EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-UNRESTRICTED

September 2023

Revised major incident reporting framework for payment schemes, payment arrangements and retail payment systems /sanitised version/

Introduction

This revised major incident reporting framework for payment schemes, payment arrangements and retail payment systems (MIRF) is part of the comprehensive Eurosystem oversight framework for payment systems, schemes and arrangements. The MIRF sets out the provisions for the reporting on incidents:

(i) by the operators of retail payment systems (RPS) and the governance bodies (GBs) of payment schemes/payment arrangements subject to oversight by a Eurosystem central bank, to the respective lead overseers[1], and

(ii) the further sharing of incident reports at Eurosystem/ESCB level by the overseers of RPSs, payment schemes and payment arrangements.

The revised framework will - as of 1 January 2024 - replace the existing major incident reporting framework for payment schemes and retail payment systems from 2018 (applicable since 1 January 2019). In consequence, all reporting entities in scope of the MIRF are requested to classify and report major incidents to their respective lead overseer(s) in accordance with the requirements and definitions laid down in this document and to use the new templates as of 1 January 2024.

The revised framework continues to be aligned with the EBA Guidelines on major incident reporting under PSD2 (EBA GL)[2].

Where a GB of a payment scheme and/or arrangement and/or an operator of a retail payment system is a licensed Payment Service Provider (PSP), an incident concerning the functioning of the respective payment scheme and/or arrangement and/or the retail payment system needs to be reported simultaneously to the lead overseer and the PSP's national competent authority[3] (provided that the respective major incident reporting thresholds are reached). Given the alignment of the reporting frameworks, the reporting entity

[1] As defined in the latest version of the "Eurosystem oversight policy framework"

[2] https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf

[3] Designated under PSD2

may report the incident to the lead overseer using the templates under the EBA GL, indicating in the comment boxes any specific aspects to its role as a payment system operator and/or GB of a payment scheme and/or payment arrangement[4].

1. Scope

This framework refers to major operational and security incidents, including cyber incidents, whose adverse impact has already materialised or will probably materialise, in line with the scope of the PSD2 and the EBA GL.

Early warnings[5] are excluded from the reporting under the new framework due to their abstract nature and the fact that they are not included in the EBA GL.

As regards the addressees, the MIRF encompasses the same retail payment systems as covered by the previous version of the framework. No distinction is made between Systemically Important Retail Payment Systems (SIRPS) and other types of RPSs, and thus all references to RPSs should be understood to involve SIRPS, Prominently Important Retail Payment Systems (PIRPS) and Other Retail Payment Systems (ORPS)[6].

In addition, the MIRF covers payment schemes and payment arrangements that are overseen according to the PISA framework, which covers also the end user perspective.[7]

The geographical scope of the MIRF is limited to entities which are overseen by the Eurosystem irrespective of the location of those entities. However, the reporting obligation extends to major incidents related to their operations in the entire EU.

Non-euro area ESCB overseers may decide to apply the new framework accordingly.

2. Definitions

All definitions are presented in Annex 1 to this note.

The definition of 'operational or security incident' adopted in this framework is aligned with the definitions in the EBA GL and the Major incident reporting framework for large value payment systems (MIRF for LVPS). Some adaptations are made however in view of the addressees: '*a singular event or a series of linked events unplanned by the RPS operator / the payment scheme's / arrangement's governance body*

[4] See Chapter 4 "Notification process and information-sharing", letters a-d.

[5] For example, found weaknesses, vulnerabilities and exploits which have not yet brought any business disruption or loss.

[6] As defined in the "Revised oversight framework for retail payment systems", published in February 2016

[7] The reporting does not apply for payment schemes or arrangements that are monitored or exempted from oversight according to rules defined in the Exemption policy of the PISA framework. See https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_3.en.pdf.

(GB) which has or will probably have an adverse impact on the integrity, availability, confidentiality and/or authenticity of payment-related services including networks'.

The meaning of each of the different dimensions which could be affected by an operational or security incident (i.e. integrity, availability, confidentiality and authenticity), as captured in the definition's part of the EBA GL[8], is also adopted for oversight purposes.

With respect to that the following is applicable:

Concerning retail payment systems, 'payment-related services' should be understood as all those services provided by the payment system operator that are needed to process a payment between participants, including services that have been outsourced or are provided by third parties. These services include, among others, those that allow the transmission of the payment order (e.g. provision of participant's interface, data storage), as well as those which allow for the clearing, netting and settlement. Other services that can be considered accessory (e.g. billing, statistical reporting) are considered to be out of the scope.

Concerning payment schemes, 'payment-related services' should be understood as all those services that are related to the payment scheme functions as defined under the PISA framework, including services that have been outsourced or are provided by third parties. Other services that can be considered accessory (e.g. billing, statistical reporting) are considered to be out of the scope.

Concerning payment arrangements, 'payment-related services' should be understood as all those services that are related to the functionalities of a given payment arrangement, such as the initiation, facilitation and requests to execute transfers of value, the storage or registering of personalised security credentials or the storage of electronic payment instrument related data. This includes services that have been outsourced or provided by third parties. Other services that can be considered accessory (e.g. billing, statistical reporting) are considered to be out of the scope.

3. Classification criteria

RPS operators and GBs of payment schemes/arrangements are required to establish the nature of an operational or security incident and assess its materiality against the following criteria (where applicable): *number of transactions affected, number of participants affected, service downtime, delayed cut-offs, breach of security of network or information systems, level of internal escalation, other relevant financial market infrastructures, payment schemes/arrangements or critical service providers (potentially) affected and reputational impact*[9]. The application of these criteria is further detailed from the perspective of RPS as well as from the perspective of payment schemes and arrangements.

In line with the definitions in Section 2 and Annex 1, the overseen entity needs to assess and report only on classification criteria that are relevant to its system and/or payment scheme/arrangement. In addition, it is acknowledged that some information may be reported only on a best effort basis as it may be relying on

[8] To a large extent, these definitions build upon the ones included in the ISO 27001 standard.

[9] This set of qualitative and quantitative criteria was chosen taking as a basis the existing practices of overseers and supervisors.

third party information or in case of limited information being available at the time of the reporting, may include estimations and approximations.

3.1 Retail payment systems

a) Transactions affected

RPS operators should determine the total number of transactions affected as a percentage of the regular level of processed transactions, understanding the notion of 'transactions' in accordance with the definitions laid down in the rules of the RPS. By 'affected transactions' it should be understood those transactions that have been or will likely be directly or indirectly impacted by the incident and, in particular, those transactions that could not be initiated or processed, for which the content of the payment message was altered, that were fraudulently ordered (whether the funds have been recovered or not) or where the proper execution is prevented or hampered in any other way by the incident. With regard to the inability to initiate and/or process transactions, the reporting should also include information concerning the timeframe (i.e. by how much the processing of the affected transactions has been delayed).

The regular level of processed transactions should be understood as the daily average of all the transactions processed by the RPS within one year, without making distinctions by type of service[10], and taking the previous calendar year as the reference period for calculations. In case the operator did not consider this figure to be representative (e.g. due to seasonality), another more representative metric could be used instead, conveying to the lead overseer(s) the underlying rationale for this approach (e.g. in the comment boxes of the reports).

The methodology for assessing this criterion foresees two sub-thresholds for the classification of "Higher impact" incidents in order to measure both the domestic and cross-border impact of the incidents.

b) Participants affected

RPS operators should determine the number of direct participants affected as a percentage of the total number of direct participants. By 'affected participants' it should be understood those that have suffered or will likely suffer the consequences of the incident, regardless of the type/number of payment instruments cleared/settled in the RPS[11]. The total number of participants should be the number of direct participants in the RPS at the time of the incident or, alternatively in case of the need of estimation, the most recent figure available. In addition, the reporting of affected "indirect participants" should take place on a best endeavours basis - to the best of the RPS operator's knowledge in order to facilitate a comprehensive overview of the situation - but should not be taken into account for calculating the number of participants that would trigger the classification of the impact.

With regard to the inability to initiate and/or process transactions, the reporting should also include information concerning the timeframe (i.e. for how long the participants have been affected).

[10] This seems more practical than trying to cater for all the different organizational setups that the different RPSs may exhibit (e.g. one single system vs. several subsystems)

[11] This means e.g. if the affected clearing/settlement platform of the RPS processes credit transfers as well as direct debits, when assessing an incident, the reporting entity should not differentiate between the participants submitting only credit transfers or only direct debits

The methodology for assessing this criterion foresees two sub-thresholds for the classification of “Higher impact” incidents in order to measure both the domestic and cross-border impact of the incidents.

c) Service downtime

RPS operators should determine the period of time within the RPS opening hours (including settlement hours) during which the system is or may have been unavailable for the participants or during which the operator is or may not have been able to process transactions. Scheduled closing hours and maintenance periods should be excluded. The service downtime should be counted from the moment the downtime started. If RPS operators are unable to determine when the service downtime started, they should exceptionally count the service downtime from the moment the downtime was detected.

d) Breach of security of network or information systems

RPS operators should determine whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of its payment-related services.

e) Delayed cut-off

RPS operators should determine whether the incident is or has been causing certain delay in the cut-offs for same-day settlement.

f) Level of internal escalation

RPS operators should determine whether the incident has been or will likely be reported to the system operator’s executive officers (Chief Information Officer or similar) outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. It is understood that this will happen, among other scenarios, in a situation when a critical process has been affected, there is a reoccurrence of the same type of incident or the disruption happens during a particularly critical time window (e.g. close to a cut-off time). Furthermore, it should be considered 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.

Although the particular case of an incident delaying a cut-off time should be considered under the criterion *delayed cut-off*, due to its importance, any such incident is typically also escalated internally.

g) Other relevant financial market infrastructures, payment schemes/arrangements or critical service providers (potentially) affected

RPS operators should determine the systemic implications the incident will likely have, i.e. its potential to spill over, either directly or indirectly, beyond the initially affected payment system. The operator should assess, among other things, whether the incident has been or will likely be replicated at other financial market infrastructures, whether it has affected or will likely affect the smooth functioning of other financial market infrastructures and/or payment schemes/arrangements and/or one or more of its critical service providers, or whether it has compromised or will probably compromise the sound operation of the financial system as a whole.

The existing interdependencies should be borne in mind (e.g. whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external, or whether the

incident has compromised or will likely compromise the participants' ability to fulfil their obligations in other infrastructures/payment schemes/payment arrangements they are members of).

h) Reputational impact

RPS operators should determine the level of visibility that, to the best of the RPS operator's knowledge, the incident has gained or will likely gain among the participants and other relevant stakeholders. In particular, the likelihood of the incident to cause harm to the market, and ultimately undermine its trust in the payment system, should be considered as a good indicator of its potential to impact the reputation of the RPS.

The RPS operator should take into account whether as a result of the incident: 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 and/or contractual obligations have been or will probably be missed, either by the system or its participants, iii) sanctions have been or will probably be imposed on the system's owner or its participants, or iv) the same type of incident has occurred before.

3.2 Payment schemes / Payment arrangements

a) Transactions affected

The GB of the payment scheme/arrangement should determine the total number of payments, in the case of card payment schemes also the number of terminals[12], service user devices[13] and payment cards, and in the case of providers of digital/electronic wallets also the number of wallets affected as a percentage of the regular level of payment transactions carried out in accordance with the payment scheme's/arrangement's rules / total number of terminals / service user devices / cards / wallets[14], respectively. The notion of "transactions" should be understood in accordance with the definitions laid down in the rules of the scheme/arrangement. 'Affected transactions' should be understood as transactions that have been or will likely be directly or indirectly affected by the incident and, in particular, those that could not be initiated or processed, for which the content of the payment message was altered, that were fraudulently ordered (whether the funds have been recovered or not) or where the proper execution is prevented or hampered in any other way by the incident. With regard to the inability to initiate and/or process transactions, the reporting should also include information concerning the timeframe (i.e. by how much the processing of the affected transactions has been delayed).

The regular level of processed transactions should be understood as the daily average of payments processed according to the rules of the affected payment scheme/arrangement, taking the previous calendar year as the reference period for calculations. In case the GB did not consider this figure to be representative (e.g. due to seasonality), another more representative metric could be used instead, conveying to the lead overseer(s) the underlying rationale for this approach.

[12] ATMs, physical POS terminals and virtual POS terminals

[13] In the sense of the definition for "payment instrument" in PSD2, Art. 4 (14)

[14] Including physical and virtual cards

The total number of terminals / cards / wallets should be the number of terminals provided / cards issued / wallets provided at the time of the incident or, alternatively, the most recent figure available.

In case of an incident where more than one ratio is able to be reported under this criterion (e.g. % of transactions affected and at the same time % of payment cards affected), the most relevant ratio for the particular incident should be taken into account and reported in the dedicated field "As a % of regular number of transactions" for the criterion "transactions affected" of the incident report. Additional ratios (if applicable) should be reported in the appropriate free text fields of the reports (e.g. the comments box for the "transactions affected" criterion).

The methodology for assessing this criterion foresees two sub-thresholds for the classification of "Higher impact" incidents in order to measure both the domestic and cross-border impact of the incidents.

b) Participants affected[15]

The GB of the payment scheme should determine the number of participants affected as a percentage of the total number of participants. By 'affected participants' it should be understood those that have suffered or will likely suffer the consequences of the incident. All participants in the payment scheme should be considered, regardless of the underlying license type or status and/or the role they play for the functioning of the payment scheme (e.g. issuers, acquirers, liquidity providers, settlement banks, stablecoin issuers, etc.). The total number of participants should be the number of participants in the payment scheme at the time of the incident or, alternatively in the case of need of an estimation, the most recent figure available. With regard to the inability to initiate and/or process transactions, the reporting should also include information concerning the timeframe (i.e. for how long the participants have been affected).

The methodology for assessing this criterion foresees two sub-thresholds for the classification of "Higher impact" incidents in order to measure both the domestic and cross-border impact of the incidents.

This criterion shall not apply in cases where the GB of a payment scheme is the only participant[16] (e.g. three-party schemes), the payment scheme has no PSPs acting as participants (e.g. certain e-money schemes) and in case of payment arrangements.

c) Service downtime

The GB of the payment scheme/arrangement should determine the time period during which the services associated to the payment scheme/arrangement has been or will likely be unavailable for the participants and/or end-users or during which the payment transaction cannot be executed by the payment scheme's/arrangement's participants/users. The time intervals when the payment scheme's/arrangement's participants/users are open for business as required for the execution of payment services, where applicable, should be considered. Scheduled closing hours and maintenance periods are excluded. The service downtime should be counted from the moment the downtime started, and if it was not possible to determine when the service downtime started, the service downtime could exceptionally be counted from the moment the downtime was detected.

[15] The payment service providers participating in the payment scheme

[16] The payment service providers' agents are not considered as participants

This criterion **shall not apply** in the specific case of a **payment scheme with no operational functions** (i.e. a payment scheme with a "pure" governance function only).

d) Breach of security of network or information systems

The GB of the payment scheme/arrangement should determine whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of its payment-related services.

e) Delayed cut-off

The GB of the payment scheme should determine whether the incident is or has been causing certain delay in the cut-offs for same-day settlement.

This criterion **shall not apply** in the specific case of a **payment scheme with no operational functions** (i.e. a payment scheme with a "pure" governance function only) and in case of **payment arrangements**.

f) Level of internal escalation

The GB of the payment scheme/arrangement should determine whether the incident has been or will likely be reported to the GB's executive officers (Chief Information Officer or similar) outside any periodical notification procedure and on a continuous basis throughout the lifetime of the incident. It is understood that this will happen, among other scenarios, in a situation when a critical process has been affected, there is a reoccurrence of the same type of incident or the disruption happens during a particularly critical time window (e.g. close to a cut-off time). Furthermore, it should be considered 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.

The particular case of an incident delaying the cut-off time for same-day settlement should be captured under the criterion *delayed cut-off* although this circumstance could be anyway reflected as part of the internal escalation process.

g) Other relevant financial market infrastructures, payment schemes/arrangements or critical service providers (potentially) affected

The GB of the payment scheme/arrangement should determine the systemic implications the incident will likely have, i.e. its potential to spill over, either directly or indirectly, beyond the initially affected payment scheme/arrangement. The GB should assess, among other things, whether the incident has been or will probably be replicated, whether it has affected or will probably affect the smooth functioning of other financial market infrastructures and/or payment schemes/arrangements and/or one or more of its critical service providers.

The existing interdependencies should be borne in mind to the best of the GB's knowledge (e.g. whether the component/software affected is proprietary or generally available, whether the compromised network is internal or external, or whether the incident has compromised or will probably compromise the participants' ability to fulfil their obligations in other relevant infrastructures/payment schemes/payment arrangements).

h) Reputational impact

The GB of the payment scheme/arrangement should determine the level of visibility that, to the best of the GB's knowledge, the incident has gained or will likely gain among the participants and other relevant stakeholders. In particular, the likelihood of the incident to cause harm to the market, and ultimately undermine its trust in the payment scheme/arrangement, should be considered as a good indicator of its potential to impact the reputation of the payment scheme/arrangement.

The GB should take into account whether: 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 and/or contractual obligations have been or will likely be missed, either by the payment scheme/arrangement, its participants and/or by end-users, iii) sanctions have been or will likely be imposed on the GB of the payment scheme/arrangement or on the participants, or iv) a similar type of incident has occurred before.

3.3 Assessment of the materiality of an incident

Payment system operators / GBs of payment schemes/arrangements are required to establish the materiality of an incident by determining, for each individual criterion, whether the relevant thresholds listed in the table below are or will probably be reached before the incident is solved. These thresholds are furthermore structured along two potential levels of severity, one lower ('Lower impact level') than the other ('Higher impact level'). Should actual data not be available, the RPS operators / GBs of payment schemes/arrangements are allowed to recur to estimations, which should aim at forecasting the levels the different criteria may reach before the incident is solved.

The payment system operator / GBs of payment schemes/arrangements would classify as major those incidents that fulfil either i) one or more criteria at the 'Higher impact level' or ii) three or more criteria at the 'Lower impact' level. In case of doubt, the reporting entity should report based on the preliminary information or estimations available and opt for the higher classification.

	Retail payment systems		**Payment schemes / Payment arrangements**	
	Lower impact	**Higher impact**	**Lower impact**	**Higher impact**
Transactions / terminals / service user devices / cards / wallets *(For operational incidents, this criterion is applicable only in case the processing[17] of the affected transactions is impossible*	≥ 5 % of the RPS transactions affected in	≥ 10 % of the RPS transactions affected in one single jurisdiction; or	≥ 5 % of the payment scheme's/arrangement's transactions / terminals / service user devices / cards / wallets affected in one single jurisdiction	≥ 10 % of the payment scheme's/arrangement's transactions / terminals / service user devices / cards / wallets affected in one single jurisdiction;

[17] For payment schemes and payment arrangements this includes also situations where the initiation of transactions is not possible

during the current business day or delayed for more than 2 hours[18])	one single jurisdiction[19]	≥ 2% of transactions affected across the EU		or ≥ 2% of transactions / terminals / cards / wallets affected across the EU
Participants[20] *(For operational incidents, this criterion is applicable only in case the processing[19] of the affected transactions is impossible during the current business day or delayed for more than 2 hours[1820])*	≥ 5 % of participants affected in one single jurisdiction	≥ 10 % of participants affected in one single jurisdiction; or ≥ 2% of participants affected across the EU	≥ 5 % of participants affected in one single jurisdiction	≥ 10 % of participants affected in one single jurisdiction; or ≥ 2% of participants affected across the EU
Downtime[21]	Not applicable	≥ 2 hours *for RPSs operating under Instant payment schemes:* ≥ 1 hour	Not applicable	≥ 2 hours *for Instant payment schemes:* ≥ 1 hour
Breach of security of network or information systems	Yes	Not applicable	Yes	Not applicable
Delayed cut-off[22]	Not applicable	cut-off time is delayed for at least 1 hour	Not applicable	cut-off time is delayed for at least 1 hour

[18] Refers to both sub-thresholds – for the single jurisdiction transactions as well as for the transactions across EU

[19] Transactions carried out when both participants (payer's and payee's PSP) belong to an individual jurisdiction (e.g. located in a single country)

[20] This criterion shall not apply in cases where the GB of a payment scheme is the only participant (e.g. three party schemes), the payment scheme has no PSPs acting as participants (e.g. certain e-money schemes) and in case of payment arrangements.

[21] This criterion shall not apply for payment schemes with no operational functions.

[22] This criterion shall not apply for payment schemes with no operational functions nor for payment arrangements.

High level of internal escalation	Yes	Yes, and a crisis mode (or equivalent) is (likely) to be triggered	Yes	Yes, and a crisis mode (or equivalent) is (likely) to be triggered
Other FMIs, payment schemes/arrangements and/or critical service providers (potentially) affected	Yes	Not applicable	Yes	Not applicable
Reputational impact	Yes	Not applicable	Yes	Not applicable

4. Notification process and information-sharing

Notwithstanding any other legal requirement to share incident-related information with domestic or European authorities, the GBs of the payment schemes/arrangements and retail payment systems' operators should provide information about major operational or security incidents to the respective lead overseer(s). The reporting entities should collect all relevant information about the incidents, produce incident reports (initial, intermediate and final reports to be collected in one file) by completing the templates provided in Annex 2, and submit them to the lead overseer(s). Reporting entities should use the same template when submitting the initial, intermediate and final reports related to the same incident, i.e. they should complete a single template in an incremental manner and update, where applicable, the information provided with previous reports. In case actual data are not available, the reporting entities should provide best effort estimates whenever possible.

If an incident has been detected that is potentially major, the GB of the overseen payment scheme/arrangement and/or the retail payment system operator should send an informal notification to the respective lead overseer(s) without undue delay and in any case before the public is informed. Thereafter a formal initial incident report should be submitted according to the below procedure. Where in the course of the later developments an incident materialises to be only of a minor nature, the overseen entity informs the lead overseer(s) by submitting a final report as described below.

Initial report:

Reporting entities should classify the incident in accordance with section 3.3 of this document in a timely manner after the incident has been detected, but no later than 24 hours after the detection of the incident, and without undue delay after the information required for the classification of the incident is available. If a

longer time is needed to classify the incident, reporting entities should explain in the initial report submitted to the lead overseer(s) the reasons why.

The initial report should be submitted to the lead overseer(s) after an operational or security incident has been classified as major. The reporting entities should send the initial report within 4 hours from the moment the operational or security incident has been classified as major, or, if the reporting channels to the lead overseers are known not to be available or operational at that time, as soon as they become available/operational again. If an incident originally classified as minor evolves into a major one, the reporting deadlines are to be interpreted as to start at this moment. In this respect, the reporting entity is invited to make all time references throughout the incident reports using the same time zone (e.g. CET), duly indicating it in the respective fields in the reports.

The lead overseer(s) should acknowledge the receipt of the initial report and assign a unique reference code unequivocally identifying the incident.[23] Reporting entities should indicate this reference code in any subsequent communication concerning the incident (including the respective sheets for the intermediate or final report as well as for updates on the initial report).

Intermediate report:

The intermediate report should be submitted to the lead overseer(s) when regular activities have been recovered and business is back to normal, informing the lead overseer(s) of this circumstance. Reporting entities should consider business is back to normal when activity/operations are restored with the same level of service/conditions as defined by the GB of the payment scheme/arrangement / the retail payment system operator or as laid out externally by a service level agreement (processing times, capacity, security requirements, etc.) and when contingency measures are no longer in place. The intermediate report should include a more detailed description of the incident and its consequences. If available in time, the final report can be sent with the intermediate report.

If regular activities have not yet been recovered within three working days from the submission of the initial report, reporting entities should submit a first intermediate report to the lead overseer(s).

Reporting entities should update the information already provided by sending an additional intermediate report when they become aware of significant changes since the submission of the previous report (e.g. whether the incident has escalated or decreased, new causes are identified or actions have been taken to fix the problem). In any case, reporting entities should submit an additional intermediate report at the request of the respective lead overseer(s).

Final report:

The GB of the payment scheme/arrangement or the retail payment system operator should send the final report when the root cause analysis has taken place (regardless of whether mitigation measures have already been implemented or the final root cause has been identified) or the incident is not considered

[23] Each lead overseer should include as a prefix the 2-digit ISO country code (ISO-3166) of their respective Member State. In case the ECB is the lead overseer of a respective RPS, payment scheme or payment arrangement, it should include ‘EU’ as a prefix to its unique reference code.

major anymore and needs to be reclassified. It should comprise all relevant information about the incident not yet provided. In particular, it should include the actual figures available in order to replace any earlier made estimates. This final report should be delivered to the lead overseer(s) within a maximum of 20 working days after business is deemed back to normal. If an extension of this deadline would be needed (e.g. if there are no actual figures on the impact available yet or the root cause has not been identified yet), the reporting entity should contact the lead overseer(s) before the deadline has lapsed and provide an additional intermediate report containing any available information for the final report along with an adequate justification for the delay, as well as a new estimated date for the final report.

Reporting entities 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 fulfils the criteria to be considered major and is not expected to fulfil them before the incident is resolved. In this case, they should send the final report as soon as this circumstance is detected and, in any case, within the deadline for the submission of the next report. In this particular situation, instead of filling out the final report section of the template, reporting entities should check the box 'incident reclassified as non-major' and provide an explanation of the reasons justifying this reclassification

The reporting entities should agree with their respective lead overseers the details on the contacts and channels of secure communication to be used, as well as the availability of these channels (i.e. specific working hours, 24/7/365, etc.).

Although based on those developed for the EBA GL, the reporting templates under the MIRF have been modified to reflect the classification criteria and the methodology applicable for the particular addressees – i.e. RPSs, payment schemes and payment arrangements. The main differences in the fields to be reported in the templates under the new framework with respect to those under the EBA GL are:

a) Criterion *"Transactions affected"*: Only the *number* of transactions is considered <u>without</u> the *value* of transactions affected; Reporting thresholds under the MIRF refer exclusively to relative ratios, while thresholds under the EBA GL also include absolute figures;
b) Criterion *"Participants affected"*: To be reported under the MIRF instead of "*Payment service users affected"* (which is to be reported under the EBA GL); Reporting thresholds under the MIRF refer exclusively to relative ratios, while thresholds under the EBA GL also include absolute figures;
c) Criterion *"Delayed cut-off*: To be reported (if applicable) under the MIRF*;*
d) "*Economic impact"* is <u>not</u> to be reported under the MIRF*.*

Where a PSP is also operating a payment scheme, a payment arrangement and/or a retail payment system it may choose to report the incident to the lead overseer(s) using the EBA GL templates[24]. In this case, the reporting entity should however indicate the specific aspects of the incident to its operations as payment system / scheme / arrangement (e.g. "Delayed cut-off" criterion) in the free text boxes of the reports (e.g. intermediate report - B1 General details).

[24] No prior approval would be needed for this from the respective lead overseer(s).

Upon receipt of the reports from the respective retail payment systems, payment schemes and payment arrangements affected by major operational or security incidents, the respective lead overseers should, without undue delay, provide the ECB with each individual report.

As major incidents may have serious implications for other entities than the directly affected parties and as the wider knowledge on new threats may help to contain the damage potentially caused by them, the sharing of relevant information on major incidents is considered very important. The lead overseer(s) will share relevant information of a payment system/scheme/arrangement major incident with the Eurosystem[25] and the ESCB[26]. Where relevant the information may in a sanitized and, if necessary, anonymised form be shared with other EU/EEA authorities on a need-to-know basis, respecting existing legal arrangements and requirements and the principle of professional secrecy. Authorities may decide also to inform other market participants about relevant general aspects or lessons obtained from such major incidents reports, provided that the originator of the report is not disclosed (unless the originator is anyway known to the public). However, it should be ensured that the sharing of such information is neither commercially sensitive nor reveals exploitable security or operational vulnerabilities that can be linked to a specific overseen entity. Therefore, the lead overseer(s) should seek prior consent of the overseen entity before sharing information obtained from major incident reports with other market participants.

When sharing such information, the authorities will act under the principle of professional secrecy and give due account to protection of personal data and the potential impact on competition.

[25] As default

[26] Decision on a case-by-case basis

ANNEX 1 – Definitions

Operational or security incident	A singular event or a series of linked events unplanned by the RPS operator / the payment scheme/arrangement GB, which has or will likely have an adverse impact on the integrity, availability, confidentiality and/or authenticity of payment-related services including networks. Cyber security incidents and data leakages are also included.
Cyber security incident	An event that: i). jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; and/or ii). violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
Cyber security	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
Processed transactions (in the context of an RPS)	Refers to payment transactions carried out within a payment system between the participants of the system. All different stages of processing should be included e.g. acceptance, validation, netting of transfer orders, clearing, settlement, etc.
Integrity	The property of safeguarding the accuracy and completeness of assets (including data).
Availability	The property of payment-related services being fully accessible and usable by authorised clients / participants.
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.
Payment-related services	For RPSs: all those services provided by the payment system operator that are needed to process a payment between participants, including services that have been outsourced or are provided by third parties. These services include, among others, those that allow the transmission of the payment order (e.g. provision of participant's interface, data storage), as well as those which allow for the clearing, netting and settlement. Other services that can be considered accessory (e.g. billing, statistical reporting) would be out of the scope. For payment schemes: all those services that are related to the payment scheme functions as defined under the PISA framework, including services that have been outsourced or are provided by third parties.. Other services that can be considered accessory (e.g. billing, statistical reporting) are considered to be out of the scope. For payment arrangements: all those services that are related to the functionalities of a given arrangement, such as the initiation, facilitation and requests to execute transfers of value, the storage or registering of personalised security credentials or the storage of electronic payment instrument related data. This include services that have been outsourced or provided by third parties. Other services that can be considered accessory (e.g. billing, statistical reporting) are considered to be out of the scope.

ANNEX 2 – Templates for major incident reporting

The major incident reports templates are provided in a separate document.

A general description of the main fields and categories to be reported is provided in the ‘Explanatory notes’ sheet included in the reporting templates (the remainder are either explained in the main document or are self-explanatory).