Commission de Surveillance du Secteur Financier

Luxembourg, 14 March 2019

To all payment service providers

CIRCULAR CSSF 19/713

Re : Guidelines of the European Banking Authority on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) - (EBA/GL/2017/17)

Ladies and Gentlemen,

The purpose of this circular is to draw your attention to the Guidelines of the European Banking Authority ("**EBA**") on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366[1] ("**PSD2**") (EBA/GL/2017/17 - the "**Guidelines**"), and with which the CSSF commits to comply, in its capacity as competent authority.

The Guidelines provide details with regard to:

(i) the annual auditing requirements as regards the security measures taken; and

(ii) the annual reporting requirements regarding the assessment of major operational and security risks.

1. The Guidelines

The Guidelines provide details for the security measures that should be taken in accordance with Article 105-1 (2) of the law of 10 November 2009 on payment services[2] (the "**Law**") in order to manage the operational and security risks in relation to the payment services provided.

2. Scope

The present circular is addressed to payment service providers as defined in Article 1 (37) of the Law, for which the CSSF is the designated competent authority for supervisory purposes ("**PSPs**").

3. Auditing of the security measures

According to point 2.6 of the Guidelines, the security measures established in accordance with the Guidelines should be audited. This audit should be carried out on an annual basis by the PSP's internal auditor.

---

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

2 The law of 10 November 2009 on payment services, on the activity of electronic money institution and settlement finality in payment and securities settlement systems.

4. Reporting period and deadlines

According to point 3.4. of the Guidelines, the updated and comprehensive assessment of the operational and security risks relating to the payment services that the PSPs provide and of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks, should be provided to the CSSF, in the form and timeframe described below:

1) for credit institutions, this assessment, signed by the management body, has to be submitted as soon as possible after the closure of the financial year and no later than 30 April of each year;

2) for payment institutions and e-money institutions, this assessment should be a dedicated section within the management report on internal control, to be issued as per the requirements of Circular CSSF 15/614, at the latest on the last day of the third month after the closing date of the financial year; and

3) for POST Luxembourg, this assessment should be a dedicated section within the management report on internal control, to be issued as per the requirements of Circular CSSF 98/143, at the latest one month after the annual general meeting approving the annual accounts of the PSP.

5. Date of application

The present circular shall apply with immediate effect.
The Guidelines are annexed to the present circular and available on the EBA website using the following link:

https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

Yours faithfully,

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER



Marco ZWICK — Director

Claude WAMPACH — Director

Jean-Pierre FABER — Director


Françoise KAUTHEN — Director

Claude MARX — Director General

EBA/GL/2017/17

12/01/2018

Guidelines

on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains Guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010.[1] In accordance with Article 16(3) of Regulation (EU) No 1093/2010, CAs and financial institutions must make every effort to comply with the Guidelines.

2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. CAs as defined in Article 4(2) of Regulation (EU) No 1093/2010 to which Guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where Guidelines are directed primarily at institutions.

Reporting requirements

3. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, CAs must notify the EBA that they comply or intend to comply with these Guidelines, or otherwise give reasons for non-compliance, by 12.03.2018. In the absence of any notification by this deadline, CAs will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to compliance@eba.europa.eu with the reference 'EBA/GL/2017/17. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their CAs. Any change in the status of compliance must also be reported to the EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

2. Subject matter, scope and definitions

Subject matter and scope

5. These Guidelines derive from the mandate given to the EBA in Article 95(3) of Directive (EU) 2015/2366[2] (PSD2).

6. These Guidelines specify requirements for the establishment, implementation and monitoring of the security measures that PSPs must take, in accordance with Article 95(1) of Directive (EU) 2015/2366, to manage the operational and security risks relating to the payment services they provide.

Addressees

7. These Guidelines are addressed to PSPs as defined in Article 4(11) of Directive (EU) 2015/2366 and as referred to in the definition of 'financial institutions' in Article 4(1) of Regulation (EU) 1093/2010 and to CAs as defined in point (i) of Article 4(2) of that Regulation by reference to the repealed Directive 2007/64/EC[3] (currently Directive (EU) 2015/2366[4]).

Definitions

8. Unless otherwise specified, terms used and defined in Directive (EU) 2015/2366 have the same meaning in these Guidelines. In addition, for the purposes of these Guidelines, the following definitions apply:

Management body	– For PSPs that are credit institutions, this term has the same meaning of the definition in point (7) of Article 3(1) of Directive 2013/36/EU[5]; – For PSPs that are payment institutions or electronic money institutions, this term means directors or persons responsible for the management of the PSP and, where

[2] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

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

[4] In accordance with the second subparagraph of Article 114 of Directive (EU) 2015/2366, any reference to the repealed Directive 2007/64/EC shall be construed as a reference to Directive (EU) 2015/2366 and shall be read in accordance with the correlation table in Annex II to Directive (EU) 2015/2366.

[5] Directive 2013/36/EU of the European Parliament and of the Council on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

	relevant, persons responsible for the management of the payment services activities of the PSP; – For PSPs referred to in points (c), (e) and (f) of Article 1(1) of Directive (EU) 2015/2366, this term has the meaning conferred on it by the applicable EU or national law.
Operational or security incident	A singular event or a series of linked events unplanned by the PSP which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.
Senior management	(a) For PSPs that are credit institutions, this term has the same meaning of the definition in point (9) of Article 3(1) of Directive 2013/36/EU; (b) For PSPs that are payment institutions and electronic money institutions, this term means natural persons who exercise executive functions within an institution and who are responsible, and accountable to the management body, for the day-to-day management of the PSP; (c) For PSPs referred to in points (c), (e) and (f) of Article 1(1) of Directive (EU) 2015/2366, this term has the meaning conferred on it by the applicable EU or national law.
Security risk	The risk resulting from inadequate or failed internal processes or external events that have or may have an adverse impact on the availability, integrity, confidentiality of information and communication technology (ICT) systems and/or information used for the provision of payment services. This includes risk from cyber-attacks or inadequate physical security.
Risk appetite	The aggregate level and types of risk an institution is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives.

3. Implementation

Date of application

9. These Guidelines apply from 13 January 2018.

4. Guidelines

Guideline 1: General principle

1.1 All PSPs should comply with all the provisions set out in these Guidelines. The level of detail should be proportionate to the PSP's size and to the nature, scope, complexity and riskiness of the particular services that the PSP provides or intends to provide.

Guideline 2: Governance

Operational and security risk management framework

2.1 PSPs should establish an effective operational and security risk management framework (hereafter 'risk management framework'), which should be approved and reviewed, at least once a year, by the management body and, where relevant, by the senior management. This framework should focus on security measures to mitigate operational and security risks and should be fully integrated into the PSP's overall risk management processes.

2.2 The risk management framework should:

a) include a comprehensive security policy document as referred to in Article 5(1)(j) of Directive (EU) 2015/2366;

b) be consistent with the risk appetite of the PSP;

c) define and assign key roles and responsibilities as well as the relevant reporting lines required to enforce the security measures and to manage security and operational risks;

d) establish the necessary procedures and systems to identify, measure, monitor and manage the range of risks stemming from the payment-related activities of the PSP and to which the PSP is exposed, including business continuity arrangements.

2.3 PSPs should ensure that the risk management framework is properly documented, and updated with documented 'lessons learned' during its implementation and monitoring.

2.4 PSPs should ensure that before a major change of infrastructure, processes or procedures and after each major operational or security incident affecting the security of the payment services they provide, they review whether or not changes or improvements to the risk management framework are needed without undue delay.

Risk management and control models

2.5 PSPs should establish three effective lines of defence, or an equivalent internal risk management and control model, to identify and manage operational and security risks. PSPs should ensure that

the aforementioned internal control model has sufficient authority, independence, resources and direct reporting lines to the management body and, where relevant, to the senior management.

2.6 The security measures set out in these Guidelines should be audited by auditors with expertise in IT security and payments and operationally independent within or from the PSP. The frequency and focus of such audits should take the corresponding security risks into consideration.

Outsourcing

2.7 PSPs should ensure the effectiveness of the security measures set out in these Guidelines when operational functions of payment services, including IT systems, are outsourced.

2.8 PSPs should ensure that appropriate and proportionate security objectives, measures and performance targets are built into contracts and service-level agreements with the providers to whom they have outsourced such functions. PSPs should monitor and seek assurance on the level of compliance of these providers with the security objectives, measures and performance targets.

Guideline 3: Risk assessment

Identification of functions, processes and assets

3.1 PSPs should identify, establish and regularly update an inventory of their business functions, key roles and supporting processes in order to map the importance of each function, role and supporting processes, and their interdependencies related to operational and security risks.

3.2 PSPs should identify, establish and regularly update an inventory of the information assets, such as ICT systems, their configurations, other infrastructures and also the interconnections with other internal and external systems in order to be able to manage the assets that support their critical business functions and processes.

Classification of functions, processes and assets

3.3 PSPs should classify the identified business functions, supporting processes and information assets in terms of criticality.

Risk assessments of functions, processes and assets

3.4 PSPs should ensure that they continuously monitor threats and vulnerabilities and regularly review the risk scenarios impacting their business functions, critical processes and information assets. As part of the obligation to conduct and provide CAs with an updated and comprehensive risk assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigating measures and control mechanisms implemented in response to those risks, as laid down in Article 95(2) of Directive (EU) 2015/2366, PSPs should carry out and document risk assessments, at least annually or at shorter intervals as determined by the CA, of the functions, processes and information assets they have identified and classified in order to

identify and assess key operational and security risks. Such risk assessments should also be done before any major change of infrastructure, process or procedures affecting the security of payment services occurs.

3.5 On the basis of the risk assessments, PSPs should determine whether and to what extent changes are necessary to the existing security measures, the technologies used and the procedures or payment services offered. PSPs should take into account the time required to implement the changes and the time to take appropriate interim security measures to minimise operational or security incidents, fraud and potential disruptive effects in the provision of payment services.

Guideline 4: Protection

4.1 PSPs should establish and implement preventive security measures against identified operational and security risks. These measures should ensure an adequate level of security in accordance with the risks identified.

4.2 PSPs should establish and implement a 'defence-in-depth' approach by instituting multi-layered controls covering people, processes and technology, with each layer serving as a safety net for preceding layers. Defence-in-depth should be understood as having defined more than one control covering the same risk, such as the four-eyes principle, two-factor authentication, network segmentation and multiple firewalls.

4.3 PSPs should ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal data, such measures should be implemented in compliance with Regulation (EU) 2016/679[6] or, if applicable, Regulation (EC) 45/2001.[7]

4.4 On an on-going basis, PSPs should determine whether changes in the existing operational environment influence the existing security measures or require the adoption of further measures to mitigate the risk involved. These changes should be part of the PSP's formal change management process, which should ensure that changes are properly planned, tested, documented and authorised. On the basis of the security threats observed and the changes made, testing should be performed to incorporate scenarios of relevant and known potential attacks.

4.5 In designing, developing and providing payment services, PSPs should ensure that segregation of duties and 'least privilege' principles are applied. PSPs should pay special attention to the segregation of IT environments, in particular to the development, testing and production environments.

[6] Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[7] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Data and systems integrity and confidentiality

4.6 In designing, developing and providing payment services, PSPs should ensure that the collection, routing, processing, storing and/or archiving and visualisation of sensitive payment data of the PSU is adequate, relevant and limited to what is necessary for the provision of its payment services.

4.7 PSPs should regularly check that the software used for the provision of payment services, including the users' payment-related software, is up to date and that critical security patches are deployed. PSPs should ensure that integrity-checking mechanisms are in place in order to verify the integrity of software, firmware and information on their payment services.

Physical security

4.8 PSPs should have appropriate physical security measures in place, in particular to protect the sensitive payment data of the PSUs as well as the ICT systems used to provide payment services.

Access control

4.9 Physical and logical access to ICT systems should be permitted only for authorised individuals. Authorisation should be assigned in accordance with the staff's tasks and responsibilities, limited to individuals who are appropriately trained and monitored. PSPs should institute controls that reliably restrict such access to ICT systems to those with a legitimate business requirement. Electronic access by applications to data and systems should be limited to the minimum that is required to provide the relevant service.

4.10 PSPs should institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as roles-based access, logging and reviewing of the systems activities of privileged users, strong authentication and monitoring for anomalies should be implemented. PSPs should manage access rights to information assets and their supporting systems on a 'need-to-know' basis. Access rights should be periodically reviewed.

4.11 Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with GL 3.1 and GL 3.2, without prejudice to the retention requirements set out in EU and national law. PSPs should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of payment services.

4.12 In order to ensure secure communication and reduce risk, remote administrative access to critical ICT components should be granted only on a need-to-know basis and when strong authentication solutions are used.

4.13 The operation of products, tools and procedures related to access control processes should protect the access control processes from being compromised or circumvented. This includes enrolment, delivery, revocation and withdrawal of corresponding products, tools and procedures.

Guideline 5: Detection

Continuous monitoring and detection

5.1 PSPs should establish and implement processes and capabilities to continuously monitor business functions, supporting processes and information assets in order to detect anomalous activities in the provision of payment services. As part of this continuous monitoring, PSPs should have in place appropriate and effective capabilities for detecting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets used in the provision of payment services.

5.2 The continuous monitoring and detection processes should cover:

a) relevant internal and external factors, including business and ICT administrative functions;

b) transactions in order to detect misuse of access by service providers or other entities; and

c) potential internal and external threats.

5.3 PSPs should implement detective measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities for software and hardware, and check for corresponding new security updates.

Monitoring and reporting of operational or security incidents

5.4 PSPs should determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as set out in the 'Definitions' section of these Guidelines, as well as early warning indicators that should serve as an alert for the PSP to enable early detection of operational or security incidents.

5.5 PSPs should establish appropriate processes and organisational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational or security incidents.

5.6 PSPs should establish a procedure for reporting such operational or security incidents as well as security-related customer complaints to its senior management.

Guideline 6: Business continuity

6.1 PSPs should establish sound business continuity management to maximise their ability to provide payment services on an on-going basis and to limit losses in the event of severe business disruption.

6.2 In order to establish sound business continuity management, PSPs should carefully analyse their exposure to severe business disruptions and assess, quantitatively and qualitatively, their

potential impact, using internal and/or external data and scenario analysis. On the basis of the identified and classified critical functions, processes, systems, transactions and interdependencies in accordance with GL 3.1 to GL 3.3, PSPs should prioritise business continuity actions using a risk-based approach, which can be based on the risk assessments carried out under GL 3. Depending on the business model of the PSP, this may, for example, facilitate the further processing of critical transactions while remediation efforts continue.

6.3 On the basis of the analysis carried out under GL 6.2, a PSP should put in place:

a) BCPs to ensure that it can react appropriately to emergencies and is able to maintain its critical business activities; and

b) mitigation measures to be adopted in the event of termination of its payment services and termination of existing contracts, to avoid adverse effects on payment systems and on PSUs and to ensure execution of pending payment transactions.

Scenario-based business continuity planning

6.4 The PSP should consider a range of different scenarios, including extreme but plausible ones, to which it might be exposed, and assess the potential impact such scenarios might have.

6.5 Based on the analysis carried out under GL 6.2 and plausible scenarios identified under GL 6.4, the PSP should develop response and recovery plans, which should:

a) focus on the impact on the operation of critical functions, processes, systems, transactions and interdependencies;

b) be documented and made available to the business and support units and readily accessible in case of emergency; and

c) be updated in line with lessons learned from the tests, new risks identified and threats and changed recovery objectives and priorities.

Testing of business continuity plans

6.6 PSPs should test their BCPs, and ensure that the operation of their critical functions, processes, systems, transactions and interdependencies are tested at least annually. The plans should support objectives to protect and, if necessary, re-establish the integrity and availability of their operations, and the confidentiality of their information assets.

6.7 Plans should be updated at least annually, based on testing results, current threat intelligence, information-sharing and lessons learned from previous events, and changing recovery objectives, as well as analysis of operationally and technically plausible scenarios that have not yet occurred, and, if relevant, after changes in systems and processes. PSPs should consult and coordinate with relevant internal and external stakeholders during the establishment of their BCPs.

6.8 PSPs' testing of their BCPs should:

a) include an adequate set of scenarios, as referred to in GL 6.4;

b) be designed to challenge the assumptions on which BCPs rest, including governance arrangements and crisis communication plans; and

c) include procedures to verify the ability of their staff and processes to respond adequately to the scenarios above.

6.9 PSPs should periodically monitor the effectiveness of their BCPs, and document and analyse any challenges or failures resulting from the tests.

Crisis communication

6.10 In the event of a disruption or emergency, and during the implementation of the BCPs, PSPs should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including external service providers, are informed in a timely and appropriate manner.

Guideline 7: Testing of security measures

7.1 PSPs should establish and implement a testing framework that validates the robustness and effectiveness of the security measures and ensure that the testing framework is adapted to consider new threats and vulnerabilities, identified through risk-monitoring activities.

7.2 PSPs should ensure that tests are conducted in the event of changes to infrastructure, processes or procedures and if changes are made as a consequence of major operational or security incidents.

7.3 The testing framework should also encompass the security measures relevant to (i) payment terminals and devices used for the provision of payment services, (ii) payment terminals and devices used for authenticating the PSU and (iii) devices and software provided by the PSP to the PSU to generate/receive an authentication code.

7.4 The testing framework should ensure that tests:

a) are performed as part of the PSP's formal change management process to ensure their robustness and effectiveness;

b) are carried out by independent testers who have sufficient knowledge, skills and expertise in testing security measures of payment services and are not involved in the development of the security measures for the corresponding payment services or systems that are to be tested, at least for final tests before putting security measures into operation; and

c) include vulnerability scans and penetration tests adequate to the level of risk identified with the payment services.

7.5 PSPs should perform on-going and repeated tests of the security measures for their payment services. For systems that are critical for the provision of their payment services (as described in

GL 3.2), these tests shall be performed at least on an annual basis. Non-critical systems should be tested regularly on a risk-based approach, but at least every three years.

7.6 PSPs should monitor and evaluate the results of the tests conducted, and update their security measures accordingly and without undue delay in the case of critical systems.

Guideline 8: Situational awareness and continuous learning

Threat landscape and situational awareness

8.1 PSPs should establish and implement processes and organisational structures to identify and constantly monitor security and operational threats that could materially affect their ability to provide payment services.

8.2 PSPs should analyse operational or security incidents that have been identified or have occurred within and/or outside the organisation. PSPs should consider key lessons learned from these analyses and update the security measures accordingly.

8.3 PSPs should actively monitor technological developments to ensure that they are aware of security risks.

Training and security awareness programmes

8.4 PSPs should establish a training programme for all staff to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures in order to reduce human error, theft, fraud, misuse or loss. PSPs should ensure that the training programme provides for training staff members at least annually, and more frequently if required.

8.5 PSPs should ensure that staff members occupying key roles identified under GL 3.1 receive targeted information security training on an annual basis, or more frequently if required.

8.6 PSPs should establish and implement periodic security awareness programmes in order to educate their personnel and to address information security related risks. These programmes should require PSP personnel to report any unusual activity and incidents.

Guideline 9: Payment service user relationship management

Payment service user awareness on security risks and risk-mitigating actions

9.1 PSPs should establish and implement processes to enhance PSUs' awareness of security risks linked to the payment services by providing PSUs with assistance and guidance.

9.2 The assistance and guidance offered to PSUs should be updated in the light of new threats and vulnerabilities, and changes should be communicated to the PSU.

9.3 Where product functionality permits, PSPs should allow PSUs to disable specific payment functionalities related to the payment services offered by the PSP to the PSU.

9.4 Where, in accordance with Article 68(1) of Directive (EU) 2015/2366, a PSP has agreed with the payer spending limits for payment transactions executed through specific payment instruments, the PSP should provide the payer with the option to adjust these limits up to the maximum agreed limit.

9.5 PSPs should provide PSUs with the option to receive alerts on initiated and/or failed attempts to initiate payment transactions, enabling them to detect fraudulent or malicious use of their account.

9.6 PSPs should keep PSUs informed about updates in security procedures which affect PSUs regarding the provision of payment services.

9.7 PSPs should provide PSUs with assistance on all questions, requests for support and notifications of anomalies or issues regarding security matters related to payment services. PSUs should be appropriately informed about how such assistance can be obtained.