EUROPEAN CENTRAL BANK

EUROSYSTEM

RECOMMENDATIONS FOR "PAYMENT ACCOUNT ACCESS" SERVICES

DRAFT DOCUMENT FOR PUBLIC CONSULTATION

I GENERAL PART

This report presents a set of recommendations to improve the security of payment account access services. 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 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.

In 2012 the Forum developed a set of recommendations for the security of internet payments (the "internet recommendations"). The internet recommendations, however, do not cover internet-based services where access to a payment account or information on a payment account involves a third-party service provider. Given the distinctive features of payment account access services, the Forum decided to address them separately from internet payment services provided without the involvement of a third party. These recommendations – which incorporate those parts of the internet recommendations that also apply to payment account access services – reflect the experience of overseers and supervisors in their home countries and take into account the feedback obtained from service providers with specific knowledge in the field of payment account access services.

The establishment of harmonised European recommendations for the security of payment account access services is expected to contribute to fighting payment fraud and enhancing consumer trust in payment account access services. The report also includes some best practices, which third-party service providers and other market participants are encouraged to adopt. These best practices are important as the safety of payment account access services depends on the responsible behaviour of all actors.

PAYMENT ACCOUNT ACCESS SERVICES

Payment service providers (PSPs)[1] issuing payment accounts to customers (account owners)[2] are "account servicing PSPs". Although third-party service providers (TPs) can be PSPs, they are often merely non-licensed service providers and not PSPs, as long as they do not enter into the possession of funds or provide one of the activities listed in the annex to the Payment Services Directive. The

1 As defined in the Payment Services Directive. 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.

2 Account owners include both consumers and companies to which payment account access services are provided.

recommendations apply to TPs providing payment account access services for accounts they have not issued themselves.[3]

These internet-based payment account access services are **account information services** and/or **payment initiation services**.

– Account information services provide information on several accounts held by a person with one or several PSPs and present that information to the person in a consolidated and user-friendly way. To provide this service the TP needs to have access to the person's payment account(s).

– Payment initiation services initiate payment transactions via a person's internet-enabled payment account. The technical implementation of this service can differ depending on whether or not the payee is actively involved in the payment initiation (e.g. during online shopping) and whether the TP's software is used by the account owner to transmit his/her credentials to the account servicing PSP.

Payment account access services can be offered as proprietary solutions by individual TPs or they can be organised in the form of a scheme, with a governance authority (GA)[4] and TPs – and usually account servicing PSPs – as the scheme participants. Some of the schemes cooperate with credit institutions or are even owned by them. Proprietary solutions, however, often do not have any affiliation with the banking industry.

From a European perspective, payment account access services are still niche products. In practice, however, they are rapidly gaining importance and payment initiation services are already among the most important payment methods for e-commerce in some Member States. The specific characteristics of payment account access services are linked to the involvement of at least one additional entity, the TP, implying additional communication sessions/re-directions and possibly greater complexity when allocating liability. Furthermore, depending on the technical implementation, payment account access services might: i) make the traceability of payment account-related processes more difficult for account servicing PSPs and/or account owners, or ii) might affect or be affected by account servicing PSPs' security and customer education measures. Moreover, unlike PSPs, those TPs that are not licensed are not subject to supervisory requirements.

OBJECTIVE OF THE RECOMMENDATIONS

The objective of the recommendations is to promote the security of payment account access services, with the ultimate purpose being to protect the account owner. More specifically, the recommendations should ensure that the following requirements are met.

– TPs should have security and control measures in place ensuring a level of security similar to that required by the internet recommendations. The security of the payment account should not be undermined by the performance of payment account access services.

– Increased transparency for account owners enabling them to assess risks and make an informed choice before and during the use of payment account access services.

3 Where an account servicing PSP only offers payment account access services for accounts issued to its own customers, the account servicing PSP does not qualify as a third party and does not fall within the scope of this report.

4 The governance authority is accountable for the overall functioning of the scheme that promotes the (initiation of the) payment instrument in question and ensuring that all the actors involved comply with the scheme's rules. Moreover, 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*, February.

– Traceability through proper authentication in all communications between the entities involved (i.e. the TP, the account servicing PSP, the e-merchant and the account owner).

– Improved exchange of information in the event of repudiation, security incidents and/or fraud.

– The duration of payment account access and the quantity of data elements obtained, processed, exchanged and stored should be minimised thus reducing the risk of misuse of those data elements.

– TPs entering into contractual agreements with e-merchants should ensure that the e-merchants comply with the necessary security requirements.

SCOPE AND ADDRESSEES

Unless stated otherwise, the recommendations, key considerations and best practices specified in this report are applicable to all TPs providing internet-based payment account access services. Certain recommendations also apply to account servicing PSPs and to GAs of schemes that provide payment account access services. The purpose of this report is to define common minimum requirements for internet-based payment account access services.

Excluded from the scope of the present recommendations are:[5]

– accounts for which making payments is not a primary function (e.g. typical savings, mortgage or securities accounts);

– payment accounts of payees;

– traditional online payments and/or the supply of account information without the involvement of a third-party service provider;

– internet services other than online payment and/or account information services provided by a PSP via its payment website (e.g. e-brokerage, online contracts);

– mobile payments other than browser-based payments;[6]

– payment transactions made by an enterprise via dedicated networks;

– clearing and settlement of payment transactions.

GUIDING PRINCIPLES

The four guiding principles outlined in the internet recommendations also apply with respect to the payment account access services recommendations: i) addressees should perform specific assessments of the risks; ii) prior registration for payment account access and any services based on such access, as well as access to sensitive payment data, should be protected by strong customer authentication; iii) effective processes for authorising transactions, as well as for monitoring transactions and systems should be implemented in order to identify abnormal customer payment patterns and prevent fraud; and iv) customer awareness and education programmes on security issues should be provided.

5 Some of these items may be the subject of a separate report at a later stage.
6 Specific recommendations applying to the release and maintenance of software applications will be the subject of a separate work stream on mobile payments.

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

The report does not attempt to set specific security or technical solutions. Nor does it redefine, or suggest amendments to, existing industry technical standards or the authorities' expectations in the areas of data protection and business continuity. Where the recommendations indicate solutions, the same result may be achieved through other means.

The recommendations outlined in this report constitute minimum expectations. They are without prejudice to the responsibility of TPs, GAs and other market participants to monitor and assess the risks involved in their services 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 account access services provided.

The present recommendations do not target individual existing or future services and providers. They should be taken neither to support nor oppose any individual provider or service. The recommendations are without prejudice to future regulatory initiatives and/or decisions that authorities may take on payment account access services.

IMPLEMENTATION

The report outlines 14 recommendations to promote the security of payment account access services. Each recommendation is specified through key considerations (KC). 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 recommendations. Addressees are expected to comply with both the recommendations and KCs or need to be able to explain and justify any deviation from them upon the request of the relevant competent authority (**"comply or explain" principle**). The report also includes some best practices (BP) which TPs and other relevant market participants are encouraged to adopt. Some core definitions are listed in the glossary.

Despite being a market reality, payment account access services are currently not covered by the Payment Services Directive.[7] The Forum would welcome an extension of the scope of the Directive, in the context of its review, to cover payment account access services and their providers.[8] In that case, the legal basis for implementation of the recommendations by the national authorities would be provided by the domestic legislation transposing the revised Payment Services Directive. Currently, the legal basis for implementation of the recommendations is 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.

The recommendations should be implemented by TPs, GAs and the relevant market participants by [xxx].[9] National authorities may wish to define a shorter transition period where appropriate.

7 As recognised, inter alia, by the Payments Committee. See the summary of the third meeting of the Payments Committee, 19 October 2010 (available on the European Commission's website at http://www.europa.eu).
8 Article 87 of the Payment Services Directive requires the European Commission to present a report on the implementation and impact of the Directive, accompanied, where appropriate, by a proposal for its revision.
9 After the public consultation and finalisation of the recommendations, the Forum will decide an appropriate time limit for their implementation.

2 RECOMMENDATIONS

GENERAL CONTROL AND SECURITY ENVIRONMENT

Recommendation 1: Governance

TPs and GAs should implement and regularly review a formal security policy for payment account access services.

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

1.2 KC The security policy should define roles and responsibilities, including the risk management function with a direct reporting line to board level, and the reporting lines for the payment account access services provided, including management of sensitive payment data with regard to the risk assessment, control and mitigation.

1.1 BP The security policy could be laid down in a dedicated document.

1.2 BP PSPs and TPs could define minimum technical and security criteria for payment account access services which are objectively necessary to reduce the potential risk associated with those services. The criteria could be made available to interested parties.

Recommendation 2: Risk assessment

TPs and GAs should carry out and document thorough risk assessments with regard to the security of payment account access services, both prior to establishing the service(s) and regularly thereafter.

2.1 KC TPs and GAs, through their risk management function, should carry out and document detailed risk assessments for payment account access services. These assessments should also include potential risks to the account servicing PSP from the performance of payment account access services. TPs and GAs should consider the results of the ongoing monitoring of security threats relating to the payment account access services they offer or plan to offer, taking into account: i) the technology solutions used by them, ii) services outsourced to external providers and, iii) the customers' technical environment. TPs and GAs should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines on their side,[10] the side of the account servicing PSP and the side of their customers,[11] as well as the results of the security incident monitoring process (see Recommendation 3).

2.2 KC On this basis, TPs and GAs 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. TPs and GAs should take into account the time required to implement the changes (including customer roll-out) and take the 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.

10 Such as the susceptibility of the system to payment session hijacking, SQL injection, cross-site scripting, buffer overflows, etc.
11 Such as risks associated with using multimedia applications, browser plug-ins, frames, external links, etc.

2.4 KC TPs and GAs should undertake a review of the risk scenarios and existing security measures after major incidents affecting their services, before a major change to the infrastructure or procedures 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.

Recommendation 3: Incident monitoring and reporting

TPs and GAs should ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints. TPs and GAs should establish a procedure for reporting such incidents to management and, in the event of major security incidents,[12] the competent authorities.

3.1 KC TPs and GAs should have a process in place to monitor, handle and follow up on security incidents and security-related customer complaints and report such incidents to the management.

3.2 KC TPs and GAs should have a procedure for notifying immediately the competent authorities (i.e. supervisory, oversight and data protection authorities), where they exist, in the event of major security incidents with regard to the payment account access services provided.

3.3 KC TPs, GAs and account servicing PSPs should have a procedure for cooperating on major security incidents, including data breaches, with the relevant law enforcement agencies.

3.4 KC TPs entering into contractual agreements with e-merchants should require e-merchants to cooperate on major security incidents, including data breaches, both with them and the relevant law enforcement agencies. If a TP becomes aware that an e-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 TPs, GAs and PSPs could provide for arrangements to inform each other of major security incidents.

Recommendation 4: Risk control and mitigation

TPs and GAs should implement security measures in line with their respective security policies in order to mitigate identified risks. These measures should incorporate multiple layers of security defences, where the failure of one line of defence is caught by the next line of defence ("defence in depth").

4.1 KC Based on their risk assessment, TPs and GAs should have appropriate security and control measures in place in order not to undermine the information technology (IT) security of the account servicing PSP.

4.2 KC In designing, developing and maintaining payment account access services, TPs and GAs should pay special attention to the adequate segregation of duties in IT environments (e.g. the development, test and production environments) and the proper implementation of the "least privilege" principle[13] as the basis for a sound identity and access management.

12 A "major security incident" is an incident which has or may have a material impact on the security, integrity or continuity of the TP's and/or PSP'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 TPs, PSPs or other payment infrastructures.

13 Programmes and users of a system should operate using the least amount of privilege necessary to complete a process.

4.3 KC TPs and GAs should have appropriate security solutions in place to protect networks, websites, servers and communication links against abuse or attacks. TPs and GAs should strip the servers of all superfluous functions 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 a strict minimum following the "least privilege" principle. In order to restrict the use of "fake" websites (imitating legitimate TP sites), websites offering payment account access services should be identified by extended validation certificates drawn up in the TP's name or by other similar authentication methods.

4.4 KC TPs and GAs 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. TPs should create, store and analyse appropriate logs and audit trails.

4.5 KC In designing,[14] developing and maintaining payment account access services, TPs should ensure that data minimisation[15] is an essential component of the core functionality: the gathering, routing, processing, storing and/or archiving, and visualisation of sensitive payment data should be kept at the absolute minimum level.

4.6 KC Security measures for payment account access services should be tested under the supervision of the risk management function 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, tests should be repeated regularly and include scenarios of relevant and known potential attacks.

4.7 KC The TP's security measures for payment account access services should be periodically audited to ensure their robustness and effectiveness. The implementation and functioning of the payment account access 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. They should not be involved in any way in the development, implementation or operational management of the payment account access services provided.

4.8 KC Whenever TPs and GAs outsource functions related to the security of payment account access services, the contract should include provisions requiring compliance with the principles and recommendations set out in this report.

4.9 KC TPs entering into contractual agreements with e-merchants should not authorise e-merchants to handle (i.e. store, process or transmit) sensitive payment data in relation to the payment account access service.

4.10 KC TPs and GAs should ensure that their security policy and their risk control and mitigation measures provide for at least the same level of security as the minimum requirements defined in the internet recommendations.

4.1 BP TPs could provide security tools (e.g. devices and/or customised browsers, properly secured) to protect the customer interface against unlawful use or attacks (e.g. "man in the browser" attacks).

14 Privacy by design.
15 Data minimisation refers to the policy of gathering the least amount of personal information necessary to perform a given function.

Recommendation 5: Traceability

TPs should have processes in place ensuring that all transactions, as well as the payment account access process flow, are appropriately traced.

5.1 KC TPs should ensure that their service incorporates security mechanisms for the detailed logging of transaction and process flow data related to payment account access services, including the transaction sequential number, timestamps for transaction data, parameterisation changes as well as access to transaction and sensitive payment data.

5.2 KC TPs should implement log files allowing any addition, change or deletion of transaction and sensitive payment data and/or access to this data to be traced.

5.3 KC TPs should query and analyse the traced data and ensure that they have tools to evaluate the log files. The respective applications should only be available to authorised personnel.

5.4 KC TPs, GAs and account servicing PSPs should cooperate in the analysis of major security incidents and in any follow-up action, in line with the procedures established under 3.3 KC.

5.5 KC TPs should ensure proper bilateral authentication when communicating with e-merchants and/or account servicing PSPs in providing payment account access services.

5.6 KC Account servicing PSPs should be able to differentiate between payment account access by TPs and access by account owners without TP involvement.

5.1 BP Account servicing PSPs could provide customers with specific credentials to be used for payment account access services. This would allow the account servicing PSP to identify whether the account owner is making use of a payment account access service.

SPECIFIC CONTROL AND SECURITY MEASURES FOR PAYMENT ACCOUNT ACCESS SERVICES

Recommendation 6: Initial customer identification and information

Customers should confirm their willingness to make use of payment account access services before being granted access to such services. TPs and GAs should provide adequate "prior" and, in the case of registered customers, "regular" or, where applicable, "ad hoc" information to the customer about the necessary requirements (e.g. equipment, procedures) for the secure use of payment account access services and the inherent risks.

6.1 KC TPs should (where applicable) ensure that the customer has undergone the customer due diligence procedures, and has provided adequate identity documents[16] and related information before being granted access to payment account access services.[17]

6.2 KC TPs should (where applicable) ensure that the prior information supplied to the customer contains specific details relating to the payment account access services. These should include, as appropriate:

16 For example, passport, national identity card or advanced electronic signature.

17 The customer identification process is without prejudice to any exemptions provided in existing anti-money laundering legislation. TPs need not conduct a separate customer identification process for the payment account access services, provided that such customer identification has already been carried out, e.g. for other existing services.

– clear information on any requirements in terms of customer 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 procedures to follow in the event of loss or theft of the personalised security credentials or the customer's hardware or software for logging in or carrying out transactions;

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

– a description of the responsibilities and liabilities of the TP and the customer respectively with regard to the use of payment account access services.

6.3 KC TPs should ensure that the framework contract with the customer specifies that the TP may block a specific transaction and/or attempts to access sensitive payment data on the basis of security concerns. It should set out the method and terms of the customer notification and how the customer can contact the TP to have the payment account access service "unblocked".

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

6.5 KC For TPs offering both account information services and payment initiation services, the account owner should be required to actively opt for each of the services separately, instead of being automatically granted access to all types of payment account access services offered by the TP.

6.1 BP The customer could sign a dedicated service contract before using payment account access services, rather than the terms being included in a broader general service contract with the TP and or/the account servicing PSP.

Recommendation 7: Strong customer authentication

TPs requiring prior registration by the account owner for payment account access services[18] and subsequently enabling direct customer authentication should ensure that the initiation of internet payments, as well as access to sensitive payment data, is protected by strong customer authentication.[19]

18 TPs generally require the customer to register before using account information services. However, registration is usually only required for certain types of payment initiation services.

19 Strong customer authentication is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: something only the user knows, e.g. static password, code, personal identification number; something only the user possesses, e.g. token, smart card, mobile phone; and something the user is, e.g. 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 via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data.

7.1 KC TPs (where applicable) should perform strong customer authentication for the customer's access to payment account access services. However, a TP could agree with an account servicing PSP to rely on the account servicing PSP's authentication methods.

7.2 KC Obtaining access to or amending sensitive payment data (including the creation and amending of white lists) requires strong customer authentication. Where a TP offers purely consultative services, with no display of sensitive payment data, the TP may adapt its authentication requirements on the basis of its risk assessment.

7.3 KC The account owner's initial registration (if any) for payment account access services should take place in a safe and trusted environment[20] while taking into account possible risks arising from devices that are not under the TP's control.

7.1 BP Strong customer authentication could include elements linking the authentication to a specific amount and payee. This could provide customers with increased certainty when authorising payments. The technology solution enabling the strong authentication data and transaction data to be linked should be tamper resistant.

Recommendation 8: Enrolment for and provision of authentication tools and/or software delivered to the customer

TPs should (where applicable) ensure that customer enrolment for and the initial provision of the authentication tools required to use the payment account access service and/or the delivery of payment account access-related software to customers is carried out in a secure manner.

8.1 KC Enrolment (if any) for and provision of authentication tools and/or payment account access-related software delivered to the customer should fulfil the following requirements.

– The related procedures should be carried out in a safe and trusted environment, while taking into account possible risks arising from devices that are not under the TP's control.

– Effective and secure procedures should be in place for the delivery of personalised security credentials, payment account access-related software and all payment account access-related personalised devices. Software delivered via the internet should also be digitally signed by the TP to allow the customer to verify its authenticity and that it has not been tampered with.

8.2 KC TPs should actively encourage customer enrolment for strong authentication.

8.3 KC TPs and GAs should ensure that (where applicable) enrolment for the payment account access services provides for at least the same level of security as the minimum requirements defined in the internet recommendations.

Recommendation 9: Log-in attempts, session time out, validity of authentication

TPs should (where applicable)[21] limit the number of log-in or authentication attempts, define rules for payment account access session "time out" and set time limits for the validity of authentication.

20 Environments where adequate authentication of the customer and of the TP offering the service and the protection of confidential/sensitive information is assured include: i) the TP's premises; ii) a secure website under the responsibility of the TP or the GA offering comparable security features inter alia as defined in Recommendation 4; or iii) automated teller machine (ATM) services. (In the case of ATMs, strong customer authentication is required. Such authentication is typically provided by chip and PIN, or chip and biometrics.)

21 Such as if the TP requires the customer to log in separately based on the registration with the TP.

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

9.2 KC TPs should (where applicable) set down the maximum number of failed log-in or authentication attempts after which access to the payment account access service is (temporarily or permanently) blocked. They should have a secure procedure in place to re-activate blocked payment account access services.

9.3 KC TPs should set down the maximum period after which inactive payment account access sessions are automatically terminated. In general, TPs should keep the internet sessions as short as possible and actively log out as soon as the requested action has been completed.

9.4 KC A TP should only access the payment account upon the customer's specific instruction and on a case-by-case basis.

Recommendation 10: Monitoring

Monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions and/or attempts to access sensitive payment data should be operated before the TP submits transactions and/or attempts to access sensitive payment data; suspicious or high risk transactions and processes should be subject to a specific screening and evaluation procedure.

10.1 KC TPs should use fraud detection and prevention systems to identify suspicious transactions and processes before the TP submits transactions and/or attempts to access sensitive payment data. Such systems should be based, for example, on parameterised rules (such as black lists), and monitor abnormal behaviour patterns of the customer or the customer's access device (such as a change of Internet Protocol (IP) address[22] or IP range during the payment account access session, sometimes identified by geolocation IP checks,[23] atypical e-merchant categories for a specific customer or abnormal transaction data, etc.). Such systems should also be able to detect signs of malware infection in the session (e.g. via script versus human validation) and known fraud scenarios. The extent, complexity and adaptability 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 TPs entering into contractual agreements with e-merchants should have fraud detection and prevention systems in place to monitor e-merchant activities.

10.3 KC TPs should perform any screening and evaluation procedures within an appropriate time period, in order not to unduly delay the initiation and/or execution of the payment transaction concerned and/or attempts to access sensitive payment data.

10.4 KC Where the TP, according to its risk policy, decides to block the initiation of a payment transaction and/or an attempt to access sensitive payment data which has been identified as potentially fraudulent, the TP should maintain the block for as short a time as possible until the security issues have been resolved.

10.5 KC In the event of an ex post dispute or suspected fraud, all professional entities involved in the payment account access service (e.g. e-merchants, TPs and account servicing PSPs) should

22 An IP address is a unique numeric code identifying each computer connected to the internet.
23 A "Geo-IP" check verifies whether the issuing country corresponds with the IP address from which the user is initiating the transaction.

cooperate actively (within the possibilities offered by data protection legislation) to analyse the root cause of the problem.

Recommendation 11: Protection of sensitive payment data

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

11.1 KC All data used to identify and authenticate customers (e.g. at log-in or when initiating internet payments), as well as the customer interface (TP or e-merchant website), should be appropriately secured against theft and unauthorised access or modification.

11.2 KC TPs should ensure that when exchanging sensitive payment data via the internet, secure end-to-end encryption[24] is applied between the communicating parties throughout the respective communication session, in order to safeguard the confidentiality and integrity of the data, using strong and widely recognised encryption techniques. Re-directions of the account owner during a payment account access session should be carried out in a safe and trusted environment, while taking into account possible risks arising from devices that are not under the TP's control.

11.3 KC TPs entering into contractual agreements with e-merchants should not make any sensitive payment data available to e-merchants. TPs should not authorise their e-merchants to store any sensitive payment data in relation to payment account access services.

11.4 KC TPs should only access payment accounts upon the account owner's specific instruction and on a case-by-case basis. The purpose of payment account access should be clearly determined and agreed between the TP and the customer prior to any attempt to access the payment account and the TP's involvement should be limited to the extent necessary to achieve this purpose ("proportionality principle").

11.5 KC TPs should not store sensitive payment data after the payment account access session of the account owner. TPs storing data should ensure that the data are appropriately protected against theft and unauthorised access or modification.

11.6 KC TPs should not use the account information for other purposes (e.g. for data mining, advertising, credit rating or data re-selling) than those actively requested by the account owner.

11.1 BP It is desirable that e-merchants handling sensitive payment data appropriately train their fraud management staff and update this training regularly to ensure that the content remains relevant to a dynamic security environment.

11.2 BP It is desirable that TPs only access data from the payment account expressly indicated by the account owner during the payment account access session, and not the account owner's other accounts, such as savings or securities accounts or other payment accounts.

24 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. ETSI EN 302 109 V1.1.1. (2003-06).

CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION

Recommendation 12: Customer education and communication

TPs should provide assistance and guidance to customers, where needed, with regard to the secure use of the payment account access services. TPs should communicate with their customers in such a way as to reassure them of the authenticity of the messages received.

12.1 KC TPs should provide at least one secured channel[25] for ongoing communication with customers regarding the correct and secure use of the payment account access services. TPs should inform customers of this channel and explain that any message on behalf of the TP via any other means, such as e-mail, which concerns the correct and secure use of the payment account access service, is not reliable. The TP should explain:

- the procedure for customers to report to the TP (suspected) fraudulent payments and/or attempts to access sensitive payment data, suspicious incidents or anomalies during the payment account access session and/or possible social engineering[26] attempts;
- the next steps, i.e. how the TP will respond to the customer;
- how the TP will notify the customer about (potential) fraudulent transactions or their non-initiation and/or attempts to access sensitive payment data, or warn the customer about the occurrence of attacks (e.g. phishing e-mails).

12.2 KC TPs should keep customers informed, through the secured channel, about updates in security procedures regarding payment account access services. Any alerts about significant emerging risks (e.g. warnings about social engineering) should also be provided via the secured channel.

12.3 KC Customer assistance should be made available by TPs for all questions, complaints, requests for support and notifications of anomalies or incidents regarding payment account access services, and customers should be appropriately informed about how such assistance can be obtained.

12.4 KC TPs, and, where relevant, GAs should initiate customer education and awareness programmes designed to ensure customers understand, at a minimum, the need:

- to protect their passwords, security tokens, personal details and other confidential data;
- to manage properly the security of the personal device (e.g. computer), through installing and updating security components (antivirus, firewalls, security patches);
- to consider the significant threats and risks related to downloading software via the internet if the customer cannot be reasonably sure that the software is genuine and has not been tampered with;
- to check that any re-direction is to a secured website and that the extended validation certificate is drawn up in the name of a trusted entity, i.e. the account servicing PSP or the TP.

25 Such as a dedicated mailbox on the TP's website or a secured website.

26 Social engineering in this context means techniques of manipulating people to obtain information (e.g. via e-mail or phone calls), or retrieving information from social networks, for the purposes of fraud or gaining unauthorised access to a computer or network.

12.5 KC TPs entering into contractual agreements with e-merchants should require e-merchants to clearly separate payment-related processes from the online shop in order to make it easier for customers to identify when they are communicating with the TP and/or the account servicing PSP and not the payee (e.g. by re-directing the customer and opening a separate window so that the payment process is not shown within a frame of the e-merchant).

12.6 KC TPs should ensure that their liability regime is transparent to customers (e.g. in the framework contract and/or the terms and conditions), including the maximum amount of indemnification in the event of unauthorised use/fraud and the functioning of the complaints process.

12.7 KC Payment account access services should not compromise the possibility for the account servicing PSP to send security-related messages, such as phishing alerts, to the customer. For example, TPs should not mark these messages as being read without ensuring that the customer has taken note of them.

12.8 KC TPs should inform customers, at each payment account access session and in clear and simple language, that they will access specific sensitive data elements for the purpose of providing the service and ask whether, based on this information, the customer would like to proceed or cancel the process.

12.9 KC The customer should expressly agree to any use by the TP of sensitive payment data, e.g. data routing, processing, storing and/or archiving, in the contract for payment account access services entered into with the TP. The TP should clearly list each data element in the contract.

12.1 BP It is desirable that TPs entering into contractual agreements with e-merchants arrange educational programmes for their e-merchants on fraud prevention.

Recommendation 13: Notifications, setting of limits

TPs should set limits for their payment initiation services and could provide their registered customers with options for further risk limitation within these limits. They may also provide alert and customer profile management services.

13.1 KC Prior to providing a customer with payment initiation services, TPs should set limits applying to those services (e.g. a maximum amount for each individual payment or a cumulative amount over a certain period of time) and should inform their customers accordingly. Where a TP offers both account information services and payment initiation services to an individual registered customer, the customer should be able to disable the payment initiation functionality.

13.1 BP Within the set limits, TPs could provide their registered customers with the facility to manage limits for payment initiation services in a safe and trusted environment.

13.2 BP TPs could implement alerts for registered customers, such as via phone calls or SMS, for suspicious or high risk payment transactions based on their risk management policies.

13.3 BP TPs could enable registered customers to specify general, personalised rules as parameters for their behaviour with regard to payment account access services, e.g. that they will only initiate payments from certain specific countries and that payments initiated from elsewhere should be blocked, or that they may include specific payees in white or black lists.

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

TPs should confirm to their customers the successful completion of the payment initiation.

14.1 KC TPs should provide customers with a near real-time facility to check the status of the payment initiation at any time in a safe and trusted environment.

14.2 KC Any detailed electronic statements should be made available in a safe and trusted environment. Where TPs 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 payment initiation) through an alternative channel, such as SMS, e-mail or letter, sensitive payment data should not be included in such communications or, if included, they should be masked.

14.1 BP In addition to the e-merchant's reference and/or the information provided by the customer, TPs could include its brand name (as known to the customer) and/or help desk details in the remittance information.

GLOSSARY OF TERMS

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

Term	Definition
Account information services	Internet-based aggregation/visualisation services that collect information on different accounts held by an account owner with one or more account servicing payment service providers (PSPs) and which can be accessed via the internet. The consolidated information of these accounts is presented to the account owner in a user friendly way via a single website.
Account owner	Customer who has the power of disposition over a payment account. The account owner has entered into a contract with the account servicing PSP, agreeing on the terms and conditions for a payment account issued by and held with the account servicing PSP. In the context of payment initiation services, the term "account owner" refers to the payer and also includes persons authorised to initiate payments from the respective account.
Account servicing PSP	Payment service provider issuing (and maintaining) payment accounts to (for) account owners. Only PSPs as defined in the Payment Services Directive are authorised to issue payment accounts. Account servicing PSPs issue (and maintain) payment accounts on behalf of customers (account owners). An account servicing PSP can decide to outsource certain functionalities to other companies (e.g. IT data processing centres, network providers), however, any outsourcing must be based on a contractual agreement defining the parties' respective rights and responsibilities and is assumed to observe the principles of the Joint Forum of the Basel Committee on Banking Supervision, the International Organization of Securities Commissions and the International Association of Insurance Supervisors.[1] Therefore, outsourcing agreements are not specifically addressed here but are considered to be under the account servicing PSP's responsibility for the purpose of the report.
Authentication	A procedure that allows the PSP to verify a customer's identity.
Credentials	The information – generally confidential – provided by a customer or PSP for the purposes of authentication. Credentials can also mean the physical tool containing the information (e.g. one-time-password generator, smart card), or something the user memorises or represents (such as biometric characteristics).
Payment account	An account issued by a PSP and used by an account owner for the main purpose of initiating and receiving payments. Other types of accounts, such as savings accounts, are not covered in this report.
Payment initiation services	Internet-based services to initiate payment transactions via payment accounts. The technical implementation of this service can differ based on whether or not the payee is actively involved in the payment initiation and whether the TP's software is used by the account owner to transmit his/her credentials to the account servicing PSP.
Sensitive payment data	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 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, etc.
Third-party service provider (TP)	Service providers offering internet-based account information services and/or payment initiation services for payment accounts for which they are not the account servicing PSP are qualified as third-party service providers (TPs). The report focuses on the legal entity offering the account information services and/or payment initiation services and which enters into an agreement with the account owner. Outsourcing agreements are considered to be under the outsourcer's responsibility and are therefore not covered in this report. Both licensed PSPs and non-licensed service providers can offer services as a TP.

1) Basel Committee on Banking Supervision (2005), *Outsourcing in Financial Services*, February.

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
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 Services 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

Address: Kaiserstrasse 29, 60311 Frankfurt am Main, Germany

Postal address: Postfach 16 03 19, 60066 Frankfurt am Main, Germany

Telephone: +49 69 1344 0; Website: http://www.ecb.europa.eu; Fax: +49 69 1344 6000

ISSN 978-92-899-0865-8 (online)
EU catalogue number QB-30-13-187-EN-N (online)