Briefing

June 2015

European Parliament

Consumer protection aspects of mobile payments

SUMMARY

Over the next few years, mobile commerce in Europe is expected to grow at an average compound annual rate of 42%. The way in which consumers purchase goods and services is changing significantly as new technologies permit the development of an increasing number of cashless payment solutions. There are various forms of mobile payment (payment, for which the payment data and the payment instruction is initiated, transmitted or confirmed via a mobile phone or device). They include payments via SMS, direct billing (by adding the payment to the monthly mobile phone bill), mobile web payments (using a credit/debit card or pre-registration at an online payment provider), and Near Field Communication (NFC).

However some of the challenges to consumer protection, such as lack of interoperability between mobile payment options, personal data protection, digital identity theft and fraud, prevent greater consumer take-up of mobile payments. Unfair commercial practices in e-commerce relevant to mobile payments include misleading advertising, hidden payment obligation and IP tracking. Other consumer protection issues are dormant assets, lack of accessibility and readability of payment-related information, and concerns related to vulnerable consumers. While the current legislative framework is undergoing revision as a result of the European Commission's new proposal for a Directive on payment services in the internal market, some stakeholders voice concerns.

In this briefing:

EPRS | European Parliamentary Research Service

Author: Jana Valant

Members' Research Service

PE 564.354

EN

Glossary

App: Short for 'application', which here typically refers to a small, specialised program that is downloaded onto mobile devices for a specific purpose.[1] In the mobile payment environment, smartphone owners who shop online seem to have a preference for using apps instead of mobile websites.[2]

Interoperability: According to ISO/IEC 2382-01 Information Technology Vocabulary, interoperability is a capability to communicate, execute programs or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units.

Mobile commerce or m-commerce: Electronic commerce (e-commerce) conducted from a mobile device, e.g., phone, tablet computer. Mobile commerce should not be confused with electronic commerce which entails all commerce over an electronic network, including purchases made from personal computers.[3]

Mobile Network Operator: Mobile telecommunications company.

Mobile Wallet: Digital container accessed by the mobile device, allowing customers to store applications and credentials used for mobile financial and non-financial services. The container may reside on the consumer's mobile device, or may be remotely hosted on a secure server or on a merchant website.

NFC: Near Field Communication, a short-range, contactless communication system, based on Radio Frequency Identification (RFID) technology that allows payment data transfer between devices.

SEPA: Single Euro Payments Area.

SMS: Short Message Service. SMS-based transactional payments are predominantly used in developing countries.

Mobile commerce and mobile payments

On average, around 60% of Europeans own a smartphone,[4] but many more own a mobile phone device, with more than nine out of ten EU households reporting they have mobile phone access. According to the European Commission, there were 67 mobile broadband subscriptions per 100 inhabitants in the EU in July 2014. Mobile commerce in Europe is expected to grow significantly over the next few years, with an average compound **annual growth rate of 42%**. In 2014, Europe[5] experienced an all-time peak in mobile revenues and mobile transactions. According to a RetailMeNot forecast based on data from some EU countries, Europeans will be spending about €45 billion via **mobile devices in 2015**;[6] this currently corresponds to **around 14% of all online purchases** made in the EU, and represents an increase of 88.7% compared to 2014. Despite the fact that a personal computer seems to remain the preferred device for shopping online in Europe as well as in the United States of America (USA), a Juniper research paper in 2014 predicted that growth would continue to be driven by purchases of physical goods via mobile devices. The findings of the report also show that, despite the sharp increase in spending via smartphones, their primary function in retail is actually as search and discovery devices, with the final purchase being made on a tablet. Mobile phone payments seem to be more popular with younger generation phone users.[7] Developed countries, however, do not lead the market in mobile payments. Globally, mobile payment seems to have caught on fastest in developing countries, where China, Chile, South Korea and India are leading.[8]

The European Commission's Green Paper from 2012 defines mobile payments as **payments for which the payment data and the payment instruction are initiated, transmitted or confirmed via a mobile phone or device**, which can apply to **online or offline purchases** of services, as well as digital or physical goods. Various forms of mobile payments exist. They can include payments via SMS, direct billing (by adding the payment to the monthly mobile phone bill), mobile web payments (using a credit/debit card or pre-registration at online payment solution), and Near Field Communication (NFC).

Furthermore, the Commission classifies payments in two main categories:

- *Remote mobile payments* mainly take place through the internet/Wireless Application Protocol or through premium SMS services which are billed to the payer through the Mobile Network Operator. Most of the remote mobile payments over the internet are based on card payment schemes.
- *Proximity payments* are made at the point of sale (i.e. at the physical retail location such as stores, public transport, parking spaces) using NFC. These kinds of payments require specifically equipped phones that can be recognised in the proximity of a reader module at the point of sale.

Relevant EU legislation

Mobile payments

Currently, two directives apply to the area of mobile payments. Directive 2007/64/EC on payment services in the internal market establishes a harmonised legal framework for payment services throughout the single market; Directive 2009/110/EC covers the taking up, pursuit and prudential supervision of the business of electronic money institutions.

After the publication of its Green Paper 'Towards an integrated European market for card, internet and mobile payments' in 2012, the European Commission proposed in 2013 a revision of the current legislation in force, namely with the proposal for a Directive on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. On 5 May 2015, agreement was reached in trilogue negotiations between the Commission, the European Parliament and the Council, and formal adoption of the proposal is expected later this year.

Consumer protection

Regulation 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws also provides tools to protect consumers in the area of electronic commerce. The regulation relates to a number of EU directives and regulations: cooperation between Member States may cover unfair or misleading commercial practices, unfair contract terms, consumer rights to information, guarantee rights and specific rights in cases of distance selling or e-commerce. Revision of this regulation is underway.

Data protection

Directive 95/46/EC deals with the protection of individuals with regard to the processing of personal data and on the free movement of such data; and Directive 2002/58/EC concerns the processing of personal data and the protection of privacy in the electronic communications sector, (a revision is underway).

Advantages of mobile payments for consumers

Mobile payments can be a **more convenient and portable** means of payment than traditional payment methods because they eliminate the burden of carrying multiple plastic cards, coins and currency in a physical wallet. A payment via a mobile device may also be an improvement in terms of flexibility, since consumers are able to link mobile payments to card accounts or use other online payment systems, such as PayPal or virtual currency schemes such as Bitcoin. Another possible advantage of mobile payments to consumers is faster transaction speeds for certain types of purchases. With contactless payment methods, including contactless cards and NFC-based mobile payments, the consumer only needs to tap or wave the contactless device in front of a reader in order to make a purchase. According to one study, this type of payment is up to 15 to 30 seconds faster than swiping a traditional card, signing the receipt or entering a PIN code. That can be important to consumers, especially to those who value saving time highly, as well as being able to pay bills at any given location.

Despite higher initial equipment costs for purchasing a more advanced mobile phone or a tablet, it is argued that ongoing costs to the consumer are lower. The payment flexibility that mobile payments provide enables consumers to choose the lowest-cost payment instrument for each purchase. On the other hand, the usage of a mobile device may entail additional mobile connection and security costs. What could also encourage the consumers to embrace mobile payments is the ability to **monitor finances and control spending**. Provided that they have the appropriate level of financial literacy (financial experience and skills) and that the payment environment is consumer-friendly, consumers are able to check account balances prior to making purchases and receive alerts when their spending reaches designated thresholds.

Current consumer protection concerns regarding mobile payments

In general, there seems to be **lack of awareness among consumers regarding their rights and obligations** when they are making mobile payments. This is particularly due to the number of parties involved in this process – financial service providers, mobile operators, internet service providers and also social media[9] in certain cases – and the fact that these parties are not all subject to the same rules. The Organisation for Economic Co-operation and Development (OECD) notes that consumers have difficulties in determining their rights, which depend both on the payment mechanism (e.g. payment charged on a mobile phone bill; credit, debit or prepaid card payment system) and on the device being used (differences when using a fixed computer, mobile phone or other mobile device). It is also not easy to determine the party responsible for addressing the problems that can arise in the transaction process, the procedures for seeking redress, and the type of remedies that can be obtained. Other concerns are payment terms and conditions that are sometimes too complex, as well as inconsistent payment-related information.

Data protection

According to the European Commission, 72% of internet users in the EU are worried about using online services through fear of revealing too much personal data online. The lack of consumer trust related to data protection online seems to be exacerbated by reports on bugs, new viruses and other cyber-threats. According to some estimates, approximately 15% of cyber-attacks that penetrate corporate networks or enterprise

systems damage or destroy physical equipment such as servers, storage devices, routers and other IT devices. The mean (average) time to detection for a data breach is still around eight months, according to industry estimates. Moreover since reporting a cyber-security breach (if and once it has been identified) can have massive legal, financial and reputational implications for a business, there are reasons to believe that not all breaches are necessarily revealed in public. A 2014 survey showed that **43% of US companies experienced a security breach** over a period of one year; these companies included banks. However in relation to the data breaches, some argue that mobile payments can offer some advantages since mobile payment options provide enhanced security. To protect consumers' financial information, Google Wallet, for instance, uses encryption while Apple Pay uses tokenisation.[10]

Tracking and geo-blocking as an example of data protection risks involved in e-commerce

Another commercial practice present in the online shopping environment, and not limited to mobile payments, is IP tracking. This refers to a method of **changing prices artificially, on the basis of tracking the Internet Protocol (IP) address** of computers or mobile devices. By identifying the IP address it is possible to know that a consumer using a specific device has already been searching for particular services on a given website. In this way, when the second search is launched, it shows results with artificially raised prices. Similarly, certain mystery shopping exercises[11] have shown online **discrimination on the basis of user location** or place of residence (e.g. application of different conditions or prices to consumers from different Member States, or specific cases of geo-blocking when the user is automatically re-directed to a national website because of his/her IP address).

Considerable personal data (i.e. geographical location, passwords and payment transaction information) is transferred during mobile payments, and is accessible to mobile network operators, app developers, payment processors and merchants (not to mention parties that can also potentially gain illegal access to that data during the payment process). Consumers do not necessarily know whether, and how, the data is stored, processed and used, which is problematic as they should have control over their personal data. The collection and use of payment data is also an issue because consumers may not agree to their activities being tracked, or their data being shared with third parties.

Cyber-security and fraud

'Man in the middle' attack

One type of fraud is a 'man in the middle' attack that involves the attacker placing himself – or his malicious tools – between the victim and a valuable resource, e.g. a banking website or an email account. For instance, an attacker could configure a wireless device to act as a WiFi hotspot in a public area, such as an airport or coffee shop, giving it a name which resembles one commonly used. When users connect to the 'router' and access sensitive sites such as online banking or e-commerce sites, the attacker is able to capture their credentials for later use.

With constant development of new techniques for fraud – besides the better known phishing scams to access sensitive consumer data, the danger of fake shops proposing products online, and identity theft techniques – cyber-security will have to evolve continuously. With the growth of the Internet of Things, ever more devices will have access to the internet and to financial service accounts and credentials. Cloud services are becoming an attractive target for cyber-criminals. According to some predictions for

2015, attacks on mobile platforms through malicious links and applications are to be expected and point-of-sale malware could become one of the most common methods of stealing data and money.

Lack of interoperability between different mobile payment options

As technology advances rapidly and options for mobile payment increase, lack of interoperability (including cross-border) between service providers is an issue. Better interoperability would provide consumers with more flexible payment options (better switching between different services and providers), leading to an increase in the number, speed and volume of mobile transactions. Better financial inclusion could be another benefit of more accessible and flexible services for consumers (also for the most vulnerable ones). Payments normally flow through the banking system, but mobile payments currently offer low regulatory entry barriers for new players, which could influence the payments markets, traditionally dominated by banks. With no interoperability in place there is a risk of **fragmentation through proprietary solutions** as certain players who control the standards and interoperability can dominate the whole payment chain (by controlling the device itself, the application platform and the security management). An extreme example, related to lack of interoperability, was the independent development of mobile phone technology in Japan (dubbed the Galapagos syndrome), originally at the forefront, but incompatible with foreign standards. As its mobile phone technology later ossified within a saturated market, Japan became a relative latecomer to the smartphone market.

The European Commission, in its 2012 Green Paper, insisted that standardisation in the mobile payments area should ensure **full interoperability** between mobile payment solutions, and favour open standards to ensure the mobility of consumers when they wish to change their telecom operator or bank. It also identified the stalemate between Mobile Network Operators, traditional payment service providers and other players (manufacturers and app developers), as one of the main barriers to a widespread take-up of mobile payments.

Unfair commercial practices

According to the Unfair Commercial Practices Directive, the legality of a commercial practice that is not banned outright can be assessed by evaluating it against specific legal criteria. The fairness or unfairness of a commercial practice is assessed against the benchmark of an average consumer (i.e. a reasonably well-informed, observant and circumspect consumer). However, certain commercial practices across EU are always prohibited (e.g. false prize winning, bait advertising). One of the examples of unfair commercial practices related to mobile payments is **misleading advertising** leading to unexpected charges for the consumers. A recent case was that of certain **in-app purchases advertised as free**.

Another unfair practice is a hidden payment obligation. For instance, to access free trial versions of cloud computing services, consumers may be asked to provide their credit card details; upon expiration of the trial period, they are automatically charged for the service without their explicit consent. Similarly, the practice of automatic contract or subscription renewal may result in consumers being charged for products or services they may not have wanted.

In-app purchases: an example of lack of consumer information and consent

In February 2014 the European Commission reported that over 50% of the EU online games market consisted of games advertised as free, although they often entailed (sometimes costly) in-app purchases. 'Free to download' games which were not necessarily 'free to play' were misleading for the consumers (and for children, who are particularly vulnerable to this type of practice). More specifically, the Commission argued that consumers were not fully aware that their credit cards were being charged for certain in-app purchases. By using the Consumer Protection Cooperation Regulation as a legal basis, national consumer protection authorities and the Commission urged some of the main actors to change those practices. By July 2014, two of the main actors concerned made engagements to better inform consumers about the true costs involved in certain online games, as well as to strengthen payment authorisation settings. Google removed the word 'free' when games contained in-app purchases and also adapted its default settings, so that payments are authorised prior to every in-app purchase. Apple also agreed to replace the word 'free' on the button used to download a game application with the word 'get'.[12]

Payment-related consumer information and vulnerable consumers

In its policy guidance paper related to mobile payments, the **OECD** addressed additional consumer protection issues, specifically the lack of accessibility and readability[13] of payment-related information and transaction uncertainty (for instance when the mobile connection is lost during the confirmation process). It also mentioned the payment security issue (advising end-to-end encryption and dynamic data authentication) and the risk of charges incurred by children (e.g. in online games or via mobile apps). In its 2014 report the **International Consumer Protection Enforcement Network** also exposed unclear billing information provided by mobile network operators regarding mobile payments, which makes it difficult for consumers to fight unlawful charges on their bills or to recover their prepaid credit. According to consumer organisations, the needs of vulnerable consumers (children, the elderly, the blind etc.) should be taken into account in the area of mobile payments to ensure financial inclusion for all.

Dormant assets in electronic wallets or electronic purses

Money can be stored in electronic wallets or electronic purses,[14] in the form of credit on mobile phones or in apps. The aggregate value of these otherwise relatively small amounts could be considerable, especially with the increase of mobile commerce. One of the non-regulated issues related to mobile payments is dormant assets, i.e. the money to which consumers lose access. The money is still on the platform used for mobile payments but is not being used by the user anymore. This can happen for a number of reasons. One would be the death of the owner of the account or device, but other reasons could also be the termination of the mobile phone number account, loss of the phone/device etc. As the access codes are normally known only to the owner, recuperation of the amount kept on a specific mobile payment platform is not obvious. According to Consumers International, there is a need for the **exact definition of the situation when money or assets become dormant**.

European Parliament

In a 2012 resolution, Parliament expressed concern at any unduly strict regulation of internet and mobile payment markets, stating that such payment methods were still in the process of development. It warned of risks, such as giving undue emphasis to already existing payment instruments, and regulations that would have negative effects

on innovation, competition and market growth. The Commission was asked to adopt a suitable approach to any future mobile payment methods, ensuring a **high level of consumer protection**, particularly for vulnerable consumers. A payer should be able to make an internet or mobile funds transfer to any payee whose account is in any SEPA-connected financial institution. Parliament also stated that while the final responsibility for security measures relating to different payment methods cannot lie with customers, they **should be informed about security precautions, and financial institutions should be responsible for fraud costs, unless caused by the customer** 'by acting fraudulently or by failing to fulfil one or more of his obligations under Article 56 of the current Payment Service Directive with intent or gross negligence'.[15] Parliament called on the Commission to take into account the **standards and recommendations of European Data Protection Supervisor (EDPS)**[16] regarding transparency, identification of the controller/processor, proportionality and rights of the data subject when developing a strategy and instruments for the integration of payment markets by card, internet and mobile phone. It also asked the Commission to **extend the concept of privacy by design**[17] beyond authentication mechanisms and security safeguards, to ensure data minimisation, the implementation of privacy by default settings, the limitation of access to individual's information to what is strictly needed to provide the service, and implementation of tools enabling users to better protect their personal data.

In its 2014 resolution on supporting consumer rights in the digital single market, Parliament called on the Commission and the Member States to further develop and implement EU and national regulatory frameworks to **allow an integrated and secure online and mobile payments market**, while ensuring the **protection of consumers and customer data**. It also underlined the need for clear and predictable rules, set out in legislation.

Recently, in its 2015 legislative resolution on the proposal for a regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions, Parliament stated that a **ban on interchange fees** for debit card transactions also removes the threat of exporting the interchange fee model to new, innovative payment services such as mobile and online systems.

Stakeholder concerns

In its response to the European Commission's consultation on the Green Paper in 2012, the **European Consumer Organisation – BEUC** mentioned several issues related to mobile payments. It also recommended 'privacy by design', stating that providers should consider consumers' privacy at each stage of product and service development. BEUC insisted that the consumers should be given the right to not be profiled, stating that the business models of companies like Google, Facebook and Apple are based on consumer profiling (recording and analysing customer data via cookies or other electronic tracking tools) without consumers' explicit and informed consent. In 2014, it also highlighted additional issues to be addressed (e.g. security related to hardware, software, contactless technologies and distribution channels; the need for harmonised liability rules in case of unauthorised payments; market fragmentation and lack of interoperability; technical shortcomings; financial inclusion). Consumers need to be better informed about their rights in cases when something goes wrong with the payment or when their device is stolen.

In its 2014 position paper, the European Association for the Co-ordination of Consumer Representation in Standardisation – **ANEC** expressed concern that no attempt had been made to ensure interoperability and accessibility of the security systems used in mobile payments. It also stressed that card, internet and mobile payment systems have **features that make them inaccessible to people with disabilities** (particularly blind and partially-sighted people).

In its Mobile Payments Initiatives Overview, the **European Payments Council** stated that different mobile payment solutions from multiple payment service providers should be able to coexist in the same mobile device. In its opinion, consumers should not be bound to a specific network operator or particular mobile equipment, but should be able to **switch between payment service providers**, with interoperability as a key feature needed to achieve these goals.

In 2012, the **European Banking Federation** argued that in relation to card, internet and mobile payments, **cash is more expensive and less secure** than other means of payments. It also stated that for the standardisation process to be successful for all types of payments, it should be led by the industry and relevant stakeholders and not by the regulator or a standard-setting body. Interoperability should be led by the market; **automatic interoperability should not be imposed**. If minimum requirements for interoperability of e-payments should need to be defined, they should apply to security features of the interoperable systems.

Further reading

Mobile payments and consumer protection, Consumers International, 2014.

Consumer Policy Guidance on Mobile and Online Payments, OECD, 2014.

Mobile Payments Initiatives Overview, European Payments Council, 2014.

Endnotes

1 See Public Records Office, State of Victoria, Australia, 2014 (http://prov.vic.gov.au/wp-content/uploads/2014/10/Mobile_Tech_Policy.pdf).

2 See ECommerce News, Utrecht, 2015 (http://ecommercenews.eu/current-mobile-commerce-situation-europe/).

3 See also: European Commission Green Paper 'Towards an integrated European market for card, internet and mobile payments' — Frequently Asked Questions, 2012 (http://europa.eu/rapid/press-release_MEMO-12-6_en.htm?locale=en).

4 The difference among countries is considerable, according to Ecommerce news. In Sweden 75% of the population has a smartphone account, in the UK 74%, in Germany and Spain 65%, in France 55% and in Poland 43%.

5 Data mentioned here refer to the UK, France, Germany, Spain, Italy, Benelux, Scandinavia and Eastern Europe –not to the whole EU.

6 According to the projections by RetailMeNot, the UK, Germany and France are set to account for 87% of all mobile spending in Europe in 2015.

7 According to a recent survey on mobile commerce in Europe, 59% of smartphone shoppers are aged 18 to 34 years.

8 In countries such as Ivory Coast, Somalia, Tanzania and Uganda, more adults have mobile money accounts than traditional bank accounts, World Bank data shows. In Africa, where a large percentage of the population still remains 'unbanked' and where bank transaction fees are onerous, especially across borders (they can represent up to 47% of the sum transmitted), mobile payments offer a good alternative.

9 Recently, Facebook announced that it is entering the US money transfer market with peer-to-peer payments via Facebook Messenger, which will allow Facebook friends to send money to each other. Twitter has also experimented with person-to-person money transfer in France.

10 Depending on specific data protection requirements, encryption, tokenisation or a combination of both methods can be used to secure data in the process of mobile payment. With encryption, plain-text card data is converted into cipher text; with tokenisation, sensitive payment data is replaced with a unique identifier known as a token.

[11] Another issue related to in-app purchases was also the lack of a clearly indicated email address that customers could use to contact the service provider (in this case Apple) when faced with questions and concerns about their purchases on its platforms and the 15 minutes' payment window set as a default setting (instead of offering a choice).

[12] Here, mystery shopping refers to tools or methods used by consumer watchdog organisations to measure the quality of certain services for consumers, evaluate compliance with consumer laws or gather specific information about products and services. These programmes enable watchdog organisations to pose as regular consumers in order not to be identified.

[13] In relation to payment-related information, the OECD emphasised that it is often provided in small print and/or in scrolling text boxes. Sometimes key payment-related information is to be found in footnotes or requires the consumer to access it via a series of additional windows. Information challenges for consumers can increase because of the relatively small screens of mobile devices (particularly smart phones), their limited storage capacity and battery life.

[14] An electronic purse is only one of the applications that could be contained in a mobile wallet. It essentially contains a store of electronic money (and can be compared to a physical purse containing just cash without credit cards).

[15] According to the new European Commission proposal, the proposed modifications are to streamline and further harmonise liability rules in case of unauthorised transactions, ensuring enhanced protection of the legitimate interests of payment users. Except in case of fraud and gross negligence, the maximum amount a user could under any circumstances be obliged to pay in case of an unauthorised payment transaction is to be decreased from the current amount of €150 to €50.

[16] In 2013, the EDPS considered, among other things, that provisions of articles 25 and 26(3) of the newly proposed directive regarding the exchange of information were too vague, and did not provide an adequate legal basis for the required processing of personal data. As regards purpose limitation, it also noted that the proposal failed to specify the purposes of the exchange of information and the kind of data to be exchanged. The EDPS also specified that the proposed directive did not lay down any concrete limitation of the period for the retention of the personal data potentially processed. All these issues have been taken into account with the amendments of the European Parliament on the new proposal for a directive on payment services in the internal market adopted in April 2014. (The mentioned data storage limitation, for instance, was set to maximum 10 years). Similarly, an EDPS recommendation to include the obligation that 'privacy by design/privacy by default' is embedded in all data processing systems developed and used in the context of the proposed directive, was taken on board with Parliament's amendments on the new proposal for a directive on payment services in the internal market.

[17] Privacy by design aims at building privacy and data protection up front, in the design specifications and architecture of information and communication systems and technologies, to facilitate compliance with privacy and data protection principles.

Disclaimer and Copyright

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)