ANNEX 2

Instructions to fill in the template in Annex 1

Payment service providers shall fill in the relevant section of the template in Annex 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: first notification that the payment service provider ("PSP") submits to the Financial Information Authority (Article 30 of the Instruction).

Intermediate report: update of a previous (initial or intermediate) report on the same incident (Article 31 (1)-(4) of the Instruction).

Last intermediate report: report which informs the Financial Information Authority that regular activities have been recovered and operations are back to normal, so no more intermediate reports will be submitted (Article 31 (5) of the Instruction).

Final report: last report the PSP sends to the Financial Information Authority 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 (Article 32 (1)-(4) of the Instruction).

Incident reclassified as non-major: the incident no longer fulfils the criteria to be considered major and is not expected to fulfil them before it is resolved (Article 32 (5) of the Instruction). PSPs shall explain the reasons for this downgrading.

Report date and time: exact date and time of submission of the report to the Financial Information Authority.

Incident identification number (for intermediate and final report): the reference number issued by the Financial Information Authority at the time of the initial report to uniquely identify the incident, if applicable.

A – Initial Report

A 1 – General Information

Payment Service Provider affected: refers to the PSP that is experiencing the incident.

- *PSP name*: full name of the PSP subject to the reporting procedure;

- *PSP authorization date*: date on which the PSP has been authorized by the Financial Information Authority;

- *Jurisdiction/s affected by the incident*: jurisdiction or jurisdictions where the impact of the incident has materialized;

- *Primary contact person*: first name and surname of the person responsible for reporting the incident or first name and surname of the person in charge of the risk management function of the PSP affected;

- *Email*: email address of the primary contact person or dedicated email address to which any requests for further clarifications could be addressed, if needed;

- *Telephone*: telephone number of the primary contact person or dedicated telephone number to call with any requests for further clarifications, if needed;

- *Secondary contact person*: first name and surname of an alternative person who could be contacted by the Financial Information Authority to inquiry about an incident, when the primary contact person is not available;

- *Email*: email address of the alternative contact person;

- *Telephone*: telephone number of the alternative contact person.

A 2 – 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: (i) a payment service user; (ii) IT function; (iii) another internal function within the PSP; (iv) none of the above. In cases (iii) and (iv), the internal function (e.g. internal audit) shall be indicated – case (iii) – or explanations shall be provided – case (iv) – in the corresponding field.

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

Estimated time for the next update: estimated date and time for the submission of the next update (interim or final report).

B – Intermediate Report

B 1 – General Information

More detailed description of the incident: describe the main features of the incident, covering at least the points featured in the template (i.e. what specific issue the PSP is facing; how it happened and developed; possible relations with a previous incident; consequences, especially for payment service users; how the incident has been detected; area affected; actions taken so far; possible third parties affected).

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 items impacted 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: date and time when the incident was or is expected to be under control, and activity was or is expected to be back to normal.

B 2 – Incident Classification and Information on the Incident

Overall impact: 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 unauthorized individuals, entities or processes;

- *Authenticity*: the property of a source being what it claims to be.

- *Continuity*: the property of an entity's processes, tasks, offices and assets needed for the delivery of payment-related services being fully accessible and running at acceptable predefined levels.

Transactions affected: PSPs shall indicate which thresholds are or will probably be reached by the incident, pursuant to Article 28 of the Instruction, and the related figures (i.e. 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), consistently with the methodology referred to in Article 27 (a) of the Instruction. PSPs shall provide specific values for these variables, which may be either actual figures or estimations.

If PSPs do not consider this figure to be representative (e.g. because of seasonality), they should use another, more representative, metric instead, and convey the underlying rationale for this approach in the field 'Comments'.

Payment service users affected: PSPs shall indicate which thresholds are or will probably be reached by the incident, pursuant to Article 28 of the Instruction, and the related figures (i.e. 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), consistently with the methodology referred to in Article 27 (b) of the Instruction. PSPs shall provide specific values for these variables, which may be either actual figures or estimations.

Service downtime: PSPs shall indicate if the threshold is or will probably be reached by the incident, pursuant to Article 28 of the Instruction, and the related figure (i.e. total service downtime), consistently with the methodology referred to in Article 27 (c) of the Instruction. PSPs shall provide specific values for this variable, which may be either actual figures or estimations.

If PSPs 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: PSPs shall indicate if the threshold is or will probably be reached by the incident, pursuant to Article 28 of the Instruction, and the related figures (i.e. direct costs and indirect costs), consistently with the methodology referred to in Article 27 (d) of the Instruction. PSPs shall provide specific values for these variables, which may be either actual figures or estimations.

In particular:

- *Direct costs*: amount of money (euro) directly attributable to the incident, including funds needed to rectify the incident (e.g. expropriated funds or assets, replacement costs of hardware and software, fees due to non-compliance with contractual obligations);

- *Indirect costs*: amount of money (euro) indirectly attributable to 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: PSPs shall assess what established by Article 26 (e) of the Instruction, consistently with the methodology referred to in Article 27 (e), including, if appropriately, the issue indicated within the template.

Other PSPs or relevant infrastructures potentially affected: PSPs shall assess what established by Article 26 (f) of the Instruction, consistently with the methodology referred to in Article 27 (f), including, if appropriately, the issue indicated within the template.

Reputational impact: PSPs shall assess what established by Article 26 (g) of the Instruction, consistently with the methodology referred to in Article 27 (g), including, if appropriately, the issue indicated within the template.

B 3 – 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*: unauthorized access, use, disclosure, disruption, modification or destruction of the PSP's assets that affect the integrity, availability, confidentiality, authenticity and/or continuity of payment-related services. This may happen when, among other things, the PSP 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 PSP (e.g. malware attacks);

- *Internal attack*: the source of the cause comes from inside, and is intentionally targeting the PSP (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*: unauthorized act of spying, snooping and stealing information through cyberspace;
>
> - *Other*: any other type of attack the PSP 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 shall be ticked. Details shall be added in the free text field.

- *External events*: the cause is associated with events generally outside the operational 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, 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 shall be provided in the free text field.

How the incident affects the PSP: an incident can target a PSP directly or affect it indirectly, through a third party. In the case of an indirect impact, provide the name of the service provider(s).

B 4 – Incident impact

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

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

- *Head office*;

- *Telephone services* (the use of telephones/fax to carry out financial transactions);

- *E-mail services* (the use of e-mails to carry out financial transactions);

- *SecureMail* (the use of *SecureMail* to carry out financial transactions);

- *ATMs* (electro-mechanical devices that allow payment service users to withdraw cash from their accounts and/or access other services);

- *Points of sale (POS)* (physical premises of the merchant at which the payment transaction is initiated);

- *Other* (the commercial channel affected is none of the above). Further details shall 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 PSP to credit it on a payment account;

- *Cash withdrawal from a payment account*: the request received by a PSP 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);

- *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 PSP 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 PSP or to the payer's own PSP;

- *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 PSP contracting with a payer to provide her with a payment instrument to initiate and process the payer's payment transactions.

- *Other*: the payment service affected is none of the above. Further details shall 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 PSP 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 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 PSP and other PSPs;

- *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 PSP 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 PSP on behalf of the affected PSP;

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

Systems and components affected: indicate which part or parts of the PSP'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 PSP;

- *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 PSPs to carry out their payment-related activity;

- *Network/infrastructure*: telecommunications networks, either public or private, that allow for 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 shall be provided in the free text field.

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

B 5 – Incident Mitigation

Actions/measures that have been taken so far or are planned to recover from the incident: details about actions that have been taken or are planned to be taken to temporarily address the incident;

Activation of the operational continuity plans and/or disaster recovery plans: indicate whether or not such plans have been activated, and, if so, provide the most relevant details of what happened (i.e. when plans were activated and what these plans consisted of);

Cancellation or weakening of the intensity of some control measures due to the incident: whether or not the PSP 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

C 1 – General Information

Update of the information from the intermediate report (summary): further information, including at least what indicated into the schedule (i.e. actions taken to recover from the incident and avoid its recurrence; final remediation actions taken, analysis of the root cause, lessons learned, additional actions taken, any other relevant information).

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

If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?: indicate whether or not controls are back in place, and provide any additional information in the free text field.

C 2 – Root Cause Analysis and Follow-up

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

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

C 3 –Additional information

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

Has any legal action/claim been taken/presented against the PSP?: indicate whether or not, at the time of filling in the final report, the PSP has suffered any legal action (e.g. been taken to court) or a claim, as a result of the incident.