments\) Regulations 2002](#).

It is important to remember that when people talk about 'e-money', they are usually referring to one of the following three categories:

- stored value or prepaid products in which a record of the funds or value available to the consumer is stored on a device in the consumer's possession. This definition includes both prepaid cards (including electronic purses) and prepaid software products that use computer networks such as the internet (sometimes called digital cash). It is issuance of this type of e-money that is regulated by the EU's E-money Directive and the UK implementing legislation, where the e-money

has been issued on receipt of funds and accepted as a means of payment by persons other than the issuer, i.e. if A pays B £10 cash for a stored value of £10 contained on a prepaid card supplied by B, which A intends to use to electronically purchase goods and services from third parties, that stored value is e-money. If A pays B £10 cash for a stored value of £10 contained on a prepaid card supplied by B in order to purchase services only from B, and not from third parties, that stored value is not e-money. Thus, the stored value on a University library photocopy card, which can only be used in the University library, is not e-money, but the stored value on a University smart card which allows staff and students to purchase goods from local retailers that are not part of the University will be e-money.

- systems that transfer funds to and from special e-money accounts, which operate under the ambit of banking regulations;
- systems that manipulate existing payment mechanisms such as credit cards e.g. PayPal. These arrangements remain unregulated because the service provider does not issue value or establish customer accounts.

Where an institution wishes to implement an e-money system it is important to determine whether that system may fall within the definition of 'e-money' regulated by UK law. The effect of the UK legislation is that issuing e-money is a regulated activity under the Financial Services and Markets Act 2000 and may only be undertaken by institutions which are authorised by the [Financial Services Authority](#) (FSA), and those institutions must comply with both the regulations and the [FSA Business Rules](#).

Institutions issuing e-money are known as "Electronic Money Institutions" (ELMIs). They must be located within the UK, and must have minimum capital of 1 million Euros or at least 2% of outstanding e-money liabilities, whichever is the higher. ELMIs may not have holdings in other businesses except those which also provide e-money related functions. They are also required to have sound and prudent systems and adequate internal control mechanisms and must comply with the FSA's money laundering requirements. The regime places a limit on electronic purse size at £1000 per purse, to protect consumers against the consequences of failure of the e-money issuer, although a larger purse may be permitted where a higher level of safeguards are in place. E-money must also be redeemable at par value (minimum of €10).

Importantly for FE and HE institutions, waivers of part, or all, of the regulatory requirements can be granted on a case-by-case basis for small e-money issuers, such as for use on a university or college campus, whose e-money devices offer a maximum storage of €150 and whose total liabilities are usually €5 million (and do not exceed €6 million). There will remain, however, an obligation to submit periodic information about their businesses to the FSA.

The [Financial Services Compensation Scheme](#) (FSCS) does not apply to e-money issuers, and thus customers will have no right to compensation should an ELMI become insolvent. ELMIs do, however, fall within the scope of the [Financial Ombudsman Service](#) and will require their own procedures for dealing with customer complaints. As the ELMI is ultimately responsible for redeeming its own e-money, in the event that it

becomes insolvent, its issued e-money is likely to be worthless. Possible implications of this could be that:

- third parties who have accepted e-money for a transaction in ignorance of the insolvency, may not be permitted to refuse to perform the transaction and/or demand some other form of payment from the payer.
- service providers who re-brand third party e-money as their own may find themselves liable to redeem that e-money, at least for their own customers.

It may be possible to ameliorate some of these risks via customer terms and conditions, although many e-money users will be consumers and thus consumer protection rules will apply to those terms and conditions, making unfair terms unenforceable against the consumer, thus institutions proposing to enter into an e-money arrangement should be aware of the potential liabilities.

## 11. Compliance Advice

It will be clear from the foregoing that within the last 5 years, the regulation of e-commerce has undergone a rapid and radical transformation. The activities of FE and HE institutions are not immune from those changes. Indeed, the FE and HE community's proactive engagement with new technologies whether to facilitate remote distance learning courses, or to provide an e-campus, or simply to harmonize the multitude of cards and tokens currently required for the smooth running of a campus in combination with an electronic purse, may now leave its members exposed to legal risks that were unforeseen when those technologies were initially implemented, or trialed. Institutions should thus be aware of the implications of:

- the [Consumer Protection \(Distance Selling\) Regulations 2000](#) for the legal provision of institutional distance services to consumers, such as remote distance learning courses/packages, in particular the rights of those consumers to be provided with particular important information about their contract in a durable medium, and to cancel the contract within the cooling off period without penalty
- the [Electronic Commerce \(EC Directive\) Regulations 2002](#) for the law governing e-commerce contracts between the institution and both its suppliers and its customers; the information provision requirements relating to e-commerce transactions; and the requirements of form for commercial communications in the course of e-commerce, and their relation to the Brussels Regulation and Rome Convention.
- the [Electronic Communications Act 2000](#) and [Electronic Signatures Regulations 2002](#) for the future treatment of both electronic and digital signatures by the courts, which may have implications for institutional policy upon the proper use of signature technologies for institutional messages and documents sent by electronic means, in particular VAT invoices.
- the [Financial Services and Markets Act 2000 \(Regulated Activities\) \(Amendment\) Order 2002](#) and the [Electronic Money \(Miscellaneous Amendments\) Regulations 2002](#) for the future introduction of e-money systems, particularly systems that will

be accepted as a means of payment by persons other than the issuing institution. Institutions should also be aware of the potential liabilities when entering schemes where the institution is not the primary issuer, but accepts a particular ELMI-issued e-money or rebrands an ELMI's e-money as its own.

## **12. Acknowledgements**

The JISC wishes to thank Andrew Charlesworth of the Centre for IT and Law, University of Bristol for writing this paper and [whoever] for their comments.

## Definitions applicable to this Briefing Paper

'B2B' - business-to-business.

'B2C' - business-to-consumer.

'C2C' - consumer-to-consumer.

'Consumer' - for the purposes of the Distance Selling Regulations and the e-Commerce Regulations, a consumer is any natural person who is acting for purposes other than those of his trade, business or profession."

'electronic commerce' or 'e-commerce' - the conduct of a financial transaction by electronic means, increasingly used to mean the buying and selling of goods and services on the Internet, especially the World Wide Web.

'European Economic Area' - the European Economic Area consists of the European Community member states plus Iceland, Liechtenstein and Norway.

'European Union' – the European Union consists of Austria, Germany, Netherlands, Belgium, Greece, Portugal, Denmark, Ireland, Spain, Finland, Italy, Sweden, France, Luxembourg, United Kingdom.

'EU Directive' – A Directive is a piece of EU legislation which set out a legislative goal for the Member States, to be reached by a certain date, but allows them significant discretion as to how exactly that goal will be obtained within their national legal systems.

'mobile commerce' or 'm-commerce' - the buying and selling of goods and services through wireless handheld devices (e.g. cellular telephone and personal digital assistants); a subset of e-commerce

'e-money' - monetary value that is stored on an electronic device (e.g. a chip or computer memory), issued on receipt of funds, that is accepted by undertakings other than the issuer and that is generally intended to make payments of a limited amount; an electronic surrogate for coins and bank notes.

'dumb card' - a plastic card that contains machine readable information, but no microprocessor or memory chip, these usually take the form of a magnetic stripe card (e.g. security access cards)

'semi-dumb card' - a integrated circuit card with a memory chip with non-programmable logic which can undertake a pre-defined operation (e.g. pre-paid phone cards). Often included in the definition of a 'smart card'.

'smart card' - a integrated circuit card that has a microprocessor and memory functions which can add, delete, and otherwise manipulate information on the card (e.g. electronic cash payment cards). In theory, data residing in the chip can be protected against external inspection or alteration, so effectively that the vital secret keys of the cryptographic systems used to protect the integrity and privacy of card-related communications can be held safely against all but the most sophisticated forms of attack.

'electronic purse' - an application in an integrated circuit card able to store and manipulate an electronic value.

'information society services' - services normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data and at the individual request of a recipient of a service

'electronic signature' – data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication (e.g. email headers or a bitmap signature)

'digital signature' or 'secure electronic signature' or 'advanced electronic signature' – a technical mechanism, usually based on asymmetric cryptography (public key cryptography) which is uniquely linked to the signatory; capable of identifying the signatory; created using means that the signatory can maintain under their sole control; and linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

'Stop Now Orders' - The Stop Now Orders (EC Directive) Regulations 2001 created a new enforcement system, under which the OFT and other enforcement partners have strengthened powers to stop businesses from breaching a wide range of UK consumer protection laws. The usual action is to seek a business's voluntary agreement to put things right - an informal undertaking. However, the ultimate sanction is court action to seek a Stop Now Order. Failure to comply with a Stop Now Order is treated as contempt of court, punishable by fines or imprisonment.

tScheme - *tScheme* is the independent, industry-led, self-regulatory scheme set up to create strict assessment criteria, against which it will approve Trust Services. - <<http://www.tscheme.org>>

'held in trust' – A trust is an equitable right, title or interest in property, real or personal, distinct from its legal ownership. To put it another way, in the mobile telecommunications example, if A places £10 in B's mobile phone electronic wallet scheme with the aim of buying services from a third party or parties, B is not in a position to spend that money, because the law says that B is holding the money on behalf of A until such time as A decides to pass the money to a third party or withdraw it from the prepayment scheme – the money is thus held in trust by B for A for the eventual payment of a third party or until the trust is revoked. Prepayment for mobile telephony services is not deemed to be held in trust, so if A buys a £10 prepayment voucher from B, B can use that money as his own, which is what mobile phone companies do with prepayment for their own services.

## 13. Useful Links

### **Convention on the law applicable to contractual obligations (Rome Convention)**

*Official Journal of the European Communities* L 266, 09 October 1980 pp. 1 – 19.

On-line database on the Convention on the Law Applicable to Contractual Obligations (Rome 1980)

<<http://www.rome-convention.org/>>

DTI, Guidance Note: Cross border consumer contractual disputes: Guidance on the rules of jurisdiction and applicable law - 1980 Rome Convention

<[http://www.dti.gov.uk/ccp/topics1/guide/jurisdiction\\_rome.htm](http://www.dti.gov.uk/ccp/topics1/guide/jurisdiction_rome.htm)>

### **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (The Data Protection Directive)**

*Official Journal of the European Communities* L 281, 23 November 1995, pp. 31-50.

The UK Data Protection Act 1998

<<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>>

### **Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in respect of Distance Contracts (The Distance Selling Directive)**

*Official Journal of the European Communities* L 144, 4 June 1997, pp. 19-27.

The Consumer Protection (Distance Selling) Regulations 2000, SI 2000 No. 2334.

<<http://www.hmso.gov.uk/si/si2000/20002334.htm>>

Consumer Protection (Distance Selling) Regulations: Guide for Business

<[http://www.dti.gov.uk/ccp/topics1/pdf1/bus\\_guide.pdf](http://www.dti.gov.uk/ccp/topics1/pdf1/bus_guide.pdf)>

### **Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (The Electronic Signatures Directive).**

*Official Journal of the European Communities* L 013, 19 January 2000, pp. 12-20.

The UK Electronic Communications Act 2000

<<http://www.hmso.gov.uk/acts/acts2000/20000007.htm>>

The UK Electronic Signatures Regulations 2002, SI 2002 No. 318

<<http://www.hmso.gov.uk/si/si2002/20020318.htm>>

### **Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (The e-Commerce Directive).**

*Official Journal of the European Communities* L 178, 17 July 2000, pp. 1-16.

The UK Electronic Commerce (EC Directive) Regulations 2002, SI 2002 No. 2013

<<http://www.legislation.hmso.gov.uk/si/si2002/20022013.htm>>

Electronic Commerce (EC Directive) Regulations: Guide for Business  
<[http://www2.dti.gov.uk/industry\\_files/pdf/businessguidance.pdf](http://www2.dti.gov.uk/industry_files/pdf/businessguidance.pdf)>

**Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions (The e-Money Directive)**

*Official Journal of the European Communities* L 275, 27 October 2000, pp. 39-43.  
The Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) Order 2002, SI 2002 No. 682  
<<http://www.hmso.gov.uk/si/si2002/20020682.htm>>  
The Electronic Money (Miscellaneous Amendments) Regulations 2002, SI 2002 No. 765  
<<http://www.hmso.gov.uk/si/si2002/20020765.htm>>

**Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (the “Brussels Regulation”)**

*Official Journal of the European Communities* L012, 16 January 2001, pp.1-23.  
DTI, Guidance Note: Cross border consumer contractual disputes within the European Union: which country has jurisdiction?  
<[http://www.dti.gov.uk/ccp/topics1/guide/jurisdiction\\_brussels.htm](http://www.dti.gov.uk/ccp/topics1/guide/jurisdiction_brussels.htm)>

**Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax**

*Official Journal of the European Communities* L 015, 17 January 2002, pp.24-28  
Value Added Tax (Amendment) (No. 6) Regulations 2003  
<<http://www.legislation.hmso.gov.uk/si/si2003/20033220.htm>>  
HM Customs and Excise VAT Information Sheet 16/03, November 2003  
<<http://www.hmce.gov.uk/forms/notices/info1603.htm>>

**Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (The Privacy and Electronic Communications Directive).**

*Official Journal of the European Communities* L 201, 31 July 2002, pp. 37-47.

Department of Trade and Industry  
<<http://www.dti.gov.uk/>>

Higher Education Smart Card Association (HESCA)  
<[http://www.hesca.com/about\\_smart\\_cards.html](http://www.hesca.com/about_smart_cards.html)>

Financial Services Authority (FSA)  
<<http://www.fsa.gov.uk/>>

FSA Handbook of rules and guidance - Electronic Money  
<http://www.fsa.gov.uk/vhb/html/elm/ELMtoc.html>

Financial Services Compensation Scheme (FSCS)  
<<http://www.fscs.org.uk/>>

The Financial Ombudsman Service  
<<http://www.financial-ombudsman.org.uk/>>

## 14. Articles

Youngerwood, A. & Mann, S., Commentary, 'Extra Armoury for Consumers: The New Distance Selling Regulations', 2000 (3) *Journal of Information, Law and Technology (JILT)*.

<<http://elj.warwick.ac.uk/jilt/00-3/youngerwood.html>>

Spyrelli, C. 'Electronic Signatures: A Transatlantic Bridge? An EU & US Legal Approach Towards Electronic Authentication', 2002 (2) *Journal of Information, Law and Technology (JILT)*

<<http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html>>.

Bamodu, G. 'The Regulation of Electronic Money Institutions in the United Kingdom', 2003 (2) *Journal of Information, Law and Technology (JILT)*.

<<http://elj.warwick.ac.uk/jilt/03-2/bamodu.html>>.

### Author

Andrew Charlesworth is Senior Research Fellow in IT and Law and Director of the Centre for IT and Law (CITL), a joint post between the School of Law and Department of Computer Science at the University of Bristol. He is currently lead researcher on the JISC Study to Explore the Legal and Records Management Issues Relating to the Concept of the Lifelong Learner Record (Lifelong Learner Legal Study).

20 June 2004

JISC Legal – 2004