EUROPEAN CENTRAL BANK

EUROSYSTEM

FINAL RECOMMENDATIONS FOR THE SECURITY OF PAYMENT ACCOUNT ACCESS SERVICES FOLLOWING THE PUBLIC CONSULTATION

NOTE: The final text of these Recommendations (Final Recommendations for the security of payment account access services following the public consultation) was not prepared in view of publication, but rather in view of transmission to the European Banking Authority (EBA). The decision not to publish the final text was taken given the ongoing revision of the Payment Services Directive (PSD), the current lack of supervisory competence over providers of payment account access services and the related proposal to introduce a licensing requirement for these providers in the revised PSD, as well as the proposed mandate for the EBA included in the revised PSD to develop (in collaboration with the ECB) guidelines on security measures encompassing also payment account access services.

The ECB has decided to make this document public following a public access request. This is without prejudice to the fact that the Recommendations remain addressed to the EBA for their drafting of guidelines on security measures. In the meantime, any implementation of these Recommendations would neither be expected nor enforced by the authorities that are members of the European Forum on the Security of Retail Payments.

TABLE OF CONTENTS

1 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 (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 EU/EEA-wide harmonised level of security in this field. The authorities participating in the work of the Forum are listed in the annex.

The report complements the recommendations for the security of internet payments ("internet payments recommendations") that were published in 2012 and excluded so-called payment account access services, in which a third-party provider (TPP) accesses the payment account of a customer making a purchase on the internet or provides information from one or several accounts with one or several account-servicing PSPs. Given the distinctive features of payment account access services, the Forum decided to address them separately.

The report outlines 14 recommendations and further specifies them with key considerations (KCs). The report also includes some best practices (BPs) which TPPs, governance authorities (GAs), account-servicing PSPs and other relevant 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.

1.1 PAYMENT ACCOUNT ACCESS SERVICES

For the purpose of this report, payment service providers that issue payment accounts to their payment service users – "account owners" – are referred to as "account-servicing PSPs" (AS PSPs). With respect to account-servicing PSPs, the Forum only outlined such aspects where the requirements of internet recommendations would need to be complemented in view of payment account access services. Therefore, it is envisaged that account-servicing PSPs will have to comply with both reports and for those providers the former exclusion of such services from the scope of the internet payments recommendations should no longer prevail.

"Third-party service providers" (TPPs) provide "payment account access services" for payment accounts for which they are not the account-servicing PSP.[1] In the proposed Payment Services Directive, it is envisaged that all account owners may decide to use such services.

Third-party providers offer so-called payment initiation services or account information services to payment service users, often without entering into the possession of the funds to be transferred.

- Account information services (AIS) provide the account owner (payment service user) with information on one or several accounts held with one or several account-servicing PSPs and present that information to the account owner in a consolidated way.
- Payment initiation services (PIS) facilitate the initiation of payment transactions, at the customer's request, via the account owner's payment account held at another payment service provider, for example via a connection to the customer's online banking platform or by issuing a payment instrument. The implementation of this service can differ depending on whether or not a payee uses the service and subsequently is actively involved in the process of preparing the payment initiation (e.g. a web merchant during online shopping supplying the relevant payment data to the TPP) and how the authentication of the account owner is transmitted to the account-servicing PSP.

TPPs may also provide both payment initiation and account information services. The services may be offered as proprietary solutions by individual TPPs or the services are organised in the form of a payment scheme, with one or more TPPs – and usually also several account-servicing PSPs – as participants, and with a governance authority (GA)[2]. The recommendations cover both models.

From a European perspective, payment account access services 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 and risks of payment account access services are linked to the involvement of at least one additional entity, the TPP, implying additional communication sessions/redirections and possibly greater complexity in the

[1] Where similar services are offered by an account-servicing PSP only for payment accounts issued to its own customers, the account-servicing PSP does not qualify as a third party and thus does not fall within the scope of this report, but falls within the scope of the internet payments recommendations. An account owner using software installed on its device, without a TPP providing payment account access services, does not fall within scope of this report either.

[2] 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.

operations and in solving problems (e.g. late, defective or non-execution, unauthorised payment transactions, fraud) and when allocating (final) liability. Furthermore, depending on their implementation, payment account access services might make the traceability of payment- or payment account-related processes more difficult for account-servicing PSPs and/or account owners, or might affect account-servicing PSPs' security measures and customer education efforts.

1.2 SCOPE AND ADDRESSEES

Unless stated otherwise, the recommendations specified in this report would be applicable to all TPPs providing payment account access services, irrespective of the device used. Certain recommendations, where indicated, would also apply to GAs of payment schemes and/or to account-servicing PSPs.

Excluded from the scope of the report are:

- similar services provided by an account-servicing PSP to its account owners without the involvement of a third-party service provider; [3]
- 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 which are not payment account access services;[4]
- digital or mobile wallets (except when being used for payment account access services);
- payment transactions made by an enterprise via dedicated networks;
- (retail) payment clearing and settlement systems.

1.3 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 conditions are met:

- TPPs should have security and control measures in place ensuring a high level of security, similar to the level required for PSPs and GAs of payment schemes by the internet payments recommendations, and thereby protect the security of the customer's payment account and related data.

[3] These services are covered by the internet payments recommendations.

[4] Specific recommendations applying to mobile payments, as well as to the release and maintenance of software applications for other types of payments, are the subject of a separate work stream.

- There should be sufficient transparency for customers (account owners and payees) enabling them to make an informed choice before and during the use of payment account access services.
- There should be traceability of all transactions and process flows; proper authentication is needed in all communications between the entities involved (i.e. the TPP, the account-servicing PSP, the merchant/payee) also to prove which entity was responsible for which part of the process in the event of repudiation, operational problems, security incidents and/or fraud.
- There should be sufficient exchange of information between the entities involved in the event of repudiation, operational problems, security incidents and/or fraud.
- There should be no sharing of credentials between the TPPs and the account-servicing PSP; the TPP should either redirect the payer in a secure manner to its account-servicing payment service provider or issue its own credentials. Both options should form part of a standardised European interface for payment account access that needs to be developed.
- The duration of payment account access should be minimised, thus reducing the risk of misuse of those data elements. Moreover, TPPs should only access the customer data needed for providing the payment account access service and should not store sensitive payment data apart from reference information, and not use any data for other purposes than explicitly requested by the payment service user.
- TPPs and GAs, when providing services to e-merchants, should ensure, e.g. through technical restrictions or by contractual provisions, that merchants comply with the necessary security requirements.

These recommendations are formulated as generically as possible to accommodate continual business and technological innovation. However, the Forum is aware that new threats can arise at any time, which may justify a review 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. Neither does the report redefine, or suggest amendments to, the authorities' expectations in the areas of data protection, anti-money laundering (AML) and business continuity. 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 are without prejudice to the responsibility of TPPs, GAs, account-servicing PSPs and other market participants to monitor and assess the specific risks involved in their service 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 recommendations do not target, support or oppose any specific individual service or their providers. It is expected that the European Banking Authority (EBA), once issuing guidelines, will align these recommendations with other regulations and/or decisions that authorities may by then have taken on payment account access services. The recommendations should not be interpreted as a warning against established TPPs in Europe. TPPs fill a gap by providing efficient and customer-convenient e-commerce services. The Forum has suggested that a secure European standard/interface for payment account access should be established and should allow any TPP to access payment accounts at any PSP throughout the EU. This standard could be defined by the EBA in close cooperation with the ECB and include technical and functional specifications, as well as related procedures. Standardisation is a normal part of European market integration and further developments should allow the industry to rely on a secure common standard that allows strong customer authentication without any sharing of the AS PSP's credentials between the AS PSP and the TPP. This would reduce technical workload for TPPs, foster innovation and at the same time ensure trust in safe and efficient payment services.

2 RECOMMENDATIONS

2.1 GENERAL CONTROL AND SECURITY ENVIRONMENT

Recommendation 1: Governance

TPPs 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 KC 2.4) 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.

Recommendation 2: Risk assessment

TPPs 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 TPPs and GAs 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 that may result from the TPP's own organisation, procedures and systems. The assessment should consider e.g. risk concentrations as well as possible threats to the confidentiality, integrity, authenticity and availability of the account-servicing PSP's data/systems.

2.2 KC TPPs 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. TPPs and GAs should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines on their side,[5] the side of the account-servicing PSP and the side of their customers,[6] as well as the results of the security incident monitoring process (see Recommendation 3).

2.3 KC On this basis, TPPs 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. TPPs 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.

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

2.5 KC TPPs 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

TPPs, GAs and account-servicing PSPs should ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints. TPPs and GAs should establish a procedure for reporting such incidents to management, to concerned account-servicing PSPs and, in the event of major security incidents,[7] to the competent authorities.

3.1 KC TPPs 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.

[5] Such as the susceptibility of the system to payment session hijacking, SQL injection, cross-site scripting, buffer overflows, etc.

[6] Such as risks associated with using multimedia applications, browser plug-ins, frames, external links, etc.

[7] A "major security incident" is an incident which has or may have a material impact on the security, integrity or continuity of the TPP'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 TPPs, PSPs or other payment infrastructures.

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

3.3 KC TPPs, GAs and account-servicing PSPs should have a procedure for cooperating with the relevant law enforcement agencies on major security incidents, including data breaches, and in any follow-up action.

3.4 KC TPPs should inform the account-servicing PSP immediately about (suspected) fraudulent payments and/or attempts of fraud affecting a customer of that account-servicing PSP.

3.5 KC Account-servicing PSPs should inform the TPP immediately about (suspected) fraudulent payments and/or attempts of fraud affecting a customer of that TPP.

3.6 KC TPPs, when providing services to e-merchants, should require, e.g. by contractual provisions, e-merchants to cooperate on major security incidents, including data breaches, both with them and the relevant law enforcement agencies. If a TPP 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.

Recommendation 4: Risk control and mitigation

TPPs and GAs should implement proportionate security measures in line with their respective security policies in order to mitigate identified risks. These measures should incorporate multiple layers of security defences, whereby the failure of one line of defence is mitigated by the next line of defence ("defence in depth"). Account-servicing PSPs should provide a dedicated interface for payment account access services.

4.1 KC Based on their risk assessment, TPPs and GAs should have appropriate security and control measures in place in order not to diminish the IT security of the account-servicing PSP.

4.2 KC In designing, developing and maintaining payment account access services, TPPs 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[8] and "need to know" principle[9] as the

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

basis for a sound identity and access management and should ensure that data minimisation[10] is an essential component of the core functionality.[11] See KC 11.5 for the storing of data when operating payment account access services.

4.3 KC TPPs and GAs should have appropriate security solutions in place to protect networks, websites, servers and communication links against abuse or attacks. TPPs 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, in line with KC 4.2. In order to restrict the use of "fake" websites (imitating legitimate TPP sites), websites offering payment account access services should be identified by extended validation certificates drawn up in the TPP's name or by other similar authentication methods.

4.4 KC TPPs 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. TPPs should create, store and regularly analyse appropriate logs and audit trails.

4.5 KC TPPs' and GAs' security measures for payment account access services should be tested 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.

4.6 KC The TPP'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.

[9] Access to information should only be given if that information is necessary for the conduct of one's work.

[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".

4.7 KC Whenever TPPs 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.

4.8 KC TPPs and GAs, when providing services to e-merchants, should ensure, e.g. through technical restrictions or by contractual provisions, that e-merchants do not handle (i.e. store, process or transmit) credentials in relation to the payment account access service.

4.9 KC Account-servicing PSPs should provide a dedicated interface to ensure data access minimisation.

4.1 BP TPPs 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).

Recommendation 5: Traceability

TPPs, GAs and account-servicing PSPs should have processes in place ensuring that all transactions, as well as the payment account access process flow, are appropriately traced.

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

5.2 KC [PIS] TPPs should implement log files allowing to trace that the payment order was sent to the account-servicing PSP, that a notification of successful delivery was received by the TPP together with the information on (non-)availability of funds, and that a secure connection to the account-servicing PSP was established and maintained.

5.3 KC Where TPPs have issued their own personalised security features to their customers, TPPs should implement log files allowing to trace that the customer has been authenticated based on the personalised security features issued by the TPP.

5.4 KC TPPs 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.

5.5 KC Account-servicing PSPs should be able to differentiate in their log files between payment account access by TPPs and access by account owners without TPP involvement.

5.6 KC TPPs and account-servicing PSPs should ensure mutual authentication when communicating in the context of providing payment account access services (e.g. through agreed technical arrangements or the adoption of a suitable standard protocol). This also applies to TPPs when communicating with e-merchants accordingly.

2.2 SPECIFIC CONTROL AND SECURITY MEASURES FOR PAYMENT ACCOUNT ACCESS SERVICES

Recommendation 6: Initial customer identification and information

All customers should confirm to the TPP their willingness to make use of payment account access services before being granted access to such services. Merchants should be properly identified by the TPP. The account owner should also be properly identified by the TPP, unless the TPP relies on the account-servicing PSP to apply its own authentication methods, i.e. following a redirection of the account owner to the account-servicing PSP's website. TPPs 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 TPPs should ensure that the merchant has undergone due diligence procedures before being granted access to payment account access services.

6.2 KC TPPs which use their own authentication methods should ensure that the account owner has undergone the customer due diligence procedures, and has provided adequate identity documents and related information before being granted access to payment account access services.

6.3 KC TPPs should ensure that the prior information supplied to the customer contains specific details relating to the payment account access services. These should include, as appropriate:

- 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 delivered by the TPP;

- 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 TPP and the customer respectively with regard to the use of payment account access services;
- the procedure to follow to terminate the services.

6.4 KC TPPs should ensure that the contract with the customer specifies that the TPP may block the initiation of a specific transaction and/or the payment account access services 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 TPP to have the payment account access service “unblocked”.

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

6.6 KC For TPPs offering different types of payment account access services, the account owner should be required to actively opt for each of the services separately, for each payment account, instead of being automatically granted access to all types of payment account access services offered by the TPP.

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

Recommendation 7: Strong customer authentication

TPPs should ensure that the initiation of payments as well as access to sensitive payment data is protected by strong customer authentication.[12]

7.1 KC TPPs should ensure that customers are appropriately authenticated by relying on strong customer authentication for the initiation of a payment transaction or access to account information either by redirecting the payment service user in a secure manner to its account-servicing PSP or by issuing its own credentials. The TPP should not be allowed to obtain access to the payment service user's credentials issued by the account-servicing PSP.

7.2 KC TPPs which use their own authentication methods should have a procedure in place for the use of strong customer authentication and protect their respective credentials.

7.3 KC [AIS] Where a TPP offers only account information services with no display of sensitive payment data, the TPP may adapt its authentication requirements on the basis of its risk assessment.

7.1 BP Strong customer authentication for the initiation of a payment transaction could include elements linking the authentication to the amount and the payee. This could provide all 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: Registration of the customer, enrolment for and provision of authentication tools and/or software delivered to the customer

TPPs requiring registration by the account owner for payment account access services[13] and that provide authentication tools and/or payment account access-related software should ensure that customer registration, enrolment for and the initial provision of the authentication tools and/or

[12] 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.

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

the delivery of the software required to use the payment account access service are carried out in a secure manner.

8.1 KC Initial registration, enrolment 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[14], while taking into account possible risks arising from devices that are not under the TPP'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 TPP to allow the customer to verify its authenticity and that it has not been tampered with.

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

The TPP should define rules for payment account access session "time out" between itself and the customer and follow the account-servicing PSP's rules between itself and the account-servicing PSP. If the TPP requires the customer to log in separately based on a registration with the TPP, the TPP should limit the number of log-in or authentication attempts and set time limits for the validity of authentication.

9.1 KC When TPPs use a one-time password as part of their own customer authentication method, they should ensure that the validity period of such passwords is limited to the strict minimum necessary.

9.2 KC TPPs using their own authentication method should 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 reactivate blocked payment account access services.

9.3 KC TPPs should set down the maximum period after which inactive payment account access sessions are automatically terminated. In general, the TPP should keep the internet sessions between itself and its customer and between itself and the account-

[14] Environments where adequate authentication of the customer and of the TPP offering the service and the protection of confidential/sensitive information is assured include: (i) the TPP's premises; (ii) a secure website under the responsibility of the TPP 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.)

servicing PSP as short as possible and actively log out as soon as the requested action has been completed.

9.4 KC [AIS] A TPP should only access the designated payment account(s) upon customer order.

9.5 KC [PIS] A TPP should only access the designated payment account upon customer order given payment by payment.

9.6. KC Account-servicing PSPs need to ensure 24/7 technical availability to respond to the TPPs' requests for the authentication of the customer. Maximum response times for the authentication should be defined by the EBA.

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 by the TPP before the TPP initiates payments and/or attempts to access sensitive payment data; suspicious or high-risk processes and transactions should be subject to a specific screening and evaluation procedure.

10.1 KC TPPs should use fraud detection and prevention systems to identify suspicious processes and transactions before the TPP initiates payments 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 the Internet Protocol (IP) address[15] or IP range during the payment account access session, sometimes identified by geo-location IP checks,[16] 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 legislation, should be commensurate with the outcome of the risk assessment.

10.2 KC TPPs, when providing services to e-merchants, should have fraud detection and prevention systems in place to monitor e-merchant activities.

[15] An IP address is a unique numeric code identifying each computer connected to the internet.

[16] A "Geo-IP" check verifies whether the issuing country corresponds with the IP address from which the user is initiating the transaction.

10.3 KC TPPs 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 TPP, 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 TPP 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, TPPs and account-servicing PSPs) should 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 payments), as well as the customer interface (i.e. the TPP or e-merchant website), should be appropriately secured against theft and unauthorised access or modification.

11.2 KC TPPs and GAs should ensure that when exchanging sensitive payment data via the internet, secure end-to-end encryption[17] is applied between the communicating parties for each communication session, in order to safeguard the confidentiality and integrity of the data, using strong and widely recognised encryption techniques. Redirections 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 TPP's control.

11.3 KC TPPs, when providing services to e-merchants, should not make any sensitive payment data available to e-merchants. TPPs should not allow, e.g. by contractual provisions, their e-merchants to store credentials in relation to payment account access services.

11.4 KC TPPs should only access designated payment accounts upon the account owner's specific order. The purpose of payment account access should be clearly determined

[17] 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).

and agreed between the TPP and the customer prior to any attempt to access the payment account and the TPP should limit its involvement to the extent necessary to achieve this purpose (“proportionality principle”). TPPs should not, unless explicitly solicited by the customer as part of account information services, access the account owner’s other accounts, such as savings or securities accounts.

11.5 KC TPPs should not store sensitive payment data of the payment service user obtained when accessing the payment service user’s payment account, apart from (i) information for identifying a payment initiated by the TPP such as the reference number, payer’s and payee’s IBAN, the transaction amount, other reference information and the settlement system information, and (ii) information about credentials they issued themselves. TPPs shall ensure that the data are appropriately protected against theft and unauthorised access or modification.

11.6 KC TPPs 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 staff in this respect and update this training regularly to ensure that the content remains relevant to a dynamic security environment.

3 CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION

Recommendation 12: Customer education and communication

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

12.1 KC TPPs should provide at least one secured channel[18] for ongoing communication with customers regarding the correct and secure use of the payment account access services. TPPs should inform customers about this channel and explain that any message on behalf of the TPP 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 TPP should explain:

- the procedure for customers to report to the TPP and the necessity to report to their account-servicing PSP (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[19] attempts;
- the next steps, i.e. how the TPP will respond to the customer;
- how the TPP 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 TPPs 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 TPPs 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 TPPs and GAs should initiate customer education and awareness programmes designed to ensure customers understand, at a minimum, the need:

[18] Such as a dedicated mailbox on the TPP's website or a secured website.

[19] 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.

- 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 redirection is either to the genuine website of the TPP or of the account-servicing PSP.

12.5 KC TPPs, when providing services to e-merchants, should require, e.g. by contractual provisions, 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 TPP and/or the account-servicing PSP and not the payee (e.g. by redirecting 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 TPPs should ensure that their liability regime is transparent to customers (e.g. in the framework contract and/or the terms and conditions).

12.7 KC TPPs should not interfere in any communication between the account-servicing PSP and the account owner on security-related messages, such as phishing alerts. For example, TPPs should not mark security-related messages as read without having ensured that the account owner has acknowledged having taken note of them.

12.8 KC TPPs should inform customers at each payment account access session 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 TPP of sensitive payment data, e.g. data routing, processing, storing and/or archiving, in the contract or terms and conditions for payment account access services entered into with the TPP. The TPP should clearly list each data element in the contract or terms and conditions.

12.1 BP It is desirable that TPPs, when providing services to e-merchants, arrange educational programmes for their e-merchants on fraud prevention.

Recommendation 13: Notifications, setting of limits

TPPs 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, TPPs 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 TPP 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, TPPs could provide their registered customers with the facility to manage limits for payment initiation services in a safe and trusted environment.

13.2 BP TPPs 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 TPPs 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

TPPs should provide immediately a confirmation to their customers of the successful initiation of the payment order with the payer's account-servicing PSP, together with information to check the correctness of the payment transaction.

14.1 KC TPPs 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[20] should be made available in a safe and trusted environment. Where TPPs inform customers about the availability of electronic

[20] The electronic statement includes a history of (payment initiation) transactions and/or aggregated account information.

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 TPPs could include in the payment initiation confirmation, in addition to the e-merchant's reference and/or the information provided by the customer, their brand names (as known to the customer) and/or help desk details.

4 GLOSSARY OF TERMS

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

Term	Definition and supporting information
Account information services	Services that collect information on different (payment) accounts held by one account owner with one or several account-servicing PSPs and present the consolidated information to the account owner in a user-friendly way.
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 account access services, the term “account owner” refers to the payer and also includes other 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.[21] Therefore, outsourcing agreements are not specifically addressed here, but are considered to be under the account-servicing PSP’s responsibility for the purpose of this report.
Authentication	A procedure that allows the verification of identity.
Credentials	The personal and confidential information provided for the purposes of authentication, i.e. personalised security features. 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).
Governance authority (of a payment scheme)	The entity accountable for the overall functioning of the scheme that promotes the payment instrument in question and 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*.
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 account access services	Account information services, payment initiation services or other services based on access to payment accounts.

[21] Source: Basel Committee on Banking Supervision (2005), *Outsourcing in Financial Services*, February.

Payment initiation services	Services to initiate payment transactions via the account owner's payment account. The implementation of this service can differ based on whether or not a payee uses the service and is actively involved in the process of preparing the payment initiation and whether or not, for the purpose of authentication, the account owner transmits his/her personalised security features to the account-servicing PSP via the TPP.
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, 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 (TPP)	Service providers offering payment account access services for payment accounts for which they are not the account-servicing PSP. The report focuses on the legal entity which offers the payment account access services and enters into an agreement with the account owner and, where applicable, the merchant/payee. Currently, both PSPs and non-licensed service providers act as a TPP. Technical service providers which support the provision of payment services are a different category and are not meant here. Providers of (free) software which do not enter into an agreement with the account owner and, where applicable, the merchant/payee are also not meant here.

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

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