BANK ĊENTRALI TA' MALTA
EUROSISTEMA
CENTRAL BANK OF MALTA

CENTRAL BANK OF MALTA

DIRECTIVE NO 1

in terms of the

CENTRAL BANK OF MALTA ACT
(*Cap. 204 of the Laws of Malta*)

THE PROVISION AND USE OF PAYMENT SERVICES

Ref: CBM 01/2018

TITLE I
SUBJECT MATTER, SCOPE AND DEFINITIONS

Subject matter

1. In terms of article 34A(1) of the Central Bank of Malta Act (*Cap.204 of the Laws of Malta*) (hereinafter referred to as "the Act"), the Central Bank of Malta (hereinafter referred to as "the Bank") has been empowered to make directives in respect of, inter alia, the provision and use of payments services. For the purposes of this Directive, terms used in this Directive shall have the same meaning as is assigned to them under the Act.

2. (1) This Directive lays down rules concerning transparency of conditions and information requirements for payment services, and the respective rights and obligations of payment service users and payment service providers in relation to the provision of payment services as a regular occupation or business activity.

   (2) The rules laid down in this Directive for the provision of payment services apply to the following payment service providers:

   (a) credit institutions licensed in terms of Banking Act (*Cap. 371 of the Laws of Malta*), and agents and branches in Malta of credit institutions which have their head offices outside Malta;

   (b) electronic money institutions licensed in terms of the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and authorised to issue electronic money, and agents and branches in Malta of electronic money institutions which have their head offices located outside Malta, in as far as the payment services provided by those agents and branches are linked to the issuance of electronic money;

   (c) payment institutions licensed in terms of the Financial Institutions Act (*Cap. 376 of the Laws of Malta*), and agents and branches in Malta of payment institutions which have their head offices licenced in another Member State;

   (d) post office giro institutions which are entitled under Maltese law to provide payment services;

   (e) account information service providers registered in terms of the Financial Institutions Act (*Cap. 376 of the Laws of Malta*);

   (f) the Bank when not acting in its capacity as monetary or public authority.

3. This Directive is modelled on the requisites of the Directive (EU) 2015/2366.

Scope

4. (1) This Directive applies to payment services provided within the European Union.

   (2) Titles III and IV apply to payment transactions in the currency of a Member State where both the payer's payment service provider and the payee's payment service provider are, or

the sole payment service provider in the payment transaction is, located within the European Union.

(3) Title III, except for Paragraphs 21(1)(b), 28(2)(e) and 32(1)(a) and Title IV, except for Paragraphs 57 to 61, applies to payment transactions in a currency that is not the currency of a Member State where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the European Union, in respect to those parts of the payments transaction which are carried out in the European Union.

(4) Title III, except for Paragraphs 21(1)(b), 28(2)(e), 28(5)(g) and 32(1)(a), and Title IV, except for Paragraphs 38(2) and (4), 52, 53, 57, 59(1), 64 and 67, applies to payment transactions in all currencies where only one of the payment service providers is located within the European Union, in respect to those parts of the payments transaction which are carried out in the European Union.

(5) This Directive shall apply to microenterprises in the same way as to consumers. However, for the purpose of Paragraphs 52 and 53, microenterprises shall not be considered as consumers.

(6) Account information service providers providing only the payment service as referred to in point (8) of Annex I of Directive (EU) 2015/2366 shall be treated as payment institutions, save that Paragraphs 14 to 76 of this Directive shall not apply to them, with the exception of Paragraphs 17, 21 and 28 where applicable, and of Paragraphs 43, 45, 70, 71 and 72 of this Directive, and Article 98 of Directive (EU) 2015/2366.

5. This Directive shall be without prejudice to the Consumer Credit Regulations (S.L. 378.12). This Directive shall also be without prejudice to other relevant European Union or national legislation regarding conditions for granting credit to consumers not harmonised by this Directive that are in conformity with European Union law.

Exclusions

6. This Directive does not apply to the following:

   (a) payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention;

   (b) payment transactions from the payer to the payee through a commercial agent authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee;

   (c) professional physical transport of banknotes and coins, including their collection, processing and delivery;

   (d) payment transactions consisting of the non-professional cash collection and delivery within the framework of a non-profit or charitable activity;

   (e) services where cash is provided by the payee to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services;

(f) cash-to-cash currency exchange operations where the funds are not held on a payment account;

(g) payment transactions based on any of the following documents drawn on the payment service provider with a view to placing funds at the disposal of the payee:

(i) paper cheques governed by the Geneva Convention of 19 March 1931 providing a uniform law for cheques;
(ii) paper cheques similar to those referred to in Paragraph 6(g)(i) and governed by the laws of Member States which are not party to the Geneva Convention of 19 March 1931 providing a uniform law for cheques;

(iii) paper-based drafts in accordance with the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(iv) paper-based drafts similar to those referred to in Paragraph 6(g)(iii) and governed by the laws of Member States which are not party to the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(v) paper-based vouchers;

(vi) paper-based traveller's cheques;

(vii) paper-based postal money orders as defined by the Universal Postal Union;

(h) payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and other participants of the system, and payment service providers, without prejudice to Paragraph 12;

(i) payment transactions related to securities asset servicing, including dividends, income or other distributions, or redemption or sale, carried out by persons referred to in Paragraph 6(h) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services and any other entities allowed to have the custody of financial instruments;

(j) services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services, with the exclusion of payment initiation services and account information services;

(k) services based on specific payment instruments that can be used only in a limited way, that meet one of the following conditions:

(i) instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a limited network of service providers under direct commercial agreement with a professional issuer;

(ii) instruments which can be used only to acquire a very limited range of goods or services;

(iii) instruments valid only in a single Member State provided at the request of an undertaking or a public sector entity and regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer;

(l) payment transactions by a provider of electronic communications networks or services provided in addition to electronic communications services for a subscriber to the network or service:

(i) for purchase of digital content and voice-based services, regardless of the device used for the purchase or consumption of the digital content and charged to the related bill; or

(ii) performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets;

provided that the value of any single payment transaction referred to in Paragraph 6(l)(i) and (ii) does not exceed EUR 50 and:

— the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month, or

— where a subscriber pre-funds its account with the provider of the electronic communications network or service, the cumulative value of payment transactions does not exceed EUR 300 per month;

(m) payment transactions carried out between payment service providers, their agents or branches for their own account;

(n) payment transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group;

(o) cash withdrawal services offered by means of ATM by providers, acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account, on condition that those providers do not conduct other payment services as referred to in Annex I of Directive (EU) 2015/2366. Nevertheless the customer shall be provided with the information on any withdrawal charges referred to in Paragraphs 21, 24, 25 and 35 before carrying out the withdrawal as well as on receipt of the cash at the end of the transaction after withdrawal.

Definitions

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

(1) ‘account information service’ means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.

(2) ‘account information service provider’ means a payment service provider pursuing business activities as referred to in point (8) of Annex I of Directive (EU) 2015/2366;

(3) 'account servicing payment service provider' means a payment service provider providing and maintaining a payment account for a payer;

(4) 'acquiring of payment transactions' means a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee;

(5) 'ADR' means Alternative Dispute Resolution established by the Arbiter for Financial Services (Designation of ADR entity) Regulations *(S.L 555.01*);

(6) 'agent' means a natural or legal person who acts on behalf of a credit institution, payment institution or electronic money institution in providing payment services;

(7) 'authentication' means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials;

(8) 'branch' means a place of business other than the head office which is a part of a credit institution, payment institution or electronic money institution, which has no legal personality and which carries out directly some or all of the transactions, as licensed or registered, inherent in the business of a credit institution, payment institution or electronic money institution; all of the places of business set up in the same Member State by a credit institution, payment institution or electronic money institution with a head office in another Member State shall be regarded as a single branch;

(9) 'business day' means a day on which the relevant payment service provider of the payer or the payment service provider of the payee involved in the execution of a payment transaction is open for business as required for the execution of a payment transaction;

(10) 'card-based payment instrument' means any payment instrument, including a card, mobile phone, computer or any other technological device containing the appropriate payment application which enables the payer to initiate a card-based payment transaction which is not a credit transfer or a direct debit as defined by Article 2 of Regulation (EU) No 260/2012;

(11) 'card-based payment transaction' means a service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device or software if this results in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services;

(12) 'co-badging' means the inclusion of two or more payment brands or payment applications of the same payment brand on the same payment instrument.

(13) 'competent authority' means a public authority or body officially recognised by national law, which is empowered by national law to supervise institutions as part of the supervisory system in operation in the Member State concerned;

(14) 'consumer' means a natural person who, in payment service contracts covered by this Directive, is acting for purposes other than his or her trade, business or profession;

(15) 'consumer association' means a consumer association as defined in the Consumer Affairs Act (*Cap. 378 of the Laws of Malta*);

(16) 'credit transfer' means a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the payment service provider which holds the payer's payment account, based on an instruction given by the payer;

(17) 'digital content' means goods or services which are produced and supplied in digital form, the use or consumption of which is restricted to a technical device and which do not include in any way the use or consumption of physical goods or services;

(18) 'direct debit' means a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider;

(19) 'Directive (EU) 2015/2366' means 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, as may be amended from time to time and includes any implementing measures, implementing technical standards, regulatory technical standards and similar measures that have been or may be issued thereunder;

(20) 'durable medium' means any instrument which enables the payment service user to store information addressed personally to that payment service user in a way accessible for future reference for a period of time adequate to the purposes of the information and which allows the unchanged reproduction of the information stored;

(21) 'EBA' means European Banking Authority established under 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 No 2009/78/EC;

(22) 'ECB' means the European Central Bank established by the Statute of the European System of Central Banks and of the European Central Bank.

(23) 'electronic communications network' means an electronic communications network as defined in the Electronic Communications (Regulation) Act (*Cap. 399 of the Laws of Malta*);

(24) 'electronic communications service' means an electronic communications service as defined in the Electronic Communications (Regulation) Act (*Cap. 399 of the Laws of Malta*);

(25) 'European Union' means the European Union as established by the Treaty on European Union;

(26) 'Financial Institutions Rules on Security of Internet Payments of Credit, Payment and Electronic Money Institutions (FIR/04/2015)' means Financial Institutions Rules on Security of Internet Payments of Credit, Payment and Electronic Money Institutions which implements the Guidelines on the security of internet payments issued by the European Banking Authority on the 19th of December 2014;

(27) 'framework contract' means a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account;

(28) 'funds' means banknotes, coins and scriptural money as defined in the Banking Act (*Cap. 371 of the Laws of Malta*) or electronic money as defined in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*);

(29) 'group' means any body corporate which is that company's subsidiary or parent company, or a subsidiary of that company's parent company, and the term "group" shall be construed accordingly as well as meaning a parent undertaking and all its subsidiary undertakings in accordance with the Companies Act (*Cap. 386 of the Laws of Malta*) or undertakings as defined in the Commissioner Delegated Regulation (EU) No 241/2014 which are linked to each other by a relationship referred to in Regulation (EU) No 575/2013;

(30) 'home Member State' means either of the following:

(a) the Member State in which the registered office of the payment service provider is situated; or

(b) if the payment service provider has, under its national law, no registered office, the Member State in which its head office is situated;

(31) 'host Member State' means the Member State other than the home Member State in which a payment service provider has an agent or a branch or provides payment services;

(32) 'issuer' means a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's card-based payment transactions;

(33) 'issuing of payment instruments' means a payment service by a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions;

(34) 'means of distance communication' means a method which, without the simultaneous physical presence of the payment service provider and the payment service user, may be used for the conclusion of a payment services contract;

(35) 'Member State' means a Member State of the European Union and includes EEA countries;

(36) 'MFSA' means the Malta Financial Services Authority established by the Malta Financial Services Authority Act (*Cap. 330 of the Laws of Malta*);

(37) 'microenterprise' means an enterprise, which at the time of conclusion of the payment service contract, is an enterprise as defined in Paragraph 3 of the Business Promotion Regulations *(S.L.325.06)*;

(38) 'money remittance' means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee;

(39) 'Office of the Arbiter' means the Office of the Arbiter for Financial Services established by the Arbiter for Financial Services Act (*Cap. 555 of the Laws of Malta*);

(40) 'own funds' means funds as defined in point 118 of Article 4(1) of Regulation (EU) No 575/2013 where at least 75% of the Tier 1 capital is in the form of Common Equity Tier 1 capital as referred to in Article 50 of that Regulation and Tier 2 is equal to or less than one third of Tier 1 capital;

(41) 'payee' means a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction;

(42) 'payer' means a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order;

(43) 'payment account' means an account held in the name of one or more payment service users which is used for the execution of payment transactions;

(44) 'payment brand' means any material or digital name, term, sign, symbol or combination of them, capable of denoting under which payment card scheme card-based payment transactions are carried out;

(45) 'payment initiation service' means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;

(46) 'payment initiation service provider' means a payment service provider pursuing business activities as referred to in point (7) of Annex I of Directive (EU) 2015/2366;

(47) 'payment institution' means a legal person that has been granted authorisation in accordance with Article 11 of Directive (EU) 2015/2366 to provide and execute payment services throughout the European Union;

(48) 'payment instrument' means a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order;

(49) 'payment order' means an instruction by a payer or payee to its payment service provider requesting the execution of a payment transaction;

(50) 'payment service' means any business activity set out in Annex I of Directive (EU) 2015/2366;

(51) 'payment service provider' means an institution referred to in paragraph 2(2) of this Directive;

(52) 'payment service user' means a natural or legal person making use of a payment service in the capacity of payer, payee, or both;

(53) 'payment system' means a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions;

(54) 'payment transaction' means an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;

(55) 'personalised security credentials' means personalised features provided by the payment service provider to a payment service user for the purposes of authentication;

(56) 'reference exchange rate' means the exchange rate which is used as the basis to calculate any currency exchange and which is made available by the payment service provider or comes from a publicly available source;

(57) 'reference interest rate' means the interest rate which is used as the basis for calculating any interest to be applied and which comes from a publicly available source which can be verified by both parties to a payment service contract;

(58) 'Regulation (EU) No 260/2012' means Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009;

(59) 'Regulation (EU) No 1093/2010' means 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 No 2009/78/EC;

(60) 'Regulation (EU) No 2015/847' means Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006;

(61) 'Regulation (EU) No 575/2013' means Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012;

(62) 'remote payment transaction' means a payment transaction initiated via internet or through a device that can be used for distance communication;

(63) 'sensitive payment data' means data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data;

(64) 'strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

(65) 'unique identifier' means a combination of letters, numbers or symbols specified to the payment service user by the payment service provider and to be provided by the payment service user to identify unambiguously another payment service user and/or the payment account of that other payment service user for a payment transaction;

(66) 'value date' means a reference time used by a payment service provider for the calculation of interest on the funds debited from or credited to a payment account;

TITLE II
PAYMENT SERVICE PROVIDERS

CHAPTER 1
Competent authorities and supervision

Competent authorities

8. (1) The Bank shall be the competent authority in the event of infringements or suspected infringements of the provisions of this Directive, carried out by the payment service providers referred to in Paragraph 2(2).

(2) In order to carry out the controls and take the necessary steps provided for in Title II of Directive (EU) 2015/2366 as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and in the Banking Act (*Cap. 371 of the Laws of Malta*) and this Directive, in accordance with Paragraph 8(1), in respect of the agent or branch in Malta of a credit institution, a payment institution or an electronic money institution located in another Member State, the Bank shall collaborate with the MFSA and the competent authorities of the home Member State.

Furthermore, with respect to the agent or branch located in another Member State of a credit institution, a payment institution or an electronic money institution located in Malta, the Bank shall collaborate with the MFSA and the competent authorities of the host Member State.

(3) The Bank, in collaboration with the MFSA, may require that credit institutions, payment institutions and electronic money institutions having agents or branches in Malta to report periodically on the activities carried out in Malta.

Such reports shall be required for information or statistical purposes and, as far as the agents and branches conduct the payment service business under the right of establishment, to monitor compliance with the provisions of this Directive. Such agents and branches shall be subject to professional secrecy requirements at least equivalent to those referred to in Article 24 of Directive (EU) 2015/2366 as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and in the Banking Act (*Cap. 371 of the Laws of Malta*).

(4) With reference to Paragraph 8(2) and (3), the exchange of all essential and/or relevant information between the competent authorities of the home or the host Member States and the Bank shall be in accordance with the provisions of the regulatory technical standards specifying the framework for cooperation and the exchange of information as developed by the EBA in accordance with their obligation laid down in Article 29(6) of Directive (EU) 2015/2366.

(5) The Bank, in collaboration with the MFSA, may require credit institutions, payment institutions and electronic money institutions operating in Malta through agents under the right of establishment, the head office of which is situated in another Member State, to appoint a central contact point in Malta to ensure adequate communication and information reporting on

compliance with this Directive, without prejudice to any provisions on anti-money laundering and countering terrorist financing provisions and to facilitate supervision by the Bank and the competent authorities of home Member State, including the provision of documents and information on request.

(6) With reference to Paragraph 8(5), the criteria to be applied when determining, in accordance with the principle of proportionality, the circumstances when the appointment of a central contact point is appropriate, and the functions of those contact points, shall be specified in the regulatory technical standards developed by the EBA in accordance with their obligation laid down in Article 29(5) of Directive (EU) 2015/2366

(7) Without prejudice to the responsibility of the competent authorities of the home Member State, where the Bank, in collaboration with the MFSA, ascertains that a credit institution, a payment institution or an electronic money institution, established in another Member State, having agents or branches in Malta, does not comply with the provisions of Title II of Directive (EU) 2015/2366 as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and in the Banking Act (*Cap. 371 of the Laws of Malta*) and this Directive, the Bank shall inform the competent authority of the home Member State without delay.

The Bank, in collaboration with the MFSA, after having evaluated the information received about a credit institution, a payment institution or an electronic money institution in Malta, having agents or branches in another Member State, which does not comply with the host Member State's national law transposing Titles II, III or IV of Directive (EU) 2015/2366, shall, without undue delay, take all appropriate measures to ensure that the credit institution, payment institution or electronic money institution concerned puts an end to its irregular situation. The Bank, in collaboration with the MFSA, shall communicate those measures without delay to the competent authority of the host Member State and to the competent authorities of any other Member State concerned.

(8) Any measures taken by the Bank in collaboration with the MFSA, pursuant to the provisions of Paragraph 8(2), (3), (4), (5), (6) and (7) of this Directive and the provisions of Articles 23, 28 and 30 of Directive 2015/2366 involving penalties or restrictions on the exercise of the freedom to provide services or the freedom of establishment shall be properly justified and communicated to the credit institution, payment institution or electronic money institution concerned.

The provisions of Paragraph 8(2), (3), (4), (5), (6) and (7) of this Directive and the provisions of Articles 28 and 30 of Directive 2015/2366 shall be without prejudice to the obligations of the Bank under the Prevention of Money Laundering Act (*Cap. 373 of the Laws of Malta*), the Prevention of Money Laundering and Funding of Terrorism Regulations (*S.L. 373.01*), and Regulation (EU) 2015/847, to supervise or monitor the compliance with the requirements laid down in those instruments.

Right to apply to Courts

9. (1) Any decisions taken by the Bank, in collaboration with the MFSA, in respect of a payment service provider(s) pursuant to the laws, regulations and administrative provisions adopted in accordance with Title II of Directive (EU) 2015/2366 as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and in the Banking Act (*Cap. 371 of the Laws of Malta*) and this Directive, may be appealed with the Financial Services Tribunal, established by the Malta Financial Services Authority Act (*Cap. 330 of the Laws of Malta*), in

accordance with Article 35 of the Central Bank of Malta Act (*Cap. 204 of the Laws of Malta*) without prejudice to the right of recourse before the Courts of Malta.

(2) Paragraph 9(1) shall apply also in respect of failure to act.

Exchange of Information

10. (1) Where appropriate, the Bank shall cooperate and exchange information with the following:
    (a) European Union regulatory authorities, including the EBA and the ECB;

    (b) competent authorities of other Member States, (in their capacity as competent authorities for Directive (EU) 2015/2366); and,

    (c) other relevant authorities designated under European Union law or national law applicable to payment service providers.

Settlement of disagreements between competent authorities of different Member States

11. (1) Where the Bank considers that, in a particular matter, cross-border cooperation with competent authorities of another Member State referred to in Paragraphs 8(2), (3), (4), (5), (6), (7), (8) and 10 of this Directive and Articles 28 and 30 of Directive (EU) 2015/2366 as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and in the Banking Act (*Cap. 371 of the Laws of Malta*) does not comply with the relevant conditions set out in those provisions, it may refer the matter to EBA and request its assistance in accordance with Article 19 of Regulation (EU) No 1093/2010.

    (2) Where the competent authority of another Member State considers that, in a particular matter, cross-border cooperation with the Bank as referred to in the Member State's national law transposing Articles 26, 28, 29, 30 or 31 of Directive (EU) 2015/2366 does not comply with the relevant conditions set out in those provisions and requests the assistance of the EBA in accordance with Article 19 of Regulation (EU) No 1093/2010, the Bank shall defer any decisions pending resolution under Article 19 of that Regulation.

CHAPTER 2
Common provisions

Access to payment systems

12. (1) The rules on access of authorised or registered payment service providers that are legal persons to payment systems approved by the Bank in terms of CBM Directive No. 13 entitled 'Approval of Payment Systems' shall be objective, non-discriminatory and proportionate and shall not inhibit access more than is necessary to safeguard against specific risks such as settlement risk, operational risk and business risk and to protect the financial and operational stability of the payment system.

    Such payment systems shall not impose on payment service providers, on payment service users or on other payment systems any of the following requirements:

    (a) restrictive rule on effective participation in other payment systems;

(b) rule which discriminates between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of participants;

(c) restriction on the basis of institutional status.

(2) In order to promote effective competition in payments markets, Paragraph 12(1) shall also apply to three-party schemes, such as three-party card schemes, which do not fall within the scope of Paragraph 6.

(3) Paragraph 12(1) shall not apply to:

(a) payment systems designated under CBM Directive No. 2 entitled 'Payment and Securities Settlement Systems';

(b) payment systems composed exclusively of payment service providers belonging to a group.

For the purposes of Paragraph 12(3)(a) where a participant in a designated system allows an authorised or registered payment service provider that is not a participant in the system to pass transfer orders through the system that participant shall, when requested, give the same opportunity in an objective, proportionate and non-discriminatory manner to other authorised or registered payment service providers in line with Paragraph 12(1).

The participant shall provide the requesting payment service provider with full reasons for any rejection.

Access to accounts maintained with a credit institution

13. Payment institutions and electronic money institutions shall have access to credit institutions' payment accounts services on an objective, non-discriminatory and proportionate basis. Such access shall be sufficiently extensive as to allow such payment institutions and electronic money institutions to provide payment services in an unhindered and efficient manner.

The credit institution shall provide the MFSA with duly motivated reasons for any rejection.

TITLE III
TRANSPARENCY OF CONDITIONS AND INFORMATION REQUIREMENTS FOR PAYMENT SERVICES

CHAPTER 1
General Rules

Application

14. This Title shall apply to single payment transactions, framework contracts and payment transactions covered by them. The parties thereto may agree that it shall not apply in whole or in part when the payment service user is not a consumer.

Other provisions in European Union Law

15. The provisions of this Title are without prejudice to any European Union law containing additional requirements on prior information.

However, where the Distance Selling (Retail Financial Services) Regulations (S.L. 330.07) is also applicable, the information requirements set out in Article 5(1)(a) of those Regulations, with the exception of sub-articles 1(b)(iii) to (viii), (c)(i), (iv), (v) and (d)(iv) shall be replaced by Paragraphs 20, 21, 27 and 28 of this Directive.

Charges for information

16. (1) The payment service provider shall not charge the payment service user for providing information under this Directive.
(2) The payment service provider and the payment service user may agree on charges for additional or more frequent information, or transmission by means of communication other than those specified in the framework contract, provided at the payment service user's request.

(3) Where the payment service provider may impose charges for information in accordance with Paragraph 16(2), they shall be reasonable and in line with the payment service provider's actual costs.

Burden of proof on information requirements

17. The burden of proof shall lie with the payment service provider to prove that it has complied with the information requirements set out in this Directive.

Derogation from information requirements for low-value payment instruments and electronic money

18. (1) In cases of payment instruments which, according to the relevant framework contract, concern only individual payment transactions that do not exceed EUR 30 or that either have a spending limit of EUR 150 or store funds that do not exceed EUR 150 at any time:
(a) by way of derogation Paragraphs 27, 28 and 32, the payment service provider shall provide the payer only with information on the main characteristics of the payment service, including the way in which the payment instrument can be used, liability, charges levied and other material information needed to take an informed decision as well as an indication of where any other information and conditions specified in Paragraph 28 are made available in an easily accessible manner;

(b) it may be agreed that, by way of derogation Paragraph 30, the payment service provider is not required to propose changes to the conditions of the framework contract in the same way as provided for in Paragraph 27(1);

(c) it may be agreed that, by way of derogation from Paragraphs 33 and 34, after the execution of a payment transaction:

(i) the payment service provider provides or makes available only a reference enabling the payment service user to identify the payment transaction, the amount of the payment transaction, any charges and/or, in the case of several payment transactions of the same kind made to the same payee, information on the total amount and charges for those payment transactions;

(ii) the payment service provider is not required to provide or make available information referred to in Paragraph 18(1)(c)(i) if the payment instrument is used anonymously or if the payment service provider is not otherwise technically in a position to provide it.

However, the payment service provider shall provide the payer with a possibility to verify the amount of funds stored.

CHAPTER 2
Single payment transactions

Application

19. (1) This Chapter applies to single payment transactions not covered by a framework contract.

(2) When a payment order for a single payment transaction is transmitted by a payment instrument covered by a framework contract, the payment service provider shall not be obliged to provide or make available information which is already given to the payment service user on the basis of a framework contract with another payment service provider or which will be given according to that framework contract.

Prior general information

20. (1) Before the payment service user is bound by a single payment service contract or offer, the payment service provider shall make available to the payment service user, in an easily accessible manner, the information and conditions specified in Paragraph 21 with regard to its own services. At the payment service user's request, the payment service provider shall provide the information and conditions on paper or on another durable medium. The information and conditions shall be given in easily understandable words and in a clear and comprehensible form, in English and/or Maltese or in any other language agreed between the parties.

(2) If the single payment service contract has been concluded at the request of the payment service user using a means of distance communication which does not enable the payment service provider to comply with Paragraph 20(1), the payment service provider shall fulfil its obligations as specified in Paragraph 20(1) immediately after the execution of the payment transaction.

(3) The obligations as specified in Paragraph 20(1) may also be discharged by supplying a copy of the draft single payment service contract or the draft payment order including the information and conditions specified in Paragraph 21.

Information and conditions

21. (1) The following information and conditions shall be provided or made available to the payment service user by the payment service provider:

(a) a specification of the information or unique identifier to be provided by the payment service user in order for a payment order to be properly executed;

(b) the maximum execution time for the payment service to be provided;

(c) all charges payable by the payment service user to the payment service provider and, where applicable, the breakdown of the amounts of those charges;

(d) where applicable, the actual or reference exchange rate to be applied to the payment transaction.

(2) In addition, the payment initiation service providers shall, prior to initiation, provide the payer with, or make available to the payer, the following clear and comprehensive information:

(a) the name of the payment initiation service provider, the geographical address of its head office and, where applicable, the geographical address of its agent or branch established in Malta where the payment service is offered, and any other contact details, including electronic mail address, relevant for communication with the payment initiation service provider; and

(b) the contact details of the MFSA or the competent authority of the home member state as applicable;

(3) Where applicable, any other relevant information and conditions specified in Paragraph 28 shall be made available to the payment service user in an easily accessible manner.

Information for the payer and payee after the initiation of a payment order

22. (1) In addition to the information and conditions specified in Paragraph 21, where a payment order is initiated through a payment initiation service provider, the payment initiation service provider shall, immediately after initiation, provide or make available all of the following data to the payer and, where applicable, the payee:

(a) confirmation of the successful initiation of the payment order with the payer's account servicing payment service provider;

(b) a reference enabling the payer and the payee to identify the payment transaction and, where appropriate, the payee to identify the payer, and any information transferred with the payment transaction;

(c) the amount of the payment transaction;

(d) where applicable, the amount of any charges payable to the payment initiation service provider for the transaction, and where applicable a breakdown of the amounts of such charges.

Information for payer's account servicing payment service provider in the event of a payment initiation service

23. When initiating a payment order, the payment initiation service provider shall make available to the payer's account servicing payment service provider the reference of the payment transaction.

Information for the payer after receipt of the payment order

24. (1) Immediately after receipt of the payment order, the payer's payment service provider shall provide or make available to the payer, in the same way as provided in Paragraph 20(1) all of the following data with regard to its own services:

(a) a reference enabling the payer to identify the payment transaction and, where appropriate, information relating to the payee;

(b) the amount of the payment transaction in the currency used in the payment order;

(c) the amount of any charges for the payment transaction payable by the payer and, where applicable, a breakdown of the amounts of such charges;

(d) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider or a reference thereto, when different from the rate provided in accordance with Paragraph 21(1)(d) and the amount of the payment transaction after that currency conversion;

(e) the date of receipt of the payment order.

Information for the payee after execution

25. (1) Immediately after the execution of the payment transaction, the payee's payment service provider shall provide or make available to the payee, in the same way as provided for in Paragraph 20(1) all of the following data with regard to its own services:

(a) a reference enabling the payee to identify the payment transaction and, where appropriate, the payer and any information transferred with the payment transaction;

(b) the amount of the payment transaction in the currency in which the funds are at the payee's disposal;

(c) the amount of any charges for the payment transaction payable by the payee and, where applicable, a breakdown of the amounts of such charges;

(d) where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion;

(e) the credit value date.

CHAPTER 3
Framework contracts

Application

26. This Chapter applies to payment transactions covered by a framework contract.

Prior general information

27. (1) The payment service provider shall, in good time before the payment service user is bound by any framework contract or offer, provide the payment service user, on paper or on another durable medium with the information and conditions specified in Paragraph 28. The

information and conditions shall be given in easily understandable words and in a clear and comprehensible form, in English and/or Maltese or in any other language agreed between the parties.

(2) If the framework contract has been concluded at the request of the payment service user using a means of distance communication which does not enable the payment service provider to comply with Paragraph 27(1), the payment service provider shall fulfil its obligations specified in Paragraph 27(1) immediately after conclusion of the framework contract.

(3) The obligations under Paragraph 27(1) may also be discharged by providing a copy of the draft framework contract including the information and conditions specified in Paragraph 28.

Information and conditions

28. The following information and conditions shall be provided to the payment service user:

(1) On the payment service provider:

(a) the name of the payment service provider, the geographical address of its head office and, where applicable, the geographical address of its agent or branch established in Malta where the payment service is offered, and any other address, including electronic mail address, relevant for communication with the payment service provider;

(b) the particulars of the relevant supervisory authorities and of any relevant public register of authorisation of the payment service provider and the registration number or equivalent means of identification in that register;

(2) On use of the payment service:

(a) a description of the main characteristics of the payment service to be provided;

(b) a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly initiated or executed;

(c) the form of and procedure for giving consent to initiate a payment order or execute a payment transaction and withdrawal of such consent in accordance with Paragraphs 40 and 56;

(d) a reference to the time of receipt of a payment order in accordance with Paragraph 54 and the cut-off time, if any, established by the payment service provider;

(e) the maximum execution time for the payment services to be provided;

(f) whether there is a possibility to agree on spending limits for the use of the payment instrument in accordance with Paragraph 44(1);

(g) in the case of co-badged, card-based payment instruments, the payment service user's rights as specified in Article 8 of Regulation (EU) 2015/751 of the European

Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions;

(3) On charges, interest and exchange rates:

(a) all charges payable by the payment service user to the payment service provider including those connected to the manner in and frequency with which information under this Directive is provided or made available and, where applicable, the breakdown of the amounts of such charges;

(b) where applicable, the interest and exchange rates to be applied or, if reference interest and exchange rates are to be used, the method of calculating the actual interest, and the relevant date and index or base for determining such reference interest or exchange rate;

(c) if agreed, the immediate application of changes in reference interest or exchange rate and information requirements related to the changes in accordance with Paragraph 30(2);

(4) On communication:

(a) where applicable, the means of communication, including the technical requirements for the payment service user's equipment and software, agreed between the parties for the transmission of information or notifications under this Directive;

(b) the manner in and frequency with which information under this Directive is to be provided or made available;

(c) the language or languages in which the framework contract will be concluded and communication during this contractual relationship undertaken;

(d) the payment service user's right to receive the contractual terms of the framework contract and information and conditions in accordance with Paragraph 29;

(5) On safeguards and corrective measures:

(a) where applicable, a description of steps that the payment service user is to take in order to keep safe a payment instrument and how to notify the payment service provider for the purposes of Paragraph 45(1)(b);

(b) the secure procedure for notification of the payment service user by the payment service provider in the event of suspected or actual fraud or security threats;

(c) if agreed, the conditions under which the payment service provider reserves the right to block a payment instrument in accordance with Paragraph 44;

(d) the liability of the payer in accordance with Paragraph 50, including information on the relevant amount;

(e) how and within what period of time the payment service user is to notify the payment service provider of any unauthorised or incorrectly initiated or executed payment transaction in accordance with Paragraph 47 as well as the payment service

provider's liability for unauthorised payment transactions in accordance with Paragraph 49;

(f) the liability of the payment service provider for the initiation or execution of payment transactions in accordance with Paragraphs 64 and 65;

(g) the conditions for refund in accordance with Paragraphs 52 and 53;

(6) On changes to, and termination of, the framework contract:

(a) if agreed, information that the payment service user will be deemed to have accepted changes in the conditions in accordance with Paragraph 30, unless the payment service user notifies the payment service provider before the date of their proposed date of entry into force that they are not accepted;

(b) the duration of the contract;

(c) the right of the payment service user to terminate the framework contract and any agreements relating to termination in accordance with Paragraphs 30(1) and 31;

(7) On redress:

(a) any contractual clause on the law applicable to the framework contract and/or the competent courts;

(b) the complaint procedures available to the payment service user in accordance with Paragraphs 73 to 75.

Accessibility of information and conditions of the framework contract

29. At any time during the contractual relationship the payment service user shall have a right to receive, on request, the contractual terms of the framework contract as well as the information and conditions specified in Paragraph 28 on paper or on another durable medium.

Changes in conditions of the framework contract

30. (1) Any changes in the framework contract or in the information and conditions specified in Paragraph 28, shall be proposed by the payment service provider in the same way as provided for in Paragraph 27(1) and no later than two months before their proposed date of application. The payment service user can either accept or reject the changes before the date of their proposed date of entry into force.
Where applicable and in accordance with Paragraph 28(6)(a), the payment service provider shall inform the payment service user that, in the absence of an objection to the proposed changes to the conditions laid down in the framework contract, the payment service user shall be deemed to have accepted these proposed changes.

The payment service provider shall also inform the payment service user that, in the event that the payment service user rejects those changes, the payment service user has the right to terminate the framework contract free of charge and with effect at any time until the date when the changes would have applied.

(2) Changes in the interest or exchange rates may be applied immediately and without notice, provided that such a right is agreed upon in the framework contract and that the changes in

the interest or exchange rates are based on the reference interest or exchange rates agreed on in accordance with Paragraph 28(3)(b) and (c). The payment service user shall be informed of any change in the interest rate at the earliest opportunity in the same way as provided for in Paragraph 27(1) unless the parties have agreed on a specific frequency or manner in which the information is to be provided or made available. However, changes in interest or exchange rates which are more favourable to the payment service users, may be applied without notice.

(3) Changes in the interest or exchange rate used in payment transactions shall be implemented and calculated in a neutral manner that does not discriminate against payment service users.

Termination

31. (1) The payment service user may terminate the framework contract at any time, unless the parties have agreed on a period of notice. Such a period shall not exceed 1 month.

(2) Termination of the framework contract shall be free of charge for the payment service user except where the contract has been in force for less than 6 months. Charges, if any, for termination of the framework contract shall be appropriate and in line with costs.

(3) On termination of the framework contract, the payment service provider shall provide the payment service user, on paper or on another durable medium and free of charge, the information referred to in Paragraphs 33(1) and 34(1), covering a period of at least thirteen months.

(4) If agreed in the framework contract, the payment service provider may terminate a framework contract concluded for an indefinite period by giving at least 2 months' notice in the same way as provided for in Paragraph 27(1).

(5) Charges for payment services levied on a regular basis shall be payable by the payment service user only proportionally up to the termination of the contract. If such charges are paid in advance, they shall be reimbursed proportionally.

(6) The provisions of Paragraph 31 are without prejudice to the relevant local legislation, including the Credit Institutions and Financial Institutions (Payment Accounts) Regulations *(S.L. 371.18)*, governing the rights of the parties to declare the framework contract unenforceable or void.

Information before execution of individual payment transactions

32. (1) In the case of an individual payment transaction under a framework contract initiated by the payer, a payment service provider shall, at the payer's request for this specific payment transaction, provide explicit information on all of the following:

(a) the maximum execution time;

(b) the charges payable by the payer;

(c) where applicable, a breakdown of the amounts of any charge.

Information for the payer on individual payment transactions

33. (1) After the amount of an individual payment transaction is debited from the payer's account or, where the payer does not use a payment account, after receipt of the payment order, the payer's payment service provider shall provide the payer, without undue delay and in the same way as laid down in Paragraph 27(1), with all of the following information:

(a) a reference enabling the payer to identify each payment transaction and, where appropriate, information relating to the payee;

(b) the amount of the payment transaction in the currency in which the payer's payment account is debited or in the currency used for the payment order;

(c) the amount of any charges for the payment transaction and, where applicable, a breakdown of the amounts of such charges, or the interest payable by the payer;

(d) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider, and the amount of the payment transaction after that currency conversion;

(e) the debit value date or the date of receipt of the payment order.

(2) A framework contract may include a condition that the information referred to in Paragraph 33(1) is to be provided, on paper or on another durable medium at least once a month and free of charge. However, the payer shall have the option to receive the information in the same manner and frequency as referred to in Paragraph 33(1). This option shall be available at any time and free of charge.

(3) Without prejudice to Paragraph 16(2), a framework contract may include a condition that the payer may require the information referred to in Paragraph 33(1) to be provided, on paper or on another durable medium at a less frequent basis than as provided in Paragraph 33(2) and free of charge. However, the payer shall be allowed to revert back to the frequency referred to in Paragraph 33(2), at any time and free of charge.

Information for the payee on individual payment transactions

34. (1) After the execution of an individual payment transaction, the payee's payment service provider shall provide the payee without undue delay in the same way as laid down in Paragraph 27(1) with all of the following information:

(a) a reference enabling the payee to identify the payment transaction and the payer, and any information transferred with the payment transaction;

(b) the amount of the payment transaction in the currency in which the payee's payment account is credited;

(c) the amount of any charges for the payment transaction and, where applicable, a breakdown of the amounts of such charges, or the interest payable by the payee;

(d) where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion;

(e) the credit value date.

(2) A framework contract may include a condition that the information referred to in Paragraph 34(1) is to be provided, on paper or on another durable medium at least once a month and free of charge.

(3) Without prejudice to Paragraph 16(2), a framework contract may include a condition that the payee may require the information referred to in Paragraph 34(1) to be provided, on paper or on another durable medium at a less frequent basis than as provided in Paragraph 34(2) and free of charge. However, the payee shall be allowed to revert back to the frequency referred to in Paragraph 34(2), at any time and free of charge.

CHAPTER 4
Common provisions

Currency and currency conversion

35. (1) Payments shall be made in the currency agreed between the parties.

(2) Where a currency conversion service is offered prior to the initiation of the payment transaction and where that currency conversion service is offered at an ATM, at the point of sale or by the payee, the party offering the currency conversion service to the payer shall disclose to the payer all charges as well as the exchange rate to be used for converting the payment transaction.

The payer shall agree to the currency conversion service on that basis.

Information on additional charges or reductions

36. (1) Where, for the use of a given payment instrument, the payee offers a reduction, the payee shall inform the payer thereof prior to the initiation of the payment transaction.

(2) Where, for the use of a given payment instrument, the payment service provider or another party involved in the transaction requests a charge, the payment service user shall be informed prior to the initiation of the payment transaction.

(3) The payer shall only be obliged to pay for the charges referred to in Paragraph 36(2), if made aware of the full amount of these charges prior to the initiation of the payment transaction.

TITLE IV
RIGHTS AND OBLIGATIONS IN RELATION TO THE PROVISION AND USE OF PAYMENT SERVICES

CHAPTER 1
Common provisions

Application

37. Where the payment service user is not a consumer, the payment service user and the payment service provider may agree that Paragraphs 38(1), 40(3), 48, 50, 52, 53, 56, 64 and 65 do not apply in whole or in part. The payment service user and the payment service provider may also agree on different time limits than those laid down in Paragraph 47.

Charges applicable

38. (1) The payment service provider shall not charge the payment service user for fulfilment of its information obligations or corrective and preventive measures under this Title, unless otherwise specified in Paragraphs 55(1), 56(5) and 63(4). Those charges shall be agreed between the payment service user and the payment service provider and shall be appropriate and in line with the payment service provider's actual costs.
(2) With respect to payment transactions provided within the European Union, where both the payer's and the payee's payment service providers are, or the sole payment service provider in the payment transaction is located therein, the payee shall pay the charges levied by his payment service provider, and the payer shall pay the charges levied by his payment service provider.

(3) The payment service provider shall not prevent the payee from steering the payer towards the use of any particular payment instrument. Furthermore, the payee shall not be prevented from offering the payer a reduction for using electronic payments.

(4) The payee is prohibited from requesting charges for electronic payment transactions.

Derogation for low value payment instruments and electronic money

39. (1) In the case of payment instruments which, according to the framework contract, solely concern individual payment transactions not exceeding EUR 30 or which either have a spending limit of EUR 150, or store funds which do not exceed EUR 150 at any time, payment service providers may agree with their payment service users that:

(a) Paragraphs 45(1)(b), 46(1)(c) and (d) and 50(3) do not apply if the payment instrument does not allow its blocking or prevention of its further use;

(b) Paragraphs 48, 49, 50(1) and (3) do not apply if the payment instrument is used anonymously or the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised;

(c) by way of derogation from Paragraph 55(1) the payment service provider is not required to notify the payment service user of the refusal of a payment order, if the non-execution is apparent from the context;

(d) by way of derogation from Paragraph 56, the payer may not revoke the payment order after transmitting the payment order or giving consent to execute the payment transaction to the payee;

(e) by way of derogation from Paragraphs 59 and 60, other execution periods apply.

(2) Paragraphs 49 and 50 shall apply also to electronic money as defined in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) except where the payer's payment service provider does not have the ability to freeze the payment account on which the electronic money is stored or block the payment instrument.

CHAPTER 2
Authorisation of payment transactions

Consent and withdrawal of consent

40. (1) A payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the payment service provider, after the execution of the payment transaction.

(2) Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the payment service provider. Consent to execute a payment transaction may also be given via the payee or the payment initiation service provider.

In the absence of consent, a payment transaction shall be considered to be unauthorised.

(3) Consent may be withdrawn by the payer at any time, but no later than at the moment of irrevocability in accordance with Paragraph 56. Consent to execute a series of payment transactions may also be withdrawn, in which case any future payment transaction shall be considered to be unauthorised.

(4) The procedure for giving consent shall be agreed between the payer and the relevant payment service provider(s).

Confirmation on the availability of funds

41. (1) An account servicing payment service provider shall, upon the request of a payment service provider issuing card-based payment instruments, immediately confirm whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer, provided that all of the following conditions are met:

(a) the payment account of the payer is accessible online at the time of the request;

(b) the payer has given explicit consent to the account servicing payment service provider to respond to requests from a specific payment service provider issuing card-based payment instruments to confirm that the amount corresponding to a certain card-based payment transaction is available on the payer's payment account;

(c) the consent referred to in Paragraph 41(1)(b) has been given before the first request for confirmation is made.

(2) The payment service provider issuing card-based payment instruments may request the confirmation referred to in Paragraph 41(1) where all of the following conditions are met:

(a) the payer has given explicit consent to the payment service provider issuing card-based payment instruments to request the confirmation referred to in Paragraph 41(1);

(b) the payer has initiated the card-based payment transaction for the amount in question using a card-based payment instrument issued by the payment service provider;

(c) the payment service provider issuing card-based payment instruments authenticates itself towards the account servicing payment service provider before each confirmation request, and securely communicates with the account servicing payment

service provider in accordance with procedures for authentication and secure communication as issued by the EBA.

(3) In accordance with the Data Protection Act (*Cap. 440 of the Laws of Malta*), the confirmation referred to in Paragraph 41(1) shall consist only in a simple 'yes' or 'no' answer and not in a statement of the account balance. That answer shall not be stored or used for purposes other than for the execution of the card-based payment transaction.

(4) The confirmation referred to in Paragraph 41(1) shall not allow for the account servicing payment service provider to block funds on the payer's payment account.

(5) The payer may request the account servicing payment service provider to communicate to the payer the identification of the payment service provider issuing card-based payment instruments and the answer provided.

(6) Paragraph 41 does not apply to payment transactions initiated through card-based payment instruments on which electronic money, as defined in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*), is stored.

Rules on access to payment account in the case of payment initiation services

42. (1) A payer has the right to make use of a payment initiation service provider to obtain payment services as referred to in point (7) of Annex I of Directive (EU) 2015/2366. The right to make use of a payment initiation service provider shall not apply where the payment account is not accessible online.

(2) When the payer gives its explicit consent for a payment to be executed in accordance with Paragraph 40 the account servicing payment service provider shall perform the actions as specified in Paragraph 42(4) in order to ensure the payer's right to use the payment initiation service.

(3) The payment initiation service provider shall:

(a) not hold at any time the payer's funds in connection with the provision of the payment initiation service;

(b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;

(c) ensure that any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's explicit consent;

(d) every time a payment is initiated, identify itself towards the account servicing payment service provider of the payer and communicate with the account servicing payment service provider, the payer and the payee in a secure way, in accordance with procedures for authentication and secure communication as issued by the EBA;

(e) not store sensitive payment data of the payment service user;

(f) not request from the payment service user any data other than those necessary to provide the payment initiation service;

(g) not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer;

(h) not modify the amount, the payee or any other feature of the transaction.

(4) The account servicing payment service provider shall:

(a) communicate securely with payment initiation service providers in accordance with procedures for authentication and secure communication as issued by the EBA;

(b) immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider;

(c) treat payment orders transmitted through the services of a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer.

(5) The provision of payment initiation services shall not be dependent on the existence of a contractual relationship between the payment initiation service providers and the account servicing payment service providers for that purpose.

Rules on access to and use of payment account information in the case of account information services

43. (1) A payment service user has the right to make use of services enabling access to account information as referred to in point (8) of Annex I of Directive (EU) 2015/2366. This right shall apply where the account(s) is accessible online.

(2) The account information service provider shall:

(a) provide services only where based on the payment service user's explicit consent;

(b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels;

(c) for each communication session, identify itself towards the account servicing payment service provider(s) of the payment service user and securely communicate with the account servicing payment service provider(s) and the payment service user, in accordance with procedures for authentication and secure communication as issued by the EBA;

(d) access only the information from designated payment accounts and associated payment transactions;

(e) not request sensitive payment data linked to the payment accounts;

(f) not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.

(3) In relation to accounts, the account servicing payment service provider shall:

(a) communicate securely with the account information service providers in accordance with procedures for authentication and secure communication as issued by the EBA; and

(b) treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons.

(4) The provision of account information services shall not be dependent on the existence of a contractual relationship between the account information service providers and the account servicing payment service providers for that purpose.

Limits of the use of the payment instrument and of the access to payment accounts by payment service providers

44. (1) Where a specific payment instrument is used for the purposes of giving consent, the payer and the payer's payment service provider may agree on spending limits for payment transactions executed through that payment instrument.

(2) If agreed in the framework contract, the payment service provider may reserve the right to block the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil its liability to pay.

(3) In such cases the payment service provider shall inform the payer of the blocking of the payment instrument and the reasons for it in an agreed manner, where possible, before the payment instrument is blocked and at the latest immediately thereafter, unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant European Union or national law.

(4) The payment service provider shall unblock the payment instrument or replace it with a new payment instrument once the reasons for blocking no longer exist.

(5) An account servicing payment service provider may deny an account information service provider or a payment initiation service provider access to a payment account for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that account information service provider or that payment initiation service provider, including the unauthorised or fraudulent initiation of a payment transaction. In such cases the account servicing payment service provider shall inform the payer that access to the payment account is denied and the reasons thereof in the form agreed. That information shall, where possible, be given to the payer before access is denied and at the latest immediately thereafter, unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant European Union or national law.

The account servicing payment service provider shall allow access to the payment account once the reasons for denying access no longer exist.

(6) In the cases referred to in Paragraph 44(5), the account servicing payment service provider shall immediately report the incident relating to the account information service provider or the payment initiation service provider to the Bank. The information shall include the relevant details of the case and the reasons for taking action. The Bank shall assess the case and shall, if necessary, take appropriate measures.

Obligations of the payment service user in relation to payment instruments and personalised security credentials

45. (1) The payment service user entitled to use a payment instrument shall:

(a) use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate;

(b) notify the payment service provider(s), or the entity specified by the latter, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

(2) For the purposes of Paragraph 45(1)(a), the payment service user shall, in particular, upon receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe.

Obligations of the payment service provider in relation to payment instruments

46. (1) The payment service provider issuing a payment instrument shall:

(a) make sure that the personalised security credentials are not accessible to parties other than the payment service user that is entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in Paragraph 45;

(b) refrain from sending an unsolicited payment instrument, except where a payment instrument already given to the payment service user is to be replaced;

(c) ensure that appropriate means are available at all times to enable the payment service user to make a notification pursuant to Paragraph 45(1)(b) or to request unblocking of the payment instrument pursuant to Paragraph 44(4);

(d) on request, the payment service provider shall provide the payment service user with the means to prove, for 18 months after notification, that the payment service user made a notification as referred to in Paragraph 46(1)(c);

(e) provide the payment service user with an option to make a notification pursuant to Paragraph 45(1)(b) free of charge and to charge, if at all, only replacement costs directly attributed to the payment instrument;

(f) prevent all use of the payment instrument once notification pursuant to Paragraph 45(1)(b) has been made.

(2) The payment service provider shall bear the risk of sending a payment instrument or any personalised security credentials relating to it to the payment service user.

Notification and rectification of unauthorised or incorrectly executed payment transactions

47. (1) The payment service user shall obtain rectification of an unauthorised or incorrectly executed payment transaction from the payment service provider only if the payment service user notifies the payment service provider without undue delay on becoming aware of any such transaction giving rise to a claim, including that under Paragraph 64, and no later than 13 months after the debit date.

The time limits for notification as specified in Paragraph 47(1) do not apply where the payment service provider has failed to provide or make available the information on the payment transaction in accordance with this Directive.

(2) Where a payment initiation service provider is involved, the payment service user shall obtain rectification from the account servicing payment service provider pursuant to Paragraph 47(1), without prejudice to Paragraphs 49(2) and 64(1), (2), (3), (4) and (5).

Evidence on authentication and execution of payment transactions

48. (1) Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.

If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

(2) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations as specified in Paragraph 45. The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user.

Payment service provider's liability for unauthorised payment transactions

49. (1) Without prejudice to Paragraph 47, in the case of an unauthorised payment transaction, the payer's payment service provider refunds the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing. Where applicable, the payer's payment service provider shall restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. This shall also

ensure that the credit value date for the payer's payment account shall be no later than the date the amount had been debited.

(2) Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund immediately, and in any event no later than by the end of the following business day the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.

If the payment initiation service provider is liable for the unauthorised payment transaction, it shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer, including the amount of the unauthorised payment transaction. In accordance with Paragraph 48(1) the burden shall be on the payment initiation service provider to prove that, within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

(3) Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the payer and the payment service provider or the contract concluded between the payer and the payment initiation service provider if applicable.

Payer's liability for unauthorised payment transactions

50. (1) By way of derogation from Paragraph 49, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.

Paragraph 50(1) shall not apply if:

(a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or

(b) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.

The payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Paragraph 45 with intent or gross negligence. In such cases, the maximum amount of EUR 50 shall not apply.

(2) Where the payer's payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. Where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider.

(3) The payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with Paragraph 45(1)(b) except where the payer has acted fraudulently.

If the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as specified in Paragraph 46(1)(c) the payer shall not be liable for the financial consequences resulting from use of that payment instrument, except where the payer has acted fraudulently.

Payment transactions where the transaction amount is not known in advance

51. (1) Where a payment transaction is initiated by or through the payee in the context of a card-based payment transaction and the exact amount is not known at the moment when the payer gives consent to execute the payment transaction, the payer's payment service provider may block funds on the payer's payment account only if the payer has given consent to the exact amount of the funds to be blocked.

(2) The payer's payment service provider shall release the funds blocked on the payer's payment account in Paragraph 51(1) without undue delay after receipt of the information about the exact amount of the payment transaction and at the latest immediately after receipt of the payment order.

Refunds for payment transactions initiated by or through a payee

52. (1) A payer is entitled to a refund from the payment service provider of an authorised payment transaction which was initiated by or through a payee and which has already been executed, if both of the following conditions are met:

(a) the authorisation did not specify the exact amount of the payment transaction when the authorisation was made;

(b) the amount of the payment transaction exceeded the amount the payer could reasonably have expected taking into account the previous spending pattern, the conditions in the framework contract and relevant circumstances of the case.

At the payment service provider's request, the payer shall bear the burden of proving such conditions are met.

The refund shall consist of the full amount of the executed payment transaction. The credit value date for the payer's payment account shall be no later than the date the amount was debited.

(2) Without prejudice to Paragraph 52(4), for direct debits as referred to in Article 1 of Regulation (EU) No 260/2012, the payer also has an unconditional right to a refund within the time limits laid down in Paragraph 53.

(3) However, for the purposes of Paragraph 52(1)(b), the payer shall not rely on currency exchange reasons if the reference exchange rate agreed with its payment service provider in accordance with Paragraphs 21(1)(d) and 28(3)(b) was applied.

(4) It may be agreed in a framework contract between the payer and the payment service provider that the payer has no right to a refund where:

(a) the payer has given consent to execute the payment transaction directly to the payment service provider; and

(b) where applicable, information on the future payment transaction was provided or made available in an agreed manner to the payer for at least 4 weeks before the due date by the payment service provider or by the payee.

Requests for refunds for payment transactions initiated by or through a payee

53. (1) A payer can request the refund referred to in Paragraph 52 of an authorised payment transaction initiated by or through a payee for a period of 8 weeks from the date on which the funds were debited.

(2) Within 10 business days of receiving a request for a refund, the payment service provider shall either refund the full amount of the payment transaction or provide a justification for refusing the refund and indicate where the payer may refer the matter to in accordance with Paragraphs 73 to 75, if the payer does not accept the reasons provided.

(3) The payment service provider's right under Paragraph 53(2) to refuse the refund shall not apply in the case set out in Paragraph 52(2).

CHAPTER 3
Execution of payment transactions

Section 1
Payment orders and amounts transferred

Receipt of payment orders

54. (1) The time of receipt is when the payment order is received by the payer's payment service provider.

The payer's account shall not be debited before receipt of the payment order. If the time of receipt is not on a business day for the payer's payment service provider, the payment order shall be deemed to have been received on the following business day. The payment service provider may establish a cut-off time near the end of a business day beyond which any payment order received shall be deemed to have been received on the following business day.

(2) If the payment service user initiating a payment order and the payment service provider agree that execution of the payment order shall start on a specific day or at the end of a certain period or on the day on which the payer has put funds at the payment service provider's disposal, the time of receipt for the purposes of Paragraph 59 is deemed to be the agreed day. If the agreed day is not a business day for the payment service provider, the payment order received shall be deemed to have been received on the following business day.

Refusal of payment orders

55. (1) Where the payment service provider refuses to execute a payment order or to initiate a payment transaction, the refusal and, if possible, the reasons for it and the procedure for correcting any factual mistakes that led to the refusal shall be notified to the payment service user, unless prohibited by other relevant European Union or national law.

The payment service provider shall provide or make available the notification in an agreed manner at the earliest opportunity, and in any case, within the periods specified in Paragraph 59.

The framework contract may include a condition that the payment service provider may charge a reasonable fee for such a refusal if the refusal is objectively justified.

(2) Where all of the conditions set out in the payer's framework contract are met, the payer's account servicing payment service provider shall not refuse to execute an authorised payment order irrespective of whether the payment order is initiated by a payer, including through a payment initiation service provider, or by or through a payee, unless prohibited by other relevant European Union or national law.
(3) For the purposes of Paragraphs 59 and 64 a payment order for which execution has been refused shall be deemed not to have been received.

Irrevocability of a payment order

56. (1) The payment service user shall not revoke a payment order once it has been received by the payer's payment service provider, unless otherwise specified in Paragraph 56.

(2) Where the payment transaction is initiated by a payment initiation service provider or by or through the payee, the payer shall not revoke the payment order after giving consent to the payment initiation service provider to initiate the payment transaction or after giving consent to execute the payment transaction to the payee.

(3) However, in the case of a direct debit and without prejudice to refund rights the payer may revoke the payment order at the latest by the end of the business day preceding the day agreed for debiting the funds.

(4) In the case referred to in Paragraph 54(2) the payment service user may revoke a payment order at the latest by the end of the business day preceding the agreed day.

(5) After the time limits laid down in Paragraph 56(1) to (4), the payment order may be revoked only if agreed between the payment service user and the relevant payment service providers. In the case referred to in Paragraph 56(2) and (3), the payee's agreement shall also be required. If agreed in the framework contract, the relevant payment service provider may charge for revocation.

Amounts transferred and amounts received

57. (1) The payment service provider(s) of the payer, the payment service provider(s) of the payee and any intermediaries of the payment service providers shall transfer the full amount of the payment transaction and refrain from deducting charges from the amount transferred.

(2) However, the payee and the payment service provider may agree that the relevant payment service provider deduct its charges from the amount transferred before crediting it to the payee. In such a case, the full amount of the payment transaction and charges shall be separated in the information given to the payee.

(3) If any charges other than those referred to in Paragraph 57(2) are deducted from the amount transferred, the payment service provider of the payer shall ensure that the payee receives the full amount of the payment transaction initiated by the payer. Where the payment

transaction is initiated by or through the payee, the payment service provider of the payee shall ensure that the full amount of the payment transaction is received by the payee.

Section 2
Execution time and value date

Application

58. (1) This Section applies to:

(a) payment transactions in euro;

(b) national payment transactions in the currency of the Member State outside the euro area;

(c) payment transactions involving only one currency conversion between the euro and the currency of a Member State outside the euro area, provided that the required currency conversion is carried out in the Member State outside the euro area concerned and, in the case of cross-border payment transactions, the cross-border transfer takes place in euro.

(2) This Section applies to payment transactions not referred to in the Paragraph 58(1), unless otherwise agreed between the payment service user and the payment service provider, with the exception of Paragraph 62, which is not at the disposal of the parties. However, if the payment service user and the payment service provider agree on a longer period than that set in Paragraph 59, for intra-European Union payment transactions, that longer period shall not exceed 4 business days following the time of receipt as referred to in Paragraph 54.

Payment transactions to a payment account

59. (1) The payer's payment service provider shall ensure that after the time of receipt as referred to in Paragraph 54, the amount of the payment transaction will be credited to the payee's payment service provider's account by the end of the following business day. That time limit may be extended by a further business day for paper-initiated payment transactions.

(2) The payment service provider of the payee shall value date and make available the amount of the payment transaction to the payee's payment account after the payment service provider has received the funds in accordance with Paragraph 62.

(3) The payee's payment service provider shall transmit a payment order initiated by or through the payee to the payer's payment service provider within the time limits agreed between the payee and the payment service provider, enabling settlement, as far as direct debit is concerned, on the agreed due date.

Absence of payee's payment account with the payment service provider

60. Where the payee does not have a payment account with the payment service provider, the funds shall be made available to the payee by the payment service provider who receives the funds for the payee within the time limit laid down in Paragraph 59.

Cash placed on a payment account

61. Where a consumer places cash on a payment account with that payment service provider in the currency of that payment account, the payment service provider shall ensure that the amount is made available and value dated immediately after receipt of the funds. Where the payment service user is not a consumer, the amount shall be made available and value dated at the latest on the following business day after receipt of the funds.

Value date and availability of funds

62. (1) The credit value date for the payee's payment account shall not be later than the business day on which the amount of the payment transaction is credited to the payee's payment service provider's account.

(2) The payment service provider of the payee shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account where, on the part of the payee's payment service provider, there is:

(a) no currency conversion; or

(b) a currency conversion between the euro and a Member State currency or between two Member State currencies.

The obligation laid down in Paragraph 62(2) shall also apply to payment transactions involving a sole payment service provider.

(3) The debit value date for the payer's payment account shall not be earlier than the time at which the amount of the payment transaction is debited to that payment account.

Section 3
Liability

Incorrect unique identifiers

63. (1) If a payment order is executed in accordance with the unique identifier, the payment order shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier.

(2) If the unique identifier provided by the payment service user is incorrect, the payment service provider shall not be liable as specified in Paragraph 64 for non-execution or defective execution of the payment transaction.

(3) However, the payer's payment service provider shall make reasonable efforts to recover the funds involved in the erroneous payment transaction. The payee's payment service provider shall cooperate in those efforts also by communicating to the payer's payment service provider all relevant information for the collection of funds.

In the event that such recovery of funds is not possible, the payer's payment service provider shall provide to the payer, upon written request, all information available to the payer's payment service provider and relevant to the payer in order for the payer to file a legal claim to recover the funds.

(4) If agreed in the framework contract, the payment service provider may charge the payment service user for recovery.

(5) If the payment service user provides information in addition to that specified in Paragraphs 21(1)(a) or 28(2)(b), the payment service provider shall be liable only for the execution of payment transactions in accordance with the unique identifier provided by the payment service user.

Payment service providers' liability for non-execution, defective or late execution of payment transactions

64. (1) Where a payment order is initiated directly by the payer, the payer's payment service provider shall, without prejudice to Paragraphs 47, 63(2) and (3) and 68, be liable to the payer for correct execution of the payment transaction, unless it can prove to the payer and, where relevant, to the payee's payment service provider that the payee's payment service provider received the amount of the payment transaction in accordance with Paragraph 59(1). In that case, the payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction.

(2) Where the payer's payment service provider is liable under Paragraph 64(1) it shall, without undue delay, refund to the payer the amount of the non-executed or defective payment transaction, and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.

The credit value date for the payer's payment account shall be no later than the date on which the amount was debited.

(3) Where the payee's payment service provider is liable under the Paragraph 64(1) it shall immediately place the amount of the payment transaction at the payee's disposal and, where applicable, credit the corresponding amount to the payee's payment account.

The credit value date for the payee's payment account shall be no later than the date on which the amount would have been value dated, had the transaction been correctly executed in accordance with Paragraph 62.

(4) Where a payment transaction is executed late, the payee's payment service provider shall ensure, upon the request of the payer's payment service provider acting on behalf of the payer, that the credit value date for the payee's payment account is no later than the date the amount would have been value dated had the transaction been correctly executed.

(5) In the case of a non-executed or defectively executed payment transaction where the payment order is initiated by the payer, the payer's payment service provider shall, regardless of liability under Paragraph 64(1) to (5), on request, make immediate efforts to trace the payment transaction and notify the payer of the outcome. This shall be free of charge for the payer.

(6) Where a payment order is initiated by or through the payee, the payee's payment service provider shall, without prejudice to Paragraphs 47, 63(2) and (3) and 68 be liable to the payee for correct transmission of the payment order to the payment service provider of the payer in accordance with Paragraph 59(3). Where the payee's payment service provider is liable under Paragraph 64(6), it shall immediately re-transmit the payment order in question to the payment service provider of the payer.

(7) In the case of a late transmission of the payment order, the amount shall be value dated on the payee's payment account no later than the date the amount would have been value dated had the transaction been correctly executed.

(8) In addition, the payment service provider of the payee shall, without prejudice to Paragraphs 47, 63(2) and (3) and 68, be liable to the payee for handling the payment transaction in accordance with its obligations as specified in Paragraph 62. Where the payee's payment service provider is liable under Paragraph 64(8), it shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account. The amount shall be value dated on the payee's payment account no later than the date the amount would have been value dated had the transaction been correctly executed.

(9) In the case of a non-executed or defectively executed payment transaction for which the payee's payment service provider is not liable under Paragraph 64(6) and (8), the payer's payment service provider shall be liable to the payer. Where the payer's payment service provider is so liable he shall, as appropriate and without undue delay, refund to the payer the amount of the non-executed or defective payment transaction and restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place. The credit value date for the payer's payment account shall be no later than the date the amount was debited.

(10) The obligation as specified in Paragraph 64(9) shall not apply to the payer's payment service provider where the payer's payment service provider proves that the payee's payment service provider has received the amount of the payment transaction, even if execution of payment transaction is merely delayed. If so, the payee's payment service provider shall value date the amount on the payee's payment account no later than the date the amount would have been value dated had it been executed correctly.

(11) In the case of a non-executed or defectively executed payment transaction where the payment order is initiated by or through the payee, the payee's payment service provider shall, regardless of liability under Paragraph 64(6) to (11), on request, make immediate efforts to trace the payment transaction and notify the payee of the outcome. This shall be free of charge for the payee.

(12) In addition, payment service providers shall be liable to their respective payment service users for any charges for which they are responsible, and for any interest to which the payment service user is subject as a consequence of non-execution or defective, including late, execution of the payment transaction.

Liability in the case of payment initiation services for non-execution, defective or late execution of payment transactions

65. (1) Where a payment order is initiated by the payer through a payment initiation service provider, the account servicing payment service provider shall, without prejudice to Paragraphs 47 and 63(2) and (3), refund to the payer the amount of the non- executed or defective payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.

The burden shall be on the payment initiation service provider to prove that the payment order was received by the payer's account servicing payment service provider in accordance with Paragraph 54 and that within its sphere of competence the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the non-execution, defective or late execution of the transaction.

(2) If the payment initiation service provider is liable for the non-execution, defective or late execution of the payment transaction, it shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer.

Additional financial compensation

66. Any financial compensation additional to that provided for under this Section may be determined in accordance with the law applicable to the contract concluded between the payment service user and the payment service provider.

Right of recourse

67. (1) Where the liability of a payment service provider as specified in Paragraphs 49, 64 and 65 is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary shall compensate the first payment service provider for any losses incurred or sums paid under Paragraphs 49, 64 and 65. That shall include compensation where any of the payment service providers fail to use strong customer authentication.

(2) Further financial compensation may be determined in accordance with agreements between payment service providers and/or intermediaries and the law applicable to the agreement concluded between them.

Abnormal and unforeseeable circumstances

68. No liability shall arise under Chapter 2 or 3 in cases of abnormal and unforeseeable circumstances beyond the control of the party pleading for the application of those circumstances, the consequences of which would have been unavoidable despite all efforts to the contrary, or where a payment service provider is bound by other legal obligations covered by European Union or national law.

CHAPTER 4
Data protection

Data protection

69. (1) The processing of personal data by payment systems and payment service providers shall be permitted when necessary to safeguard the prevention, investigation and detection of payment fraud. The provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive shall be carried out in accordance with the Data Protection Act (*Cap. 440 of the Laws of Malta*), 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, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) and any applicable legislation.

(2) Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.

CHAPTER 5
ICT and security risk management and authentication

Management of ICT and security risks

70. (1) Payment service providers shall establish a framework with appropriate mitigation measures and control mechanisms to manage the Information and Communication Technology (ICT) and security risks, relating to the payment services they provide. As part of that framework, payment service providers shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

(2) Payment service providers shall provide to the Bank on an annual basis, or at shorter intervals as determined by the Bank, an updated and comprehensive assessment of the ICT and security risk management relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

(3) The establishment, implementation and monitoring of the security measures, including certification processes where relevant, shall be in line with the provisions stipulated in Annex 3 of this Directive.

(4) The Bank shall cooperate in the area of ICT and security risk management associated with payment services, including the sharing of information, with the MFSA and other competent authorities, the ECB and, where relevant, the European Union Agency for Network and Information Security.

Incident reporting

71. (1) In the case of a major operational or security incident, payment service providers shall, without undue delay, where Malta is the home Member State, notify the Bank. For the classification of major operational or security incidents, and on the content, the format, including standard notification templates, and the procedures for notifying such incidents, payment service providers shall refer to Annex 1 of this Directive.

Where the incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident.

(2) Upon receipt of the notification referred to in Paragraph 71(1), the Bank shall, in cooperation with the MFSA, and without undue delay, provide the relevant details of the incident to the EBA and to the ECB. The Bank shall, in cooperation with the MFSA, assess the relevance of the incident to relevant authorities in Malta, and notify any such authorities accordingly. For the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities, the Bank, in cooperation with the MFSA, shall refer to Annex 1 of this Directive.

The Bank shall, in cooperation with the MFSA, cooperate with the EBA and the ECB for the purpose of assessing the relevance of the incident to other relevant European Union and national authorities in accordance with the obligations of the EBA and the ECB as laid down in Article 96(2) of Directive (EU) 2015/2366.

The Bank shall, on the basis of notifications received from the EBA and/or the ECB in accordance with their obligations as laid down in Article 96(2) of Directive (EU) 2015/2366, where appropriate and in cooperation with the MFSA, take all of the necessary measures to protect the immediate safety of the financial system.

(3) Payment service providers shall provide, at least on an annual basis, statistical data on fraud relating to different means of payment to the Bank in line with the procedures stipulated in Annex 4 of this Directive. The Bank shall, in cooperation with the MFSA, provide the EBA and the ECB with such data in an aggregated format in line with the procedures stipulated in Annex 4 of this Directive.

Authentication

72. (1) Payment service providers shall apply strong customer authentication where the payer:

(a) accesses its payment account online;

(b) initiates an electronic payment transaction;

(c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

(2) Further to Paragraph 72(1)(b), for the initiation of electronic remote payment transactions, payment service providers shall apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

(3) With regard to Paragraph 72(1), payment service providers shall have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

(4) Paragraph 72(2) and (3) shall also apply where payments are initiated through a payment initiation service provider. Paragraph 72(1) and (3) shall also apply when the information is requested through an account information service provider.

(5) Account servicing payment service providers shall allow the payment initiation service provider and the account information service provider to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user in accordance with Paragraph 72(1) and (3) and, where the payment initiation service provider is involved, in accordance with Paragraph 72(1) to (3).

(6) Provisions established in the Financial Institutions Rules on Security of Internet Payments of Credit, Payment and Electronic Money Institutions (FIR/04/2015) with regards to strong customer authentication are applicable but will be superseded by the regulatory technical standards referred to in Article 98 of Directive (EU) 2015/2366, 18 months after the date of entry into force of such regulatory technical standards.

CHAPTER 6
Dispute resolution, complaints procedure, ADR procedure and penalties

Dispute resolution

73. (1) Payment service providers shall put in place and apply adequate and effective complaint resolution procedures for the settlement of complaints of payment service users concerning the rights and obligations arising from the provisions of this Directive.

With respect to payment services provided in Malta, payment service providers shall make such complaint resolution procedures available in English and/or in Maltese or in any other language agreed upon between the payment service provider and the payment service user.

(2) Payment service providers shall make every possible effort to reply, on paper or on another durable medium, to the payment service users' complaints. Such a reply shall address all points raised, within an adequate timeframe and at the latest within 15 business days of receipt of the complaint. In exceptional situations, if the answer cannot be given within 15 business days for reasons beyond the control of the payment service provider, it shall be required to send a holding reply, clearly indicating the reasons for a delay in answering to the complaint and specifying the deadline by which the payment service user will receive the final reply. In any event, the deadline for receiving the final reply shall not exceed 35 business days.

(3) The payment service provider shall inform the payment service user, where such a payment service user is an eligible customer falling within the meaning of paragraph 74(1)(a), about the services offered by the Office of the Arbiter, which is competent to deal with disputes concerning the rights and obligations arising under this Directive.

(4) The information referred to in Paragraph 73(3) shall be mentioned in a clear, comprehensive and easily accessible way on the website of the payment service provider, where one exists, at the branch, and in the general terms and conditions of the contract between the payment service provider and the payment service user. The information referred to in Paragraph 73(3) shall also specify how the payment service user can access further information on the Office of the Arbiter and on the conditions for using such services.

Complaints

74. (1) Any complaint relating to an alleged infringement of this Directive by a payment service provider may be submitted by:

a) a payment service user, being an eligible customer in terms of the Arbiter for Financial Services Act;

b) a payment service user, not being an eligible customer in terms of the Arbiter for Financial Services Act;

c) other interested parties, including consumer associations.

(2) Complaints falling within the meaning of Paragraph 74(1)(a) shall be directed to the Office of the Arbiter.

(3) Complaints falling within the meaning of Paragraph 74(1)(b) and (c) shall be directed to the Bank.

(4) The procedures for complaints of alleged infringements of this Directive shall be in line with the provisions stipulated in Annex 2 of this Directive.

ADR Procedure

75. (1) Without prejudice to Paragraphs 73 and 74, a payment service user may resort to the Office of the Arbiter for the settlement of a dispute with a payment service provider concerning the rights and obligations arising under this Directive.

Provided that the preceding sub-paragraph shall not apply to a payment service user who is not an eligible customer in terms of the Arbiter for Financial Services Act.

(2) The Bank shall assist the Office of the Arbiter to cooperate effectively with other relevant authorities for the resolution of cross-border disputes concerning the rights and obligations arising under this Directive.

Penalties

76. (1) Where a payment service provider contravenes or fails to comply with a provision contained in this Directive, the Bank may impose an administrative penalty in accordance with Article 56 of the Central Bank of Malta Act (*Cap. 204 of the Laws of Malta*).

(2) Any administrative penalties imposed on payment service providers in accordance with Paragraph 76(1) and in line with provisions laid down in CBM Directive No.12 entitled 'Administrative Measures and Penalties for Infringements under the Central Bank of Malta Act' shall be effective, proportionate and dissuasive.

(3) The Bank may disclose to the public any administrative penalty that is imposed for infringement of the provisions of this Directive, unless such disclosure would seriously jeopardise the financial markets or cause disproportionate damage to the parties involved.

TITLE V
FINAL PROVISIONS

Obligation to inform consumers of their rights

77. (1) Payment service providers shall ensure that the user-friendly electronic leaflet, listing in a clear and easily comprehensible manner the rights of consumers under this Directive and related European Union law, as published by the European Commission in accordance with its obligations laid down in Article 106(1) and (2) of Directive (EU) 2015/2366, is made available in an accessible manner on their websites, if existing, and on paper at their branches, their agents and the entities to which their activities are outsourced.

(2) In respect of persons with disabilities, the provisions of Paragraph 77(1) shall be applied using appropriate alternative means, allowing the information to be made available in an accessible format.

(3) Payment service providers shall not charge their clients for making information available under Paragraph 77.

(4) The Bank shall also make available in an easily accessible manner on its website the leaflet referred to in Paragraph 77(1).

Full harmonisation

78. (1) Without prejudice to Article 2, Article 38(2), Article 55(6), Article 57(3), Article 58(3), Article 61(2) and (3), Article 62(5), Article 63(3) and the fourth subparagraph of Article 74(1) of Directive (EU) 2015/2366, for the purpose of full harmonisation at the European Union level, the Bank did not introduce provisions other than those laid down in that Directive.

(2) The Bank shall inform the European Commission of any of the options referred to in Paragraph 78(1), as well as of any subsequent changes. Such information will be made public by the European Commission on a website or other easily accessible means as per obligations laid down in Article 107(2) of Directive (EU) 2015/2366.

(3) Payment service providers shall not derogate, to the detriment of payment service users, from the provisions of this Directive except where explicitly provided for therein. However, payment service providers may decide to grant more favourable terms to payment service users than those laid down in this Directive.

Transposition

79. (1) By way of derogation from Paragraph 81, the application of the security measures referred to in Paragraphs 41, 42, 43 and Paragraph 72(1) to (5) shall apply from 18 months after the date of entry into force of the regulatory technical standards referred to in Article 98 of Directive (EU) 2015/2366.

(2) Until individual account servicing payment service providers comply with the regulatory technical standards referred to in Article 98 of Directive (EU) 2015/2366, account servicing payment service providers shall not abuse their non-compliance to block or obstruct the use of payment initiation and account information services for the accounts that they are servicing.

Validity of Direct Debit Mandates

80. (1) A payee authorisation to collect recurring direct debits, issued in Malta after 1 February 2014, shall be carried out in accordance with the technical requirements and obligations set out in Regulation (EU) No 260/2012.

(2) A payee authorisation to collect recurring direct debits, issued in Malta prior to 1 February 2014 shall remain valid after the said date, provided the direct debit mandate allows for unconditional refunds and refunds backdated to the date of the refunded payment where such refunds have been provided for within the framework of the existing direct debit mandate.

Entry into force

81. This Directive shall enter into force on the 13th of January 2018.

ANNEX 1
MAJOR INCIDENT REPORTING UNDER CBM DIRECTIVE NO 1

Scope

1. The Scope of this Annex is to adopt the provisions prescribed in the Guidelines on major incident reporting under Directive (EU) 2015/2366, issued by the EBA on the 27 July 2017.

2. This Annex applies in relation to the classification and reporting of major operational or security incidents in accordance with Paragraph 71 of this Directive. This Annex applies to all incidents included under the definition of 'major operational or security incident', which covers both external and internal events that could be either malicious or accidental.

3. This Annex applies also where the major operational or security incident originates outside the Union (e.g. when an incident originates in the parent company or in a subsidiary established outside the Union) and affects the payment services provided by a payment service provider located in the Union either directly (a payment-related service is carried out by the affected non-Union company) or indirectly (the capacity of the payment service provider to keep carrying out its payment activity is jeopardised in some other way as a result of the incident).

Definitions

4. For the purposes of this Annex, in addition to the definitions laid down in this Directive, the following definitions shall apply:

   (a) 'Operational or security incident' means a singular event or a series of linked events unplanned by the payment service provider which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment related services;

(b) ‘Integrity’ means the property of safeguarding the accuracy and completeness of assets (including data);

(c) ‘Availability’ means the property of payment-related services being accessible and usable by payment service users;

(d) ‘Confidentiality’ means the property that information is not made available or disclosed to unauthorized individuals, entities or processes;

(e) ‘Authenticity’ means the property of a source being what it claims to be;

(f) ‘Continuity’ means the property of an organisation’s processes, tasks and assets needed for the delivery of payment-related services being fully accessible and running at acceptable predefined levels;

(g) ‘Payment-related services’ means any business activity in the meaning of Paragraph 7(49) of this Directive, and all the necessary technical supporting tasks for the correct provision of payment services.

Classification as major incident

5. (1) Payment service providers should classify as major those operational or security incidents that fulfil:

(a) one or more criteria at the ‘Higher impact level’; or

(b) three or more criteria at the ‘Lower impact level’

as set out in Paragraph 5(4), and following the assessment set out in this Annex.

(2) Payment service providers should assess an operational or security incident against the following criteria and their underlying indicators:

i. Transactions affected

Payment service providers should determine the total value of the transactions affected, as well as the number of payments compromised as a percentage of the regular level of payment transactions carried out with the affected payment services;

ii. Payment service users affected

Payment service providers should determine the number of payment service users affected both in absolute terms and as a percentage of the total number of payment service users;

iii. Service downtime

Payment service providers should determine the period of time when the service will probably be unavailable for the payment service user or when the payment order, in the meaning of Paragraph 7(48) of this Directive, cannot be fulfilled by the payment service provider;

iv. Economic impact

Payment service providers should determine the monetary costs associated with the incident holistically and take into account both the absolute figure and, when applicable, the relative importance of these costs in relation to the size of the payment service provider (i.e. to the payment service provider's Tier 1 capital);

v. High level of internal escalation

Payment service providers should determine whether or not this incident has been or will probably be reported to their executive officers;

vi. Other payment service providers or relevant infrastructures potentially affected

Payment service providers should determine the systemic implications that the incident will probably have, i.e. its potential to spill over beyond the initially affected payment service provider to other payment service providers, financial market infrastructures and/or card payment schemes;

vii. Reputational impact

Payment service providers should determine how the incident can undermine users' trust in the payment service provider itself and, more generally, in the underlying service or the market as a whole.

(3) Payment service providers should calculate the value of the indicators according to the following methodology:

i. Transactions affected

As a general rule, payment service providers should understand as 'transactions affected' all domestic and cross-border transactions that have been or will probably be directly or indirectly affected by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered and those that were fraudulently ordered (whether the funds have been recovered or not).

Furthermore, payment service providers should understand the regular level of payment transactions to be the daily annual average of domestic and cross-border payment transactions carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. If payment service providers do not consider this figure to be representative (e.g. because of seasonality), they should use another, more representative, metric instead and convey to the Bank the underlying rationale for this approach in the corresponding field of template in Appendix 1.

ii. Payment service users affected

Payment service providers should understand as 'payment service users affected' all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected payment service provider that grants them access to the affected payment service, and that have suffered or will probably suffer the consequences of the incident. Payment service providers should resort to estimations based on past activity to determine the number of payment service users that may have been using the payment service during the lifetime of the incident.

In the case of groups, each payment service provider should consider only its own payment service users. In the case of a payment service provider offering operational

services to others, that payment service provider should consider only its own payment service users (if any), and the payment service providers receiving those operational services should assess the incident in relation to their own payment service users.

Furthermore, payment service providers should take as the total number of payment service users the aggregated figure of domestic and cross-border payment service users contractually bound to them at the time of the incident (or, alternatively, the most recent figure available) and with access to the affected payment service, regardless of their size or whether they are considered active or passive payment service users.

iii. Service downtime

Payment service providers should consider the period of time that any task, process or channel related to the provision of payment services is or will probably be down and, thus, prevents (i) the initiation and/or execution of a payment service and/or (ii) access to a payment account. Payment service providers should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for business as required for the execution of payment services as well as the closing hours and maintenance periods, where relevant and applicable. If payment service providers are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

iv. Economic impact

Payment service providers should consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident. Among other things, payment service providers should take into account expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, payment service providers should consider only those that are already known or very likely to materialize.

v. High level of internal escalation

Payment service providers should consider whether or not, as a result of its impact on payment-related services, the Chief Information Officer (or similar position) has been or will probably be informed about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. Furthermore, payment service providers should consider whether or not, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

vi. Other payment service providers or relevant infrastructures potentially affected

Payment service providers should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or card payment schemes that support them and other payment service providers. In particular, payment service providers should assess whether or not the incident has been or will probably be replicated at other payment service providers, whether or not it has affected or will probably affect the smooth functioning of financial market infrastructures and whether or not it has compromised or will probably compromise the sound operation of the financial system as a whole. Payment service providers should bear in mind various dimensions such as whether the component/software

affected is proprietary or generally available, whether the compromised network is internal or external and whether or not the payment service provider has stopped or will probably stop fulfilling its obligations in the financial market infrastructures of which it is a member.

vii. Reputational impact

Payment service providers should consider the level of visibility that, to the best of their knowledge, the incident has gained or will probably gain in the marketplace. In particular, payment service providers should consider the likelihood that the incident will cause harm to society as a good indicator of its potential to affect their reputation. Payment service providers should take into account whether or not (i) the incident has affected a visible process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.), (ii) regulatory obligations have been or will probably be missed, (iii) sanctions have been or will probably be breached or (iv) the same type of incident has occurred before.

(4) Payment service providers should assess an incident by determining, for each individual criterion, if the relevant thresholds in Table 1 are or will probably be reached before the incident is resolved.

Table 1: Thresholds

Criteria	Lower impact level	Higher impact level
Transactions affected	> 10% of the payment service provider's regular level of transactions (in terms of number of transactions) **AND** > EUR 100,000	> 25% of the payment service provider's regular level of transactions (in terms of number of transactions) **OR** > EUR 5 million
Payment service users affected	> 5,000 **AND** > 10% of the payment service provider's payment service users	> 50,000 **OR** > 25% of the payment service provider's payment service users
Service downtime	> 2 hours	Not applicable
Economic impact	Not applicable	> Max. (0.1% Tier 1 capital,* EUR 200,000) **OR** > EUR 5 million
High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is likely to be called upon
Other payment service providers or relevant infrastructures potentially affected	Yes	Not applicable
Reputational impact	Yes	Not applicable

**Tier 1 capital as defined in Article 25 of Regulation (EU) No 575/2013 of the European Parliament and of the Council, of 26 June 2013, on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.*

(5) Payment service providers should resort to estimations if they do not have actual data to support their judgments of whether or not a given threshold is or will probably be reached before the incident is resolved (e.g. this could happen during the initial investigation phase).

(6) Payment service providers should carry out this assessment on a continuous basis during the lifetime of the incident, to identify any possible status change, either upwards (from non-major to major) or downwards (from major to non-major).

Notification Process

6. (1) Payment service providers should collect all relevant information, produce an incident report using the template in Appendix 1 and submit it to the Bank. Payment service providers should fill out the template following the instructions in Appendix 2.

(2) Payment service providers should also use the template in Appendix 1 to inform the Bank throughout the lifetime of the incident (i.e. for initial, intermediate and final reports, as described in Paragraph 6(7) to (21) of this Annex). Payment service providers should complete the template in Appendix 1 in an incremental manner, on a best effort basis, as more information becomes readily available in the course of their internal investigations.

(3) Payment service providers should also present to the Bank, if applicable, a copy of the information provided (or that will be provided) to their users, as laid down in the second sub-paragraph of Paragraph 71(1) of this Directive, as soon as it is available.

(4) Payment service providers should furnish the Bank, if available and deemed relevant for the Bank, with any additional information by appending supplementary documentation to the standardised template as one or various annexes.

(5) Payment service providers should follow up on any requests from the Bank to provide additional information or clarifications regarding already submitted documentation.

(6) Payment service providers should at all times preserve the confidentiality and integrity of the information exchanged with the Bank and also authenticate themselves properly towards the Bank.

Initial Report

(7) Payment service providers should submit an initial report to the Bank when a major operational or security incident is first detected.

(8) Payment service providers should send the initial report to the Bank within 4 hours from the moment the major operational or security incident was first detected, or, if the reporting channels of the Bank are known not to be available or operational at that time, as soon as they become available/operational again.

(9) Payment service providers should also submit an initial report to the Bank when a previously non-major incident becomes a major incident. In this particular case, payment service providers should send the initial report to the Bank immediately after the change of status is identified, or, if the reporting channels of the Bank are known not to be available or operational at that time, as soon as they become available/operational again.

(10) Payment service providers should include headline-level information (i.e. section A of the template in Appendix 1) in their initial reports, thus featuring some basic characteristics of the incident and its expected consequences based on the information available immediately after it was detected or reclassified. Payment service providers should resort to estimations when actual data are not available. Payment service providers should also include in their initial report the date for the next update, which should be as soon as possible and under no circumstances go beyond 3 business days.

Intermediate Report

(11) Payment service providers should submit intermediate reports every time they consider that there is a relevant status update and, as a minimum, by the date for the next update indicated in the previous report (either the initial report or the previous intermediate report).

(12) Payment service providers should submit to the Bank a first intermediate report with a more detailed description of the incident and its consequences (section B of the template in Appendix 1). Moreover, payment service providers should produce additional intermediate reports by updating the information already provided in sections A and B of the template in Appendix 1 at least, when they become aware of new relevant information or significant changes since the previous notification (e.g. whether the incident has escalated or decreased, new causes identified or actions taken to fix the problem). In any case, payment service providers should produce an intermediate report at the request of the Bank.
(13) As in the case of initial reports, when actual data are not available payment service providers should make use of estimations.

Final Report

(17) Payment service providers should send a final report when the root cause analysis has taken place (regardless of whether or not mitigation measures have already been implemented or the final root cause has been identified) and there are actual figures available to replace any estimates.

(18) Payment service providers should deliver the final report to the Bank within a maximum of 2 weeks after business is deemed back to normal. Payment service providers needing an extension of this deadline (e.g. if there are no actual figures on the impact available yet) should contact the Bank before it has lapsed and provide an adequate justification for the delay, as well as a new estimated date for the final report.

(19) Should payment service providers be able to provide all the information required in the final report (i.e. section C of the template in Appendix 1) within the 4-hour window since the incident was detected, they should aim to submit in their initial report the information related to initial, last intermediate and final reports.

(20) Payment service providers should aim to include in their final reports full information, i.e. (i) actual figures on the impact instead of estimations (as well as any other update needed in sections A and B of the template in Appendix 1) and (ii) section C of the template in Appendix 1, which includes the root cause, if already known, and a summary of measures adopted or planned to be adopted to remove the problem and prevent its recurrence in the future.

(21) Payment service providers should also send a final report when, as a result of the continuous assessment of the incident, they identify that an already reported incident no longer fulfills the criteria to be considered major and is not expected to fulfill them before the incident is resolved. In this case, payment service providers should send the final report as soon as this circumstance is detected and, in any case, by the estimated date for the next report. In this particular situation, instead of filling out section C of the template in Appendix 1,

payment service providers should tick the box 'incident reclassified as non-major' and explain the reasons justifying this downgrading.

Delegated and consolidated reporting

7. (1) Where permitted by the Bank, in collaboration with the MFSA, payment service providers wishing to delegate reporting obligations under this Directive to a third party should inform the Bank and ensure the fulfillment of the following conditions:

    (a) The formal contract or, where applicable, existing internal arrangements within a group, underpinning the delegated reporting between the payment service provider and the third party unambiguously defines the allocation of responsibilities of all parties. In particular, it clearly states that, irrespective of the possible delegation of reporting obligations, the affected payment service provider remains fully responsible and accountable for the fulfilment of the requirements set out in Paragraph 71 of this Directive and for the content of the information provided to the Bank;

    (b) The delegation complies with the requirements for the outsourcing of important operational functions as set out in:

        i. Article 19(6) of Directive (EU) 2015/2366 as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and in the Banking Act (*Cap. 371 of the Laws of Malta*) in relation to credit institutions, payment institutions and e-money institutions, applicable mutatis mutandis in accordance with Article 3 of Directive 2009/110/EC as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*); or

        ii. the CEBS Guidelines on outsourcing in relation to credit institutions;

    (c) The information is submitted to the Bank in advance and, in any case, following any deadlines and procedures established by the Bank, where applicable;

    (d) The confidentiality of sensitive data and the quality, consistency, integrity and reliability of the information to be provided to the Bank is properly ensured.

    (2) Payment service providers wishing to allow the designated third party to fulfill the reporting obligations in a consolidated way (i.e. by presenting one single report referred to several payment service providers affected by the same major operational or security incident) should inform the Bank, include the contact information included under 'Affected payment service provider' in the template in Appendix 1 and make certain that the following conditions are satisfied:

    (a) Include this provision in the contract underpinning the delegated reporting;

    (b) Make the consolidated reporting conditional on the incident's being caused by a disruption in the services provided by the third party;

    (c) Confine the consolidated reporting to payment service providers established in Malta;

    (d) Ensure that the third party assesses the materiality of the incident for each affected payment service provider and includes in the consolidated report only those payment service providers for which the incident is classified as major. Furthermore, ensure

that, in case of doubt, a payment service provider is included in the consolidated report as long as there is no evidence that it should not;

(e) Ensure that, when there are fields of the template in Appendix 1 where a common answer is not possible (e.g. section B2, B4 or C3), the third party either (i) fills them out individually for each affected payment service provider, further specifying the identity of each payment service provider to which the information relates, or (ii) uses ranges, in those fields where this is an option, representing the lowest and highest values as observed or estimated for the different payment service providers;

(f) Payment service providers should ensure that the third party keeps them informed at all times of all the relevant information regarding the incident and all the interactions that the third party may have with the Bank and of the contents thereof, but only as far as is compatible with avoiding any breach of confidentiality as regards the information that relates to other payment service providers.

(3) Payment service providers should not delegate their reporting obligations before informing the Bank or after having been informed that the outsourcing agreement does not meet the requirements referred to in Paragraph 7(1)(b) of this Annex.

(4) Payment service providers wishing to withdraw the delegation of their reporting obligations should communicate this decision to the Bank, in accordance with the deadlines and procedures established by the latter, in collaboration with the MFSA. Payment service providers should also inform the Bank of any material development affecting the designated third party and its ability to fulfill the reporting obligations.

(5) Payment service providers should materially complete their reporting obligations without any recourse to external assistance whenever the designated third party fails to inform the Bank of a major operational or security incident in accordance with Paragraph 71 of this Directive and this Annex. Furthermore, payment service providers should ensure that an incident is not reported twice, individually by said payment service provider and once again by the third party.

Operational and security policy

8. Payment service providers should ensure that their general operational and security policy clearly defines all the responsibilities for incident reporting under this Directive, as well as the processes implemented to fulfill the requirements defined in this Annex.

Assessment of the relevance of the incident

9. (1) The Bank, in collaboration with the MFSA, should assess the relevance of a major operational or security incident to other domestic authorities, taking as a basis their own expert opinion and using the following criteria as primary indicators of the importance of said incident:

(a) The causes of the incident are within the regulatory remit of the other domestic authority (i.e. its field of competence);

(b) The consequences of the incident have an impact on the objectives of another domestic authority (e.g. safeguarding of financial stability);

(c) The incident affects, or could affect, payment service users on a wide scale;

(d) The incident is likely to receive, or has received, wide media coverage.

(2) The Bank, in collaboration with the MFSA, should carry out this assessment on a continuous basis during the lifetime of the incident, to identify any possible change that could make an incident relevant that was previously not considered as such.

Information to be shared with other domestic authorities

10. (1) Notwithstanding any other legal requirement to share incident-related information with other domestic authorities, the Bank, in collaboration with the MFSA, should provide information about major operational or security incidents to the domestic authorities identified following the application of Paragraph 9(1) (i.e. 'other relevant domestic authorities'), as a minimum, at the time of receiving the initial report (or, alternatively, the report that prompted the sharing of information) and when they are notified that business is back to normal (i.e. last intermediate report).

(2) The Bank, in collaboration with the MFSA should submit to other relevant domestic authorities the information needed to provide a clear picture of what happened and the potential consequences. To do so, they should provide, as a minimum, the information given by the payment service provider in the following fields of the template (either in the initial or in the intermediate report):

(a) date and time of detection of the incident;

(b) date and time of beginning of the incident;

(c) date and time when the incident was restored or is expected to be restored;

(d) short description of the incident (including non-sensitive parts of the detailed description);

(e) short description of measures taken or planned to be taken to recover from the incident;

(f) description of how the incident could affect other PSPs and/or infrastructures;

(g) description (if any) of the media coverage;

(h) cause of the incident.

(3) The Bank, in collaboration with the MFSA, should conduct proper anonymisation, as needed, and leave out any information that could be subject to confidentiality or intellectual property restrictions before sharing any incident-related information with other relevant domestic authorities. Nevertheless, the Bank, in collaboration with the MFSA, should provide other relevant domestic authorities with the name and address of the reporting payment service provider when said domestic authorities can guarantee that the information will be treated confidentially.

(4) The Bank, in collaboration with the MFSA should at all times preserve the confidentiality and integrity of the information stored and exchanged with other relevant domestic authorities

and also authenticate themselves properly towards other relevant domestic authorities. In particular, the Bank, in collaboration with the MFSA, should treat all information received under this Annex in accordance with the professional secrecy obligations set out in Directive (EU) 2015/2366 as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and in the Banking Act (*Cap. 371 of the Laws of Malta*), without prejudice to applicable Union law and national requirements.

Information to be shared with the EBA and the ECB

11. The Bank, in collaboration with the MFSA, should always provide the EBA and the ECB with all reports received from (or on behalf of) payment service providers affected by a major operational or security incident (i.e. initial, intermediate and final reports).

Communication

12. (1) The Bank, in collaboration with the MFSA, should at all times preserve the confidentiality and integrity of the information stored and exchanged with the EBA and the ECB and also authenticate themselves properly towards the EBA and the ECB. In particular, the Bank, in collaboration with the MFSA, should treat all information received under this Annex in accordance with the professional secrecy obligations set out in Directive (EU) 2015/2366 as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and in the Banking Act (*Cap. 371 of the Laws of Malta*), without prejudice to applicable Union law and national requirements.

(2) To avoid delays in the transmission of incident-related information to the EBA/ECB and help minimise the risks of operational disruptions, the Bank, in collaboration with the MFSA, should support appropriate means of communication.

Appendix 1 - Reporting templates for payment service providers

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date: DD/MM/YYYY — Time: HH:MM

Incident identification number, if applicable (for interim and final reports):

A - Initial report

A 1 - GENERAL DETAILS

Type of report					
Type of report	☐ Individual ☐ Consolidated				
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT			
Overall impact	☐ Integrity ☐ Availability	☐ Confidentiality ☐ Authenticity	☐ Continuity
Transactions affected [2]	Number of transactions affected As a % of regular number of transactions Value of transactions affected in EUR Comments:		☐ Actual figure ☐ Estimation ☐ Actual figure ☐ Estimation ☐ Actual figure ☐ Estimation
Payment service users affected [3]	Number of payment service users affected As a %-of total payment service users		☐ Actual figure ☐ Estimation ☐ Actual figure ☐ Estimation
Service downtime [4]	Total service downtime	DD:HH:MM	☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR Indirect costs in EUR		☐ Actual figure ☐ Estimation ☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe		
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures		
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)		
B 3 - INCIDENT DESCRIPTION			
Type of Incident	☐ Operational ☐ Security		
Cause of incident	☐ Under investigation ☐ External attack ☐ Internal attack → Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other If Other, specify ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other If Other, specify		
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly	If indirectly, please provide the service provider's name	
B 4 - INCIDENT IMPACT			
Building(s) affected (Address), if applicable			
Commercial channels affected	☐ Branches ☐ E-banking ☐ Telephone banking ☐ Mobile banking ☐ ATMs ☐ Point of sale ☐ Other If Other, specify:		
Payment services affected	☐ Cash placement on a payment account ☐ Cash withdrawal from a payment account ☐ Operations required for operating a payment account ☐ Acquiring of payment instruments ☐ Credit transfers ☐ Direct debits ☐ Card payments ☐ Issuing of payment instruments ☐ Money remittance ☐ Payment initiation services ☐ Account information services ☐ Other If Other, specify:		
Functional areas affected	☐ Authentication/authorisation ☐ Communication ☐ Clearing ☐ Direct settlement ☐ Indirect settlement ☐ Other If Other, specify:		
Systems and components affected	☐ Application/software ☐ Database ☐ Hardware ☐ Network/infrastructure ☐ Other If Other, specify:		
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)		
B 5 - INCIDENT MITIGATION			
Which actions/measures have been taken so far or are planned to recover from the incident?			
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated? If so, when? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM		
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO		

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - additional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐ YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐ YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐ YES ☐ NO
If so, please provide details	

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5000 and > 10% payment service users; > 50000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs		
PSP Name	**PSP Unique Identification Number**	**PSP Authorisation number**

Appendix 2 - Instructions for filling out the templates

Payment service providers should fill out the relevant section of the template in Appendix 1, depending on the reporting phase they are in: section A for the initial report, section B for intermediate reports and section C for the final report. All fields are mandatory, unless it is clearly specified otherwise.

Headline

Initial report: this is the first notification that the payment service provider submits to the Bank.

Intermediate report: this is an update of a previous (initial or intermediate) report on the same incident.

Last intermediate report: this informs the Bank that regular activities have been recovered and business is back to normal, so no more intermediate reports will be submitted.

Final report: it is the last report the payment service provider will send on the incident, since **(i)** a root cause analysis has already been carried out and estimations can be replaced with real figures or **(ii)** the incident is not considered major any more.

Incident reclassified as non-major: the incident no longer fulfills the criteria to be considered major and is not expected to fulfill them before it is resolved. Payment service providers should explain the reasons for this downgrading.

Report date and time: exact date and time of submission of the report to the Bank. Incident identification number, if applicable (for intermediate and final report): the reference number issued by the Bank at the time of the initial report to uniquely identify the incident, if applicable (i.e. if such a reference is provided by the Bank).

A – Initial Report

A1 – General Details

Type of report:

> **Individual:** the report refers to a single payment service provider.
>
> **Consolidated:** the report refers to several payment service providers making use of the consolidated reporting option. The fields under 'Affected Payment Service Provider' should be left blank (with the exception of the field 'Country/countries affected by the incident') and a list of the payment service providers included in the report should be provided by filling in the corresponding table (Consolidated report – List of payment service providers).

Affected payment service provider: refers to the payment service provider that is experiencing the incident.

> **Payment service provider name:** full name of the payment service provider subject to the reporting procedure as it appears in the applicable official national payment service provider registry.
>
> **Payment service provider unique identification number, if relevant:** the relevant unique identification number used in each Member State to identify the payment service provider, to be provided by the payment service provider if the field payment service provider authorisation number' is not filled in.

Payment service provider authorisation number: home Member State authorisation number.

Head of group: in case of groups of entities as defined in Paragraph 7(29) of this Directive, please indicate the name of the head entity.

Home country: Member State in which the registered office of the payment service provider is situated; or if the payment service provider has, under its national law, no registered office, the Member State in which its head office is situated.

Country/countries affected by the incident: country or countries where the impact of the incident has materialised (e.g. several branches of a payment service provider located in different countries are affected). It may or may not be Malta.

Primary contact person: first name and surname of the person responsible for reporting the incident or, if a third party reports on behalf of the affected payment service provider, first name and surname of the person in charge of the incident management/risk department or similar area, at the affected payment service provider.

Email: email address to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email.

Telephone: telephone number to call with any requests for further clarifications, if needed. It can be either a personal or a corporate phone number.

Secondary contact person: first name and surname of an alternative person who could be contacted by the Bank to inquiry about an incident when the primary contact person is not available. If a third party reports on behalf of the affected payment service provider, first name and surname of an alternative person in the incident management/risk department or similar area, at the affected payment service provider.

Email: email address of the alternative contact person to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number of the alternative contact person to call with any requests for further clarifications, if needed. It can be either a personal or a corporate phone number.

Reporting entity: this section should be completed if a third party fulfills the reporting obligations on behalf of the affected payment service provider.

Name of the reporting entity: full name of the entity that reports the incident, as it appears in the applicable official national business registry.

Unique identification number, if relevant: the relevant unique identification number used in the country where the third party is located to identify the entity that is reporting the incident, to be provided by the reporting entity if the field 'Authorisation number' is not filled in.

Authorisation number, if applicable: the authorisation number of the third party in the country where it is located, when applicable.

Primary contact person: first name and surname of the person responsible for reporting the incident.

Email: email address to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email.

Telephone: telephone number to call with any requests for further clarifications, if needed. It can be either a personal or a corporate phone number.

Secondary contact person: first name and surname of an alternative person in the entity that is reporting the incident who could be contacted by the Bank when the primary contact person is not available.

Email: email address of the alternative contact person to which any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate email address.

Telephone: telephone number of the alternative contact person to call with any requests for further clarifications could be addressed, if needed. It can be either a personal or a corporate phone number.

A2 – Incident detection and initial classification

Date and time of detection of the incident: date and time at which the incident was first identified.

Incident detected by: indicate whether the incident was detected by a payment service user, some other party from within the payment service provider (e.g. internal audit function) or an external party (e.g. external service provider). If it was none of those, please provide an explanation in the corresponding field.

Short and general description of the incident: please explain briefly the most relevant issues of the incident, covering possible causes, immediate impacts, etc.

What is the estimated time for the next update?: indicate the estimated date and time for the submission of the next update (interim or final report).

B – Intermediate report

B1 – General details

More detailed description of the incident: describe the main features of the incident, covering at least the points featured in the questionnaire (what specific issue the payment service provider is facing, how it started and developed, possible connection with a previous incident, consequences, especially for payment service users, etc.).

Date and time of beginning of the incident: date and time at which the incident started, if known.

Incident status:

Diagnostics: the characteristics of the incident have just been identified.

Repair: the attacked items are being reconfigured.

Recovery: the failed items are being restored to their last recoverable state.

Restoration: the payment-related service is being provided again.

Date and time when the incident was restored or is expected to be restored: indicate the date and time when the incident was or is expected to be under control and business was or is expected to be back to normal.

B2 – Incident classification/Information on the incident

Overall impact: please indicate which dimensions have been affected by the incident. Multiple boxes may be ticked.

> **Integrity:** the property of safeguarding the accuracy and completeness of assets (including data).
>
> **Availability:** the property of payment-related services being accessible and usable by payment service users.
>
> **Confidentiality:** the property that information is not made available or disclosed to unauthorised individuals, entities or processes.
>
> **Authenticity:** the property of a source being what it claims to be.
>
> **Continuity:** the property of an organisation's processes, tasks and assets needed for the delivery of payment-related services being fully accessible and running an acceptable predefined levels.

Transactions affected: Payment service providers should indicate which thresholds are or will probably be reached by the incident, if any, and the related figures: number of transactions affected, percentage of transactions affected in relation to the number of payment transactions carried out with the same payment services that have been affected by the incident, and total value of the transactions.

Payment service providers should provide specific values for these variables, which may be either actual figures or estimations. Entities reporting on behalf of several payment service providers (i.e. consolidated reporting) may provide value ranges instead, representing the lowest and highest values observed or estimated within the group of payment service providers included in the report, separated by a hyphen. As a general rule, payment service providers should understand as 'transactions affected' all domestic and cross-border transactions that have been or will probably be directly or indirectly affected by the incident and, in particular, those transactions that could not be initiated or processed, those for which the content of the payment message was altered, and those that were fraudulently ordered (whether the funds have been recovered or not).

Furthermore, payment service providers should understand the regular level of payment transactions to be the daily annual average of domestic and cross-border payment transactions carried out with the same payment services that have been affected by the incident, taking the previous year as the reference period for calculations. If payment service providers do not consider this figure to be representative (e.g. because of seasonality), they should use another, more representative, metric instead and convey to the Bank the underlying rationale for this approach in the field 'Comments'.

Payment service users affected: Payment service providers should indicate which thresholds are or will probably be reached by the incident, if any, and the related figures: total number of payment service users that have been affected and percentage of payment service users affected in relation to the total number of payment service users. Payment service providers should provide concrete values for these variables, which may be either actual figures or estimations.

Entities reporting on behalf of several payment service providers (i.e. consolidated reporting) may provide value ranges instead, representing the lowest and highest values observed or estimated within the group of payment service providers included in the report, separated by a hyphen. Payment service providers should understand as 'payment service users affected' all customers (either domestic or from abroad, consumers or corporates) that have a contract with the affected payment service provider that grants them access to the affected payment service, and that have suffered or will probably suffer the consequences of the incident.

Payment service providers should resort to estimations based on past activity to determine the number of payment service users that may have been using the payment service during the lifetime of the incident. In the case of groups, each payment service provider should consider only its own payment service users. In the case of a payment service provider offering operational services to others, that a payment service provider should consider only its own payment service users (if any), and the payment service providers receiving those operational services should also assess the incident in relation to their own payment service users. Furthermore, payment service providers should take as the total number of payment service users the aggregated figure of domestic and cross-border payment service users contractually bound to them at the time of the incident (or, alternatively, the most recent figure available) and with access to the affected payment service, regardless of their size or whether they are considered active or passive payment service users.

Service downtime: Payment service providers should indicate if the threshold is or will probably be reached by the incident and the related figure: total service downtime. Payment service providers should provide concrete values for this variable, which may be either actual figures or estimations. Entities reporting on behalf of several payment service providers (i.e. consolidated reporting) may provide a value range instead, representing the lowest and highest values observed or estimated within the group of payment service providers included in the report, separated by a hyphen. Payment service providers should consider the period of time that any task, process or channel related to the provision of payment services is or will probably be down and, thus, prevents **(i)** the initiation and/or execution of a payment service and/or **(ii)** access to a payment account. Payment service providers should count the service downtime from the moment the downtime starts, and they should consider both the time intervals when they are open for business as required for the execution of payment services as well as the closing hours and maintenance periods, where relevant and applicable.

If payment service providers are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime is detected.

Economic impact: Payment service providers should indicate if the threshold is or will probably be reached by the incident and the related figures: direct costs and indirect costs. Payment service providers should provide concrete values for these variables, which may be either actual figures or estimations. Entities reporting on behalf of several payment service providers (i.e. consolidated reporting) may provide a value range instead, representing the lowest and highest values observed or estimated within the group of payment service providers included in the report, separated by a hyphen. Payment service providers should consider both the costs that can be connected to the incident directly and those which are indirectly related to the incident. Among other things, the payment service providers should take into account expropriated funds or assets, replacement costs of hardware or software, other forensic or remediation costs, fees due to non-compliance with contractual obligations, sanctions, external liabilities and lost revenues. As regards the indirect costs, payment service providers should consider only those that are already known or very likely to materialise.

> **Direct costs:** amount of money (euro) directly cost by the incident, including funds needed to rectify the incident (e.g. expropriated funds or assets, replacement costs of hard- and software, fees due to non-compliance with contractual obligations).
>
> **Indirect costs:** amount of money (euro) indirectly cost by the incident (e.g. customer redress/compensation costs, revenues lost as a result of missed business opportunities, potential legal costs).

High level of internal escalation: Payment service providers should consider whether or not, as a result of its impact on payment-related services, the Chief Information Officer (or similar position) has been or will probably be informed about the incident outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. In the case of delegated reporting, the escalation would take place within the third party. Furthermore, payment service providers should

consider whether or not, as a result of the impact of the incident on payment-related services, a crisis mode has been or is likely to be triggered.

Other payment service providers or relevant infrastructures potentially affected: payment service providers should assess the impact of the incident on the financial market, understood as the financial market infrastructures and/or card payment schemes that support it and the rest of the payment service providers. In particular, payment service providers should assess whether or not the incident has been or will probably be replicated at other payment service providers, whether or not it has affected or will probably affect the smooth functioning of financial market infrastructures and whether or not it has compromised or will probably compromise the solidity of the financial system as a whole. The payment service providers should bear in mind various dimensions such as whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external and whether or not the payment service providers has stopped or will probably stop fulfilling its obligations in the financial market infrastructures of which it is a member.

Reputational impact: Payment service providers should consider the level of visibility that, to the best of their knowledge, the incident has gained or will probably gain in the marketplace. In particular, the payment service providers should consider the likelihood that the incident will cause harm to society as a good indicator of its potential to affect their reputation. Payment service providers should take into account whether or not (i) the incident has affected a visible process and is therefore likely to receive or has already received media coverage (considering not only traditional media, such as newspapers, but also blogs, social networks, etc.), **(ii)** regulatory obligations have been or are likely to be missed, **(iii)** sanctions have been or are likely to be breached or **(iv)** the same type of incident has occurred before.

B3 - Incident description

Type of Incident: indicate whether, to the best of your knowledge, it is an operational or a security incident.

> **Operational:** incident stemming from inadequate or failed processes, people and systems or events of force majeure that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services.
>
> **Security:** unauthorised access, use, disclosure, disruption, modification or destruction of the payment service provider's assets that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services. This may happen when, among other things, the payment service provider experiences cyber-attacks, inadequate design or implementation of security policies, or inadequate physical security.

Cause of incident: indicate the cause of the incident or, if it is not known yet, the one that it is most likely to be. Multiple boxes may be ticked.

> **Under investigation:** the cause has not been determined yet.
>
> **External attack:** the source of the cause comes from outside, and is intentionally targeting the payment service providers (e.g. malware attacks).
>
> **Internal attack:** the source of the cause comes from inside, and is intentionally targeting the payment service providers (e.g. internal fraud).
>
> **Type of attack:**
>
> > **Distributed/Denial of Service (D/DoS):** an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Infection of internal systems: harmful activity that attacks computer systems, trying to steal hard disk space or CPU time, access private information, corrupt data, spam contacts, etc.

Targeted intrusion: unauthorised act of spying, snooping and stealing information through cyberspace.

Other: any other type of attack the payment service provider may have suffered, either directly or through a service provider. In particular, if there has been an attack aimed at the authorisation and authentication process, this box should be ticked. Details should be added in the free text field.

External events: the cause is associated with events generally outside the organisation's control (e.g. natural disasters, legal issues, business issues and service dependencies).

Human error: the incident was caused by the unintentional mistake of a person, be it as part of the payment procedure (e.g. uploading the wrong payments batch file to the payments system) or related to it somehow (e.g. the power is accidentally cut off and the payment activity is put on hold).

Process failure: the cause of the incident was poor design or execution of the payment process, the process controls and/or the supporting processes (e.g. process for change/migration, testing, configuration, capacity, monitoring).

System failure: the cause of the incident is associated with inadequate design, execution, components, specifications, integration or complexity of the systems that support the payment activity.

Other: the cause of the incident is none of the above. Further details should be provided in the free text field.

Was the incident affecting you directly, or indirectly through a service provider?: an incident can target a payment service provider directly or affect it indirectly, through a third party. In the case of an indirect impact, please provide the name of the service provider(s).

B4 – Incident impact

Building(s) affected (Address), if applicable: if a physical building is affected, please indicate its address.

Commercial channels affected: indicate the channel or channels of interaction with payment service users that have been affected by the incident. Multiple boxes may be ticked.

Branches: place of business (other than the head office) which is a part of a payment service provider, has no legal personality and carries out directly some or all of the transactions inherent in the business of a payment service provider. All of the places of the business set up in the same Member State by a payment service provider with a head office in another Member State should be regarded as a single branch.

E-banking: the use of computers to carry out financial transactions over the internet.

Telephone banking: the use of telephones to carry out financial transactions.

Mobile banking: the use of a specific banking application on a smartphone or similar device to carry out financial transactions.

ATMs: electromechanical devices that allow payment service users to withdraw cash from their accounts and/or access other services.

Point of sale: physical premise of the merchant at which the payment transaction is initiated.

Other: the commercial channel affected is none of the above. Further details should be provided in the free text field.

Payment services affected: indicate those payment services that are not working properly as a result of the incident. Multiple boxes may be ticked.

Cash placement on a payment account: the handing of cash to a payment service provider to credit it on a payment account.

Cash withdrawal from a payment account: the request received by a payment service provider from its payment service user to provide cash and debit his/her payment account by the corresponding amount.

Operations required for operating a payment account: those actions needed to be performed in a payment account to activate, deactivate and/or maintain it (e.g. opening, blocking).

Acquiring of payment instruments: a payment service consisting in a payment service provider from contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.

Credit transfers: a payment service for crediting a payee's payment account with a payment transaction or a series of payment transactions from a payer's payment account by the payment service provider which holds the payer's payment account, based on an instruction given by the payer.

Direct debits: a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider.

Card payments: a payment service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunication, digital or IT device, or software if this results in a debit or a credit card transaction. Card-based payment transactions exclude transactions based on other kinds of payment services.

Issuing of payment instruments: a payment service consisting in a payment service provider from contracting with a payer to provide her with a payment instrument to initiate and process the payer's payment transactions.

Money remittance: a payment service whereby funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or whereby such funds are received on behalf of and made available to the payee.

Payment initiation services: payment services to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.

Account information services: online payment services to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or more than one payment service provider.

Other: the payment service affected is none of the above. Further details should be provided in the free text field.

Functional areas affected: indicate the step or steps of the payment process that have been affected by the incident. Multiple boxes may be ticked.

Authentication/authorisation: procedures which allow the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials and the payment service user (or a third party acting on behalf of that user) giving his/her consent to transfer funds or securities.

Communication: flow of information for the purpose of identification, authentication, notification and information between the account-servicing payment service provider and payment initiation service providers, account information service providers, payers, payees and other payment service providers.

Clearing: a process of transmitting, reconciling and, in some cases, confirming transfer orders prior to settlement, potentially including the netting of orders and the establishment of final positions for settlement.

Direct settlement: the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by the affected payment service provider itself.

Indirect settlement: the completion of a transaction or of processing with the aim of discharging participants' obligations through the transfer of funds, when this action is carried out by another payment service provider on behalf of the affected payment service provider.

Other: the functional area affected is none of the above. Further details should be provided in the free text field.

Systems and components affected: indicate which part or parts of the payment service provider's technological infrastructure have been affected by the incident. Multiple boxes may be ticked.

Application/software: programs, operating systems, etc. that support the provision of payment services by the payment service provider.

Database: data structure which stores personal and payment information needed to execute payment transactions.

Hardware: physical technology equipment that runs the processes and/or stores the data needed by payment service providers to carry out their payment-related activity.

Network/infrastructure: telecommunications networks, either public or private, that allow the exchange of data and information during the payment process (e.g. the internet).

Other: the system and component affected is none of the above. Further details should be provided in the free text field.

Staff affected: indicate whether or not the incident has had any effects on the payment service provider's staff and, if so, provide details in the free text field.

B5 – Incident mitigation

Which actions/measures have been taken so far or are planned to recover from the incident?: please provide details about actions that have been taken or planned to be taken to temporarily address the incident.

Have the Business Continuity Plans and/or Disaster Recovery Plans been activated?: please indicate whether or not and, if so, provide the most relevant details of what happened (i.e. when they were activated and what these plans consisted of).

Has the payment service providers cancelled or weakened some controls because of the incident?: please indicate whether or not the payment service provider has had to override some controls (e.g. stop using the four eyes principle) to address the incident and, if so, provide details of the underlying reasons justifying the weakening or cancelling of controls.

C – Final report

C1 – General details

Update of the information from the intermediate report (summary): please provide further information on the actions taken to recover from the incident and avoid its recurrence, analysis of the root cause, lessons learnt, etc.

Date and time of closing the incident: indicate the date and time when the incident was considered closed.

Are the original controls back in place?: if the payment service provider had to cancel or weaken some controls because of the incident, indicate whether or not such controls are back in place and provide any additional information in the free text field.

C2 – Root cause analysis and follow-up

What was the root cause, if already known?: please explain which is the root cause of the incident or, if it is not known yet, the preliminary conclusions drawn from the root cause analysis. Payment service providers may attach a file with detailed information if considered necessary.

Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known: please describe the main actions that have been taken or are planned to be taken to prevent a future reoccurrence of the incident.

C3 – Additional information

Has the incident been shared with other payment service providers for information purposes?: please provide an overview of which payment service providers have been contacted, either formally or informally, to debrief them about the incident, providing details of the payment service providers that have been informed, the information that has been shared and the underlying reasons for sharing this information.

Has any legal action been taken against the payment service providers?: please indicate whether or not, at the time of filling out the final report, the payment service provider has suffered any legal action (e.g. been taken to Court or lost its license) as a result of the incident.

ANNEX 2
PROCEDURES FOR COMPLAINTS OF ALLEGED INFRINGEMENTS OF CBM DIRECTIVE NO 1

Scope

1. The Scope of this Annex is to adopt the provisions prescribed in the Guidelines on procedures for complaints of alleged infringements of Directive (EU) 2015/2366, issued by the EBA on the 13 October 2017.

2. This Annex applies to complaints submitted to the Bank and the Office of the Arbiter with regard to payment service providers' alleged infringements of this Directive as laid down in Paragraph 74 of this Directive. These complaints are to be taken into consideration by the Bank, in collaboration with the MFSA, to ensure and monitor effective compliance with this Directive, as referred to in Article 100(6) of Directive 2015/2366. These complaints may be submitted by payment service users and other interested parties, including payment service providers that are affected by the situation(s) that gave rise to the complaint and consumer associations ('complainants').

Definitions

3. Unless otherwise specified, terms used and defined in this Directive have the same meaning in this Annex.

Channels for the submission of complaints of alleged infringements of CBM Directive No 1

4. (1) The Bank and the Office of the Arbiter should ensure that at least two different channels are available for complainants to submit their complaints of alleged infringement of this Directive and that at least one of these channels is easily accessible for all types of complainants.

   (2) The Bank and the Office of the Arbiter should ensure that at least one of the channels referred to in Paragraph 4(1) is digital and accessible online, such as an email or a web form.

Information to be requested from complainants

5. (1) The Bank and the Office of the Arbiter should request from complainants to provide, where possible, information which includes but is not limited to:

   (a) the identity and contact details of the complainant;

   (b) an indication of whether the complainant is a natural or a legal person;

   (c) an indication of whether or not the complainant is a payment service user;

   (d) the identity of the payment service provider(s) that has/have given rise to the complaint of an alleged infringement of this Directive; and

   (e) A description of the situation that gave rise to the complaint of an alleged infringement of this Directive.

(2) The Bank and the Office of the Arbiter should record the information provided by the complainants under Paragraph 5(1).

(3) The Bank and the Officer of the Arbiter should make means available for complainants to submit any documentary evidence in support of the complaint, such as a copy of their contract with the payment service provider, any correspondence exchanged with the payment service provider(s) or with any other entity, and information related to their payment account if relevant.

Reply to complainants

6. (1) When responding to the complainants and, where appropriate, informing them of the existence of ADR procedures, the Bank and the Officer of the Arbiter should also provide:

    (a) an acknowledgement of receipt of the complaint;

    (b) information on the general competence of the Bank or the Office of the Arbiter in respect of the procedure for complaints of alleged infringements of this Directive;

    (c) information on whether the Bank or the Office of the Arbiter has forwarded the complaint to another authority or body, which may be located in Malta or in another Member State, and including the name and contact details of that authority or body; and

    (d) information on either the timing and form of any further communication with the complainant on the alleged infringement of this Directive, or if the reply represents the end of the complaints procedure with the Bank or the Office of the Arbiter.

    (2) The Bank and the Office of the Arbiter should send the reply to the complainant without undue delay.

    (3) The Bank and the Office of the Arbiter should include information as set out in Paragraph 6(1)(d) in any subsequent communication that they may have with the complainant.

Aggregate analysis of complaints

7. (1) Taking into account at least the information collected under Paragraph 5(1), the Bank and the Office of the Arbiter should have a complaints procedure in place that allows for the aggregate analysis of complaints of alleged infringements of this Directive and enables the Bank and the Office of the Arbiter to identify, understand and assess, for a given timeframe:

    (a) the total number of complaints of alleged infringements of this Directive received;

    (b) the nature of the most common types of complainants;

    (c) the identity of the payment service providers that are most often complained about;

    (d) the issues and, where possible, the provisions of this Directive most complained about;

    (e) the payment services most complained about, where possible; and

(f) the most common measures taken by the Bank and the Office of the Arbiter in response to the complaints received to ensure effective compliance with this Directive.

(2) The Bank, in collaboration with the MFSA, should take into account the aggregate analysis of complaints referred to in Paragraph 7(1) to ensure and monitor effective compliance of payment service providers with this Directive.

(3) The Bank and the Office of the Arbiter should treat complaints from the same complainant, about the same payment service provider and with the same description of the situation that gave rise to the complaint, as a single complaint for the purposes of the aggregate analysis of complaints referred to in Paragraph 7(1).

Documentation of complaints procedures

8. The Bank and the Office of the Arbiter should document their complaints procedures by outlining the procedure for the receipt of complaints submitted by payment service users and other interested parties, as laid down in this Annex, and the internal governance of that procedure.

Public information on complaints procedures

9. The Bank and the Office of the Arbiter should make publicly available information on their procedures for complaints of alleged infringements of this Directive. This information should be up to date and easily accessible, and include but not be limited to:

(a) the objective and scope of the complaints procedures;

(b) the channels through which complaints can be submitted, and how to access them;

(c) the information that complainants are requested to provide as set out in Paragraph 5(1);

(d) the sequential steps of the complaints procedures and any deadlines that may apply;

(e) the general competence of the Bank and the Office of the Arbiter in respect of the procedure for complaints of alleged infringements of this Directive; and

(f) the various measures available to the Bank, in collaboration with the MFSA, to ensure and monitor effective compliance with this Directive.

ANNEX 3
INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) AND SECURITY RISKS MANAGEMENT UNDER CBM DIRECTIVE NO 1

Scope

The Scope of this Annex is to adopt the provisions prescribed in the Guidelines on Information and Communication Technology (ICT) and security risk management of payment services under Directive (EU) 2015/2366, issued by the EBA on the 28 November 2019. These Guidelines have been formulated to be addressed to payment service providers listed in paragraph 2(2) of this Directive and to credit institutions for all their activities beyond payment services (hereinafter collectively referred to as 'financial institutions').This Annex set out how financial institutions should manage the ICT and security risks that they are exposed to, in accordance with Paragraph 70(1) of this Directive.

Definitions

1. Unless otherwise specified, terms used and defined in this Directive, Directive 2013/36/EU (CRD) and Regulation (EU) No 575/2013 have the same meaning in this Annex. In addition, for the purpose of this Annex, the following definitions apply:

   (a) ICT and security risk means risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility) . This includes security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security.

   (b) Management body means either of the following:

      i. For payment service providers that are credit institutions, this term has the same meaning as the definition in point (7) of Article 3(1) of Directive 2013/36/EU;

      ii. For payment service providers that are payment institutions or electronic money institutions, this term means directors or persons responsible for the management of the payment institutions and electronic money institutions and, where relevant, persons responsible for the management of the payment services activities of the payment institutions and electronic money institutions;

      iii. For payment service providers referred to in Paragraph 2(2)(d) and (f) of this Directive, this term has the meaning conferred on it by the applicable EU or national law;

   (c) 'Operational or security incident' means a singular event or a series of linked events unplanned by the financial institution which has or will probably have an adverse impact on the integrity, availability, confidentiality, and/or authenticity of services;

   (d) 'Senior management' means either of the following:

      i. For payment service providers that are credit institutions, this term has the same meaning as the definition in point (9) of Article 3(1) of Directive 2013/36/EU;

      ii. For payment service providers 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 institution;

iii. For payment service providers referred to in Paragraph 2(2)(d) and (f) of this Directive, this term has the meaning conferred on it by the applicable EU or national law;

(e) 'Risk appetite' means 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;

(f) 'Audit function' means either of the following:

i. For credit institutions, the audit function is as referred to in Section 22 of the EBA guidelines on internal governance (EBA/GL/2017/11);
ii. For payment service providers other than credit institutions, the audit function must be independent within or from the payment service provider and may be an internal and/or an external audit function.

(g) 'ICT projects' means any project, or part thereof, where ICT systems and services are changed, replaced, dismissed or implemented. ICT projects can be part of wider ICT or business transformation programmes.

(h) 'Third party' means an organisation that has entered into business relationships or contracts with an entity to provide a product or service.

(i) 'Information asset' means a collection of information, either tangible or intangible, that is worth protecting.

(j) 'ICT asset' means an asset of either software or hardware that is found in the business environment.

(k) 'ICT systems' means an ICT set-up as part of a mechanism or an interconnecting network that supports the operations of a financial institution.

(l) 'ICT services' means services provided by ICT systems to one or more internal or external users. Examples include data entry, data storage, data processing and reporting services, but also, monitoring, and business and decision support services.

General Principle

2. All financial institutions should comply with all the provisions set out in this Annex. The level of detail should be proportionate to, and takes account of, the financial institutions' size, their internal organisation, and to the nature, scope, complexity and riskiness of the services and products that the financial institutions provide or intend to provide.

Governance and strategy

Governance

3. The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information

security risk management, and business continuity, including those for the management body and its committees.

4. The management body should ensure that the quantity and skills of financial institutions' staff is adequate to support their ICT operational needs and their ICT and security risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy. The management body should ensure that the allocated budget is appropriate to fulfil the above. Furthermore, financial institutions should ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required.
5. The management body has overall accountability for setting, approving and overseeing the implementation of financial institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks.

Strategy

6. The ICT strategy should be aligned with financial institutions' overall business strategy and should define:

   (1) how financial institutions' ICT should evolve to effectively support and participate in their business strategy, including the evolution of the organisational structure, ICT system changes and key dependencies with third parties;

   (2) the planned strategy and evolution of the architecture of ICT, including third party dependencies;

   (3) clear information security objectives, focusing on ICT systems and ICT services, staff and processes.

7. Financial institutions should establish sets of action plans that contain measures to be taken to achieve the objective of the ICT strategy. These should be communicated to all relevant staff (including contractors and third party providers where applicable and relevant). The action plans should be periodically reviewed to ensure their relevance and appropriateness. Financial institutions should also establish processes to monitor and measure the effectiveness of the implementation of their ICT strategy

Use of third-party providers

8. Without prejudice to the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) and Article 19 of PSD2, financial institutions should ensure the effectiveness of the risk-mitigating measures as defined by their risk management framework, including the measures set out in these guidelines, when operational functions of payment services and/or ICT services and ICT systems of any activity are outsourced, including to group entities, or when using third parties.

9. To ensure continuity of ICT services and ICT systems, financial institutions should ensure that contracts and service level agreements (both for normal circumstances as well as in the event of service disruption) with providers (outsourcing providers, group entities, or third party providers) include the following:

(1) appropriate and proportionate information security-related objectives and measures including requirements such as minimum cybersecurity requirements; specifications of the financial institution's data life cycle; any requirements regarding data encryption, network security and security monitoring processes, and the location of data centres;

(2) operational and security incident handling procedures including escalation and reporting.

10. Financial institutions should monitor and seek assurance on the level of compliance of these providers with the security objectives, measures and performance targets of the financial institution.

ICT and security risk management framework

Organisation and objectives

11. Financial institutions should identify and manage their ICT and security risks. The ICT function(s) in charge of ICT systems, processes and security operations should have appropriate processes and controls in place to ensure that all risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the financial institution's risk appetite and that the projects and systems they deliver and the activities they perform are in compliance with external and internal requirements.

12. Financial institutions should assign the responsibility for managing and overseeing ICT and security risks to a control function, adhering to the requirements of Section 19 of the EBA Guidelines on internal governance (EBA/GL/2017/11). Financial institutions should ensure the independence and objectivity of this control function by appropriately segregating it from ICT operations processes. This control function should be directly accountable to the management body and responsible for monitoring and controlling adherence to the ICT and security risk management framework. It should ensure that ICT and security risks are identified, measured, assessed, managed, monitored and reported. Financial institutions should ensure that this control function is not responsible for any internal audit.

    The internal audit function should, following a risk-based approach, have the capacity to independently review and provide objective assurance of the compliance of all ICT and security-related activities and units of a financial institution with the financial institution's policies and procedures and with external requirements, adhering to the requirements of Section 22 of the EBA Guidelines on internal governance (EBA/GL/2017/11).

13. Financial institutions should define and assign key roles and responsibilities, and relevant reporting lines, for the ICT and security risk management framework to be effective. This framework should be fully integrated into, and aligned with, financial institutions' overall risk management processes.

14. The ICT and security risk management framework should include processes in place to:

    (1) determine the risk appetite for ICT and security risks, in accordance with the risk appetite of the financial institution;
    (2) identify and assess the ICT and security risks to which a financial institution is exposed;
    (3) define mitigation measures, including controls, to mitigate ICT and security risks;
    (4) monitor the effectiveness of these measures as well as the number of reported incidents, including for payment service providers the incidents reported in accordance with Article

96 of the PSD2 affecting the ICT-related activities, and taken action to correct the measures where necessary;

(5) report to the management body on the ICT and security risks and controls;

(6) identify and assess whether there are any ICT and security risks resulting from any major change in ICT system of ICT services, processes or procedures, and/or after any significant operational or security incident.

15. Financial institutions should ensure that the ICT and security risk management framework is documented, and continuously improved, based on 'lessons learned' during its implementation and monitoring. The ICT and security risk management framework should be approved and reviewed, at least once a year, by the management body

Identification of functions, processes and assets

16. Financial institutions should identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.

17. In addition, financial institutions should identify, establish and maintain updated mapping of the information assets supporting their business functions and supporting processes, such as ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that support their critical business functions and processes

Classification and risk assessment

18. Financial institutions should classify the identified business functions, supporting processes and information assets referred to in paragraphs 15 and 16 in terms of criticality.

19. To define the criticality of these identified business functions, supporting processes and information assets, financial institutions should, at a minimum, consider the confidentiality, integrity and availability requirements. There should be clearly assigned accountability and responsibility for the information assets.

20. Financial institutions should review the adequacy of the classification of the information assets and relevant documentation, when risk assessment is performed.

21. Financial institutions should identify the ICT and security risks that impact the identified and classified business functions, supporting processes and information assets, according to their criticality. This risk assessment should be carried out and documented annually or at shorter intervals if required. Such risk assessments should also be performed on any major changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets, and consequently the current risk assessment of financial institutions should be updated.

22. Financial institutions should ensure that they continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and should regularly review the risk scenarios impacting them.

Risk mitigation

23. Based on the risk assessments, financial institutions should determine which measures are required to mitigate identified ICT and security risks to acceptable levels and whether changes are necessary to the existing business processes, control measures, ICT systems and ICT services. A financial institution should consider the time required to implement these changes and the time to take appropriate interim mitigating measures to minimise ICT and security risks to stay within the financial institution's ICT and security risk appetite.

24. Financial institutions should define and implement measures to mitigate identified ICT and security risks and to protect information assets in accordance with their classification.

Reporting

25. Financial institutions should report risk assessment results to the management body in a clear and timely manner. Such reporting is without prejudice to the obligation of PSPs to provide competent authorities with an updated and comprehensive risk assessment, as laid down in Article 95(2) of Directive (EU) 2015/2366.

Audit

26. A financial institution's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the financial institution. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.

27. A financial institution's management body should approve the audit plan, including any ICT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent ICT and security risks in the financial institution and should be updated regularly.

28. A formal follow-up process including provisions for the timely verification and remediation of critical ICT audit findings should be established.

Information security

Information security policy

29. Financial institutions should develop and document an information security policy that should define the high-level principles and rules to protect the confidentiality, integrity and availability of financial institutions' and their customers' data and information. For PSPs this policy is identified in the security policy document to be adopted in accordance with Article 5(1)(j) of Directive (EU) 2015/2366. The information security policy should be in line with the financial institution's information security objectives and based on the relevant results of the risk assessment process. The policy should be approved by the management body.

30. The policy should include a description of the main roles and responsibilities of information security management, and it should set out the requirements for staff and contractors, processes and technology in relation to information security, recognising that staff and contractors at all levels have responsibilities in ensuring financial institutions' information

security. The policy should ensure the confidentiality, integrity and availability of a financial institution's critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy should be communicated to all staff and contractors of the financial institution.

31. Based on the information security policy, financial institutions should establish and implement security measures to mitigate the ICT and security risks that they are exposed to. These measures should include:
    (a) organisation and governance in accordance with paragraphs 10 and 11;
    (b) logical security;
    (c) physical security;
    (d) ICT operations security;
    (e) security monitoring ;
    (f) information security reviews, assessment and testing ;
    (g) information security training and awareness .

Logical security

32. Financial institutions should define, document and implement procedures for logical access control (identity and access management). These procedures should be implemented, enforced, monitored and periodically reviewed. The procedures should also include controls for monitoring anomalies. These procedures should, at a minimum, implement the following elements, where the term 'user' also includes technical users:

    (1) **Need to know, least privilege and segregation of duties**: financial institutions should manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including for remote access. Users should be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), i.e. to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').

    (2) **User accountability**: financial institutions should limit, as much as possible, the use of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems.

    (3) **Privileged access rights**: financial institutions should implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access entitlements (e.g. administrator accounts). In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used.

    (4) **Logging of user activities**: at a minimum, all activities by privileged users should be logged and monitored. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, without prejudice to the retention requirements set out in EU and national law. A financial institution should use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of services.

(5) **Access management**: access rights should be granted, withdrawn or modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed (information asset owner). In the case of termination of employment, access rights should be promptly withdrawn.

(6) **Access recertification**: access rights should be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are withdrawn when no longer required.

(7) **Authentication methods**: financial institutions should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, information or the process being accessed. This should, at a minimum, include complex passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.

33. Electronic access by applications to data and ICT systems should be limited to a minimum required to provide the relevant service.

Physical security

34. Financial institutions' physical security measures should be defined, documented and implemented to protect their premises, data centres and sensitive areas from unauthorised access and from environmental hazards.

35. Physical access to ICT systems should be permitted to only authorised individuals. Authorisation should be assigned in accordance with the individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access rights are promptly revoked when not required.

36. Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.

ICT operations security

37. Financial institutions should implement procedures to prevent the occurrence of security issues in ICT systems and ICT services and should minimise their impact on ICT service delivery. These procedures should include the following measures:

(1) identification of potential vulnerabilities, which should be evaluated and remediated by ensuring that software and firmware are up to date, including the software provided by financial institutions to their internal and external users, by deploying critical security patches or by implementing compensating controls;

(2) implementation of secure configuration baselines of all network components;

(3) implementation of network segmentation, data loss prevention systems and the encryption of network traffic (in accordance with the data classification);

(4) implementation of protection of endpoints including servers, workstations and mobile devices; financial institutions should evaluate whether endpoints meet the security standards defined by them before they are granted access to the corporate network;

(5) ensuring that mechanisms are in place to verify the integrity of software, firmware and data;

(6) encryption of data at rest and in transit (in accordance with the data classification).

38. Furthermore, on an ongoing basis, financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. These changes should be part of the financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented, authorised and deployed.

Security monitoring

39. Financial institutions should establish and implement policies and procedures to detect anomalous activities that may impact financial institutions' information security and to respond to these events appropriately. As part of this continuous monitoring, financial institutions should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous monitoring and detection processes should cover:

a) relevant internal and external factors, including business and ICT administrative functions;
b) transactions to detect misuse of access by third parties or other entities and internal misuse of access;
c) potential internal and external threats.

40. Financial institutions should establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their abilities to provide services. Financial institutions should actively monitor technological developments to ensure that they are aware of security risks. Financial institutions should implement detective measures, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and should check for corresponding new security updates.

41. The security monitoring process should also help a financial institution to understand the nature of operational or security incidents, to identify trends and to support the organisation's investigations.

Information security reviews, assessment, and testing

42. Financial institutions should perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, financial institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the institution should consider good

practices such as source code reviews, vulnerability assessments, penetration tests and red team exercises.

43. Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.

44. The information security testing framework should ensure that tests:
    (1) are carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures and who are not involved in the development of the information security measures;
    (2) include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.

45. Financial institutions should perform ongoing and repeated tests of the security measures. For all critical ICT systems (paragraph 18), these tests should be performed at least on an annual basis and, for PSPs, they will be part of the comprehensive assessment of the security risks related to the payment services they provide, in accordance with Article 95(2) of PSD2. Noncritical systems should be tested regularly using a risk-based approach, but at least every 3 years.

46. Financial institutions should ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet-facing critical applications.

47. Financial institutions should monitor and evaluate the results of the security tests and update their security measures accordingly without undue delays in the case of critical ICT systems.

48. For PSPs, the testing framework should also encompass the security measures relevant to (1) payment terminals and devices used for the provision of payment services, (2) payment terminals and devices used for authenticating the payment service users (PSU), and (3) devices and software provided by the PSP to the PSU to generate/receive an authentication code.

49. Based on the security threats observed and the changes made, testing should be performed to incorporate scenarios of relevant and known potential attacks.

Information security training and awareness

50. Financial institutions should establish a training programme, including periodic security awareness programmes, for all staff and contractors to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security related risks. Financial institutions should ensure that the training programme provides training for all staff members and contractors at least annually

ICT operations management

51. Financial institutions should manage their ICT operations based on documented and implemented processes and procedures (which, for PSPs, include the security policy document in accordance with Article 5(1)(j) of PSD2) that are approved by the management body. This set of documents should define how financial institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations and should enable financial institutions to maintain up-to-date ICT asset inventory.

52. Financial institutions should ensure that performance of their ICT operations is aligned to their business requirements. Financial institutions should maintain and improve, when possible, efficiency of their ICT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks.

53. Financial institutions should implement logging and monitoring procedures for critical ICT operations to allow the detection, analysis and correction of errors.

54. Financial institutions should maintain an up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). The ICT asset inventory should store the configuration of the ICT assets and the links and interdependencies between the different ICT assets, to enable a proper configuration and change management process.

55. The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks.

56. Financial institutions should monitor and manage the life cycles of ICT assets, to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor whether their ICT assets are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated.

57. Financial institutions should implement performance and capacity planning and monitoring processes to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.

58. Financial institutions should define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups should be set out in line with business recovery requirements and the criticality of the data and the ICT systems and evaluated according to the performed risk assessment. Testing of the backup and restoration procedures should be undertaken on a periodic basis.

59. Financial institutions should ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.

ICT incident and problem management

60. Financial institutions should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable financial

institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying events as operational or security incidents, as set out in the 'Definitions' section of this Directive, as well as early warning indicators that should serve as alerts to enable early detection of these incidents. Such criteria and thresholds, for PSPs, are without prejudice to the classification of major incidents in accordance with Article 96 of PSD2 and the Guidelines on major incident reporting under PSD2 (EBA/GL/2017/10).

61. To minimise the impact of adverse events and enable timely recovery, financial institutions should establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling and follow-up of operational and security incidents and to make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents. The incident and problem management process should establish:

(1) the procedures to identify, track, log, categorise and classify incidents according to a priority, based on business criticality;

(2) the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);

(3) problem management procedures to identify, analyse and solve the root cause behind one or more incidents — a financial institution should analyse operational or security incidents likely to affect the financial institution that have been identified or have occurred within and/or outside the organisation and should consider key lessons learned from these analyses and update the security measures accordingly;

(4) effective internal communication plans, including incident notification and escalation procedures — also covering security-related customer complaints — to ensure that:

(a) incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management and ICT senior management;

(b) the management body is informed on an ad hoc basis in the event of significant incidents and, at least, informed of the impact, the response and the additional controls to be defined as a result of the incidents.

(5) incident response procedures to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner;

(6) specific external communication plans for critical business functions and processes in order to:

(a) collaborate with relevant stakeholders to effectively respond to and recover from the incident;
(b) provide timely information to external parties (e.g. customers, other market participants, the supervisory authority) as appropriate and in line with an applicable regulation.

ICT project and change management

ICT project management

62. A financial institution should implement a programme and/or a project governance process that defines roles, responsibilities and accountabilities to effectively support the implementation of the ICT strategy.

63. A financial institution should appropriately monitor and mitigate risks deriving from their portfolio of ICT projects (programme management), considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.

64. A financial institution should establish and implement an ICT project management policy that includes as a minimum:

    a) project objectives;
    b) roles and responsibilities;
    c) a project risk assessment;
    d) a project plan, timeframe and steps;
    e) key milestones;
    f) change management requirements.

65. The ICT project management policy should ensure that information security requirements are analysed and approved by a function that is independent from the development function.

66. A financial institution should ensure that all areas impacted by an ICT project are represented in the project team and that the project team has the knowledge required to ensure secure and successful project implementation.

67. The establishment and progress of ICT projects and their associated risks should be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. Financial institutions should include project risk in their risk management framework.

ICT systems acquisitions and development

68. Financial institutions should develop and implement a process governing the acquisition, development and maintenance of ICT systems. This process should be designed using a risk-based approach.

69. A financial institution should ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management.

70. A financial institution should ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.

71. Financial institutions should have a methodology in place for testing and approval of ICT systems prior to their first use. This methodology should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended. They should also use test environments that adequately reflect the production environment.

72. Financial institutions should test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.

73. A financial institution should implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, a financial institution should ensure the segregation of production environments from development, testing and other non-production environments. A financial institution should ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorised users.

74. Financial institutions should implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. They should also document the development, implementation, operation and/or configuration of the ICT systems comprehensively to reduce any unnecessary dependency on subject matter experts. The documentation of the ICT system should contain, where applicable, at least user documentation, technical system documentation and operating procedures.

75. A financial institution's processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside the ICT organisation (e.g. end user computing applications) using a risk-based approach. The financial institution should maintain a register of these applications that support critical business functions or processes.

ICT change management

76. Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner. Financial institutions should handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards.

77. Financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require the adoption of additional measures to mitigate the risks involved. These changes should be in accordance with the financial institutions' formal change management process.

Business continuity management

78. Financial institutions should establish a sound business continuity management (BCM) process to maximise their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption in line with Article 85(2) of Directive 2013/36/EU and Title VI of the EBA Guidelines on internal governance (EBA/GL/2017/11).

Business impact analysis

79. As part of sound business continuity management, financial institutions should conduct business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario analysis. The BIA should also consider the criticality of the identified and

classified business functions, supporting processes, third parties and information assets, and their interdependencies.

80. Financial institutions should ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.

Business continuity planning

81. Based on their BIAs, financial institutions should establish plans to ensure business continuity (business continuity plans, BCPs), which should be documented and approved by their management bodies. The plans should specifically consider risks that could adversely impact ICT systems and ICT services. The plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets. Financial institutions should coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.

82. Financial institutions should put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident). In cases of severe business disruption that trigger specific business continuity plans, financial institutions should prioritise business continuity actions using risk-based approach, which can be based on the risk assessments carried out under the Section on 'Classification and risk assessment' . For PSPs this may include, for example, facilitating the further processing of critical transactions while remediation efforts continue.

83. A financial institution should consider a range of different scenarios in its BCP, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it should assess the potential impact that such scenarios might have. Based on these scenarios, a financial institution should describe how the continuity of ICT systems and services, as well as the financial institution's information security, are ensured.

Response and recovery plans

84. Based on the BIAs (paragraph 79) and plausible scenarios (paragraph 83), financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plans and what actions should be taken to ensure the availability, continuity and recovery of, at least, financial institutions' critical ICT systems and ICT services. The response and recovery plans should aim to meet the recovery objectives of financial institutions' operations.

85. The response and recovery plans should consider both short-term and long-term recovery options. The plans should:

    (1) focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of financial institutions and on the financial system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions;

(2) be documented and made available to the business and support units and readily accessible in the event of an emergency;
(3) be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.

86. The plans should also consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances.

87. Furthermore, as part of the response and recovery plans, a financial institution should consider and implement continuity measures to mitigate failures of third party providers, which are of key importance for a financial institution's ICT service continuity (in line with the provisions of the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) regarding business continuity plans).

Testing of plans

88. Financial institutions should test their BCPs periodically. In particular, they should ensure that the BCPs of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually, in accordance with paragraph 90.

89. BCPs should be updated at least annually, based on testing results, current threat intelligence and lessons learned from previous events. Any changes in recovery objectives (including RTOs and RPOs) and/or changes in business functions, supporting processes and information assets, should also be considered, where relevant, as a basis for updating the BCPs.

90. Financial institutions' testing of their BCPs should demonstrate that they are able to sustain the viability of their businesses until critical operations are re-established. In particular they should:
(1) include testing of an adequate set of severe but plausible scenarios including those considered for the development of the BCPs (as well as testing of services provided by third parties, where applicable); this should include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that they can be run in this way for a sufficiently
(2) representative period of time and that normal functioning can be restored afterwards;
(3) be designed to challenge the assumptions on which BCPs rest, including governance arrangements and crisis communication plans; and
(4) include procedures to verify the ability of their staff and contractors, ICT systems and ICT services to respond adequately to the scenarios defined in paragraph 90(1).

91. Test results should be documented and any identified deficiencies resulting from the tests should be analysed, addressed,
92. and reported to the management body.

Crisis communications

93. In the event of a disruption or emergency, and during the implementation of the BCPs, financial institutions should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the competent authorities when required by national regulations, and also relevant providers (outsourcing

providers, group entities, or third party providers) are informed in a timely and appropriate manner.

Payment service user relationship management

94. Payment service providers should establish and implement processes to enhance payment service users' awareness of security risks linked to the payment services by providing payment service users with assistance and guidance.

95. The assistance and guidance offered to payment service users should be updated in the light of new threats and vulnerabilities, and changes should be communicated to the payment service user.

96. Where product functionality permits, payment service providers should allow payment service users to disable specific payment functionalities related to the payment services offered by the payment service provider to the payment service user.

97. Where, in accordance with Paragraph 44(1) of this Directive, a payment service provider has agreed with the payer on spending limits for payment transactions executed through specific payment instruments, the payment service provider should provide the payer with the option to adjust these limits up to the maximum agreed limit.

98. Payment service providers should provide payment service users 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.

99. Payment service providers should keep payment service users informed about updates in security procedures which affect payment service users regarding the provision of payment services.

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

ANNEX 4
FRAUD REPORTING UNDER CBM DIRECTIVE NO 1

Scope

1. The Scope of this Annex is to adopt the provisions prescribed in the Guidelines on fraud reporting under Directive (EU) 2015/2366, issued by the EBA on the 18 July 2018 and which have been subsequently amended by EBA/GL/2020/01 published on 22 January 2020.

2. This Annex provides detail on statistical data on fraud related to different means of payment that payment service providers have to report to the Bank, as well as on the aggregated data that the Bank has to share with the EBA and the ECB, in accordance with Paragraph 71(3) of this Directive.

3. This Annex applies in relation to the reporting by payment service providers to the Bank of statistical data on fraud for payment transactions that have been initiated and executed (including acquired where applicable), including the acquiring of payment transactions for card payments, identified by reference to:

    (a) fraudulent payment transactions data over a defined period of time; and

    (b) payment transactions over the same defined period.

4. Data reported under the credit transfers breakdown should include credit transfers performed via automated teller machines with a credit transfer function. Credit transfers used to settle outstanding balances of transactions using cards with a credit or delayed debit function should also be included.

5. Data reported under the direct debit breakdown should include direct debits used to settle outstanding balances of transactions using cards with a credit or delayed debit function.

6. Data reported under the card payments breakdowns should include data on all payment transactions by means of payment cards (electronic and non-electronic). Payments with cards with an e-money function only (e.g. prepaid cards) should not be included in card payments but reported as e-money.

7. This Annex also sets out how the Bank should aggregate the data mentioned in Paragraph 3 of this Annex that shall be provided to the ECB and the EBA in accordance with Paragraph 71(3) of this Directive.

8. This Annex is subject to the principle of proportionality, which means that all payment service providers within the scope of this Annex are required to be compliant with the provisions of this Annex, but the precise requirements, including on frequency of reporting, may differ between payment service providers, depending on the payment instrument used, the type of services provided or the size of the payment service provider.

Addressees

9. This Annex is addressed to:

(a) credit institutions licensed in terms of Banking Act (*Cap. 371 of the Laws of Malta*) and their agents, and branches in Malta of credit institutions which have their head offices outside Malta;
(b) electronic money institutions licensed in terms of the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and their agents which are authorised to issue electronic money, and branches in Malta of electronic money institutions which have their head offices located outside Malta, in as far as the payment services provided by those branches are linked to the issuance of electronic money;

(c) payment institutions licensed in terms of the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) and their agents, and branches in Malta of payment institutions which have their head offices licenced in another Member State;

(d) post office giro institutions which are entitled under Maltese law to provide payment services;

(e) The Bank as a designated competent authority of the provisions under this Directive.

Definitions

10. Unless otherwise specified, terms used and defined in Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions, in Regulation (EU) No 260/2012 of the European Parliament and of the Council establishing technical and business requirements for credit transfers and direct debit in euro, this Directive (CBM Directive No 1 on the provision and use of payment services) and in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) have the same meaning in this Annex.

Date of application

11. This Annex applies from 1 January 2019, with the exception of the reporting of data related to the exemptions to the requirement to use strong customer authentication provided for in Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, which will be applicable from 14 September 2019. The data relating to these exemptions are detailed in Appendix 2 in Data Breakdowns A (1.3.1.2.4 to 1.3.1.2.9 and 1.3.2.2.4 to 1.3.2.2.8), C (3.2.1.3.4 to 3.2.1.3.10 and 3.2.2.3.4 to 3.2.2.3.8), D (4.2.1.3.4 to 4.2.1.3.8 and 4.2.2.3.4 to 4.2.2.3.7) and F (6.1.2.4 to 6.1.2.11 and 6.2.2.4 to 6.2.2.8).

GUIDELINES ON FRAUD DATA REPORTING APPLICABLE TO PAYMENT SERVICE PROVIDERS

Payment transactions and fraudulent payment transactions

12. For the purposes of reporting statistical data on fraud in accordance with this Annex, the payment service provider should report for each reporting period:

    (a) unauthorised payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer ('unauthorised payment transactions'); and

    (b) payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee ('manipulation of the payer').

13. For the purposes of Paragraph 12 of this Annex, the payment service provider (including the payment instrument issuer where applicable) should report only payment transactions that have been initiated and executed (including acquired where applicable). The payment service provider should not report data on payment transactions that, however linked to any of the circumstances referred to in Paragraph 12 of this Annex, have not been executed and have not resulted in a transfer of funds in accordance with the provisions of this Directive.

14. In the case of money remittance services where funds were transferred from a payer's payment service provider to a payer's money remitter payment service provider (as part of a money remittance payment transaction), it is the payer's payment service provider, rather than the money remitter payment service provider, who should report the payment transactions from the payer's payment service provider to the money remitter. Such transactions should not be reported by the payment service provider of the beneficiary of the money remittance payment transaction.

15. Transactions and fraudulent transactions where funds have been transferred by a money remitter payment service provider from its accounts to a beneficiary account, including through arrangements offsetting the value of multiple transactions (netting arrangements), should be reported by the money remitter payment service provider in accordance with Data Breakdown G in Appendix 2 of this Annex.

16. Transactions and fraudulent transactions where e-money has been transferred by an e-money provider to a beneficiary account, including where the payer's payment service provider is identical to the payee's payment service provider, should be reported by the e-money provider in accordance with Data Breakdown F in Appendix 2 of this Annex. Where the payment service providers are different, payment is only reported by the payer's payment service provider to avoid double counting.

17. Payment service providers should report all payment transactions and fraudulent payment transactions in accordance with the following:

(a) 'Total fraudulent payment transactions' refer to all transactions mentioned in Paragraph 12 of this Annex, regardless of whether the amount of the fraudulent payment transaction has been recovered.

(b) 'Losses due to fraud per liability bearer' refers to the losses by the reporting payment service provider, its payment service user or others, reflecting the actual impact of fraud on a cash flow basis. Since the registering of financial losses borne may be disassociated time-wise from the actual fraudulent transactions and in order to avoid revisions of reported data purely due to this immanent time lag, the final fraud losses should be reported in the period when they are recorded in the payment service provider's books. The final fraud loss figures should not take into account refunds by insurance agencies because they are not related to fraud prevention for the purposes of this Directive.

(c) 'Modification of a payment order by the fraudster' is a type of unauthorised transaction as defined in Paragraph 12(a) of this Annex and refers to a situation where the fraudster intercepts and modifies a legitimate payment order at some point during the electronic communication between the payer's device and the payment service provider (for instance through malware or attacks allowing attackers to eavesdrop on the communication between two legitimately communicating hosts (man-in-the middle attacks)) or modifies the payment instruction in the payment service provider's system before the payment order is cleared and settled.

(d) 'Issuance of a payment order by the fraudster' is a type of unauthorised transaction as defined in Paragraph 12(a) of this Annex and refers to a situation where a fake payment order is issued by the fraudster after having obtained the payer/payee's sensitive payment data through fraudulent means.

General data requirements

18. The payment service provider should report statistical information on:

(a) total payment transactions in line with the different breakdowns in Appendix 2 of this Annex and in accordance with the provisions of Paragraphs 12 to 17 of this Annex; and

(b) total fraudulent payment transactions in line with the different breakdowns in Appendix 2 of this Annex and as defined in Paragraph 17(a) of this Annex.

19. The payment service provider should report the statistical information specified in Paragraph 18 of this Annex in terms of both volume (i.e. number of transactions or fraudulent transactions) and value (i.e. amount of transactions or fraudulent transactions). They should report volumes and values in actual units, with two decimals for values.

20. A payment service provider authorised, or a branch established, in Malta should report the values in euro currency. The reporting payment service providers should convert data for values of transactions or fraudulent transactions denominated in a currency other than the euro currency into the euro currency, using the relevant exchange rates applied to these transactions or the average ECB reference exchange rate for the applicable reporting period.

21. The payment service provider should report only payment transactions that have been executed, including those transactions that have been initiated by a payment initiation service

provider. Prevented fraudulent transactions that are blocked before they are executed due to suspicion of fraud should not be included.

22. The payment service provider should report the statistical information with a breakdown in accordance with the breakdowns specified in the provisions of Paragraphs 48 to 62 of this Annex and compiled in Appendix 2 of this Annex.

23. The payment service provider should identify the applicable data breakdown(s), depending on the payment service(s) and payment instrument(s) provided, and submit the applicable data to the Bank.

24. The payment service provider should ensure that all data reported to the Bank can be cross-referenced in accordance with Appendix 2 of this Annex.

25. The payment service provider should allocate each transaction to only one sub-category for each row of each data breakdown.

26. In the case of a series of payment transactions being executed, or fraudulent payment transactions being executed, the payment service provider should consider each payment transaction or fraudulent payment transaction in the series to count as one.

27. The payment service provider can report zero ('0') where there were no transactions or fraudulent transactions taking place for a particular indicator in the reporting period established. Where the payment service provider cannot report data for a specific breakdown because that particular data breakdown is not applicable to that PSP, the data should be reported as 'NA'.

28. For the purpose of avoiding double-counting, the payer's payment service provider should submit data in its issuing (or initiating) capacity. As an exception, data for card payments should be reported both by the payer's payment service provider and by the payee's payment service provider acquiring the payment transaction. The two perspectives should be reported separately, with different breakdowns as detained in Appendix 2 of this Annex. In the event that there is more than one acquiring payment service provider involved, the provider that has the contractual relationship with the payee should report. In addition, for direct debits, transactions must be reported by the payee's payment service provider only, given that these transactions are initiated by the payee.

29. In order to avoid double counting when calculating the total transactions and fraudulent transactions across all payment instruments, the payment service provider that executes credit transfers initiated by a payment initiation service provider should indicate the breakdown for the volume and value of the total transactions and fraudulent payment transactions that have been initiated via a payment initiation service provider when reporting under Data Breakdown A.

Frequency, reporting timelines and reporting period

30. The payment service provider should report data every six months based on the applicable data breakdown(s) in Appendix 2 of this Annex.

31. The payment service provider that benefit from an exemption under Article 32 of Directive (EU) 2015/2366 as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of*

Malta) and in the Banking Act (*Cap. 371 of the Laws of Malta*) and e-money institutions that benefit from the exemption under Article 9 of Directive 2009/110/EC as transposed in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) on the taking up, pursuit and prudential supervision of the business of electronic money institutions should only report the set of data requested under the applicable form(s) in Appendix 2 of this Annex on an annual basis with data broken down in two periods of six months.

32. The payment service provider should submit their data within the timelines set by the Bank.

Geographical breakdown

33. The payment service provider should report data for transactions that are domestic, cross border within the European Economic Area (EEA), and cross-border outside the EEA.

34. For non-card based payment transactions, and remote card based payment transactions, 'domestic payment transactions' refer to payment transactions initiated by a payer, or by or through a payee, where the payer's payment service provider and the payee's payment service provider are located in Malta.

35. For non-remote card-based payment transactions, 'domestic payment transactions' refer to payment transactions where the payer's payment service provider (issuer), the payee's payment service provider (acquirer) and the point of sale (POS) or automated teller machine (ATM) used are located in Malta.

36. For EEA branches established in Malta as the host Member State, domestic payment transactions refer to the payment transactions where both the payer's and the payee's payment service providers are located in Malta.

37. For non-card based payment transactions and remote card based payment transactions, 'cross-border payment transaction within the EEA' refers to a payment transaction initiated by a payer, or by or through a payee, and either the payer's or the payee's payment service provider is located in Malta while the other is located in another Member State.

38. For non-remote card-based payment transactions, 'cross-border payment transactions within the EEA' refer to payment transactions where either the payer's payment service provider (issuer) or the payee's payment service provider (acquirer), POS or ATM is located in Malta while the other is located in another Member State.

39. 'Cross-border payment transactions outside the EEA' refer to payment transactions initiated by a payer, or by or through a payee, where either the payer's or the payee's payment service provider is located in Malta while the other is located outside the EEA.

40. A payment service provider offering payment initiation services should report the executed payment transactions it initiated and the executed fraudulent transactions it initiated in accordance with the following:

    (a) 'Domestic payment transactions' refer to payment transactions, where the payment initiation service provider and the account servicing payment service provider are located in Malta;

(b) 'Cross-border payment transactions within the EEA' refer to payment transactions, where the payment initiation service provider is located in Malta and the account servicing payment service provider is located in another Member State;

(c) 'Cross-border payment transactions outside the EEA' refer to payment transactions, where the payment initiation service provider is in Malta and the account servicing payment service provider is located outside the EEA.

Reporting to the competent authority

41. The payment service provider shall report to the Bank, where Malta is the home Member State.

42. The payment service provider should record data from all its agents, providing payment services in the EEA and aggregate these data with the rest of the data before reporting to the Bank, where Malta is the home Member State. When doing so, the location of the agent is irrelevant for determining the geographical perspective.

43. Within the framework of the monitoring and reporting set out in Paragraph 8(3) of this Directive and in Regulation 6 of the European Passport Rights for Credit Institutions Regulations *(S.L 371.11)*, an established branch of an EEA's payment service provider should report to the Bank, where Malta is the host Member State, separately from the reporting data of the payment service provider in the home Member State.

44. When reporting data to the Bank, a payment service provider should mention the identification details mentioned in Appendix 1 of this Annex.

Recording/reference dates

45. The date to be considered by payment service providers for recording payment transactions and fraudulent payment transactions for the purpose of this statistical reporting is the day the transaction has been executed in accordance with this Directive. In the case of a series of transactions, the date recorded should be the date when each individual payment transaction was executed.

46. The payment service provider should report all fraudulent payment transaction from the time fraud has been detected, such as through a customer complaint or other means, regardless of whether or not the case related to the fraudulent payment transaction has been closed by the time the data are reported.

47. The payment service provider should report all adjustments to the data referring to any past reporting period at least up to one year old during the next reporting window after the information necessitating the adjustments is discovered. It should indicate that the data reported are revised figures applicable to the past period and should report this revision according to the methodology established by the Bank.

Data breakdown

48. For e-money payment transactions as defined in the Financial Institutions Act (*Cap. 376 of the Laws of Malta*) the payment service provider should provide data in accordance with Data Breakdown F in Appendix 2 of this Annex.

49. When providing data on e-money transactions, the payment service provider should include e-money payment transactions

(a) where the payer's PSP is identical to the payee's PSP; or

(b) where a card with an e-money functionality is used.

50. The payment service provider for the purpose of e-money payment transactions should report data on volumes and values of all payment transactions, as well as volumes and values of fraudulent payment transactions, with the following breakdowns:.

(a) geographical perspective;

(b) payment channel;
(c) authentication method;

(d) reason for not applying strong customer authentication (referring to the exemptions to strong customer authentication detailed in Chapter 3 of the regulatory technical standards on strong customer authentication and common and secure communication, Commission Delegated Regulation (EU) 2018/389, or to either of the categories "Merchant initiated transactions" and "Other", where applicable); and

(e) fraud types.

51. For money remittance services, the payment service provider should provide data in accordance with Data Breakdown G in Appendix 2 of this Annex and as specified in Paragraph 14 of this Annex. The payment service provider offering these services should report data on volumes and values of all payment transactions and fraudulent payment transactions in Paragraph 18 of this Annex with the geographical perspective.

52. When providing payment initiation services, the payment service provider should provide data in accordance with Data Breakdown H in Appendix 2 of this Annex. The payment service provider should report the executed payment transactions it initiated and the executed fraudulent transactions it initiated, both by volume and value.

53. For those payment transactions that qualify for Data Breakdown H in Appendix 2 of this Annex, the payment service provider offering payment initiation services should record and report data on volumes and values with the following breakdowns:

(a) geographical perspective;

(b) payment instrument;

(c) payment channel; and

(d) authentication method.

54. A payment service provider that does not manage the account of the payment service user but issues and executes card-based payments (a card-based payment instrument issuer) should provide data on volumes and values, in accordance with Data Breakdown C and/or E

in Appendix 2 of this Annex. When such data are provided, the account service payment service provider should ensure that no double-reporting of such transactions occur.

55. The payment service provider offering credit transfer and card based payment services should provide data in accordance with Data Breakdowns A, C and/or D in Appendix 2 of this Annex, depending on the payment instrument used for a given payment transaction and on the role of the payment service provider. The data include:

(a) geographical perspective;

(b) payment channel;

(c) authentication method;

(d) reason for not applying strong customer authentication (referring to exemptions to strong customer authentication detailed in Chapter 3 of the RTS on SCA and CSC, or to either of the categories “Merchant initiated transactions” and “Other”, where applicable);

(e) fraud types;

(f) card function for Data Breakdowns C and D; and

(g) payment transactions initiated via a payment initiation service provider for Data Breakdown A.

56. The payment service provider should provide data in accordance with Data Breakdown A in Appendix 2 of this Annex for all payment transactions and fraudulent payment transactions executed using credit transfers.

57. The payment service provider should provide data in accordance with Data Breakdown B in Appendix 2 of this Annex for all payment transactions and fraudulent payment transactions executed using direct debits. The data include:

(a) geographical perspective;

(b) channel used for the consent to be given; and

(c) fraud types.

58. The payment service provider should provide data in accordance with Data Breakdown C in Appendix 2 of this Annex for all payment transactions and fraudulent payment transactions on the issuer side where a payment card was used and the payment service provider was the payer’s payment service provider.

59. The payment service provider should provide data in accordance with Data Breakdown D in Appendix 2 of this Annex for all payment transactions and fraudulent payment transactions on the acquiring side where a payment card was used and the payment service provider is the payee’s payment service provider.

60. The payment service provider providing data in accordance with Data Breakdowns A to F in Appendix 2 of this Annex should report all losses due to fraud per liability bearer during the reporting period.

61. The payment service provider reporting card payment transactions in accordance with Data Breakdowns C and D in Appendix 2 of this Annex should exclude cash withdrawals and cash deposits.

62. The payment service provider (issuer) should provide data in accordance with Data Breakdown E in Appendix 2 of this Annex for all cash withdrawals and fraudulent cash withdrawals at ATMs (including via apps), at bank counters and through retailers ('cash back') using a card.

Guidelines on aggregate fraud data reporting by the Bank to the EBA and the ECB

Payment transactions and fraudulent payment transactions

63. For the purposes of reporting statistical data on fraud to the EBA and the ECB in accordance with this Annex and with Paragraph 71(3) of this Directive, the Bank should report for each reporting period:

(a) unauthorised payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer ('unauthorised payment transaction'); and

(b) payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee ('manipulation of the payer').

64. For the purposes of Paragraph 63 of this Annex, the Bank should report only payment transactions that have been initiated and executed (including acquired where applicable) by payment service providers (including card based payment instrument issuers where applicable). The Bank should not report data on payment transactions that, however linked to any of the circumstance referred to in Paragraph 63 of this Annex, have not been executed and have not resulted in a transfer of funds in accordance with the provisions of this Directive.

65. The Bank should report all payment transactions and fraudulent payment transactions in accordance with the following:

(a) For non-card based payment transactions and remote card based payment transactions, 'domestic payment transactions' refer to payment transactions initiated by a payer, or by or through a payee, where the payer's payment service provider and the payee's payment service provider are located in Malta,

(b) For EEA branches established in Malta as the host Member State, domestic payment transactions refer to the payment transactions where both the payer's and the payee's payment service providers are located in Malta.

(c) For non-card based payment transactions and remote card based payment transactions, 'cross-border payment transactions within the EEA' refer to payment transactions initiated by a payer, or by or through a payee, where either the payer's or the payee's payment service provider is located in Malta while other is located in another Member State.

(d) For non-remote card-based payment transactions, 'domestic payment transactions' refer to payment transactions where the payer's payment service provider (issuer), the payee's payment service provider (acquirer) and the POS or ATM used are located in Malta. If either the payer's payment service provider or the payee's payment service provider, POS or ATM is located in Malta while the other is located in another Member State, the transaction is a 'cross-border payment transaction within the EEA'.

(e) 'Cross-border payment transactions outside the EEA' refer to payment transactions initiated by a payer, or by or through a payee, where either the payer's or the payee's payment service provider is located in Malta while the other is located outside the EEA.

(f) 'Total fraudulent payment transactions' refer to all the transactions mentioned in Paragraph 63 of this Annex, regardless of whether the amount of the fraudulent payment transaction has been recovered.

(g) 'Modification of a payment order by the fraudster' is a type of unauthorised transaction as defined in Paragraph 63(a) of this Annex and refers to a situation where the fraudster intercepts and modifies a legitimate payment order at some point during the electronic communication between the payer's device and the payment service provider (for instance through malware or man-in-the middle attacks) or modifies the payment instruction on the payment service provider's system before the payment order is cleared and settled.

(h) 'Issuance of a payment order by the fraudster' is a type of unauthorised transaction as defined in Paragraph 63(a) of this Annex and refers to a situation where a fake payment order is issued by the fraudster after having obtained the payer's/payee's sensitive payment data through fraudulent means.

66. The Bank should report data from payment service providers offering payment initiation services in accordance with the following:

(a) 'Domestic payment transactions' refer to payment transactions, where the payment initiation service provider and the account servicing payment service provider are located in Malta.

(b) 'Cross-border payment transactions within the EEA' refer to payment transactions, where the payment initiation service provider is located in Malta and the account servicing payment service provider is located in another Member State.

(c) 'Cross-border payment transactions outside the EEA' refer to payment transactions, where the payment initiation service provider is located in Malta and the account servicing payment service provider is located outside the EEA.

Data collection and aggregation

67. The Bank should report statistical information on:

(a) total payment transactions in line with the different breakdowns in Appendix 2 of this Annex and in accordance with Paragraph 64 of this Annex; and

(b) total fraudulent payment transactions in line with the different breakdowns in Appendix 2 of this Annex and as defined under Paragraph 65(f) of this Annex.

68. The Bank should report the statistical information in Paragraph 67 of this Annex both in volume (i.e. number of transactions or fraudulent transactions) and value (i.e. amount of transactions or fraudulent transactions). It should report volumes and values in actual units, with two decimals for values.

69. The Bank should report the values in euro currency. It should covert data for values of transactions or fraudulent transactions denominated in a currency other than the euro, using the relevant exchange rates applied to these transactions or the average ECB reference exchange rate for the applicable reporting period.

70. The Bank can report zero ('0') where there were no transactions or fraudulent transactions taking place for a particular indicator in the reporting period established.

71. The Bank should aggregate the data collected within Malta from the addressees of this Annex by summing the figures reported for each individual payment service provider in line with the data breakdowns in Appendix 2 of this Annex.

72. The Bank should define the secure communication procedures and the format for the reporting of the data by payment service providers. The Bank should also ensure that an appropriate deadline is given to payment service providers to ensure the quality of the data and to account for the potential delay in reporting fraudulent payment transactions.

73. The Bank should ensure that the data reported under this Annex can be cross-referenced and used by the EBA and the ECB in accordance with the data breakdowns in Appendix 2 of this Annex.

Practical data reporting

74. The Bank should report the volumes and values of payment transactions and fraudulent payment transactions in line with Paragraphs 67 and 68 of this Annex. To avoid double counting, data should not be aggregated across the different data breakdowns in Appendix 2 of this Annex.

75. The Bank should report adjustments to data on any payment transaction and fraudulent payment transactions reported in any past reporting period during the next reporting window after the information necessitating the adjustments is obtained from given payment service provider(s) and up to 13 months after the transaction was executed (and/or acquired) to

enable the payment service user to exercise its right to notify the payment service provider no later than 13 months after the transaction was executed in accordance with Paragraph 47 of this Directive.

76. The Bank should at all times ensure the confidentiality and integrity of the information stored and exchanged and the proper identification when submitting data to the ECB and the EBA.

77. The Bank should send the aggregated data to the ECB and the EBA within six months from the day after the end of the reporting period.

78. The Bank should agree with the ECB and the EBA the secure communication procedures and the specific format in which the Bank should report the data.

Cooperation among competent authorities

79. The Bank and the MFSA shall co-ordinate the data collection to ensure that only one set of data is reported for Malta to the ECB and the EBA.

80. Upon request by the competent authority in a home Member State, where Malta is the host Member State, the Bank should make available information and data that established branches in Malta have reported to the Bank.

Appendix 1 – General data to be provided by all reporting payment service providers

General identification data on the reporting payment service provider

Name: full name of the payment service provider subject to the data reporting procedure as it appears in the applicable national register for credit institutions, payment institutions or electronic money institutions

Unique identification number: the relevant unique identification number used in each Member State to identify the payment service provider, where applicable.

Authorisation number: home Member State authorisation number, where applicable.

Country of authorisation: home Member State where the licence has been issued.

Contact person: name and surname of the person responsible for reporting the data or, if a third party provider reports on behalf of the payment service provider, name and surname of the person in charge of the data management department or similar area, at the level of the payment service provider.

Contact e-mail: email address to which any requests for further clarification should be addressed, if needed. It can be either a personal or a corporate e-mail address.

Contact telephone: telephone number through which any requests for further clarification should be addressed, if needed. It can be either a personal or a corporate phone number.

Data breakdown

All data reported by PSPs using the different breakdowns in Appendix 2 of this Annex should follow the geographical breakdown defined below and should provide both number of transactions *(Actual*

units, total for the period) and value of transactions *(EUR/local current actual units, total for the period)*

	Value and volume
Area	Domestic;
	Cross-border *within the* EEA; and
	Cross-border *outside the* EEA

.

Appendix 2 – Data reporting requirements for payment service providers

A – Data breakdown for credit transfers

	Item	Payment transactions	Fraudulent payment transactions
1	**Credit transfers**	**X**	**X**
1.1	Of which initiated by payment initiation service providers	X	X
1.2	Of which initiated non-electronically	X	X
1.3	Of which Initiated electronically	X	X
1.3.1	Of which initiated via remote payment channel	X	X
1.3.1.1	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent credit transfers by fraud types:		
1.3.1.1.1	Issuance of a payment order by the fraudster		X
1.3.1.1.2	Modification of a payment order by the fraudster		X
1.3.1.1.3	Manipulation of the payer by the fraudster to issue a payment order		X
1.3.1.2	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent credit transfers by fraud types:		
1.3.1.2.1	Issuance of a payment order by the fraudster		X
1.3.1.2.2	Modification of a payment order by the fraudster		X
1.3.1.2.3	Manipulation of the payer by the fraudster to issue a payment order		X
	of which broken down by reason for authentication via non-strong customer authentication		
1.3.1.2.4	Low value (Art.16 RTS)	X	X
1.3.1.2.5	Payment to self (Art.15 RTS)	X	X

1.3.1.2.6	Trusted beneficiary (Art.13 RTS)	X	X
1.3.1.2.7	Recurring transaction (Art.14 RTS)	X	X
1.3.1.2.8	Use of secure corporate payment processes or protocols (Art. 17 RTS)	X	X
1.3.1.2.9	Transaction risk analysis (Art.18 RTS)	X	X
1.3.2	Of which initiated via non-remote payment channel	X	X
1.3.2.1	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent credit transfers by fraud types:		
1.3.2.1.1	Issuance of a payment order by the fraudster		X
1.3.2.1.2	Modification of a payment order by the fraudster		X
1.3.2.1.3	Manipulation of the payer by the fraudster to issue a payment order		X
1.3.2.2	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent credit transfers by fraud types:		
1.3.2.2.1	Issuance of a payment order by the fraudster		X
1.3.2.2.2	Modification of a payment order by the fraudster		X
1.3.2.2.3	Manipulation of the payer by the fraudster to issue a payment order		X
	of which broken down by reason for non-strong customer authentication		
1.3.2.2.4	Payment to self (Art.15 RTS)	X	X
1.3.2.2.5	Trusted beneficiary (Art.13 RTS)	X	X
1.3.2.2.6	Recurring transaction (Art.14 RTS)	X	X
1.3.2.2.7	Contactless low value (Art. 11 RTS)	X	X
1.3.2.2.8	Unattended terminal for transport or parking fares (Art. 12 RTS)	X	X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user (payer)	X
Others	X

Validation

1.2 + 1.3 = 1; 1.1 does not equate 1 but is a subset of 1
1.3.1 + 1.3.2 = 1.3
1.3.1.1 + 1.3.1.2 = 1.3.1
1.3.2.1 + 1.3.2.2 = 1.3.2
1.3.1.1.1 + 1.3.1.1.2 + 1.3.1.1.3 = fraudulent payment transaction figure of 1.3.1.1; 1.3.1.2.1 + 1.3.1.2.2 + 1.3.1.2.3 = fraudulent payment transaction figure of 1.3.1.2; 1.3.2.1.1 + 1.3.2.1.2 + 1.3.2.1.3 = fraudulent payment transaction figure of 1.3.2.1; 1.3.2.2.1 + 1.3.2.2.2 + 1.3.2.2.3 = fraudulent payment transaction figure of 1.3.2.2
1.3.1.2.4 + 1.3.1.2.5 + 1.3.1.2.6 + 1.3.1.2.7 + 1.3.1.2.8 + 1.3.1.2.9 = 1.3.1.2
1.3.2.2.4 + 1.3.2.2.5 + 1.3.2.2.6 + 1.3.2.2.7 + 1.3.2.2.8 = 1.3.2.2

B – Data breakdown for direct debits

	Item	Payment transactions	Fraudulent payment transactions
2	**Direct debits**	X	X
2.1	Of which consent given via an electronic mandate	X	X
	of which fraudulent direct debits by fraud type:		
2.1.1.1	Unauthorised payment transactions		X
2.1.1.2	Manipulation of the payer by the fraudster to consent to a direct debit		X
2.2	Of which consent given in another form than an electronic mandate	X	X
	of which fraudulent direct debits by fraud type:		
2.2.1.1	Unauthorised payment transactions		X
2.2.1.2	Manipulation of the payer by the fraudster to consent to a direct debit		X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The payment service user (payee)	X
Others	X

Validation

2.1 + 2.2 = 2
2.1.1.1 + 2.1.1.2 = fraudulent payment transaction figure of 2.1
2.2.1.1 + 2.2.1.2 = fraudulent payment transaction figure of 2.2

C – Data breakdown for card-based payment transactions to be reported by the issuing payment service provider

	Item	Payment transactions	Fraudulent payment transactions
3	**Card payments (except cards with an e-money function only)**	X	X
3.1	Of which initiated non-electronically	X	X
3.2	Of which initiated electronically	X	X
3.2.1	Of which initiated via remote payment channel	X	X
	of which broken down by card function:		
3.2.1.1.1	Payments with cards with a debit function	X	X
3.2.1.1.2	Payments with cards with a credit or delayed debit function	X	X
3.2.1.2	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
3.2.1.2.1	Issuance of a payment order by a fraudster		X
3.2.1.2.1.1	Lost or stolen card		X
3.2.1.2.1.2	Card not received		X
3.2.1.2.1.3	Counterfeit card		X
3.2.1.2.1.4	Card details theft		X
3.2.1.2.1.5	Other		X
3.2.1.2.2	Modification of a payment order by the fraudster		X
3.2.1.2.3	Manipulation of the payer to make a card payment		X
3.2.1.3	**Of which Authenticated via non-strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
3.2.1.3.1	Issuance of a payment order by a fraudster		X
3.2.1.3.1.1	Lost or stolen card		X
3.2.1.3.1.2	Card not received		X
3.2.1.3.1.3	Counterfeit card		X
3.2.1.3.1.4	Card details theft		X

3.2.1.3.1.5	Other		X
3.2.1.3.2	Modification of a payment order by the fraudster		X
3.2.1.3.3	Manipulation of the payer to make a card payment		X
	of which broken down by reason for non-strong customer authentication		
3.2.1.3.4	Low value (Art.16 RTS)	X	X
3.2.1.3.5	Trusted beneficiary (Art.13 RTS)	X	X
3.2.1.3.6	Recurring transaction (Art.14 RTS)	X	X
3.2.1.3.7	Use of secure corporate payment processes or protocols (Art. 17 RTS)	X	X
3.2.1.3.8	Transaction risk analysis (Art.18 RTS)	X	X
►A1 3.2.1.3.9	Merchant initiated transactions[4]	X	X
►A1 3.2.1.3.10	Other	X	X
3.2.2	Of which initiated via non-remote payment channel	X	X
	of which broken down by card function:		
3.2.2.1.1	Payments with cards with a debit function	X	X
3.2.2.1.2	Payments with cards with a credit or delayed debit function	X	X
3.2.2.2	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
3.2.2.2.1	Issuance of a payment order by a fraudster		X
3.2.2.2.1.1	Lost or stolen card		X
3.2.2.2.1.2	Card not received		X
3.2.2.2.1.3	Counterfeit card		X
3.2.2.2.1.4	Other		X
3.2.2.2.2	Modification of a payment order by the fraudster		X
3.2.2.2.3	Manipulation of the payer to make a card payment		X
3.2.2.3	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
3.2.2.3.1	Issuance of a payment order by a fraudster		X
3.2.2.3.1.1	Lost or stolen card		X
3.2.2.3.1.2	Card not received		X

[4] **►A1** i.e, card-based payment transactions that meet the conditions specified by the European Commission in Q&A 2018_4131 and Q&A 2018_4031 and which are, as a result, considered as payee initiated and not subject to the requirement in Article 97 PSD2 to apply SCA

3.2.2.3.1.3	Counterfeit card		X
3.2.2.3.1.4	Other		X
3.2.2.3.2	Modification of a payment order by the fraudster		X
3.2.2.3.3	Manipulation of the payer to make a card payment		X
	of which broken down by reason for non-strong customer authentication		
3.2.2.3.4	Trusted beneficiary (Art.13 RTS)	X	X
3.2.2.3.5	Recurring transaction (Art.14 RTS)	X	X
3.2.2.3.6	Contactless low value (Art.11 RTS)	X	X
3.2.2.3.7	Unattended terminal for transport or parking fares (Art.12 RTS)	X	X
►A1 3.2.2.3.8	Other	X	X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user (payer)	X
Others	X

Validation

3.1 + 3.2 = 3
3.2.1 + 3.2.2 = 3.2
3.2.1.1.1 + 3.2.1.1.2 = 3.2.1; 3.2.2.1.1 + 3.2.2.1.2 = 3.2.2
3.2.1.2 + 3.2.1.3 = 3.2.1; 3.2.2.2 + 3.2.2.3 = 3.2.2
3.2.1.2.1 + 3.2.1.2.2 + 3.2.1.2.3 = fraudulent payment transaction figure of 3.2.1.2; 3.2.1.3.1 + 3.2.1.3.2 + 3.2.1.3.3 = fraudulent payment transaction figure of 3.2.1.3; 3.2.2.2.1 + 3.2.2.2.2 + 3.2.2.2.3 = fraudulent payment transaction figure of 3.2.2.2; 3.2.2.3.1 + 3.2.2.3.2 + 3.2.2.3.3 = fraudulent payment transaction figure of 3.2.2.3
3.2.1.2.1.1 + 3.2.1.2.1.2 + 3.2.1.2.1.3 + 3.2.1.2.1.4 + 3.2.1.2.1.5 = fraudulent payment transaction figure of 3.2.1.2.1; 3.2.1.3.1.1 + 3.2.1.3.1.2 + 3.2.1.3.1.3 + 3.2.1.3.1.4 + 3.2.1.3.1.5 = fraudulent payment transaction figure of 3.2.1.3.1; 3.2.2.2.1.1 + 3.2.2.2.1.2 + 3.2.2.2.1.3 + 3.2.2.2.1.4 = fraudulent payment transaction figure of 3.2.2.2.1; 3.2.2.3.1.1 + 3.2.2.3.1.2 + 3.2.2.3.1.3 + 3.2.2.3.1.4 = fraudulent payment transaction figure of 3.2.2.3.1
►A1 3.2.1.3.4 + 3.2.1.3.5 + 3.2.1.3.6 + 3.2.1.3.7 + 3.2.1.3.8 + 3.2.1.3.9 + 3.2.1.3.10 = 3.2.1.3; 3.2.2.3.4 + 3.2.2.3.5 + 3.2.2.3.6 + 3.2.2.3.7 + 3.2.2.3.8 = 3.2.2.3

D – Data breakdown for card-based payment transactions to be reported by the acquiring payment service provider (with a contractual relationship with the payment service user)

	Item	Payment transactions	Fraudulent payment transactions
4	**Card payments acquired (except cards with an e-money function only)**	X	X
4.1	Of which initiated non-electronically	X	X
4.2	Of which initiated electronically	X	X
4.2.1	Of which acquired via a Remote channel	X	X
	of which broken down by card function:		
4.2.1.1.1	Payments with cards with a debit function	X	X
4.2.1.1.2	Payments with cards with a credit or delayed debit function	X	X
4.2.1.2	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
4.2.1.2.1	Issuance of a payment order by a fraudster		X
4.2.1.2.1.1	Lost or stolen card		X
4.2.1.2.1.2	Card not received		X
4.2.1.2.1.3	Counterfeit card		X
4.2.1.2.1.4	Card details theft		X
4.2.1.2.1.5	Other		X
4.2.1.2.2	Modification of a payment order by the fraudster		X
4.2.1.2.3	Manipulation of the payer to make a card payment		X
4.2.1.3	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
4.2.1.3.1	Issuance of a payment order by a fraudster		X
4.2.1.3.1.1	Lost or stolen card		X
4.2.1.3.1.2	Card not received		X
4.2.1.3.1.3	Counterfeit card		X
4.2.1.3.1.4	Card details theft		X
4.2.1.3.1.5	Other		X

4.2.1.3.2	Modification of a payment order by the fraudster		X
4.2.1.3.3	Manipulation of the payer to make a card payment		X
	of which broken down by reason for non-strong customer authentication		
4.2.1.3.4	Low value (Art.16 RTS)	X	X
4.2.1.3.5	Recurring transaction (Art.14 RTS)	X	X
4.2.1.3.6	Transaction risk analysis (Art.18 RTS)	X	X
►A1 4.2.1.3.7	Merchant initiated transactions[5]	X	X
►A1 4.2.1.3.8	Other	X	X
4.2.2	Of which acquired via a non-remote channel	X	X
	of which broken down by card function:		
4.2.2.1.1	Payments with cards with a debit function	X	X
4.2.2.1.2	Payments with cards with a credit or delayed debit function	X	X
4.2.2.2	**Of which Authenticated via strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
4.2.2.2.1	Issuance of a payment order by a fraudster		X
4.2.2.2.1.1	Lost or stolen card		X
4.2.2.2.1.2	Card not received		X
4.2.2.2.1.3	Counterfeit card		X
4.2.2.2.1.4	Other		X
4.2.2.2.2	Modification of a payment order by the fraudster		X
4.2.2.2.3	Manipulation of the payer to make a card payment		X
4.2.2.3	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent card payments by fraud types:		
4.2.2.3.1	Issuance of a payment order by a fraudster		X
4.2.2.3.1.1	Lost or stolen card		X
4.2.2.3.1.2	Card not received		X
4.2.2.3.1.3	Counterfeit card		X
4.2.2.3.1.4	Other		X
4.2.2.3.2	Modification of a payment order by the fraudster		X
4.2.2.3.3	Manipulation of the payer to make a card payment		X

[5] ►A1 See footnote 4

	of which broken down by reason for non-strong customer authentication		
4.2.2.3.4	Recurring transaction (Art.14 RTS)	X	X
4.2.2.3.5	Contactless low value (Art.11 RTS)	X	X
4.2.2.3.6	Unattended terminal for transport or parking fares (Art.12 RTS)	X	X
►A1 4.2.2.3.7	Other	X	X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user (payee)	X
Others	X

Validation

4.1 + 4.2 = 4
4.2.1 + 4.2.2 = 4.2
4.2.1.1.1 + 4.2.1.1.2 = 4.2.1; 4.2.2.1.1 + 4.2.2.1.2 = 4.2.2
4.2.1.2 + 4.2.1.3 = 4.2.1; 4.2.2.2 + 4.2.2.3 = 4.2.2
4.2.1.2.1 + 4.2.1.2.2 + 4.2.1.2.3 = fraudulent payment transaction figure of 4.2.1.2; 4.2.1.3.1 + 4.2.1.3.2 + 4.2.1.3.3 = fraudulent payment transaction figure of 4.2.1.3; 4.2.2.2.1 + 4.2.2.2.2 + 4.2.2.2.3 = fraudulent payment transaction figure of 4.2.2.2; 4.2.2.3.1 + 4.2.2.3.2 + 4.2.2.3.3 = fraudulent payment transaction figure of 4.2.2.3
4.2.1.2.1.1 + 4.2.1.2.1.2 + 4.2.1.2.1.3 + 4.2.1.2.1.4 + 4.2.1.2.1.5 = fraudulent payment transaction figure of 4.2.1.2.1; 4.2.1.3.1.1 + 4.2.1.3.1.2 + 4.2.1.3.1.3 + 4.2.1.3.1.4 + 4.2.1.3.1.5 = fraudulent payment transaction figure of 4.2.1.3.1; 4.2.2.2.1.1 + 4.2.2.2.1.2 + 4.2.2.2.1.3 + 4.2.2.2.1.4 = fraudulent payment transaction figure of 4.2.2.2.1; 4.2.2.3.1.1 + 4.2.2.3.1.2 + 4.2.2.3.1.3 + 4.2.2.3.1.4 = fraudulent payment transaction figure of 4.2.2.3.1
►A1 4.2.1.3.4 + 4.2.1.3.5 + 4.2.1.3.6 + 4.2.1.3.7 + 4.2.1.3.8 = 4.2.1.3; 4.2.2.3.4 + 4.2.2.3.5+ 4.2.2.3.6 + 4.2.2.3.7 = 4.2.2.3

E – Data breakdown for cash withdrawals using cards to be reported by the card issuer's payment service provider

	Item	Payment transactions	Fraudulent payment transactions
5	**Cash withdrawals**	X	X
	Of which broken down by card function		
5.1	Of which cash withdrawals with cards with a debit function	X	X
5.2	Of which cash withdrawals with cards with a credit or delayed debit function	X	X
	of which fraudulent cash withdrawals by fraud types:		
5.3.1	Issuance of a payment order (cash withdrawal) by the fraudster		X
5.3.1.1	Lost or stolen card		X
5.3.1.2	Card not received		X
5.3.1.3	Counterfeit card		X
5.3.1.4	Other		X
5.3.2	Manipulation of the payer to make a cash withdrawal		X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user (account holder)	X
Others	X

Validation

5.1 + 5.2 = 5
5.3.1 + 5.3.2 = 5
5.3.1.1 + 5.3.1.2 + 5.3.1.3 + 5.3.1.4 = 5.3.1

F – Data breakdown to be provided for e-money payment transactions

	Item	Payment transactions	Fraudulent payment transactions
6	**E-money payment transactions**	**X**	**X**
6.1	**Of which via remote payment initiation channel**	X	X
6.1.1	**of which authenticated via strong customer authentication**	X	X
	of which fraudulent e-money payment transactions by fraud types:		
6.1.1.1	Issuance of a payment order by the fraudster		X
6.1.1.2	Modification of a payment order by the fraudster		X
6.1.1.3	Manipulation of the payer by the fraudster to issue a payment order		X
6.1.2	**of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent e-money payment transactions by fraud types:		
6.1.2.1	Issuance of a payment order by the fraudster		X
6.1.2.2	Modification of a payment order by the fraudster		X
6.1.2.3	Manipulation of the payer by the fraudster to issue a payment order		X
	of which broken down by reason for non-strong customer authentication		
6.1.2.4	Low value (Art.16 RTS)	X	X
6.1.2.5	Trusted beneficiary (Art.13 RTS)	X	X
6.1.2.6	Recurring transaction (Art.14 RTS)	X	X
6.1.2.7	Payment to self (Art. 15 RTS)	X	X
6.1.2.8	Use of secure corporate payment processes or protocols (Art. 17 RTS)	X	X
6.1.2.9	Transaction risk analysis (Art.18 RTS)	X	X
►A1 6.1.2.10	Merchant initiated transactions[6]	X	X
►A1 6.1.2.11	Other	X	X
6.2	**Of which via non-remote payment initiation channel**	X	X

[6] ►A1 See footnote 4

6.2.1	**Of which authenticated via strong customer authentication**	X	X
	of which fraudulent e-money payment transactions by fraud types:		
6.2.1.1	Issuance of a payment order by the fraudster		X
6.2.1.2	Modification of a payment order by the fraudster		X
6.2.1.3	Manipulation of the payer by the fraudster to issue a payment order		X
6.2.2	**Of which authenticated via non-strong customer authentication**	X	X
	of which fraudulent e-money payment transactions by fraud types:		
6.2.2.1	Issuance of a payment order by the fraudster		X
6.2.2.2	Modification of a payment order by the fraudster		X
6.2.2.3	Manipulation of the payer by the fraudster to issue a payment order		X
	of which broken down by reason for non-strong customer authentication		
6.2.2.4	Trusted beneficiary (Art.13 RTS)	X	X
6.2.2.5	Recurring transaction (Art.14 RTS)	X	X
6.2.2.6	Contactless low value (Art.11 RTS)	X	X
6.2.2.7	Unattended terminal for transport or parking fares (Art.12 RTS)	X	X
►A1 6.2.2.8	Other	X	X

Losses due to fraud per liability bearer:	Total losses
The reporting payment service provider	X
The Payment service user	X
Others	X

Validation

6.1 + 6.2 = 6
6.1.1 + 6.1.2 = 6.1; 6.2.1 + 6.2.2 = 6.2
6.1.1.1 + 6.1.1.2 + 6.1.1.3 = fraudulent payment transaction figure of 6.1.1; 6.1.2.1+ 6.1.2.2 + 6.1.2.3 = fraudulent payment transaction figure of 6.1.2; 6.2.1.1 + 6.2.1.2 + 6.2.1.3 = fraudulent payment transaction figure of 6.2.1; 6.2.2.1 + 6.2.2.2 + 6.2.2.3 = fraudulent payment transaction figure of 6.2.2
►**A1** 6.1.2.4 + 6.1.2.5 + 6.1.2.6 + 6.1.2.7 + 6.1.2.8 + 6.1.2.9 + 6.1.2.10 + 6.1.2.11 = 6.1.2; 6.2.2.4 + 6.2.2.5 + 6.2.2.6 + 6.2.2.7 + 6.2.2.8 = 6.2.2

G – Data breakdown to be provided for money remittance payment transactions

	Item	Payment transactions	Fraudulent payment transactions
7	Money remittances	X	X

H – Data breakdown for transactions initiated by payment initiation service providers

	Item	Payment transactions	Fraudulent payment transactions
8	**Payment transactions initiated by payment initiation service providers**	**X**	**X**
8.1	Of which initiated via remote payment channel	X	X
8.1.1	Of which authenticated via strong customer authentication	X	X
8.1.2	Of which authenticated via non-strong customer authentication	X	X
8.2	Of which initiated via non-remote payment channel	X	X
8.2.1	Of which authenticated via strong customer authentication	X	X
8.2.2	Of which authenticated via non-strong customer authentication	X	X
	of which broken down by payment instrument		
8.3.1	Credit transfers	X	X
8.3.2	Other	X	X

Validation

8.1 + 8.2 = 8
8.3.1 + 8.3.2 = 8
8.1.1 + 8.1.2 = 8.1
8.2.1 + 8.2.2 = 8.2