Electric dream

AS THE EU'S PAYMENT SERVICES DIRECTIVE COMES INTO FORCE, **GRAHAM BUCK** REVIEWS THE CONTRACTUAL ASPECTS OF E-COMMERCE

Executive summary

If your company handles credit transfers, direct debits, money remittance, debit and credit card transactions, or any other form of electronic payment, then it must comply with the Payment Services Directive, which is now in force in the UK.

The regulations governing the various electronic payment systems used in e-commerce – also known as e-money or digital money – have recently undergone a shake-up. 1 November 2009 marked the deadline for the European Economic Area (the 27 EU member states plus Iceland, Liechtenstein and Norway) to implement the EU's Payment Services Directive.

Adopted in the European Parliament in late 2007, the Payment Services Directive aims to create a single market in Europe for retail payment services. It will affect electronic payment systems and payment accounts, including easy access savings accounts as well as current accounts.

According to the European Commission, the directive aims "to ensure that electronic payments within the EU – in particular, credit transfer, direct debit and card payments – become as easy, efficient and secure as domestic payments within a member state, by providing the legal foundation to make the Single Euro Payments Area (SEPA) possible".

The SEPA project to develop pan-European electronic banking was launched by European banks at the start of 2008 to make electronic payments across the euro zone simpler by introducing common processing standards and systems. SEPA stands to benefit from the directive. EU officials recently admitted that SEPA take-up had been unimpressive, with Europeans reluctant to reduce their reliance on cash; under 5% of credit transfers currently use SEPA standards.

The European Commission says the Payment Services Directive "will reinforce the rights and protection of all users of payment services (consumers, retailers, large and small companies and public authorities)". It's a laudable intent, but progress in transferring the basic text of the directive into national laws has proved slower than anticipated, with differing interpretations by each European country cited as the main reason. Germany and Italy are singled out as actively blocking progress of the legislation, and France and Spain also stand accused of delaying tactics.

The main obstacles to progress appear to be a total of 23 additional optional services that are open to member states as they transpose the Payment Services Directive into national law.

Differing interpretations create inconsistencies, including:

- the treatment of currencies and whether they come within the directive's remit;
- whether small businesses should be classified as consumers or corporates; and
- the definition of payment accounts and direct debit products.

A recent report suggested "every country is using additional optional services to protect historical products, services and infrastructures".

ALREADY OPERATIONAL IN THE UK Despite its stumbling progress the directive came into force in the UK on 1 November, courtesy of the Payment Services Regulations (2009). Banks have already sent their customers a notice of variation to the terms and conditions of those products and services that are affected.

The Payment Services Directive requires countries to regulate payment services that include credit transfers, direct debits, money remittance, debit and credit card transactions. It will therefore affect all firms providing payment services and not just banks and building societies. It also extends to some services provided through mobile phones or other digital and IT devices.

In addition to two types of payment provider – retail banks/credit institutions and e-money issuers – the directive

adds a new category of payment institutions. These are defined as providers of payment services that:

- are not classified under the other two categories;
- are authorised/registered with a competent authority in the EU;
- take possession of funds; and
- provide a service beyond simply selling their own goods.

These non-bank providers will be allowed to offer their services across the EU on the basis of a single licence obtained in one member state. The directive introduces a single authorisation regime, tiered according to the size of the operator, for businesses operating cross-border.

The directive also applies information and liability requirements, so that users and providers of payment services have greater legal certainty in the event of a transaction going wrong. And it sets out agreed time limits for the execution of a transaction.

The rights and obligations for users and providers of payment services set out in the directive include new rules being introduced from January 2012. These lay down that electronic credit transfers not involving any currency conversion must be carried out by the end of the next business day. Until those rules come into force, a maximum execution time of three business days will apply.

As part of its consumer protection remit, the directive provides for companies and their banks to opt out of some, but not all of the legal provisions.

An example is Article 59, which deals with evidence of authorisation of a payment transaction. Where a customer denies having authorised a payment, it is up to the bank to prove proper authorisation. Use of a "payment instrument" (meaning some sort of personalised device) such as a PIN or token is not, in itself, sufficient to prove that a payment was properly authorised, as was previously the case with the majority of electronic banking agreements.

The position on non-authorised payments differs in the US. Article 4a of the US Uniform Commercial Code, sections 202 and 203 (see end of article for web link), applies to many transactions in the US and makes banks responsible for providing reasonable security systems. If a loss results from an unauthorised payment order, the customer suffers the loss if the bank accepted the order in good faith and complied with a commercially reasonable security procedure to verify its authenticity.

The customer can shift the loss to the bank by showing that its own organisation did not cause the loss. If the loss falls on the bank, the bank refunds any payment to the customer and, where applicable, interest on the refundable amount. There is, however, no liability for consequential loss.

Last April, the European Parliament agreed changes to the regulations applying to cross-border payments and the conditions for issuing electronic money in the EU. The cross-border revisions came into force on 1 November, and EU member states must make them national law by 2011.

The latter changes are aimed at lowering the barriers to market entry for newcomers, so that there is greater consistency with the Payment Services Directive and the e-money market can begin to realise its potential (annual volumes are expected to reach up to €10bn by 2012).

The minimum requirement for initial capital will be reduced from €1m to €350,000, and new rules on the calculation of own-funds will take effect. Electronic money institutions engaged in other business activities, such as telecoms, will find it easier to develop innovative services in the payments market. At the same time, the e-money directive imposes high standards for protecting consumers.

ANTI-FRAUD ACTION As e-commerce develops, there will doubtless be more industry measures to deter fraudsters. Most recent figures suggest that credit card fraud in the first half of 2009 was down by 23% year on year. The reduction was helped by the fact that the two main card schemes, Visa and MasterCard, which together account for around 85% of the payment cards in circulation, have online security initiatives: Verified by Visa and MasterCard SecureCode.

By contrast, Financial Fraud Action UK (formerly the anti-fraud unit of APACS) reported that the cost of online banking fraud in the period January to June 2009 totalled £39m, an increase of 55% from a year before. This follows an increase from £22.6m for the whole of 2007 to £52.5m during 2008.

The increase reflects the growing sophistication of cybercrooks in two main areas. The first is malware scams targeting weaknesses in customers' PCs rather than the banks' own systems, which are generally better protected. The second is the increasing frequency of phishing scams, which showed a 26% rise to 26,000 reported incidents in the first half of 2009.

As regards liability for online fraud, the March 2008 revisions to the Banking Code have been interpreted as shifting more of the burden away from banks onto their customers. The code stipulates that online account holders should act with "reasonable care" to avoid incurring liability for losses resulting from third-party fraud. Reasonable care includes the regular updating by businesses and individuals of antivirus and spyware software as well as their personal firewalls. As losses increase, banks are expected to adopt a harder line in cases where fraudulent losses apparently result from carelessness.

In all other cases, customers who suffer losses from online fraud can invoke the banks' formal complaints procedure. Paragraph 12.12 of the Banking Code confirms that banks must reimburse in full all funds withdrawn fraudulently where customers retain their card. Where the card has been either lost or stolen, they are liable for the balance of any loss that exceeds £50.

In cases where the bank and the customer are in dispute over a loss resulting from online fraud, independent adjudication is provided by the Financial Ombudsman Service, which results in either a negotiated settlement or a decision by the ombudsman to which the bank must adhere.

Graham Buck is a reporter on The Treasurer.
editor@treasurers.org

For Article 4a of the US Uniform Commercial Code, go to:
http://tinyurl.com/ycoeb6g