

Electronic payments – key conclusions of study undertaken for European Commission on public perceptions

September 2003

In a nutshell

- European Union (EU) citizens, especially those who are regular Internet users, show a reasonably high level of trust in electronic payments, although there still remain significant doubts about security, fraud and privacy threats. The picture is not consistent across the EU: there are significant national and regional variations.
- There exist secure, economically feasible Electronic Payment Instruments (EPIs), with more advanced underlying technology being rolled out in the near future. Electronic banking and online transfers have particularly good levels of security.
- Fraud is clearly present on the Internet, using EPIs as a means to perpetrate that fraud. However, actual fraudulent and criminal activity reported as being directly attributable to the inherent security features of EPIs has been virtually non-existent.
- Consumers are not very well informed at the point of use of the EPI, although banks and merchants generally comply with legislative requirements in this area.

There does appear to be a significant gap between the perception of the security of EPIs, with EU citizens being reasonably confident in systems that show little or no real risk in terms of crime caused by their actual use. The information communicated to users is generally not sufficient to overcome the doubts that hold some (potential) users back, and this would seem to be the easiest area to address in any initiative to improve public confidence in EPIs.

Answers to Key Questions

What is consumers' perception about the security of payment instruments?

The level of public confidence in Electronic Payment Instruments in the countries of the EU is generally reasonably high: an indicator devised for this study shows an overall score of 7.08 (maximum 10)¹.

To what extent does media hype exaggerate citizens' real perception ?

There is indeed a significant 'hype factor' in the media presentation of public confidence, or the lack of it, in EPIs, as opposed to the reality as reflected in the research. This hype factor is, however, not so great that the media coverage is not fundamentally grounded in reality².

What are citizens' biggest concerns ?

The principal negative factors cited by existing EPI users were: security concerns (30%), fraud (25%) and (lack of) privacy (17%), respectively. Amongst non-EPI users, the concerns (negative factors) were almost identical to those amongst EPI users. IT might have been expected that the non-users would have greater concern in this area, which would prevent or discourage them from becoming users. It would seem in practice that many EPI users are

¹ However this level of confidence is not consistent across the continent: indicator values range from the highest of 8.41 (Finland) to 5.25 (Greece).

² Indicators for the Media view, as well as for both existing and original direct research were devised (again maximum 10). For the EU, the Media indicator returns a value of 6.57, whereas the two Direct Indicators return values of 6.93 and 7.37 respectively.

aware that there are risks, but consider that the advantages of online payments outweigh the negative factors.

Which payment instruments are (or might be) more secure than others and why?

Purely from a security perspective, electronic banking systems, on-line bank transfers, SET³ card payments and electronic payment account systems are the preferred systems. In all but the last case this is due to the usage of 2-factor authentication. The least secure system on this basis is "card not present" payment over the Internet when no specific means of cardholder authentication are used. This threat to security is primarily due to authentication procedures heavily based on credit card numbers and expiration dates that cannot be considered secrets. In addition, further elements of potential risk are the usage of weak versions of SSL⁴ (or no SSL at all), storage of credit card details on the merchant's server, and inadequate protection of the merchant's server against hacking, potentially exposing credit card information (credit card numbers and expiration dates).

What is the result of comparing the public perception with the real security situation?

Although the public does have reservations about the security of EPIs, the security measures actually used seem to be well-established (if still not at the technological leading edge) and inherently secure.

Well established fraud schemes, however, remain in existence and can now make use of newly available communication channels such as the Internet. But even in these cases financial risk for consumers is very low, and hardly justifies the perception that paying over the Internet is not safe.

When the current efforts of the payment industry to provide more secure cards (chip-cards) combined with some new but cost-efficient control measures (3D Secure or equivalent) are implemented, the perception of unsafe payments over the Internet will have even less justification.

What security measures are actually implemented in practice (as opposed to the security which is or will shortly be available, but is not yet implemented)?

A wide range of payment technologies exists, and more are on the brink of being introduced in the market. However, when looking at the current real world, one observes that payments over the Internet are still an almost exclusive 'classic credit card' business⁵. Such payments are almost completely dominant for cross-border payments. Although new, more secure solutions (including those that make credit card usage more secure) are available, "traditional" solutions with a relatively low degree of security are still the most used. Some of the newer solutions, whilst they are technically advanced, have nevertheless found great difficulty in achieving significant market penetration.

How far are consumers informed about existing security measures?

The actual levels of security of solutions in use for making payments is not presented very clearly to consumers. The majority of banks and merchants consider that they comply with the general fair trade practices and principles stipulating the timely and accurate

³ Secure Electronic Transaction (see glossary at the end of this report for details)

⁴ Please see glossary at the end of this report for definition of terms.

⁵ This is far from being uniform in all EU states, e.g. Finland has a very different profile

communication of comprehensive information to consumers. They also feel that they are proactive enough to implement consumer-friendly approaches in the communication of security-related information before specific problems arise. On the other hand, consumer organisations stress that there are still many e-payment issues that remain unclear to consumers (for instance, the liability, role and responsibilities of all parties intervening in an e-transaction if a security threat occurs).

Generally speaking⁶, the quality of information provided to consumers tends to be better when coming from sources such as banks and other financial institutions. Merchants often have less comprehensive information or refer customers to the site of the EPI provider.

⁶ Again this varies greatly from state to state: see individual country analyses in Part 4 of this report

Glossary

Term	Explanation
(Electronic) Wallet	An encrypted storage medium holding payment card or other financial information that can be used to complete electronic transactions without re-entering the stored data at the time of the transaction. Wallets may also be employed to store electronic cash.
A3/A8	Techniques used to authenticate GSM subscribers. GSM operators can choose from several options, one such option is COMP128.
A5	Encryption used to protect the confidentiality of the communication on GSM networks.
Building Blocks	Technologies or concepts that are used for a variety of payment systems and which are explained in a separate sections of the report.
Card Not Present transaction (CNP)	Payment card transactions during which the payment card is not present at the merchant. The term of Card Not Present transaction is broader than the term of MOTO transaction as it is not related to mail or telephone. In practice both terms are often used synonymously.
Card Verification Value (CVV)	A number printed, but not embossed, on payment cards in addition to the card number and expiry date that can be used to verify possession of the card in MOTO transactions.
Https	Http secured with SSL or TLS.
Mail Order Telephone Order (MOTO)	MOTO transactions are payment card transactions during which the payment card is not present at the merchant. Originating from the time when this typically occurred when a cardholder ordered using mail or telephone, the term is used nowadays also the refer to Internet payment card transactions that are carried out by simply stating the card number and expiry date.
Payment Service Provider (PSP)	Payment service providers (PSPs) offer the service of handling payments to Internet merchants. Merchants redirect their customers to the PSP's site. The PSP offers a range of payment methods. After payment is completed, the PSP will inform the merchant of this. In this way, the merchant deals with one rather than multiple parties while still offering payment flexibility to its customers.
Person-to-Person (P2P) payment	A non-cash payment (transfer) from one subscriber (consumer) to another subscriber of a compatible system. Also known as Peer-to-Peer payment (transfer)
SET (Secure Electronic Transaction)	A payments protocol developed by Visa and Mastercard
SIM Toolkit	Software that makes it possible to place GSM operator specific applications on GSM phones. Such application

Term	Explanation
	typically have their own menus, can work together with the SIM card and can communicate via Short Message Service (SMS) with the GSM operator.
SSL (Secure Sockets Layer)	Generic method to cryptographically secure communication on the Internet taking place between a client and a server. SSL is based on public key encryption usually only the server is using a certificate. SSL is best known for securing the World Wide Web protocol http, resulting in https. However this is only one example of the use of SSL.
TLS (Transaction Layer Security)	A form of SSL that is adopted by the Internet Engineering Taskforce.
WTLS (Wireless Transaction Layer Security)	Form of TLS to cryptographically secure Wireless Application Protocol (WAP) communication.

List of Acronyms

Acronym	Explanation
CNP	Card Not Present
CVV	Card Verification Value
DG	Directorate General
EPI	Electronic Payment Instrument
EU	European Union
GSM	Global System for Mobile Telephony
http	Hyper Text Transfer Protocol
https	Hyper Text Transfer Protocol (Secure)
IETF	Internet Engineering Taskforce
MOTO	Mail Order/Telephone Order
P2P	Person-to-Person or Peer-to-Peer
PSP	Payment Service Provider
PwC	PricewaterhouseCoopers
SET	Secure Electronic Transaction
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
WTLS	Wireless Transaction Layer Security