EUROPEAN CENTRAL BANK

EUROSYSTEM

RECOMMENDATIONS FOR THE SECURITY OF MOBILE PAYMENTS

DRAFT DOCUMENT FOR PUBLIC CONSULTATION

1 GENERAL PART

This report presents a set of recommendations to improve the security of mobile payments. These recommendations were developed by the European Forum on the Security of Retail Payments, SecuRe Pay (the "Forum"). The Forum was set up in 2011 as a voluntary cooperative initiative between authorities. It aims to facilitate common knowledge and understanding, in particular between supervisors of payment service providers (PSPs) and overseers, of issues related to the security of electronic retail payment services and instruments provided within the European Union (EU)/European Economic Area (EEA) Member States. The Forum's work focuses on the whole processing chain of electronic retail payment services (excluding cheques and cash), irrespective of the payment channel. The Forum aims to address areas where major weaknesses and vulnerabilities are detected and, where appropriate, makes recommendations. The ultimate aim is to foster the establishment of a harmonised EU/EEA-wide minimum level of security. The authorities participating in the work of the Forum are listed in the annex.

Having started by making recommendations for internet payments, followed by recommendations for payment account access services, the Forum has now turned its attention to mobile payments. Although recently introduced types of mobile payments are still at an early stage of development and deployment, the use of mobile technology for payments may result in additional security exposures attributable to:

- the fact that the current generation of mobile devices and their operating systems were generally not designed with the security of payments in mind;
- the reliance on radio technology (i.e. wireless small range technologies such as Bluetooth and Near Field Communication (NFC) or the over-the-air (OTA) data channels provided by the mobile network operator) for transmission of sensitive payment data and personal data;
- the involvement of additional actors, such as mobile network operators (MNOs) and trusted service managers (TSMs), compared with traditional payments; and

– the general reduced security awareness of mobile device users or unsafe customer behaviour.

The Forum realises that mobile payments, as a new technology for payments, face the particular challenges that customers' perception of security is a basic condition for the use of mobile payment services, and that security incidents could (temporarily) damage the image of mobile payment services.

Moreover, as mobile payment solutions can potentially be deployed more easily than traditional payment instruments, including across borders, a harmonised European approach is warranted.

For the above reasons, the Forum decided to develop recommendations for the security of mobile payments. These reflect the experience gathered from work carried out by overseers and supervisors in their home countries.

The establishment of harmonised European high-level recommendations for the security of mobile payments is expected to contribute to mitigating payment fraud and enhancing consumer trust in mobile payments. Customer trust in mobile payments is all the more important, given that the mobile technology can introduce previously "remote" payment instruments and solutions into the "bricks-and-mortar" environment; mobile payments are therefore an alternative for cash, cheques and "card-present" payments. For card-present payments, a high level of security has been reached throughout Europe thanks to the efforts made over recent years migrating cards and payment terminals to the EMV specifications, which allow for robust card authentication (e.g. by using dynamic or combined data authentication) and cardholder verification (PIN), together forming strong customer authentication. For mobile payments at the point of sale, an equivalent level of security should be aimed for. Similarly, for those mobile payments that compete with internet payments, an equivalent level of security should be aimed for as in the *Recommendations for the security of internet payments*. For both use cases, the specific vulnerabilities and threats, as well as the opportunities, related to the use of mobile technology for payments should be taken into account.

Scope and addressees

Mobile payments can take several forms, but a generic definition, as defined in the 7th SEPA Progress Report (2010), is "payments for which the payments data and the payment instruction are transmitted and/or confirmed via mobile communication and data transmission technology through a mobile device[1] between the customer and his/her payment service provider in the course of an online or

[1] For the purpose of this document, a mobile device is a handheld machine: (i) connected to other devices or systems via radio technologies or via telecommunication networks based on wireless ("over-the-air") technology (e.g. GSM/GPRS/UMTS, Wi-Fi, NFC, RFID, Bluetooth); (ii) designed with a multimedia interface for user interaction (e.g. display, keyboard, sound-speaker); (iii) equipped with a storage facility for "user identification data" (for instance a SIM card, other UICC, or a micro-SD card); and (iv) equipped with a mobile operating system.

offline purchase of services, digital or physical goods"[2]. In one typical use case of mobile payments, the initiation of the payment takes place through a wireless communication between the customer's mobile device and the merchant's payment terminal (e.g. using NFC capability pre-installed on the mobile device or delivered separately on a SIM or SD card). In another use case, the initiation of the payment may take place through the scanning of a QR (Quick Response) code provided by the merchant (e.g. on display at the cash register, generated by its payment terminal, in a printed publication, or on the e-commerce website) followed by a wireless or over-the-air communication between the customer's mobile device and the mobile payment solution provider using an MNO's network or a Wi-Fi connection and the internet. In yet another use case, mobile payments are used for person-to-person (P2P) payments. Further use cases exist and are still being developed.

In the scope of this report are three categories of mobile payments, based on different technologies: contactless payments (e.g. using NFC technology), payments using a mobile payment application ("app") previously downloaded onto the customer's mobile device, and payments using the MNO's channels (e.g. SMS, USSD, voice telephony) without a specific "app" previously downloaded onto the customer's mobile device. Some digital or mobile wallets enable customers to access some of the above, as well as non-payment services, within a single application.

Unless stated otherwise, the recommendations specified in this report are applicable to all PSPs, as defined in the Payment Services Directive[3], when providing mobile payment services, as well as to governance authorities (GAs) of payment instrument schemes developing and offering mobile payment services (including card schemes, credit transfer schemes, direct debit schemes, e-money schemes, etc.). Throughout this document, these are generally referred to as *mobile payment solution providers (MPSPs)*.

The purpose of this report is to define common minimum requirements for the mobile payment services allowing the initiation of payments through a mobile device such as card payments (including the registration of card payment data for use in "wallet solutions"), credit transfers, direct debits, e-money transfers, etc. Excluded from the scope of the report[4] are:

– payments through a mobile device where the customer only uses a *standard* web browser – or a mobile banking or payment application that is strictly acting as a proprietary web browser – to

[2] For the purpose of this document, a payment where the mobile device is only used for authentication of an online banking transaction should not be considered as a mobile payment.

[3] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, p. 1.

[4] Some of these items may be the subject of a separate report at a later stage.

access the internet[5]. These payments are internet payments and already covered by the existing SecuRe Pay *Recommendations for the security of internet payments*.

- technologies transforming mobile devices into physical card payment acceptance devices (e.g. a POS terminal).
- "sticker solutions" (i.e. applying stickers enabled with NFC technology to a mobile device). These sticker solutions are considered contactless card payment services, since the stickers do not actually interact with the mobile device.
- payment transactions outside the scope of the revised PSD (as per the legislative proposal of 24 July 2013), i.e. payment transactions carried out by a provider of electronic communication networks or services where the transaction is provided for a subscriber to the network or service and for purchase of digital content as ancillary services to electronic communications services, regardless of the device used for the purchase or consumption of the content, provided that the value of any single payment transaction does not exceed EUR 50 and the cumulative value of payment transactions does not exceed EUR 200 in any billing month.
- (retail) payment clearing and settlement systems.

Guiding principles

The recommendations are based on five high-level guiding principles.

Firstly, MPSPs should identify, assess and mitigate the specific risks associated with providing mobile payment services. They should give due consideration to, and factor in, risks resulting from reliance on third parties, such as MNOs, TSMs as well as Secure Element and other component manufacturers. Where other actors are involved in the provision of the mobile payment service, MPSPs should ensure that the former's services are provided in compliance with the recommendations set out in this document. They should also consider the mobile device as inherently vulnerable to security issues. In view of the speed of technological advances, the evolution of security threats and fraud mechanisms as well as the introduction of new ways of effecting mobile payments, an ongoing identification and assessment of the relevant risks is of utmost importance.

Secondly, as a general notion, the security of mobile payments relies heavily on the robustness of authentication and registration controls configured within the design of individual mobile payment services. Therefore, MPSPs should protect the initiation of mobile payments, as well as access to sensitive payment data, by strong customer authentication. For the purpose of this report, sensitive

[5] However, providers of mobile banking and payment applications that enable mobile payment services via a proprietary web browser solution are expected to take into account the recommendations in this report applying to the release and the maintenance of applications previously downloaded onto customers' mobile devices. Naturally, providers of mobile banking and payment applications enabling mobile payment services through a comprehensive application previously downloaded onto the customer's mobile device are expected to take into account all the recommendations in this report.

payment data is defined as data which could be used to carry out fraud. These include data enabling a payment order to be initiated, data used for authentication, data used for ordering payment instruments or authentication tools to be sent to customers, as well as data, parameters and software which, if modified, may affect a legitimate party's ability to verify payment transactions or control the payment account.

Strong customer authentication is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: (i) something only the user knows (e.g. a static password, code or personal identification number); (ii) something only the user possesses (e.g. a token, smart card or mobile device[6]); and (iii) something the user is (e.g. a biometric characteristic, such as a fingerprint). In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen.

The strong customer authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data. As an example, where a static password or PIN is used as an element to perform strong customer authentication, MPSPs should ensure that the entry is performed in a way that prevents it from being compromised.

MPSPs could consider adopting alternative customer authentication measures, including no PIN entry, e.g. for low-value payments as referred to in the Payment Services Directive[7]. From the Forum's perspective, MPSPs with no or only weak authentication procedures cannot, in the event of a disputed transaction, provide proof that the customer has authorised the transaction.

Thirdly, MPSPs should implement a robust data protection mechanism to protect sensitive data wherever it is transmitted, processed or stored. Sensitive data include personal data and sensitive payment data as described above. The software installed in the mobile device and used to manage sensitive data should be distributed via a secure channel and regularly checked against tampering. Customers should be able to deactivate the payment functionality of their mobile device and MPSPs should be in a position to deactivate the payment functionality remotely.

Fourthly, MPSPs should implement secure processes for authorising transactions, as well as robust processes for monitoring transactions and systems in order to identify abnormal customer payment patterns and prevent fraud.

[6] The definition includes a mobile device as an example of something only the user possesses. For it to be used as an element in strong customer authentication, all parts of the definition of strong customer authentication need to be met. For example, where the mobile device is used as a strong customer authentication factor related to "something only the user possesses", security measures must be implemented at the mobile device level in order to ensure that the second factor, related to "something only the user knows" or "something the user is", cannot be easily breached due to the use of the mobile device.

[7] See the definition of low-value payment instruments in Articles 34(1) and 53(1) of the Payment Services Directive.

Finally, MPSPs should engage in enhancing customer understanding and provide information on security issues related to the use of mobile payment services with a view to enabling customers[8] to use such services in a safe and secure manner.

The recommendations are formulated as generically as possible to accommodate continual business and technological innovation. However, the Forum is aware that new threats can emerge at any time and will therefore review the recommendations from time to time.

This report does not attempt to set specific security or technical solutions. Nor does it redefine, or suggest amendments to, existing industry technical standards. In this respect, the Forum welcomes the development by the market of technical and security standards for mobile payment services which include objectively necessary non-discriminatory measures to reduce the potential risk associated with these services. Neither does the report redefine, or suggest amendments to, the authorities' expectations in the areas of data protection, anti-money laundering and business continuity. When assessing compliance with the security recommendations, the authorities may take into account conformity with the relevant international standards. Where the recommendations do indicate solutions, the same result may be achieved through other means.

The recommendations outlined in this report constitute minimum expectations. They do not absolve the responsibility of MPSPs and other market participants to monitor and assess the risks involved in their payment operations, develop their own detailed security policies and implement adequate security, contingency, incident management and business continuity measures that are commensurate with the risks inherent in the payment services provided.

Implementation

The report outlines 14 recommendations to promote the security of mobile payments. Each recommendation is specified through key considerations (KCs). The latter must be read along with the recommendations in order to achieve a full understanding of what is expected as a minimum in order to comply with the security recommendations. Addressees must comply with both the recommendations and the KCs or be able to explain and justify any deviation from them upon the request of the relevant competent authority (**"comply or explain" principle**). In addition, the report describes some best practices (BPs) which addressees as well as indirectly the relevant market participants, such as MNOs, mobile device manufacturers and mobile device operating system providers, are encouraged to adopt. These BPs play an important role in the achievement of the

[8] Customers include both consumers and corporate entities to which a payment service is provided.

overall aim to ensure safety of mobile payments as the latter depends on the responsible behaviour of all actors.

The legal basis for the implementation of the recommendations by the national authorities is provided by the domestic legislation transposing the Payment Services Directive and/or the existing oversight and supervisory competence of the relevant authorities. The members of the Forum are committed to supporting the implementation of the recommendations in their respective jurisdictions and will integrate them in existing supervisory/oversight frameworks. The Forum will also strive to ensure effective and consistent implementation across jurisdictions and may cooperate with other competent authorities for this purpose to ensure a level playing field and avoid market fragmentation.

The recommendations should be implemented by MPSPs by <1 February 2017, two years after publication of the final report, to be confirmed>. National authorities may wish to define a shorter transition period where appropriate.

Outline of the report

The recommendations are organised into three categories.

1. **General control and security environment** of the platform supporting the mobile payment service. As part of their risk management procedures, MPSPs should evaluate the adequacy of their internal security controls against internal and external risk scenarios. Recommendations in the first category address issues related to governance, risk identification and assessment, monitoring and reporting, risk control and mitigation issues as well as traceability.
2. **Specific control and security measures for mobile payments**. Recommendations in the second category cover all of the steps of payment transaction processing, from access to the service (customer information, enrolment, authentication solutions) to payment initiation, monitoring and authorisation, as well as the protection of sensitive payment data.
3. **Customer awareness, education and communication**. Recommendations in the third category include customer protection, what customers are expected to do in the event of an unsolicited request for personalised security credentials, how to use mobile payment services safely and, finally, how customers can check that the transaction has been initiated and executed.

The report also contains a glossary of some core definitions. The annex lists the Forum members.

2 RECOMMENDATIONS

General control and security environment

Recommendation 1: Governance

Mobile payment solution providers (MPSPs) should implement a formal security policy for mobile payment services which is subject to periodic review, monitoring and challenge.

1.1 KC *The security policy should be adequately documented, regularly reviewed (in line with KC 2.4) and approved by senior management. It should define security objectives and the underlying risk appetite.*

1.2 KC *The security policy should define roles and responsibilities for enforcing security principles. This should be supported by a robust operating model and clear articulation of roles and responsibilities for risk assessment, control and mitigation, including management of sensitive payment data, for instance via the firm's Three Lines of Defence (3LoD) model.*

1.3 KC *The security policy should address proper and secure design and implementation of all components of mobile payment services. MPSPs should give due consideration to, and factor in, risks resulting from reliance on third parties (e.g. MNOs, TSMs, mobile device manufacturers, application developers) in designing and implementing their security policy for mobile payments.*

1.1 BP *The security policy could be set out in a dedicated document.*

1.2 BP *MPSPs could invite MNOs, TSMs, mobile device manufacturers and application developers to consider in their own security policy the risks their activity may present for the mobile payment services and their users.*

Recommendation 2: Risk assessment

MPSPs should identify and assess risks on an ongoing basis (supported by a formal policy and strategy) in order to ensure the security of mobile payments and ancillary services, but also prior to establishing the service(s).

2.1 KC *MPSPs should carry out, review and document detailed risk assessments for mobile payment services. MPSPs should consider the results of the ongoing monitoring of security threats relating to the mobile payment services they offer or plan to offer, taking into account: (i) the technology solutions used by them; (ii) services outsourced to or provided by external providers; (iii) the* *customers' mobile device; and (iv) the mobile payment acceptance device. MPSPs should consider the risks associated with the relevant technology platforms, application architecture, programming techniques and routines relevant to their own operations as well as the users (consumers and merchants), mobile device (and/or mobile device operating system) manufacturers and external service providers. The assessments should incorporate the results of the security incident monitoring process (see Recommendation 3).*

2.2 KC *On this basis, MPSPs should determine whether and to what extent changes may be necessary to the existing security measures, the technologies used and the procedures or services offered. MPSPs should take into account the time required to implement the changes (including customer roll-out, and external parties' adaptations, especially concerning the MNOs) and initiate appropriate interim measures to minimise security incidents and fraud, as well as potential disruptive effects.*

2.3 KC *The assessment of risks should address the need to protect and secure sensitive payment data.*

2.4 KC *MPSPs should undertake a review of key risk scenarios and existing security measures, after major incidents affecting their services, before and/or after a major change to the infrastructure or procedures including third party infrastructures (and major changes in mobile devices' operating system releases) and when new threats are identified through risk monitoring activities. In addition, a general review of the risk assessment should be carried out at least once a year. The results of the risk assessments and reviews should be submitted to senior management for approval.*

2.1 BP *MPSPs could request that external providers (such as MNOs) take into account security requirements related to mobile payments when carrying out their risk assessments and when qualifying mobile devices and, where applicable, Universal Integrated Circuit Cards (UICCs)****.***

Recommendation 3: Security incident monitoring and reporting

MPSPs should ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints. MPSPs should establish a procedure for reporting such incidents to management and, in the event of major payment security incidents, to competent authorities.

3.1 KC *MPSPs should have a process in place to identify, monitor, handle and follow up on security incidents and security-related customer complaints related to mobile payments.*

3.2 KC *MPSPs should define with all actors involved in the provision of the mobile payment service (e.g. MNOs, TSMs) relevant procedures for collaborating on incident monitoring, handling and follow-up, including security-related customer complaint management.*

3.3 KC *MPSPs should have a procedure for prompt notification to the competent authorities (i.e. supervisory, oversight and data protection authorities) in the event of major payment security incidents with regard to the payment services provided, including data breaches.*

3.4 KC *MPSPs should have a procedure for cooperating with the relevant law enforcement agencies on major payment security incidents, including data breaches.*

3.5 KC *Acquiring MPSPs should contractually require merchants that store, process or transmit sensitive payment data to cooperate on major payment security incidents, including data breaches, both with them and the relevant law enforcement agencies. If an MPSP becomes aware that a merchant is not cooperating as required under the contract, it should take steps to enforce this contractual obligation, or terminate the contract.*

3.1 BP *MPSPs could work in cooperation with MNOs to implement a single point of entry/escalation for customer incidents, including declaration of a lost or stolen mobile device, or develop other measures to simplify the reporting of an incident for the customer**.***

Recommendation 4: Risk control and mitigation

MPSPs should implement proportionate security measures aligned with the risks in order to mitigate identified risks. These measures should incorporate multiple layers of security, whereby the failure of one line of defence is mitigated by the next line of defence (“defence in depth”).

4.1 KC *MPSPs should assume that mobile devices are exposed to security vulnerabilities and take appropriate measures when designing, developing and maintaining mobile payment services.*

4.2 KC *In designing, developing and maintaining mobile payment services, MPSPs should adequately separate information technology environments (e.g. the development, test and production environments) and pay special attention to adequate segregation of duties and access rights, including the proper implementation of the “least privilege” principle*[9] *as the basis for a sound identity and access management.*

[9] Programmes and users of a system should operate using the least amount of rights necessary to complete a process.

4.3 KC *MPSPs should have appropriate security solutions in place to protect all components of mobile payment services (e.g. networks, servers, databases, payment terminals and communication links). These components should be securely configured in order to protect (harden) them and eliminate or reduce vulnerabilities of applications at risk. Access by the various applications to the data and resources required should be kept to an absolute minimum following the "least privilege" principle.*

4.4 KC *MPSPs should have appropriate processes in place to monitor, track and restrict access to: (i) sensitive payment data; and (ii) logical and physical critical resources, such as networks, systems, databases, security modules, etc. MPSPs should create, store and analyse appropriate logs and audit trails of access to logical and physical critical resources.*

4.5 KC *In designing, developing and maintaining mobile payment services, MPSPs should ensure that data minimisation*[10] *is an essential principle of the core functionality*[11]*: the gathering, routing, processing, storing and/or archiving, and visualisation of sensitive payment data should be kept at the absolute minimum level. MPSPs should also ensure that the data used by the payment application are not accessible to other applications/processes of the mobile device ("application sandboxing").*

4.6 KC *In designing, developing and maintaining mobile payment services, MPSPs should ensure that the payment-related software is the genuine one (e.g. via digital signature) upon each access to the service.*

4.7 KC *MPSPs should regularly check that the user's payment-related software is up to date for critical security patches.*

4.8 KC *Security measures for mobile payment services should be periodically assessed, for instance using the firm's 3LoD model, to ensure their robustness and effectiveness. All changes should be subject to a formal change management process ensuring that changes are properly planned, tested, documented and authorised. On the basis of the changes made and the security threats observed, regression testing should be performed to incorporate scenarios of relevant and known potential attacks.*

4.9 KC *MPSPs' security measures for mobile payment services, including payment terminals, should be periodically audited to ensure their robustness and effectiveness. The implementation and*

[10] Data minimisation refers to the policy of gathering the least amount of personal information necessary to perform a given function.

[11] With regard to design, this is also known as "privacy by design".

functioning of the mobile payment services should also be audited. The frequency and focus of such audits should take into consideration, and be in proportion to, the security risks involved. Trusted and independent (internal or external) experts should carry out the audits. The audit should be based on an objective and independent evaluation, i.e. the auditors should not be involved in any way in the development, implementation or operational management of the mobile payment services provided.

4.10 KC *Whenever MPSPs outsource functions that may impact the security of the mobile payment services, the contract should include provisions requiring compliance with the principles and recommendations set out in this report.*

Recommendation 5: Traceability

MPSPs should have processes in place ensuring that all transactions are logged with an appropriate audit trail.

5.1 KC *MPSPs should ensure that their service incorporates security mechanisms for the detailed logging of transaction data, including the transaction sequential number, relevant date and time stamps for transaction data, parameterisation changes as well as access to transaction data.*

5.2 KC *MPSPs should have robust log files allowing retrieval of historical data including a full audit trail of additions, modifications or deletions of transactions.*

5.3 KC *MPSPs should query and analyse the transaction data and ensure that they have tools to evaluate the log files. Access to such tools, including privileged responsibilities, should only be available to authorised personnel and should be appropriately logged.*

5.4 KC *Where payments can be initiated via mobile and other channels (e.g. contact payments, contactless payments, internet payments, etc.) with the same payment instrument (e.g. card, e-money account), MPSPs should ensure that mobile payments are clearly identifiable in the log files.*

5.5 KC *MPSPs should be able to identify and keep track of the source through which the payment was initiated (point of sale, internet) and the beneficiary of the payment (merchant, peer-to-peer, etc.).*

Specific control and security measures for mobile payments

Recommendation 6: Initial customer identification and provision of information

MPSPs should properly identify customers (payers and payees) in line with the European anti-money laundering legislation[12] and should obtain the confirmation of their willingness to make and/or to accept mobile payments using the services before being granted access to such services. MPSPs should provide adequate "prior", "regular" or, where applicable, "ad hoc" information to the customer about the necessary requirements (e.g. equipment features, procedures) for performing and/or accepting secure mobile payment transactions including the inherent risks.

6.1 KC *MPSPs should ensure that, in accordance with legislation, the customer has undergone relevant customer due diligence procedures and has provided adequate documents for establishing his/her identity*[13] *and related information before being granted access to the mobile payment services.*[14]

6.2 KC *MPSPs should ensure that the prior information*[15] *supplied to the customer contains specific details relating to the mobile payment services. These should include:*

– *clear information on any requirements in terms of customer mobile equipment, software or other necessary tools (e.g. antivirus software, firewalls);*

– *guidelines for the proper and secure use of personalised security credentials;*

– *a step-by-step description of the procedure for the customer to submit and authorise a payment transaction and/or obtain information, including the consequences of each action;*

– *guidelines for the proper and secure use of all hardware and software provided to the customer;*

– *the procedure to follow in the event of loss or theft of the personalised security credentials or the customer's hardware or software, including the mobile device, for logging in or carrying out transactions;*

[12] For example, Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, pp. 15-36. See also Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of "politically exposed person" and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis, OJ L 214, 4.8.2006, pp. 29-34.

[13] For example, a passport, a national identity card or an electronic identification with an adequate electronic signature and certificate.

[14] The customer identification process is without prejudice to any exemptions provided for in existing anti-money laundering legislation. PSPs do not need to conduct a separate customer identification process for the mobile payment services, provided that such customer identification has already been carried out by them, e.g. for other existing payment-related services or for the opening of an account.

[15] This information complements Article 42 of the Payment Services Directive which specifies the information that the PSP must provide to the payment service user before entering into a contract for the provision of payment services.

– *the procedure for the customer to follow if he/she changes his/her telephone number or acquires a new mobile device;*

– *the procedure to follow if an abuse is detected or suspected;*

– *a description of the respective responsibilities and liabilities of the MPSP and the customer with regard to the use of the mobile payment service.*

6.3 KC *MPSPs should also ensure that customers are provided with clear and straightforward instructions explaining their responsibilities regarding the secure use of the service, on an ongoing or, where applicable, ad hoc basis, and via appropriate means (e.g. leaflets, website pages).*

6.4 KC *MPSPs should ensure that the framework contract with the customer specifies that the MPSP may block a specific mobile payment transaction or the mobile payment service*[16] *on the basis of security concerns. The framework contract should set out the method and terms of the customer notification and how the customer can contact the MPSP to have the mobile payment transaction or mobile payment service "unblocked", in line with the Payment Services Directive.*

6.1 BP *MPSPs could design specific terms and conditions for conducting mobile payment transactions, rather than the terms being included in a broader general service contract.*

Recommendation 7: Strong customer authentication

MPSPs should ensure that the initiation of mobile payments, as well as access to sensitive payment and personal data, is protected by strong customer authentication.

7.1 KC *MPSPs should have a strong customer authentication procedure in line with the definition provided in this report.*

7.2 KC *MPSPs should perform strong customer authentication for the authorisation of mobile payments. However, MPSPs could consider adopting alternative customer authentication measures, for:*

– *transfers within the same PSP justified by a transaction risk analysis;*

– *low-value payments, as referred to in the Payment Services Directive*[17]*. Where an MPSP authorises low-value payments with alternative customer authentication measures, the MPSP should implement solutions that limit the financial risk for the customer such as to limit the cumulative amount for consecutive payments and to require strong customer authentication to reset the cumulative counters including on-line and off-line payments, if applicable.*

[16] See Article 55 of the Payment Services Directive on limits of the use of the payment instrument.

[17] See the definition of low-value payment instruments in Articles 34(1) and 53(1) of the Payment Services Directive.

For remote payments, i.e. payments where the payer or originator is not physically present at the merchant's physical location, the use of alternative customer authentication measures could also be considered for pre-identified categories of low-risk transactions, e.g. based on a transaction risk analysis.

7.3 KC *Obtaining access to or amending sensitive payment data (including the creation and amending of "white lists") requires strong customer authentication. Where an MPSP offers purely consultative services, with no display of sensitive customer or payment information, such as payment card data, that could be easily misused to commit fraud, the MPSP may adapt its authentication requirements on the basis of its risk assessment.*

7.4 KC *Where a static password or PIN is used as an element to perform customer authentication, MPSPs should ensure that the entry is performed in a way that prevents it from being compromised.*

7.5 KC *MPSPs should ensure secure bilateral authentication when communicating with merchants' acceptance devices for mobile payments (such as payment terminals).*

7.1 BP *Where a static password or PIN is used as an element to perform strong customer authentication for the authorisation of a mobile payment, the entry could be performed on an independent device.*

7.2 BP *MPSPs could provide solutions that enable their customers to be aware of the activation of the payment interface of their mobile devices (such as a sound played by the mobile device each time a payment is authorised).*

Recommendation 8: Enrolment for and provision of authentication tools and/or software

MPSPs should ensure that customer enrolment for and the initial provision of the customer's authentication tools and/or the delivery of software required to use the mobile payment service is carried out in a secure manner.

8.1 KC *MPSPs should distribute the payment-related software and authentication tools, including personalised security credentials, installed in the mobile device via a secure "distribution channel" (e.g. software preloading managed by qualified vendors following auditable procedures; off-line* *software loading at authorised agents or local branches; or on-line downloading from trusted entities using security procedures*[18]*).*

***8.2 KC** Enrolment for and provision of authentication tools and/or payment-related sensitive data delivered to the customer should fulfil the following requirements:*

– *the related procedures should be carried out in a safe and trusted environment*[19] *while taking into account possible risks arising from components (such as TSM components, mobile devices and UICCs) that are not under the PSP's control;*

– *effective and secure procedures should be in place for the delivery of personalised security credentials, payment-related software and all mobile payment-related personalised devices (such as a microSD card); such procedures should at least ensure that credentials are delivered to the legitimate customer and that credentials cannot be intercepted and reused.*

***8.3 KC** MPSPs should:*

– *provide sufficiently secure solutions that allow the customer to activate/deactivate the payment functionality of the mobile device;*

– *be in a position to deactivate the payment functionality of mobile devices remotely.*

***8.4 KC** If a customer wishes to change mobile operator, the handset or the removable devices with user credentials (e.g. SD card, SIM card, etc.), the transfer of such user credentials into the new devices/environment should be carried out in a secure manner (e.g. via trusted agents, secure OTA services, etc.).*

***8.1 BP** MPSPs could provide solutions/procedures that enable the user to perform initial pairing of the personalised security credentials, payment-related software and all mobile payment-related personalised devices using strong customer authentication to ensure that the user's personalised security credentials are used with authentic software and devices. Every change of one of the initially paired security-related components requires the same procedure to be enforced as for pairing or else the payment-related software should prevent the user from accessing the mobile payment service.*

[18] Examples of *on-line* software downloading:
- the user interface "app" (UI_App) is downloadable from a trusted "market store" with clear security policies and sound security measures (e.g. Apps Public Store requiring security evaluation and digital signature of "apps");
- the payment software application that is resident in the SE (SE_Applet) is downloadable inside the SE, using a secure channel between the central server and the SE itself (e.g. encrypted SMS messages, secure OTA services, internet banking services).

[19] The structure of safe and trusted environments depends on the issuing model, e.g.:
- pre-issuing personalisation: the customer's credentials set-up is carried out on the device (handset or SE) by qualified manufacturers or personalisation facilities; the device (SE or handset) is delivered in a secure manner to the customers (e.g. secure mail services, local branches, etc.);
- over-the-air (OTA) provisioning: sensitive data and secret keys are downloaded via network connections using a secure channel, e.g. SMS encrypted messages, TSM/OTA services, dedicated mailbox on the PSP's website or secure website.

8.2 BP *If a mobile payment solution uses MSISDN (or an equivalent mobile subscriber number) as a user identifier, the payment-related software could prevent the user from accessing the mobile payment service using the device when attached to another such identifier (e.g. upon a SIM card change).*

Recommendation 9: Authentication attempts and time-out

MPSPs should limit the number of log-in or authentication attempts (e.g. wrong PIN entries), implement time-out controls and set time limits for the validity of authentication.

9.1 KC *When using a one-time password for authentication purposes, MPSPs should ensure that the validity period of such passwords is limited to the strict minimum necessary.*

9.2 KC *MPSPs should define the maximum number of failed authentication attempts after which access to the mobile payment service is temporarily or permanently blocked. They should have a secure procedure in place to reactivate blocked mobile payment services.*

9.3 KC *MPSPs should define the maximum duration after which inactive mobile payment service sessions are automatically terminated.*

9.1 BP *The period of inactivity resulting in the session termination, as described above, could be made shorter where the user leaves the application or switches the application to run as a background process.*

Recommendation 10: Transaction monitoring

MPSPs should operate transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions; suspicious or high-risk transactions should be subject to a specific screening, filtration and evaluation procedure.

10.1 KC *MPSPs should use fraud detection and prevention systems to identify suspicious transactions before the MPSP finally authorises transactions. Such systems should be based, for example, on parameterised rules (such as black lists of potentially compromised or stolen data resulting from lost or stolen devices), atypical transaction speed (such as long response delay resulting from a man-in-the-middle attack) or abnormal transaction data (such as proximity transactions performed in locations geographically far from one another in a short time), etc. Such systems should also be able to detect signs of malware infection (e.g. via script versus human validation) and known fraud* *scenarios. The nature and scale of the monitoring solutions, while complying with the relevant data protection legislation, should be commensurate with the outcome of the risk assessment.*

10.2 KC *MPSPs should have proportionate fraud detection and prevention systems in place to monitor merchant and payees' payment activities (e.g. detection of compromised points of sale).*

10.3 KC *MPSPs should perform comprehensive transaction screening and evaluation procedures (as defined in KCs 10.1 and 10.2) within an acceptable time period, in order to prevent inordinate delays in the initiation and/or execution of the payment service concerned.*

10.4 KC *Where the MPSP, according to its risk policy, decides to block a payment transaction which has been identified as potentially fraudulent, the MPSP should maintain the block for as short a time as possible until the security issues have been resolved.*

10.1 BP *MPSPs could consider setting up formal agreements to exchange real-time information on mobile payment-related fraud (e.g. fraudulent use cases, attempted fraud, compromised devices and compromised points of sale).*

Recommendation 11: Protection of sensitive payment data and personal data

Sensitive payment data and personal data should be protected when stored, processed or transmitted.

11.1 KC *All data used to identify and authenticate customers (e.g. when initiating mobile payments) should be appropriately secured against theft, unauthorised access or modification.*
11.2 KC *MPSPs should ensure that the unencrypted sensitive payment data are stored and managed in approved hardware/software components (e.g. secure elements).*

11.3 KC *MPSPs should ensure that either no sensitive payment data and personal data is exchanged over the air (e.g. where using Near Field Communication between the mobile device and the payment terminal) or, where sensitive payment data and personal data are exchanged over the air, that secure end-to-end encryption*[20] *is applied in order to safeguard its confidentiality and integrity, using strong and widely recognised encryption techniques.*

11.4 KC *MPSPs should ensure that no sensitive payment data and personal data can be accessed or modified by an unauthorised party through the contactless interface (e.g. NFC) of the mobile device.*

[20] End-to-end-encryption refers to encryption within or at the source end system, with the corresponding decryption occurring only within or at the destination end system.

11.5 KC *MPSPs should ensure that no sensitive payment data can be accessed on lost or stolen mobile devices.*

11.6 KC *MPSPs should have the capability to disable the mobile payment application in handsets that, for example, have been lost, stolen or misused. MPSPs should put in place specific end-of-life procedures with reference to components storing sensitive payment data (e.g. secure removal of user credentials stored in a handset chip or SIM card, secure SE destruction, etc.).*

11.7 KC *In order to mitigate cross-contamination risks, MPSPs should ensure that no sensitive payment data related to mobile payments, including authentication data such as a PIN, can be reused to make fraudulent payments in other environments (e.g. internet payments or counterfeit cards).*

11.1 BP *Where mobile payments are associated with payment cards, MPSPs could use dedicated PANs for mobile transactions to ensure that mobile payments and payments made with the associated cards are uniquely distinguishable.*

11.2 BP *MPSPs could use solutions to remotely erase sensitive payment data from the device upon receipt of a user's report on a lost or stolen device.*

Customer awareness, education and communication

Recommendation 12: Customer education and communication

MPSPs should provide assistance and guidance to customers, where needed, with regard to the secure use of mobile payment services. MPSPs should communicate with their customers in a manner that reassures them of the authenticity of the messages received.

12.1 KC *MPSPs should provide at least one secure channel*[21] *for ongoing communication with customers regarding the correct and secure use of the mobile payment service. MPSPs should inform customers about this channel and explain that any message on behalf of the MPSP via any other means, such as e-mail, is not reliable. MPSPs should explain:*

- *the procedure for customers to report to the MPSP (suspected) fraudulent payments, suspicious incidents or anomalies during the mobile payment services session and/or possible social engineering*[22] *attempts;*
- *the next steps, i.e. how the MPSP will respond to the customer;*
- *how the MPSP will notify the customer about (potential) fraudulent transactions or their non-initiation, or warn the customer about the occurrence of attacks.*

12.2 KC *Through the secure channel, MPSPs should keep customers informed about updates to security procedures regarding mobile payment services. Any alerts about significant emerging risks should also be provided via the secure channel. These could include, for example, warnings about attempts by potential fraudsters to extract customers' personal account information.*

12.3 KC *Customer assistance should be made available by MPSPs for all questions, complaints, requests for support and notifications of anomalies or incidents regarding mobile payments and related services, and customers should be appropriately informed about how such assistance can be obtained with regard to a possible involvement of third parties.*

12.4 KC *MPSPs should initiate customer education and awareness programmes designed to ensure that customers understand, at a minimum, the need:*

- *to protect their passwords, PIN codes, personal details and other confidential data;*
- *to manage properly the security of the personal device (e.g. mobile handset), through installing and updating security components (antivirus, security patches);*

[21] Such as a dedicated mailbox on the PSP's website or a secure website.

[22] Social engineering in the context of payment security refers to attempts by fraudsters to manipulate people into divulging confidential information which could be used to fraudulently access their accounts and remove money from them.

- *to consider significant threats and risks related to downloading software if the customer does not have reasonable knowledge that the software is genuine and has not been tampered with.*

12.5 KC *Where the risk has crystallised before being mitigated, MPSPs should ensure that it has a consumer redress strategy in place.*

12.1 BP *It is desirable that MPSPs offering acquiring services arrange educational programmes for their merchants on fraud prevention.*

12.2 BP *It is desirable that MPSPs and third parties such as the MNOs draft appropriate customer education and communication policies based on a common understanding of risks.*

Recommendation 13: Notifications, setting of limits

MPSPs should set limits for mobile payment services and could provide their customers with options for further risk mitigation within these limits. They may also provide alert and customer profile management services.

13.1 KC *Prior to providing a customer with mobile payment services, MPSPs should set limits relevant to those services (e.g. a cumulative amount over a certain period of time) and should inform their customers accordingly.*

13.2 KC *MPSPs should implement alerts for customers, e.g. via phone calls, SMSs or e-mails, for suspicious or high-risk payment transactions based on their risk management policies.*

13.1 BP *MPSPs could allow customers to lower the limits that may be applied to mobile payment services.*

13.2 BP *MPSPs could allow payers to perform low-value transactions (e.g. buying a city-transport ticket), before completion of enrolment (as covered by Recommendation 8).*

Recommendation 14: Customer access to information on the status of payment initiation and execution

MPSPs should notify customers of the payment initiation and provide customers with timely information necessary to check that a payment transaction has been correctly initiated and/or executed.

***14.1 KC** MPSPs should provide customers with a near real-time facility to check the status of the execution of transactions as well as account balances at any time*[23] *in a safe and trusted environment.*

***14.2 KC** Any detailed electronic statements should be made available in a safe and trusted environment. Where MPSPs inform customers about the availability of electronic statements (e.g. regularly when a periodic e-statement has been issued, or on an ad hoc basis after execution of a transaction) through an alternative channel, such as e-mail or letter, sensitive payment data should not be included in such communications or, if included, they should be masked.*

***14.1 BP** Where mobile payment services allow for person-to-person payments using the same initiation methods as "merchant payments" (e.g. proximity or e-commerce payments), MPSPs could allow the payer to clearly distinguish the payee identity and status (merchant or "person-to-person user") before making a payment.*

[23] Excluding exceptional non-availability of the facility for technical maintenance purposes, or as a result of major incidents.

GLOSSARY OF TERMS AND ACRONYMS

The following terms are defined for the purpose of this report.

Term	Definition and supporting information
3LoD model	The European Confederation of Institutes of Internal Auditing (ECIIA) endorses the 3LoD (Three Lines of Defence) model for internal governance. The 3LoD model can be illustrated as follows: As a first line of defence, the organisation's operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks. As a second line of defence, the risk management function (and also other supporting functions like compliance and quality) facilitates and monitors the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk-related information up and down the organisation. As a third line of defence, the internal auditing function will, through a risk-based approach, provide assurance to the organisation's board and senior management on how effective the organisation assesses and manages its risks, including the manner in which the first and second lines of defence operate. This assurance task covers all elements of an organisation's risk management framework, i.e. from risk identification, assessment and response to communication of risk-related information.
Authorisation	A procedure that checks whether a customer or PSP has the right to perform a certain action, e.g. the right to transfer funds, or to have access to sensitive data.
Credentials	The personal and confidential information provided for the purposes of authentication. Credentials can also refer to the physical tool used for obtaining the information (e.g. one-time-password generator, smart card), or to something the user memorises or represents (such as biometric characteristics).
Governance authority (of a payment instrument scheme)	The entity accountable for the overall functioning of the scheme that promotes the payment instrument in question and for ensuring that all the actors involved comply with the scheme's rules. It is responsible for ensuring the scheme's compliance with oversight standards. European Central Bank (2009), *Harmonised oversight approach and oversight standards for payment instruments*.

Major payment security incident	An incident which has or may have a material impact on the security, integrity or continuity of the MPSP's payment-related systems and/or the security of sensitive payment data or funds. The assessment of materiality should consider the number of potentially affected customers, the amount at risk and the impact on (other) PSPs or other payment infrastructures.
MNO	**Mobile network operator**
MPSP	**Mobile payment solution provider** A PSP providing mobile payment services or a governance authority of a payment instrument scheme developing and offering mobile payment services.
MSISDN	**Mobile Subscriber Integrated Services Digital Network Number** is a number uniquely identifying a subscription in a GSM or UMTS mobile network, i.e. the telephone number associated with the SIM card in a mobile (telephony) device.
Phishing	The act of attempting to acquire personal information such as user names, passwords and details of payment instruments by masquerading as a trustworthy entity in an electronic communication. Variations include "vishing" – using voice communications such as phone calls.
POS payment	Payment where the payer or originator is physically present at the merchant's physical location (or point of sale).
PSP	**Payment service provider**, as defined in the Payment Services Directive.
Regression testing	Regression testing is performed to obtain accurate conclusions regarding the effects of changes or corrections to a program, with a view to ensuring that such changes and corrections have not introduced new errors that may impact system functionality.
Remote payment	Payment where the payer or originator is not physically present at the merchant's physical location.
SD card	A **Secure Digital** or SD card is a non-volatile memory card format for use in portable devices, such as mobile telephones, digital cameras, GPS navigation devices and tablet computers. SD cards are available in standard (SD), miniSD and microSD sizes.
Secure Element	A certified tamper-resistant platform (device or component) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. Examples include the UICC, an embedded Secure Element, a chip card and an SD card.

Sensitive payment data	Data which could be used to carry out fraud, excluding the name of the account owner and the account number, including data enabling a payment order to be initiated (e.g. PAN, card expiry date, CVx2), data used for authentication (customer identifiers, birth date, passwords, codes, PIN, secret questions, passwords/codes for reset, telephone number, certificates), data used for ordering payment instruments or authentication tools to be sent to customers (customer's physical address, telephone number, e-mail address), as well as data, parameters and software which, if modified, may affect the legitimate party's ability to verify payment transactions, authorise e-mandates or control the account (such as "black" and "white" lists, customer-defined limits), and browser plug-ins and java applets provided by PSPs to their customers.
SIM card	A subscriber identity module or **Subscriber Identification Module** (SIM) is an integrated circuit that securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices (such as mobile telephones and computers).
Transaction risk analysis	Evaluation of the risk related to a specific transaction taking into account criteria such as customer payment patterns (behaviour), the value of the related transaction, the type of product and the payee profile.
TSM	A **trusted service manager** acts as a neutral broker that sets up business agreements and technical connections with mobile network operators, mobile device manufacturers or other entities controlling the secure element on mobile devices. The TSM enables service providers to distribute and manage their contactless applications remotely by allowing access to the secure element in NFC-enabled handsets.
UICC	The **Universal Integrated Circuit Card** is the smart card used in mobile terminals in GSM and UMTS networks. In a GSM network, the UICC contains a SIM application and in a UMTS network it is the USIM application.
Wallet solutions	Solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several e-merchants.

ANNEX: LIST OF AUTHORITIES PARTICIPATING IN THE WORK OF THE EUROPEAN FORUM ON THE SECURITY OF RETAIL PAYMENTS

Members

BE	Nationale Bank van België/Banque Nationale de Belgique
BG	Българска народна банка (Bulgarian National Bank)
CZ	Česká národní banka
DK	Danmarks Nationalbank
	Finanstilsynet
DE	Deutsche Bundesbank
	Bundesanstalt für Finanzdienstleistungsaufsicht
EE	Eesti Pank
	Finantsinspektsioon
IE	Central Bank of Ireland
GR	Bank of Greece
ES	Banco de España
FR	Banque de France
	Autorité de Contrôle Prudentiel
HR	Hrvatska narodna banka
IT	Banca d'Italia
CY	Central Bank of Cyprus
LV	Latvijas Banka
	Finanšu un kapitāla tirgus komisija
LT	Lietuvos bankas
LU	Banque centrale du Luxembourg
	Commission de Surveillance du Secteur Financier
HU	Magyar Nemzeti Bank
	Pénzügyi Szervezetek Állami Felügyelete
MT	Central Bank of Malta
NL	De Nederlandsche Bank
AT	Oesterreichische Nationalbank
	Österreichische Finanzmarktaufsicht
PL	Narodowy Bank Polski
	Komisja Nadzoru Finansowego
PT	Banco de Portugal
RO	Banca Națională a României
SI	Banka Slovenije
SK	Národná banka Slovenska
FI	Suomen Pankki – Finlands Bank
	Finanssivalvonta
SE	Sveriges Riksbank
	Finansinspektionen
UK	Financial Conduct Authority
	European Banking Authority
	European Central Bank

Observers

IS	Central Bank of Iceland
	Fjármálaeftirlitið
LI	Liechtensteinische Landesbank 1861
	Finanzmarktaufsicht Liechtenstein
NO	Norges Bank
	Finanstilsynet – The Financial Supervisory Authority of Norway
	European Commission
	Europol