
I. Introduction

The Government of the Federal Republic of Germany supports the European Commission’s initiative to develop further the European single market for cashless payments and to make this effective for all market participants. We agree with the European Commission’s assessment that secure, efficient, competitive and innovative electronic payments are necessary if consumers, retailers and companies are to enjoy the full benefits of the Single Market. This applies particularly in the case of e-commerce, where growth has been restricted because simple, secure and consumer-oriented payment systems are unable to keep pace with consumer demands. Existing barriers in the area of internet and mobile payments are particularly problematic for the development of e-commerce. Although this currently represents only 3.4% of all European retail trade, its considerable growth potential remains untapped. According to a study by Forrester Research, the number of online shoppers in Europe could increase from 141 million in 2009 to 190 million by 2014. Annual growth rates of the e-commerce market size over the next five years are projected at around 10%. The per capita average spend in the EU in 2009 was €483. By 2014 this may have risen to €601.

The Single Euro Payments Area (SEPA) with its single rulebooks for credit transfers and direct debits has already made a major contribution to the development of a harmonised and efficient payments area. These rulebooks should form the basis for further harmonisation efforts of the European Commission in relation to card, internet and mobile payments. It is important to ensure that all stakeholders are involved in the process. Not only the views of the banking industry but also those of acceptors of payments, consumers and service providers need to be heard and taken into consideration.

Common standards established by the banking industry (i.e. the European Payment Council (EPC)) can have far-reaching effects on the commercial activities of seemingly unconnected organisations. For example, the SEPA direct debit rulebook also has implications for commerce. Following the introduction of SEPA, the well-established German system of electronic direct debits, developed by commerce in accordance with banking standards, can no longer be used. Consequently, it has to be ensured that user interests are given sufficient consideration when harmonisation measures are adopted or standards developed.

The European Commission and the Member States are faced with an ever-changing payments landscape. Having regard to the technical developments in the area of payment systems, the Green Paper should be seen as useful basis for discussions. It makes a timely and substantive contribution to this area allowing for a better overview of the current market situation in the area of payment systems and an assessment whether European harmonisation measures are necessary. The Government of the Federal Republic of Germany shares the view of the
European Commission that more market integration in payment systems may produce many benefits, for example, more competition, more choice and transparency for consumers, more innovation and more payment security and customer trust – objectives already pursued through the existing SEPA rulebooks.

Given the constant advances in the state of technical progress in the payments market, the account of ‘innovative payment systems’ provided by the Green Paper is undoubtedly incomplete. That is why, for the purposes of analysis in this area, categories of payment systems need to be identified – also in relation to card, internet and mobile payments in Europe – independently of the technology involved but within the context of existing legislative standards. In the case of payments made via the internet (e-payment), using mobile payment systems (m-payment) and proximity payments using a radio chip incorporated in a mobile phone (Near Field Communication (NFC)), the line between these payment methods is often blurred. The products and payment systems already established or developing within the market do not differ simply in their technical aspects. There are also significant legal and supervisory distinctions which are of crucial importance particularly for users and consumers. Thus, the Commission’s efforts to integrate these different payment forms within a common system – as set out in its vision – will need to accommodate those distinctions. However, there is no reason why this should jeopardise efforts for improvements in this area.

II. General observations

1. Analysis of the factual situation presented in the Green Paper

Before any answers can be given to the questions raised in the Green Paper, the facts set out in the document need to be supplemented from a regulatory perspective.

1.1 Card payments

In relation to cards, the Green Paper does not distinguish, for example, between different card functions (debit card, credit card or card with e-money function). However, a distinction along those lines is necessary as each may involve a different payment instrument governed by a different rulebook/regulatory framework with the provider of those payment systems subject to different supervisory regimes (for example, the Payment Services Directive or the e-Money Directive).

1.2 Mobile payments

In the case of mobile payments (m-payments), too, distinctions need to be made in relation to the different payment functions which can be triggered – on the basis of existing technology – using a mobile phone. For example, a mobile phone can be used as a device to initiate a payment / access a payment system or it can be used directly as payment instrument itself. This is another crucial distinction for the purposes of further discussion. If a mobile phone is used as means of access to make a proximity mobile payment (for example, on a contactless
basis in place of a card), the payment is likely to be based on a direct debit. On the other hand, if a mobile phone is used as a device to make a remote mobile payment, the underlying payment transaction could be an online credit transfer. In addition, the type of use involved may impact on the requirements that the telecommunications operator must satisfy as provider of the various payment functions.

2. Categorisation of the situations addressed by the Green Paper and their classification in the list of payment services set out in the Annex to Directive 2007/64

Before any answers can be given to the questions raised in the Green Paper, a more rigorous categorisation of the various elements involved is needed. This will allow for better identification of different markets and the relevant market participants. In turn, this will make it easier to identify where in the context of the European single market for payments further regulatory action is needed and to determine the measures most appropriate to tackling the existing challenges. With that in mind, it may be helpful to consider, inter alia, the following distinctions:

- Through which devices or media can a payment be initiated (for example, cards, internet, telephone, wristwatch)?
- Which technologies are used to communicate the payment data (for example, NFC, networks, internet)?
- How is the payment authorised (for example, via text message (SMS), using biometric data, entering a PIN and transaction authorisation code, with a signature)?
- How should the underlying payment transaction be classified (credit transfer, direct debit, card payment)?
- What ‘type’ of money is transferred (for example, cash, scriptural money, e-money, virtual money)?
- Who is the provider of the relevant service (for example, credit institutions, network operators, payment institutions)?

In the light of a classification of that kind, in relation to each segment concerned an assessment could made of (i) the current situation in the European payments market; (ii) likely technical developments; and (iii) whether further action is needed.

3. Putting the facts in the context of existing European legislation and reform proposals of the European Commission

The questions raised in the Green Paper address issues of competition law, private law, data protection and supervision. In each of these different areas, there is already a European
regulatory framework which is applicable to cashless payments. Thus, the questions raised in the Green Paper are closely linked to matters already subject to regulation in instruments such as the Payment Services Directive,\(^1\) the Regulation on cross-border payments in euro,\(^2\) the SEPA Regulation,\(^3\) the e-Money Directive,\(^4\) the Settlement Finality Directive,\(^5\) the Data Protection Directive\(^6\) and the Money Laundering Directive.\(^7\) Therefore, further deliberations on how to improve market integration for innovative payment methods ought to take place in the context of those provisions.

In particular, the upcoming review of the Payment Services Directive, required pursuant to Article 87 of that directive, and of the Regulation on cross-border payments in euro should take account of the questions raised in the Green Paper. In that connection, regard should be had to the provision made for e- and m-payments under the SEPA Regulation. Recital 6 in the preamble to the SEPA Regulation establishes that, where a payment card at the point of sale or some other device such as a mobile phone is used as the means to initiate a payment transaction, either at the point of sale or remotely, which directly results in a credit transfer or a direct debit to and from a payment account, that payment transaction should be covered by the SEPA Regulation. On the other hand, payments via mobile phone or any other means of telecommunication or digital or IT device are not intended to fall within the scope of those provisions. Finally, the questions raised by the Green Paper should also be assessed in light of the European Commission’s Digital Agenda,\(^8\) currently under discussion, and the Eurosystem recommendations concerning the security of internet payments.\(^9\)

The issue of harmonisation of innovative payment methods is directly linked to the existing supervisory and private law regimes established by the Payment Services Directive, the Regulation on cross-border payments in euro and the SEPA Regulation, which entered into force in March. For that reason, those questions should not be examined independently of one another. Bearing in mind issues of timing, a detailed examination of the Payment Services

\(^7\) Directive 2005/60/EC, currently under review by the European Commission.
\(^8\) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe, COM(2010) 245 final/2.
Directive which takes account of the questions raised by the Green Paper is needed. This should be followed by a prompt revision of the Directive in light of that assessment.

III. Detailed observations

1. Competition issues raised by the Green Paper

The Government of the Federal Republic of Germany takes the view that competition between payment service providers at all market levels is crucial to the development of the payment markets mentioned in the Green Paper. Priority in this respect should be accorded to the removal of existing barriers to market entry and the prevention of new barriers to market entry emerging. According to observations by the Federal Cartel Office, competition on price and with regard to innovation is most likely to be initiated by providers from outside of the banking sector. These include, for example, providers of technical processing services, responsible for developing the electronic direct debit scheme commonly used in Germany to process point of sale (POS) card transactions, and providers of online credit transfer facilities used in e-commerce.

To the extent that – as has hitherto been the case in relation to merchant fees levied under the domestic scheme for debit card payments (known as electronic cash) – fees continue to be based on collective arrangements established by one side of industry, the Government of the Federal Republic of Germany would like to see the establishment of negotiating structures involving the various market participants with a view to prices being determined under the conditions of competition. This requires, in particular, that card acceptors have alternative options and the freedom to take the necessary action. In relation to the electronic cash scheme, this means, primarily, the possibility to switch to the electronic direct debit scheme and, in addition, to levy a surcharge and/or offer a rebate for the use of particular payment means.

According to the assessment of the Federal Cartel Office, the markets for payments in the Member States differ significantly, inter alia, in relation to the provider structure and the products tailored to meet the specific needs of users. Measures intended to improve market integration should not lead to the disappearance from the market of providers or products which are key drivers of competition. Interventions seeking to regulate prices directly carry with them considerable risks. These include not only the choice of the correct price level but also the risk that within card payment schemes constructions will develop allowing regulation to be circumvented, leading, ultimately, to a shifting of costs to acceptors.

As regards other issues arising in this area, the Commission is referred to the separate response of the Federal Cartel Office of 16 May 2012.
2. Relevance of the Green Paper for the definitions set out in the Payment Services Directive

E- and m-payments do not constitute independent payment services for the purposes of the Payment Services Directive

From the perspective of the Federal Republic of Germany, payments through the internet (e-payments) and mobile payments (m-payments) constitute, at present, merely ‘new’ technical means of accessing (i.e. initiating) the established payment infrastructure provided by the banking industry and not new payment services within the meaning of the Payment Services Directive. Therefore, to that extent, no amendments are needed with regard to the scope of the supervisory provisions in the Payment Services Directive.

The possibility for telecommunication-based techniques to operate as an authentication instrument pursuant to Article 4(23) of the Payment Services Directive

In the framework of the forthcoming revision of the Payment Services Directive, the European Commission should examine whether the definition of payment instrument provided for in Article 4(23) needs to be amended to take account of authentication techniques used in e- and m-payments.

The definition of payment instrument provided for in Article 4(23) of the Payment Services Directive requires a ‘personalised device’ or a ‘personalised set of procedures’. Having regard to the scheme of Directive 2007/64, payment instruments must be regarded, in the first place, as personalised where a payment user has been notified of the instrument’s personalised security features which allows his authentication with the payment instrument. Given the use of the term ‘personalised security feature’ in Article 56(2) of Directive 2007/64, this would indicate that the features covered by this term are those which must be kept confidential and are known only to bank customers themselves (for example, PIN number, transaction code, or password).

However, innovative technologies available in connection with e- and m-payments (for example, identification by text message (SMS), or biometric recognition) may render obsolete the use of such customer authentication features. If use of those technologies becomes widespread, it will need to be examined whether they satisfy the requirements of Article 4(23). In this connection, it is important that the Payment Services Directive is capable of accommodating future technological developments in that area.

3. Bank – consumer relationship: issues raised by the Green Paper

Transparency on fees (Question 15)

Merchants should inform consumers about the charges that they are required to pay to the merchant for the use of different payment instruments. Before using a particular payment
instrument a consumer should be informed of the costs involved and have the possibility of choosing the instrument which is most convenient from a consumer perspective.

In contrast, it does not appear necessary to require payment service providers to inform consumers of the merchant service charge levied / the multilateral interchange fee (MIF) income received from customer transactions. That information is unlikely to influence a consumer’s decision.

**Harmonisation of pricing schemes governing the use of payment instruments (Question 16)**

There does not appear to be any need at present for further harmonisation of rebates, surcharges and other steering practices in relation to the use of payment instruments. The Consumer Rights Directive (Directive 2011/83/EU) already restricts the possibility to impose surcharges on consumers. In accordance with Article 19 of that Directive, Member States shall prohibit traders from charging consumers, in respect of the use of a given means of payment, fees that exceed the cost borne by the trader for the use of such means. It needs to be seen how that provision works in practice before considering any further harmonisation in this area.

**4. Payments security issues raised by the Green Paper**

To the extent that further regulation is necessary, the European Commission should examine how measures on payments security can be incorporated in the revised Payment Services Directive. Whatever payment instruments are used it needs to be ensured without exception that they are secure, can withstand criminal attacks and are difficult to counterfeit. Further, it is necessary to ensure equal conditions of competition and the avoidance of gaps in regulation, which might allow individual market participants to offer services that circumvent the data protection requirements otherwise applicable to payment systems and fail to meet the relevant security standards.

**Uniform security requirements (Questions 25-28)**

On the current revision of the Payment Services Directive, a common regulatory framework for payments security should be established which is binding on all participants in the payments process. In this connection, the Government of the Federal Republic of Germany supports the Eurosystem recommendations for the security of internet payments. They offer a viable regulatory solution within the framework of the Payment Services Directive which, if considered desirable, could also be extended to mobile payments. Moreover, on the implementation of such an approach, regard should be had, in addition, to the existing legal standards on data protection such as those established in the Data Protection Directive (Directive 95/46) and the Data Protection Regulation currently proposed by the European Commission. In developing security-related due diligence requirements in the area of e- and

---

10 Ibid.
m-payments, useful guidance may be obtained from the provisions of the Money Laundering Directive.\textsuperscript{11}

When adopting new regulations, account should be taken of the fact that banks as card issuers, payment systems and payment service providers are already subject to numerous legislative provisions which impose strict requirements on the operation of systems and products. None the less, it would be in the interests of consumers and help strengthen confidence in efficient payment instruments to ensure that all technical and other service providers involved in the processing of payments made via e- and m-payment products (without necessarily constituting a payment service provider and, where applicable, involving a service excluded from the scope of the Payment Services Directive pursuant to Article 3 of that directive) are subject to the same provisions on data protection, transparency and security. The issue of security is important not only for customers but also for the providers of services of that kind as it helps strengthen trust in the product.

Unless trust, security and transparency can be established on behalf of payment services users, existing payment services and products – and newly developed electronic retail payment schemes or possible new financial services products – will not be used to their full extent. In the case of card payments, the EMV standard establishes procedures whose security features are sufficient to ensure card security. However, security weaknesses may occur if the EMV chip feature is not used systematically whether by the card issuer or acceptor. In addition, certain card payment systems continue to allow cardholders to make transactions using the card’s magnetic strip in addition to chip-based transactions. This constitutes a weakness for the security of the entire system. However, when card features are changed, consideration needs to be given to the fact that the electronic direct debit scheme in Germany continues (at present) to make use of the information stored on debit cards issued under the domestic scheme (known as ‘girocard’). On switching to cards without a magnetic strip, this information must remain accessible in order to ensure that this scheme – which is an important source of competition – can continue to operate in the long-term. In the case of m-payments, however, the weakness is the mobile device itself. The models currently on the market have not been equipped with the technical features to process a payment transaction with the same reliability and confidence as can be done on a standard basis using a chip card in a merchant’s POS terminal. If the many existing users of domestic card schemes are to have the opportunity to make m-payments enjoying high standards of security protection using a smartphone, the mobile devices used by consumers have to be capable of securely hosting the necessary functions and cryptographic keys. As this infrastructure is controlled by mobile phone operators, device manufacturers and the manufacturers of mobile operating systems, it needs to be ensured that providers of innovative m-payment solutions including

those from outside the mobile telecommunications industry can access this infrastructure on a non-discriminatory basis.

**Third-party access to account information (Question 13)**

The security issues involved with third-party access can become a problem for competition and may lead to banks abusing their superior market position.

This issue has recently arisen in Germany in connection with the payment messenger service ‘sofortüberweisung’ [‘sofortbanking’] provided by the firm Payment Network AG. This kind of service which is also offered by certain players in the banking sector (known as ‘Giropay’) redirect consumers from a payment platform to their own familiar online banking environment where they can make an online credit transfer and the merchant is then informed in real time that the transaction has been made. There are several messenger services within the European Union which operate on the same principle, including the service ‘sofortüberweisung’ provided by Payment Network AG – with one crucial difference. Consumers enter their PIN number and transaction authorisation code on the website of ‘sofortüberweisung’; no formal involvement of their bank is needed in this process. This messenger service operates without any need for registration, storage of bank details or credit to be loaded. Using banking interfaces, the messenger service ensures that an automated credit transfer is made directly within seconds transferring funds from the account of the customer to the account of the merchant. For the purposes of the transaction, all that is needed are bank account number, bank identifier, PIN number and transaction authorisation code. In contrast to conventional online messenger services, ‘sofortüberweisung’, as a non-bank provider, is capable of reaching 99% of all bank accounts which can be operated online.

Clearly, for data security reasons, access to the banks’ transaction processing systems should not be opened up generally to service providers of all kind. As a matter of principle, it should only be possible to request the information needed for the purpose of a specific payment transaction. Were a rule to be introduced making third-party access to account information available to all, this would not only quite clearly endanger security and confidence in the payment system – of particular importance to customers – but also raise numerous issues concerning data protection, copyright and banking secrecy, all of which could no longer be guaranteed if unlimited access was granted on a general basis.

5. **Standardisation issues raised by the Green Paper (Questions 18-22)**

There are always benefits to be gained from standardisation whenever different systems interact (interface standardisation). That is why the Government of the Federal Republic of Germany supports the standardisation activities undertaken by the relevant stakeholders in commerce and industry to improve cross-border interoperability in the areas of card and e- and m-payments. However, given that it is in the interests of customers and merchants that the possibility to make uncomplicated card and e- and m-payments is not limited simply to Europe, it is preferable that standardisation in this area takes place at an international level.
Standardisation is a self-regulatory task to be undertaken by industry in conjunction with other stakeholders. In that connection, the European standardisation bodies, European Committee for Standardisation (ECS) and the European Telecommunications Standards Institute (ETSI), can assist industry and commerce to advance the international standardisation of card, online and mobile payments on the basis of European developments.

In order to ensure that account is taken of public interest objectives, such as data security, standardisation processes need to be transparent and consensus-based, provide for the involvement of all interested parties and allow for public comments/objections to be made. Standardisation carried out by the traditional European and international bodies for standardisation, ESC, ETSI, the International Organisation for Standardisation (ISO) or the International Electrotechnical Commission (IEC) satisfies those procedural requirements. In areas in which forums and consortia have developed technical specifications it is particularly important to ensure effective cooperation between the standardisation bodies and those forums and consortia.