MFSA

MALTA FINANCIAL SERVICES AUTHORITY

BANKING SUPERVISION UNIT

FINANCIAL INSTITUTIONS RULES

SECURITY OF INTERNET PAYMENTS OF CREDIT, PAYMENT AND ELECTRONIC MONEY INSTITUTIONS

Ref: FIR/04/2015

SECURITY OF INTERNET PAYMENTS OF CREDIT, PAYMENT AND ELECTRONIC MONEY INSTITUTIONS

INTRODUCTION

1. In terms of Article 13(2) of the Financial Institutions Act 1994 (the "Act") the competent authority (the "authority"), as appointed under Article 2(1) of the Act, may make Financial Institutions Rules as may be required for carrying into effect any of the provisions of this Act. The authority may also amend or revoke such Financial Institutions Rules. The Financial Institutions Rules and any amendment or revocation thereof shall be officially communicated to financial institutions and the authority shall make copies thereof available to the public.

2. In terms of Article 5(4)(b) of the Act, for the better carrying out of the provisions of this Act and to better transpose the provisions of the Electronic Money Directive (Directive 2009/110/EC) and the Payment Services Directive (Directive 2007/64/EC) as defined in the Act, the authority may, from time to time, issue and publish Rules which shall be binding on licence holders and others as may be specified therein. Such Rules may lay down additional requirements and conditions in relation to activities of licence holders, the conduct of their business, their relations with customers, the public and other parties, their responsibilities to the authority, reporting requirements and any other matters as the authority may consider appropriate.

SCOPE

3. The scope of this Rule (the "Rule") is to adopt the provisions prescribed in the Guidelines on the security of internet payments, issued by the EBA on the 19th of December 2014 (the "Guidelines"). The Guidelines establish a set of minimum requirements in the field of the security of internet payments and build on the rules of the Payment Services Directive (the "PSD") concerning information requirements for payment services and obligations of payment service providers ("PSPs") in relation to the provision of payment services, which locally, have been transposed in Directive No. 1 of the Central Bank of Malta on the Provision and Use of Payment Services. Furthermore, in accordance with article 5(1)(d) of the Act [Article 10(4) of the PSD], payment institutions are also required to, *inter alia*, have in place robust governance arrangements and adequate internal control mechanisms.

4. Notwithstanding the provisions of the Act and of the Banking Act (Chapter 371 of the Laws of Malta) and any rules issued thereunder, this Rule applies to the provision of internet payment services by all categories of PSPs as defined in point (r) of paragraph 7:

   Provided that where payment integrators offering payment initiation services are external technical service providers of PSPs, these PSPs shall contractually require such payment integrators to comply with the provisions of this Rule:

Provided further that the Recommendations for the security of internet payments, issued by the European Central Bank in January 2013, shall also be applicable for the purposes of the oversight function exercised by the Central Bank .

5. This Rule is without prejudice to the obligation of PSPs to monitor and assess the risks involved in their payment operations, develop their own detailed security policies and implement adequate security, contingency, incident management and business continuity measures that are commensurate with the risks inherent in the payment services provided.

6. This Rule shall not apply to:

   a) Internet payment services other than those listed in point (l) of paragraph 7 (such as e-brokerage and online contracts);

   b) Payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology;

   c) Mobile payments other than browser-based payments;

   d) Credit transfers where a third party accesses the customer's payment account;

   e) Payment transactions made by an enterprise via dedicated networks;

   f) Card payments using anonymous and non-rechargeable physical or virtual prepaid cards where there is no ongoing relationship between the issuer and the cardholder; and

   g) Clearing and settlement of payment transactions.

DEFINITIONS

7. For the purposes of this Rule, the following definitions shall apply:

   a) "authentication" means a procedure that allows the PSP to verify a customer's identity;

   b) "authorisation" means a procedure that checks whether a customer or PSP has the right to perform a certain action, such as the right to transfer funds, or to have access to sensitive data;

   c) "card scheme" means a technical and commercial arrangement set up to serve one or more brands of card which provides the organisational, legal and operational framework necessary for the functioning of the services marketed by those brands;

   d) "CBM Directive" means Directive No. 1 of the Central Bank of Malta on the Provision and use of Payment Services;

   e) "Central Bank" means the Central Bank of Malta as defined by the Central Bank of Malta Act (Chapter 204 of the Laws of Malta);

   f) "credentials" means:

i) the information, generally confidential, provided by a customer or PSP for the purposes of authentication;

ii) the possession of a physical tool containing the information (such as a one-time password generator or smart card); or

iii) something the user memorises or represents (such as biometric characteristics);

g) "data minimisation" shall refer to a data protection principle which requires that the collection and processing of personal information should be limited to the minimum necessary to achieve a specific purpose;

h) "end-to-end encryption" means encryption within or at the source end system, with the corresponding decryption occurring only within or at the destination end system;

i) "European Central Bank" means the European Central Bank established in accordance with Article 13 of the Treaty on European Union;

j) "governance authority" shall refer to an entity which is accountable for the overall functioning of the card scheme that promotes the payment instrument in question and ensures that all the actors involved comply with the card scheme's rules and that the card scheme is compliant with oversight standards;

k) "Information and Data Protection Commissioner" means the Information and Data Protection Commissioner appointed in terms of the Data Protection Act (Chapter 440 of the Laws of Malta);

l) "internet payment services" shall refer to the following payment services, irrespective of the access device used:

i) the execution of card payments on the internet, including virtual card payments, as well as the registration of card payment data for use in "wallet solutions";

ii) the execution of credit transfers on the internet;

iii) the issuance and amendment of direct debit electronic mandate; and

iv) transfers of electronic money between two e-money accounts via the internet;

m) "Internet Protocol address" shall refer to a unique numeric code identifying each computer connected to the internet;

n) "'least privilege' principle" means the principle in according to which every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job;

o) "major payment security incident" means an incident which has, or may have, a material impact on the security, integrity or continuity of the PSP's payment-related systems and/or the security of sensitive payment data or funds:

Provided that the assessment of materiality shall consider the number of potentially affected customers, the amount at risk and the impact on other PSPs or other payment infrastructures;

p) "outsourcing service provider" means the supplier of goods, services or facilities, which may or may not be a licensed entity, and which may be an affiliated entity within a corporate group or an entity that is external to the group;

q) "payment integrators offering payment initiation services" means acquirers of internet payment services which provide the payee with a standardised interface to payment initiation services provided by PSPs;

r) "payment service providers" or "PSPs" means:

   i) credit institutions licensed in terms of the Banking Act;

   ii) payment institutions licensed in terms of the Act in order to undertake Activity 4 in the first Schedule to the Act; and

   iii) electronic money institutions licensed in terms of the Act in order to undertake Activity 10 in the first Schedule to the Act.

s) "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

t) "safe and trusted environment" means an environment under the PSP's responsibility where adequate authentication of the customer and of the PSP offering the service and the protection of confidential or sensitive information is assured, including the PSPs premises, internet banking or other secure website (for example where the governance authority offers comparable security features inter alia as defined in paragraphs 23 to 31) or automated teller machine services;

u) "sensitive payment data" means data which could be used to carry out fraud, including:

   (i) data enabling a payment order to be initiated;

   (ii) data used for authentication;

   (iii) data used for ordering payment instruments or authentication tools to be sent to customers; and

   (iv) 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-identified limits, etc.;

v) "social engineering" means techniques of manipulating people to obtain information, for example 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;

w) "strong customer authentication" means a procedure designed in such a way as to protect the confidentiality of the authentication data and which is based on the use of two or more of the following elements:

i) knowledge - something only the user knows, such as a static password, code or personal identification number;

ii) ownership - something only the user possesses, such as a token, smart card or mobile phone;

iii) inherence - something the user is, such as a biometric characteristic, for instance a fingerprint;

Provided that:

i) the selected elements are mutually independent and the breach of one does not compromise the other(s);

ii) at least one of the elements is non-reusable, non-replicable (except for inherence) and not capable of being surreptitiously stolen via the internet;

x) "transaction risk analysis" means the evaluation of the risk related to a specific transaction, taking into account criteria such as, for example, customer payment patterns (behaviour), value of the related transaction, type of product and payee profile;

y) "virtual card" means a card-based payment solution where an alternative, temporary card number with a reduced validity period, limited usage and a pre-defined spending limit is generated which can be used for internet purchases;

z) "wallet solutions" means solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several e-merchants.

GENERAL CONTROL AND SECURITY ENVIRONMENT

Governance

8. PSPs shall implement and regularly review a formal security policy for internet payment services.

9. The security policy shall be properly documented, regularly reviewed in accordance with paragraph 15 and approved by senior management. It shall define security objectives and the risk appetite.

10. The security policy shall define roles and responsibilities (including the risk management function with a direct reporting line to the Board of Directors) and the reporting lines for the internet payment services provided (including management of sensitive payment data with regard to the risk assessment, control and mitigation).

Risk Assessment

11. PSPs shall carry out and document thorough risk assessments, with regard to the security of internet payments and related services, both prior to establishing the service(s) and regularly thereafter, at least on a yearly basis.

12. PSPs, through their risk management function, shall carry out and document detailed risk assessments for internet payments and related services. PSPs should consider the results of the ongoing monitoring of security threats relating to the internet payment services they offer or plan to offer, taking into account:

    a) the technology solutions used by them;

    b) services outsourced to external providers; and

    c) the customers' technical environment.

    PSPs should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines both on their side[1] and the side of their customers[2], as well as the results of the security incident monitoring process outlined in paragraphs 16 to 22.

13. PSPs should, on the basis of paragraph 12, determine whether and to what extent changes may be necessary to the existing security measures, the technologies used and the procedures or services offered. PSPs shall 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.

14. The assessment of risks shall address the need to protect and secure sensitive payment data.

15. PSPs shall 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 shall be carried out at least once a year. The results of the risk assessments and reviews shall be submitted to senior management for approval.

Incident Monitoring and Reporting

16. PSPs shall ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints. PSPs shall establish a procedure for reporting such incidents to management and, in the event of major payment security incidents, the authority and the Central Bank.

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

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

17. PSPs shall 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.

18. PSPs shall have a procedure for notifying immediately the authority and the Central Bank in the event of major payment security incidents with regard to the payment services provided.

19. PSPs shall have a procedure for cooperating on major payment security incidents with the authority, the Central Bank and the relevant law enforcement agencies.

20. PSPs offering acquiring services shall contractually require e-merchants that store, process or transmit sensitive payment data to cooperate on major payment security incidents with the PSPs providing them with the acquiring service, with the authority, with the Central Bank and with the relevant law enforcement agencies. If a PSP becomes aware that an e-merchant is not cooperating as required under the contract, it shall take steps to enforce this contractual obligation, or terminate the contract.

21. In the event of a security incident leading to a personal data breach, PSPs shall notify the Information and Data Protection Commissioner immediately upon becoming aware that such incident took place. The procedure for such notification, including specific time frames and modalities for submitting a personal data breach notification, shall be established in accordance with the data protection legal framework applicable at the time when such notification is submitted. For these purposes, the Information and Data Protection Commissioner may also issue guidelines in accordance with his functions and powers at law.

22. In the absence of specific legal provisions or guidelines regulating the notification of personal data breaches, PSPs may establish their own internal practices for submitting such notification, provided that these practices furnish the Information and Data Protection Commissioner with all meaningful information, being technical or otherwise, which is collected following the detection of the personal data breach.

Risk Control and Mitigation

23. PSPs shall implement security measures in line with their respective security policies in order to mitigate identified risks. These measures shall 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').

24. In designing, developing and maintaining internet payment services, PSPs shall pay special attention to the adequate segregation of duties in information technology (IT) environments (such as the development, test and production

environments) and the proper implementation of the 'least privilege' principle as the basis for a sound identity and access management.

25. PSPs shall have appropriate security solutions in place to protect networks, websites, servers and communication links against abuse or attacks. PSPs shall 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 shall be kept to a strict minimum following the 'least privilege' principle. In order to restrict the use of 'fake' websites (imitating legitimate PSP sites), transactional websites offering internet payment services shall be identified by extended validation certificates drawn up in the PSP's name or by other similar authentication methods.

26. PSPs shall have appropriate processes in place to monitor, track and restrict access to:

    a) sensitive payment data; and

    b) logical and physical critical resources, such as networks, systems, databases, security modules, etc.

    PSPs shall create, store and analyse appropriate logs and audit trails.

27. In designing, developing and maintaining internet payment services, PSPs shall ensure that data minimisation is an essential component of the core functionality: the gathering, routing, processing, storing and/or archiving, and visualisation of sensitive payment data shall be kept at the absolute minimum level.

28. Security measures for internet payment services shall be tested under the supervision of the risk management function to ensure their robustness and effectiveness. All changes shall 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 shall be repeated regularly in accordance with the PSP's risk profile and at least on an annual basis, and shall include scenarios of relevant and known potential attacks.

29. The PSP's security measures for internet payment services shall be periodically audited to ensure their robustness and effectiveness. The implementation and functioning of the internet payment services shall also be audited. The frequency and focus of such audits shall take into consideration, and be in proportion to, the security risks involved. Trusted and independent (internal or external) experts shall carry out the audits. Such experts shall not be involved in any way in the development, implementation or operational management of the internet payment services provided.

30. Without prejudice to the provisions of Article 19A of the Banking Act and of Article 8B of the Act, whenever PSPs outsource functions related to the security of the internet payment services, PSPs shall contractually require

outsourcing service providers to comply with the provisions of this Rule and with those found in Banking Rule BR/14.

31. PSPs offering acquiring services shall contractually require e-merchants handling (that is storing, processing or transmitting) sensitive payment data to implement security measures in their IT infrastructure in accordance with paragraphs 24 to 30, in order to avoid the theft of such sensitive payment data through their systems. If a PSP becomes aware that an e-merchant does not have the required security measures in place, it shall take steps to enforce this contractual obligation, or terminate the contract.

Traceability

32. PSPs shall have processes in place ensuring that all transactions, as well as the e-mandate process flow, are appropriately traced.

33. PSPs shall ensure that their service incorporates security mechanisms for the detailed logging of transaction and e-mandate data, including the transaction sequential number, timestamps for transaction data, parameterisation changes as well as access to transaction and e-mandate data.

34. PSPs shall implement log files allowing any addition, change or deletion of transaction and e-mandate data to be traced.

35. PSPs shall query and analyse the transaction and e-mandate data and ensure that they have tools to evaluate the log files. The respective applications shall only be available to authorised personnel.

SPECIFIC CONTROL AND SECURITY MEASURES FOR INTERNET PAYMENTS

Initial Customer Identification and Information

36. PSPs shall, before granting customers access to internet payment services, properly identify customers in line with:

    (a) the Prevention of Money Laundering and Funding of Terrorism Regulations (Legal Notice 180 of 2008);

    (b) the Implementing Procedures issued by the Financial Intelligence Analysis Unit in terms of the said Regulations; and

    (c) any anti-money laundering legislation in other relevant jurisdictions, as may be applicable;

    and shall confirm the customers' willingness to make internet payments using the services offered by the PSP. PSPs shall provide adequate 'prior', 'regular' or, where applicable, '*ad hoc*' information to the customer about the necessary requirements (such as equipment and procedural requirements) for performing secure internet payment transactions and the inherent risks.

37. PSPs shall ensure that the customer has undergone the customer due diligence procedures and has provided adequate identity documents (such as a passport, national identity card or advanced electronic signature) and related information before being granted access to the internet payment services:

Provided that the customer identification process shall be without prejudice to any exemptions provided in the Prevention of Money Laundering and Funding of Terrorism Regulations (Legal Notice 180 of 2008) and any anti-money laundering legislation in other relevant jurisdictions, as may be applicable.

38. PSPs are not obliged to conduct a separate customer identification process for the internet payment services, provided that such customer identification has already been carried out, for example in relation to other existing payment-related services or to the opening of an account.

39. Without prejudice to paragraph 20 of the CBM Directive [Article 42 of the PSD], which specifies the information that the PSP must provide to the payment service user before entering into a contract for the provision of payment services, PSPs shall ensure that the prior information supplied to the customer contains specific details relating to the internet payment services. Such information shall include, as appropriate:

a) clear information on any requirements in terms of customer equipment, software or other necessary tools (such as antivirus software and firewalls);

b) guidelines for the proper and secure use of personalised security credentials;

c) 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;

d) guidelines for the proper and secure use of all hardware and software provided to the customer;

e) 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;

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

g) a description of the responsibilities and liabilities of the PSP and the customer respectively with regard to the use of the internet payment service.

40. PSPs shall ensure that the framework contract with the customer specifies that the PSP may, in accordance with paragraph 33 of the CBM Directive [Article 55 of the PSD], block a specific transaction or the payment instrument on the basis of security concerns. The framework contract shall set out the method and terms of the customer notification and how the customer can contact the PSP to have the internet payment transaction or service unblocked in accordance with the provisions of the CBM Directive.

Strong Customer Authentication

41. Without prejudice to paragraphs 42, 46 and 48, PSPs shall have a strong customer authentication procedure in place in order to protect the initiation of internet payments, identify abnormal customer payment patterns, prevent fraud and protect access to sensitive payment data.

42. In relation to the internet payment services defined in points (ii), (iii) and (iv) of paragraph 7(l), PSPs shall perform strong customer authentication for the customer's authorisation of internet payment transactions (including bundled credit transfers) and the issuance or amendment of electronic direct debit mandates. However, PSPs may, subject to the prior notification to the authority and the Central Bank, adopt alternative customer authentication measures for:

    a) outgoing payments to trusted beneficiaries included in previously established white lists[3] for that customer;

    b) transactions between two accounts of the same customer held at the same PSP;

    c) transfers within the same PSP justified by a transaction risk analysis;

    d) low-value payments in accordance with paragraphs 12 and 31 of the CBM Directive [Articles 34(1) and 53(1) of the PSD].

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

44. In relation to the internet payment service defined in point (i) of paragraph 7(l), all card issuing PSPs shall, for card transactions, implement a strong authentication procedure of the cardholder. All cards issued must be technically ready (registered) to be used with strong authentication.

45. In relation to the internet payment service defined in point (i) of paragraph 7(l), PSPs offering acquiring services shall implement technologies allowing the issuer to perform strong authentication of the cardholder for the card schemes in which the acquirer participates.

46. In relation to the internet payment service defined in point (i) of paragraph 7(l), PSPs offering acquiring services shall require e-merchants to implement solutions allowing the issuer to perform strong authentication of the cardholder for card transactions via the internet. However, PSPs may, subject to the prior notification to the authority and the Central Bank, use alternative authentication measures for pre-identified categories of low-risk transactions,

[3] A 'white list' is a list of trusted beneficiaries selected by a customer, where the inclusion of trusted beneficiaries in such a white list is confirmed by strong customer authentication.

such as categories identified by means of a transaction risk analysis, or transactions involving low-value payments as referred to in paragraphs 12 and 31 of the CBM Directive.

47. In relation to the internet payment service defined in point (i) of paragraph 7(l), providers of wallet solutions shall, for the card schemes accepted by the service, require strong authentication by the issuer when the legitimate holder first registers the card data.

48. Providers of wallet solutions shall support strong customer authentication when customers log in to the wallet payment services or carry out card transactions via the internet. However, PSPs may, subject to the prior notification to the authority and the Central Bank, use alternative authentication measures for pre-identified categories of low-risk transactions, such as categories identified by means of a transaction risk analysis, or transactions involving low-value payments as referred to in paragraphs 12 and 31 of the CBM Directive.

49. In relation to internet payment services as defined in point (i) of paragraph 7(l), the initial registration for virtual cards shall take place in a safe and trusted environment. If the card is issued in the internet environment, PSPs shall apply strong customer authentication for the virtual card data generation process.

50. PSPs shall ensure proper bilateral authentication when communicating with e-merchants for the purpose of initiating internet payments and accessing sensitive payment data.

Enrolment for, and Provision of, Authentication Tools and/or Software Delivered to the Customer

51. PSPs shall ensure that customer enrolment for and the initial provision of the authentication tools required to use the internet payment service and/or the delivery of payment-related software to customers is carried out in a secure manner.

52. Enrolment for and provision of authentication tools and/or payment-related software delivered to the customer shall fulfil the following requirements:

    a) The related procedures shall be carried out in a safe and trusted environment while taking into account possible risks arising from devices that are not under the PSP's control;

    b) Effective and secure procedures shall be in place for the delivery of personalised security credentials, payment-related software and all internet payment-related personalised devices;

    c) Software delivered via the internet shall be digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with;

d) In relation to the internet payment services defined in point (i) of paragraph 7(l), the customer shall, for card transactions, have the option to register for strong authentication independently of a specific internet purchase. Where activation during online shopping is offered, this shall be done by re-directing the customer to a safe and trusted environment.

53. In relation to the internet payment service defined in point (i) of paragraph 7(l), issuers shall actively encourage cardholder enrolment for strong authentication and allow their cardholders to bypass enrolment only in an exceptional and limited number of cases where justified by the risk related to the specific card transaction.

Log-in Attempts, Session Time Out and Validity of Authentication

54. PSPs shall limit the number of log-in or authentication attempts, define rules for internet payment services session 'time out' and set time limits for the validity of authentication.

55. When using a one-time password for authentication purposes, PSPs shall ensure that the validity period of such passwords is limited to the strict minimum necessary.

56. PSPs shall set down the maximum number of failed log-in or authentication attempts after which access to the internet payment service is (temporarily or permanently) blocked. They shall have a secure procedure in place to re-activate blocked internet payment services.

57. PSPs shall set down the maximum period after which inactive internet payment services sessions are automatically terminated.

Transaction Monitoring

58. PSPs shall, before final authorisation is given, use transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions. Suspicious or high risk transactions shall be subject to a specific screening and evaluation procedure. Equivalent security monitoring and authorisation mechanisms shall also be in place for the issuance of e-mandates.

59. PSPs shall, before finally authorising transactions or e-mandates, use fraud detection and prevention systems to identify suspicious transactions. Such systems shall be based, for example, on parameterised rules (such as black lists of compromised or stolen card data), and shall monitor abnormal behaviour patterns of the customer or the customer's access device (such as a change of Internet Protocol address or Internet Protocol range during the internet payment services session, sometimes identified by geolocation Internet Protocol checks which verify whether the issuing country corresponds

with the Internet Protocol address from which the user is initiating the transaction, atypical e-merchant categories for a specific customer or abnormal transaction data, etc.). Such systems shall also be able to detect signs of malware infection in the session (for example 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, shall be commensurate with the outcome of the risk assessment.

60. PSPs offering acquiring services shall have fraud detection and prevention systems in place to monitor e-merchant activities and identify abnormal customer payment patterns.

61. PSPs shall perform any transaction screening and evaluation procedures within an appropriate time period, in order not to unduly delay the initiation and/or execution of the payment service concerned.

62. Where the PSP, according to its risk policy, decides to block a payment transaction which has been identified as potentially fraudulent, the PSP shall maintain the block for as short a time as possible until the security issues have been resolved.

Protection of Sensitive Payment Data

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

64. All data used to identify and authenticate customers (for example at log-in, when initiating internet payments, and when issuing, amending or cancelling e-mandates), as well as the customer interface (PSP or e-merchant website), shall be appropriately secured against theft and unauthorised access or modification.

65. PSPs shall ensure that when exchanging sensitive payment data via the internet, secure end-to-end encryption 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.

66. PSPs offering acquiring services shall encourage their e-merchants not to store any sensitive payment data. In the event e-merchants handle, that is, store, process or transmit sensitive payment data, such PSPs shall contractually require the e-merchants to have the necessary measures in place to protect these data. PSPs shall carry out regular checks and if a PSP becomes aware that an e-merchant handling sensitive payment data does not have the required security measures in place, it shall take steps to enforce this contractual obligation, or terminate the contract.

CUSTOMER AWARENESS, EDUCATION, AND COMMUNICATION

Customer Education and Communication

67. PSPs shall provide assistance and guidance to customers, where needed, with regard to the secure use of the internet payment services, with a view to enabling customers to use such services safely and efficiently. PSPs shall communicate with their customers in such a way as to reassure them of the authenticity of the messages received.

68. PSPs shall provide at least one secured channel for ongoing communication with customers regarding the correct and secure use of the internet payment service, such as a dedicated mailbox on the PSP's website or a secured website. PSPs shall inform customers of this channel and explain that any message on behalf of the PSP via any other means, such as e-mail, which concerns the correct and secure use of the internet payment service, is not reliable. The PSP shall explain:

    a) the procedure for customers to report to the PSP (suspected) fraudulent payments, suspicious incidents or anomalies during the internet payment services session and/or possible social engineering attempts;

    b) the next steps, that is, how the PSP will respond to the customer; and

    c) how the PSP will notify the customer about (potential) fraudulent transactions or their non-initiation, or warn the customer about the occurrence of attacks (such as phishing e-mails).

69. Through the secured channel, PSPs shall keep customers informed about updates in security procedures regarding internet payment services. Any alerts about significant emerging risks (such as warnings about social engineering) shall also be provided via the secured channel.

70. Customer assistance shall be made available by PSPs for all questions, complaints, requests for support and notifications of anomalies or incidents regarding internet payments and related services, and customers shall be appropriately informed about how such assistance can be obtained.

71. PSPs shall initiate and execute customer education and awareness programmes designed to ensure customers understand, at a minimum, the need:

    a) to protect their passwords, security tokens, personal details and other confidential data;

    b) to manage properly the security of the personal device (for example the computer), through installing and updating security components (such as antivirus, firewalls and/or security patches);

    c) 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;

    d) to use the genuine internet payment website of the PSP.

72. PSPs offering acquiring services shall 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 PSP and not the payee (for example 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).

Notifications and Setting of Limits

73. PSPs shall set limits for internet payment services and may provide their customers with options for further risk limitation within these limits. PSPs may also provide alert and customer profile management services.

74. Prior to providing a customer with internet payment services, PSPs shall set limits applying to those services, such as a maximum amount for each individual payment or a cumulative amount over a certain period of time, and shall inform their customers accordingly. Such limits may either apply globally, that is to all payment instruments enabling internet payments, or individually. PSPs shall also allow customers to disable the internet payment functionality.

Customer Access to Information on the Status of Payment Initiation and Execution

75. PSPs shall confirm to their customers the payment initiation and provide customers in good time with the information necessary to check that a payment transaction has been correctly initiated and/or executed.

76. In relation to internet payment services as defined in points (ii) and (iii) of paragraph 7(l), PSPs shall, except when such a facility is exceptionally not available for technical maintenance purposes or as a result of major incidents, provide customers with a near real-time facility to check the status of the execution of transactions as well as account balances at any time in a safe and trusted environment.

77. Any detailed electronic statements shall be made available in a safe and trusted environment. Where PSPs inform customers about the availability of electronic statements (for example in relation to the regular issue of periodic e-statements, or, on an ad hoc basis, after execution of a transaction) through an alternative channel, such as SMS, e-mail or letter, sensitive payment data shall not be included in such communications or, if included, it shall be masked.

INTERPRETATION AND IMPLEMENTATION

78. This Rule is to be read in conjunction with the EBA Guidelines.

79. This Rule shall enter into force on the 7th of August 2015.