Allegato 1 – Modulo di segnalazione per i prestatori di servizi di pagamento

CLASSIFICATION: RESTRICTED

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 ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected — ☐ Actual figure ☐ Estimation As a % of regular number of transactions — ☐ Actual figure ☐ Estimation Value of transactions affected in EUR — ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected — ☐ Actual figure ☐ Estimation As a %-of total payment service users — ☐ Actual figure ☐ Estimation
Service downtime[4]	Total service downtime DD:HH:MM — ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR — ☐ Actual figure ☐ Estimation Indirect costs in EUR — ☐ 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 ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ 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 - addittional 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 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 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 200,000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs

PSP Name	PSP Unique Identification Number	PSP Authorisation number

ISTRUZIONI PER LA COMPILAZIONE DEGLI SCHEMI

I prestatori di servizi di pagamento dovrebbero compilare la pertinente sezione del modulo, a seconda della fase di segnalazione in cui si trovano: sezione A per il rapporto iniziale, sezione B per i rapporti intermedi e sezione C per il rapporto finale. Tutti i campi sono obbligatori, a meno che non diversamente specificato.

Titolo

Rapporto iniziale: primo rapporto che il PSP sottomette all'autorità competente dello Stato membro di origine.

Rapporto intermedio: aggiornamento di un rapporto precedente (iniziale o intermedio) relativo allo stesso incidente.

Ultimo rapporto intermedio: rapporto che informa l'autorità competente dello Stato membro di origine che le normali attività sono state ripristinate e che le operazioni sono tornate alla normalità, per cui non verranno presentati nuovi rapporti intermedi.

Rapporto finale: ultimo rapporto che il PSP invia in merito all'incidente, poiché (i) è già stata eseguita un'analisi delle cause all'origine dell'incidente e le stime possono essere sostituite con dati effettivi o (ii) l'incidente non è più considerato grave.

Incidente riclassificato come non grave: l'incidente non soddisfa più i criteri per essere classificato come grave e non si prevede che li soddisfi prima che il problema venga risolto. I PSP dovrebbero spiegare le ragioni di questa riclassificazione.

Data e ora del rapporto: data e ora esatte di sottomissione del rapporto all'autorità competente.

Numero di identificazione dell'incidente, se applicabile (per i rapporti intermedi e finali): numero di riferimento rilasciato dall'autorità competente al momento della segnalazione iniziale per identificare in modo univoco l'incidente, se applicabile (ossia se tale riferimento è fornito dall'autorità competente).

A – Rapporto iniziale

A 1 – Informazioni generali

Tipo di rapporto

Individuale: il rapporto si riferisce a un solo PSP.

Consolidato: il rapporto si riferisce a diversi PSP che si avvalgono dell'opzione di segnalazione consolidata. I campi sotto il titolo «PSP interessato» dovrebbero essere lasciati vuoti (ad eccezione del campo «paese/paesi interessato/i dall'incidente») e dovrebbe essere fornito un elenco dei PSP inclusi nel rapporto compilando la tabella corrispondente (Rapporto consolidato - Elenco dei PSP).

PSP interessato: si riferisce al PSP coinvolto nell'incidente.

Nome PSP: nome completo del PSP soggetto alla procedura di segnalazione, come appare nell'apposito registro nazionale ufficiale dei PSP.

Numero di identificazione del PSP, se pertinente: il numero di identificazione univoco utilizzato in ciascuno Stato membro per identificare il PSP, da comunicare se il campo «Numero di autorizzazione PSP» non è compilato.

Numero di autorizzazione del PSP: numero di autorizzazione dello Stato membro di origine.

Capogruppo: in caso di gruppi di entità, come definiti nell'articolo 4, paragrafo 40, della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive

2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e che abroga la direttiva 2007/64/CE, indicare il nome dell'entità capogruppo.

Paese di origine: Stato membro in cui è situata la sede legale del PSP o, laddove il PSP, ai sensi della propria legislazione nazionale, non disponga di una sede legale, lo Stato membro in cui è situata la sede centrale.

Paese/paesi interessato/i dall'incidente: paese o paesi in cui si è verificato l'incidente (ad esempio, sono interessate diverse succursali di un PSP situate in vari Stati). Può essere o meno lo stesso Stato membro di origine.

Referente principale da contattare: nome e cognome della persona responsabile della segnalazione dell'incidente oppure, se una terza parte effettua la segnalazione per conto del PSP interessato, nome e cognome del responsabile della gestione degli incidenti o della funzione di gestione dei rischi o di una funzione con compiti simili del PSP interessato.

E-mail: indirizzo e-mail a cui inviare eventuali richieste di ulteriori chiarimenti, se necessario. Può essere un'e-mail personale o aziendale.

Telefono: numero di telefono cui richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

Referente secondario da contattare: nome e cognome di una seconda persona che potrebbe essere contattata dall'autorità competente per chiedere informazioni su un incidente quando il referente principale non è disponibile. Se una terza parte effettua la segnalazione per conto del PSP interessato, nome e cognome di una seconda persona responsabile della gestione degli incidenti o della funzione di gestione dei rischi o di una funzione con compiti simili del PSP interessato

E-mail: indirizzo e-mail del referente secondario a cui inviare eventuali richieste di ulteriori chiarimenti, se necessario. Può essere un indirizzo e-mail personale o aziendale.

Telefono: numero di telefono del referente secondario cui richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

Entità segnalante: questa sezione dovrebbe essere compilata se un terza parte adempie gli obblighi di segnalazione per conto del PSP interessato.

Nome dell'entità segnalante: nome completo dell'entità che segnala l'incidente, come indicato nell'apposito registro nazionale ufficiale delle imprese.

Numero di identificazione, se pertinente: numero di identificazione univoco utilizzato nel paese in cui ha sede la terza parte per identificare l'entità che effettua la segnalazione dell'incidente, fornito dall'entità segnalante se il campo «Numero di autorizzazione» non è compilato.

Numero di autorizzazione, se applicabile: numero di autorizzazione della terza parte nel paese dove questo ha sede, se applicabile.

Referente principale da contattare: nome e cognome della persona responsabile della segnalazione dell'incidente.

E-mail: indirizzo e-mail a cui inviare eventuali richieste di ulteriori chiarimenti, se necessario. Può essere un'e-mail personale o aziendale.

Telefono: numero di telefono per richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

Referente secondario da contattare: nome e cognome di una seconda persona dell'entità che effettua la segnalazione dell'incidente che potrebbe essere contattata dall'autorità competente quando il referente principale da contattare non è disponibile.

E-mail: indirizzo e-mail della seconda persona di contatto a cui inviare eventuali richieste di ulteriori chiarimenti, se necessario. Può essere un indirizzo e-mail personale o aziendale.

Telefono: numero di telefono della seconda persona di contatto per richiedere ulteriori chiarimenti, se necessario. Può essere un numero di telefono personale o aziendale.

A 2 – Rilevazione dell'incidente e classificazione iniziale

Data e ora di rilevazione dell'incidente: data e ora in cui l'incidente è stato identificato per la prima volta.

Incidente rilevato da: indicare se l'incidente è stato rilevato da un utente di servizi di pagamento, da un'altra funzione interna del PSP (ad esempio, la funzione di audit interno) o da una entità esterna (ad esempio, un prestatore di servizi esterno). Se nessuno dei casi precedenti fosse applicabile, fornire una spiegazione nel campo corrispondente.

Breve descrizione generale dell'incidente: chiarire brevemente le problematiche più rilevanti dell'incidente, includendo le possibili cause, gli impatti immediati, ecc.

Qual è il momento stimato del prossimo aggiornamento?: indicare data e ora stimate per la presentazione dell'aggiornamento successivo (rapporto intermedio o finale).

B – Rapporto intermedio

B 1 – Informazioni generali

Descrizione più dettagliata dell'incidente: descrivere le caratteristiche principali dell'incidente, trattando quantomeno i punti contenuti nel questionario (qual è il problema specifico che il PSP deve affrontare, come ha avuto inizio e come si è sviluppato, possibile collegamento con un incidente precedente, conseguenze, in particolare per gli utenti di servizi di pagamento, ecc.).

Data e ora di inizio dell'incidente: data e ora in cui l'incidente è iniziato, se noto.

Status dell'incidente

Diagnosi: le caratteristiche dell'incidente sono appena state identificate.

Riparazione: gli elementi impattati sono in riconfigurazione.

Recupero: gli elementi impattati vengono ripristinati all'ultimo salvataggio recuperabile.

Ripristino: i servizi connessi ai pagamenti sono nuovamente forniti.

Data e ora in cui l'incidente è stato risolto o si prevede di risolverlo: indicare la data e l'ora in cui l'incidente è stato o sarà sotto controllo e l'attività è o sarà tornata alla normalità.

B 2 – Classificazione degli incidenti/Informazioni sull'incidente

Impatto generale: indicare quali dimensioni sono state interessate dall'incidente. È possibile contrassegnare più caselle.

Integrità: proprietà di salvaguardia dell'esattezza e della completezza delle risorse (inclusi i dati).

Disponibilità: proprietà dei servizi connessi ai pagamenti di essere accessibili e utilizzabili da parte degli utenti dei servizi di pagamento.

Riservatezza: proprietà per cui l'informazione non è resa disponibile o divulgata a persone, entità o procedure non autorizzate.

Autenticità: proprietà di una fonte di essere quella che dichiara di essere.

Continuità: Proprietà delle procedure, attività e risorse di un'organizzazione funzionali all'erogazione dei servizi connessi ai pagamenti di essere pienamente fruibili e operative a livelli di servizio accettabili e predefiniti.

Transazioni interessate: i PSP dovrebbero indicare quali soglie sono o saranno probabilmente raggiunte dall'incidente, se del caso, e i relativi dati: il numero di transazioni interessate, la percentuale di transazioni interessate in relazione al numero di transazioni di pagamento effettuate con gli stessi servizi di pagamento che sono stati interessati dall'incidente e al valore

totale delle transazioni. Per queste variabili, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. Le entità che effettuano la segnalazione per conto di più PSP (ossia la segnalazione consolidata) possono invece indicare intervalli di valori che rappresentano i valori più bassi e più elevati osservati o stimati all'interno del gruppo di PSP inclusi nel rapporto, separati da un trattino. Come regola generale, i prestatori di servizi di pagamento dovrebbero considerare come «transazioni interessate» tutte le transazioni nazionali e transfrontaliere che sono state o saranno probabilmente interessate, direttamente o indirettamente, dall'incidente e, in particolare, quelle transazioni che potrebbero non essere avviate o gestite, quelle per le quali è stato modificato il contenuto del messaggio di pagamento e quelle ordinate in modo fraudolento (a prescindere dal fatto che i fondi siano stati recuperati o meno). Inoltre, i PSP dovrebbero intendere come livello normale di transazioni di pagamento la media annuale giornaliera delle transazioni di pagamento nazionali e transfrontaliere effettuate con gli stessi servizi di pagamento interessati dall'incidente, considerando l'anno precedente come periodo di riferimento per i calcoli. Se i prestatori di servizi di pagamento non ritengono che tale dato sia rappresentativo (ad esempio, a causa della stagionalità), essi dovrebbero utilizzare un'altra metrica, più rappresentativa, e comunicare all'autorità competente la motivazione alla base di tale approccio compilando il campo «Commenti».

Utenti di servizi di pagamento interessati: i PSP dovrebbero indicare quali soglie sono o saranno probabilmente raggiunte dall'incidente, se del caso, e i relativi dati: il numero totale di utenti di servizi di pagamento che sono stati interessati e la percentuale di utenti di servizi di pagamento interessati rispetto al numero totale di utenti di servizi di pagamento. Per queste variabili, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. Le entità che effettuano la segnalazione per conto di più PSP (ossia la segnalazione consolidata) possono invece indicare intervalli di valori che rappresentano i valori più bassi e più elevati osservati o stimati all'interno del gruppo di PSP inclusi nel rapporto, separati da un trattino. I PSP dovrebbero considerare come «utenti di servizi di pagamento interessati» tutti i clienti (nazionali o stranieri, consumatori o imprese) che hanno un contratto con il prestatore di servizi di pagamento interessato che fornisce loro accesso al servizio di pagamento interessato e che hanno subito o probabilmente subiranno le conseguenze dell'incidente. I PSP, per determinare il numero di utenti di servizi di pagamento che potrebbero aver utilizzato il servizio di pagamento durante l'incidente, dovrebbero ricorrere a stime basate sulla propria attività passata. Nel caso di gruppi, ogni PSP dovrebbe considerare solo i propri utenti dei servizi di pagamento. Nel caso di un PSP che offre servizi operativi ad altri, tale PSP dovrebbe considerare solo i propri utenti di servizi di pagamento (se esistenti) e i PSP che ricevono tali servizi operativi dovrebbero valutare l'incidente in relazione ai propri utenti dei servizi di pagamento. Inoltre, i PSP dovrebbero calcolare il numero totale degli utenti di servizi di pagamento considerando il totale degli utenti di servizi di pagamento nazionali e transfrontalieri contrattualmente vincolati al momento dell'incidente (o, in alternativa, il numero più recente disponibile) e aventi accesso al servizio di pagamento interessato, a prescindere dalla loro dimensione o dal fatto che siano considerati utenti attivi o passivi di servizi di pagamento.

Periodo di indisponibilità del servizio: i PSP dovrebbero indicare se la soglia è stata o probabilmente sarà raggiunta dall'incidente e i dati relativi: periodo totale di indisponibilità del servizio. Per questa variabile, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. Le entità che effettuano la segnalazione per conto di più PSP (ossia la segnalazione consolidata) possono invece indicare un intervallo di valori che includa i valori più bassi e più elevati osservati o stimati all'interno del gruppo di PSP inclusi nella rapporto, separati da un trattino. I PSP dovrebbero considerare il periodo di tempo in cui qualsiasi attività, processo o canale connesso alla prestazione di servizi di pagamento è o sarà probabilmente interrotto e, di conseguenza, impedirà (i) l'iniziazione e/o l'esecuzione di un servizio di pagamento e/o (ii)

l'accesso a un conto di pagamento. I PSP dovrebbero considerare il periodo di indisponibilità del servizio dal momento del suo inizio e dovrebbero considerare sia gli intervalli di tempo in cui sono operativi, come richiesto per l'esecuzione dei servizi di pagamento, sia gli orari di chiusura e i periodi di manutenzione, se del caso e se applicabile. Se i prestatori di servizi di pagamento non sono in grado di determinare il momento di inizio del periodo di indisponibilità del servizio, essi dovrebbero eccezionalmente calcolare tale periodo a partire dal momento in cui si rileva l'indisponibilità.

Impatto economico: i PSP dovrebbero indicare se la soglia è stata o probabilmente sarà raggiunta dall'incidente e i relativi dati: costi diretti e indiretti. Per queste variabili, i PSP dovrebbero fornire valori significativi, che possono essere dati effettivi o stime. Le entità che effettuano la segnalazione per conto di più PSP (ossia la segnalazione consolidata) possono invece indicare un intervallo di valori che includa i valori più bassi e più elevati osservati o stimati all'interno del gruppo di PSP inclusi nella rapporto, separati da un trattino. I PSP dovrebbero considerare sia i costi che possono essere collegati direttamente all'incidente sia quelli che lo sono indirettamente. Tra le altre cose, i PSP dovrebbero tener conto dei fondi o delle attività espropriati, dei costi di sostituzione dell'hardware o del software, di altri costi forensi o di bonifica, delle spese dovute alla mancata osservanza di obblighi contrattuali, delle sanzioni, delle responsabilità esterne e delle perdite sulle entrate. Per quanto riguarda i costi indiretti, i PSP dovrebbero considerare solo quelli già noti o molto probabili.

Costi diretti: importo di denaro (euro) imputabile direttamente all'incidente, compresi i fondi necessari per risolvere l'incidente (ad esempio, fondi o beni espropriati, costi di sostituzione di hardware e software, penali dovute alla mancata osservanza degli obblighi contrattuali).

Costi indiretti: importo di denaro (euro) imputabile indirettamente all'incidente (ad esempio, risarcimenti, perdita di entrate a causa della mancata operatività, possibili costi legali).

Alto livello di escalation interna: i prestatori di servizi di pagamento dovrebbero considerare se, in conseguenza dell'impatto dell'incidente sui servizi connessi ai pagamenti, il direttore della funzione informatica (CIO o posizione analoga) è stato o sarà probabilmente informato dell'accaduto in via straordinaria rispetto alle procedura di informazione periodica e in modo continuativo per tutta la durata dell'incidente

Nel caso di notifiche delegate, l'escalation avrebbe luogo all'interno della terza parte. Inoltre, i prestatori di servizi di pagamento dovrebbero considerare se, a seguito dell'impatto dell'incidente sui servizi connessi ai pagamenti, è stata o sarà probabilmente attivata la modalità di crisi aziendale.

Altri PSP o infrastrutture rilevanti potenzialmente interessati: i prestatori di servizi di pagamento dovrebbero valutare l'impatto dell'incidente sui mercati finanziari, inteso come infrastrutture dei mercati finanziari e/o schemi di pagamento con carte che li supportano e altri prestatori di servizi di pagamento. In particolare, i prestatori di servizi di pagamento dovrebbero valutare se l'incidente si è ripetuto o probabilmente si ripeterà presso altri prestatori di servizi di pagamento, se ha influenzato o probabilmente influenzerà il buon funzionamento delle infrastrutture dei mercati finanziari e se ha compromesso o probabilmente comprometterà la solidità del sistema finanziario nel suo complesso. I prestatori di servizi di pagamento dovrebbero tener conto di vari elementi, ad esempio se il componente/software interessato è proprietario o genericamente disponibile, se la rete compromessa è interna o esterna e se il prestatore di servizi di pagamento ha cessato o

probabilmente cesserà di adempiere i propri obblighi nelle infrastrutture del mercato finanziario di cui è membro.

Impatto sulla reputazione: i prestatori di servizi di pagamento dovrebbero considerare il livello di visibilità che, per quanto di loro conoscenza, l'incidente ha ricevuto o probabilmente riceverà sul mercato. In particolare, i prestatori di servizi di pagamento dovrebbero considerare la probabilità che l'incidente causi danni alla società quale indicatore affidabile del suo potenziale di influenzare la loro reputazione. I prestatori di servizi di pagamento dovrebbero considerare se (i) l'incidente ha influito su un processo visibile e pertanto riceverà probabilmente o ha già ricevuto copertura mediatica (non solo tramite i media tradizionali, come i giornali, ma anche blog, social networks, ecc.), (ii) non si sono adempiuti o probabilmente non si adempiranno obblighi regolamentari, (iii) sono state o probabilmente saranno violate sanzioni o (iv) lo stesso tipo di incidente si è già verificato in passato.

B 3 – Descrizione dell'incidente

Tipo di incidente: indicare se, per quanto noto, si tratta di un incidente operativo o di sicurezza.

Operativo: incidente derivante da processi inadeguati o malfunzionanti, persone e sistemi o eventi di forza maggiore che influenzano l'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi di pagamento.

Di sicurezza: accesso, uso, divulgazione, interruzione, modifica o distruzione non autorizzati delle risorse del PSP che influenzano l'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi di pagamento. Ciò può avvenire quando, tra le altre cose, il PSP è soggetto ad attacchi informatici, inadeguata progettazione o implementazione di politiche di sicurezza o inadeguata sicurezza fisica.

Causa dell'incidente: indicare la causa dell'incidente o, se questa non è ancora nota, quella più probabile. È possibile contrassegnare più caselle.

In fase di analisi: la causa non è ancora stata determinata.

Attacco esterno: l'origine della causa è esterna ed è intenzionalmente mirato al PSP (ad esempio, attacchi mediante malware).

Attacco interno: l'origine della causa è interna ed è intenzionalmente mirato al PSP (ad esempio, frode interna).

Tipo di attacco

Distributed/Denial of Service (D/DoS): tentativo di rendere non disponibile un servizio online richiedendolo con traffico da più fonti.

Contagio dei sistemi interni: attività malevola verso sistemi informatici che cerca di rubare spazio su disco rigido o tempo sulla CPU, accedere a informazioni private, alterare dati, mandare messaggi ai contatti, ecc.

Intrusione mirata: atto non autorizzato di spionaggio e sottrazione di informazioni attraverso il cyber-spazio.

Altro: qualsiasi altro tipo di attacco che il PSP possa aver subito, direttamente o tramite un prestatore di servizi tecnologici. In particolare, questa casella dovrebbe essere contrassegnata se vi è stato un attacco mirato al processo di autorizzazione e autenticazione. Dettagli dovrebbero essere aggiunti nel campo di testo libero.

Eventi esterni: la causa è associata a eventi generalmente al di fuori del controllo dell'organizzazione (ad esempio, disastri naturali, problemi legali, problemi aziendali e interdipendenze dei servizi).

Errore umano: l'incidente è stato causato dall'errore involontario di una persona nella procedura di pagamento (ad esempio, caricamento del file dei pagamenti errato nel sistema di pagamento) o in qualche modo correlato (ad esempio, la corrente elettrica viene accidentalmente staccata e l'attività di pagamento viene messa in attesa).

Malfunzionamento del processo: la causa dell'incidente è stata l'inadeguata progettazione o esecuzione del processo di pagamento, dei controlli di processo e/o dei processi di supporto (ad esempio, processo per modifica/migrazione, test, configurazione, capacità, monitoraggio).

Malfunzionamento del sistema: la causa dell'incidente è associata a inadeguatezza di progettazione, esecuzione, componenti, specifiche, integrazione o complessità dei sistemi che supportano l'attività di pagamento.

Altro: la causa dell'incidente non è nessuna di quelle precedentemente elencate. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

L'incidente vi ha interessati direttamente o indirettamente attraverso un fornitore di servizi?: un incidente può essere direttamente mirato a un PSP o interessarlo indirettamente, tramite un terza parte. In caso di impatto indiretto, fornire il nome del/i prestatore/i di servizi.

B 4 – Impatto dell'incidente

Edificio/i interessato/i (indirizzo), se applicabile: se è interessato un edificio fisico, indicarne l'indirizzo.

Canali commerciali interessati: indicare il canale o i canali di interazione con gli utenti di servizi di pagamento che sono stati interessati dall'incidente. È possibile contrassegnare più caselle.

Succursali: sede di attività (diversa dalla sede centrale) facente capo a un PSP, che è sprovvista di personalità giuridica ed effettua direttamente alcune operazioni o l'insieme delle operazioni inerenti all'attività di un PSP. Tutte le sedi di attività costituite nello stesso Stato membro da un PSP avente la sede centrale in un altro Stato membro dovrebbero essere considerate come un'unica succursale.

E-banking: utilizzo di computer per effettuare transazioni finanziarie su Internet.

Servizi bancari telefonici: uso di telefoni per effettuare transazioni finanziarie.

Mobile banking: utilizzo di un'applicazione bancaria specifica su smartphone o dispositivi simili per effettuare transazioni finanziarie.

Sportelli automatici per il prelievo di contante (ATM): dispositivi elettromeccanici che consentono agli utenti di servizi di pagamento di prelevare contanti dai propri conti e/o accedere ad altri servizi.

Punto vendita: sede fisica del commerciante dalla quale viene avviata l'operazione di pagamento.

Altro: il canale commerciale interessato non è uno di quelli citati in precedenza. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Servizi di pagamento interessati: indicare i servizi di pagamento che non funzionano correttamente a seguito dell'incidente. È possibile contrassegnare più caselle.

Deposito di contanti su un conto di pagamento: consegna di denaro a un PSP per accredito su un conto di pagamento.

Prelievo di contanti da un conto di pagamento: richiesta ricevuta da un PSP da parte del suo utente di servizi di pagamento relativa all'erogazione di contante e conseguente addebito dell'importo corrispondente sul suo conto di pagamento.

Operazioni necessarie per gestire un conto di pagamento: azioni che devono essere eseguite su un conto di pagamento per attivarlo, disattivarlo e/o mantenerlo (ad esempio, apertura e blocco).

Acquiring di strumenti di pagamento: servizio di pagamento che consiste in un contratto tra PSP e un merchant per accettare ed elaborare le transazioni di pagamento, con un conseguente trasferimento di fondi al merchant.

Bonifici: servizio di pagamento per l'accredito sul conto di pagamento del beneficiario mediante una transazione di pagamento o una serie di transazioni di pagamento dal conto di pagamento del pagatore eseguite dal prestatore di servizi di pagamento detentore del conto di pagamento del pagatore, sulla base di un'istruzione impartita dal pagatore.

Addebiti diretti: servizio di pagamento per l'addebito di un conto di pagamento del pagatore in cui una transazione di pagamento è disposta dal beneficiario in base al consenso dato dal pagatore al beneficiario, al prestatore di servizi di pagamento del beneficiario o al prestatore di servizi di pagamento del pagatore stesso.

Pagamento basato su carta: servizio di pagamento basato sull'infrastruttura e le regole commerciali di un circuito di carte di pagamento per effettuare un'operazione di pagamento con carte, dispositivi di telecomunicazione, dispositivi digitali o IT, o software, quando il risultato è una transazione tramite carta di debito o di credito. Tra le operazioni di pagamento basate su carta non rientrano le operazioni basate su altri tipi di servizi di pagamento.

Emissione di strumenti di pagamento: servizio di pagamento fornito da un PSP che stipula un contratto per fornire al pagatore uno strumento di pagamento per disporre e trattare le transazioni di pagamento del pagatore.

Rimessa di denaro: servizio di pagamento in cui i fondi sono consegnati da un pagatore, senza che siano stati aperti conti di pagamento intestati al pagatore o al beneficiario, unicamente allo scopo di trasferire una somma corrispondente a un beneficiario o a un altro PSP che agisce per conto del beneficiario, e/o in cui tali fondi sono riscossi per conto del beneficiario e resi disponibili a quest'ultimo.

Servizi di disposizione di ordini di pagamento: servizi di pagamento che dispongono l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro PSP.

Servizi di informazione sui conti: servizi online che forniscono informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro PSP o presso più PSP.

Altro: il servizio di pagamento interessato non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Aree funzionali interessate: indicare la fase o le fasi del processo di pagamento interessate dall'incidente. È possibile contrassegnare più caselle.

Autenticazione/autorizzazione: procedure che consentono al PSP di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, compreso l'uso delle credenziali di sicurezza personalizzate dell'utente e il consenso dell'utente di servizi di pagamento (o terzi che agiscono per conto di quell'utente) al trasferimento di fondi o titoli.

Comunicazione: flusso di informazioni ai fini dell'identificazione, dell'autenticazione, della notifica e dell'informazione tra il PSP che gestisce il conto e i prestatori di servizi di

ordine di pagamento, i prestatori di servizi di informazione sui conti, i pagatori, i beneficiari e altri PSP.

Compensazione: processo di trasmissione, riconciliazione e, in alcuni casi, conferma degli ordini di pagamento prima del regolamento, che potenzialmente include la compensazione degli ordini e la definizione delle posizioni finali per il regolamento.

Regolamento diretto: completamento di una transazione o di un'elaborazione allo scopo di adempiere gli obblighi dei partecipanti mediante il trasferimento di fondi, quando questa azione viene eseguita dal PSP interessato.

Regolamento indiretto: completamento di un'operazione o di un'elaborazione allo scopo di adempiere gli obblighi dei partecipanti mediante il trasferimento di fondi, quando questa azione viene eseguita da un altro PSP per conto del PSP interessato.

Altro: l'area funzionale interessata non rientra nei casi precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Sistemi e componenti interessati: indicare quale parte o quali parti dell'infrastruttura tecnologica del PSP sono state interessate dall'incidente. È possibile contrassegnare più caselle.

Applicativi/software: programmi, sistemi operativi, ecc. che supportano la prestazione di servizi di pagamento da parte del PSP.

Base di dati: struttura in cui sono archiviate le informazioni personali e di pagamento necessarie per eseguire operazioni di pagamento.

Hardware: apparecchiature tecnologiche fisiche che gestiscono i processi e/o archiviano i dati necessari ai PSP per svolgere le attività relative ai pagamenti.

Rete/infrastruttura: reti di telecomunicazione, pubbliche o private, che consentono lo scambio di dati e informazioni durante il processo di pagamento (ad esempio, Internet).

Altro: il sistema e il componente interessati non sono tra quelli precedentemente elencati. Ulteriori dettagli dovrebbero essere inseriti nel campo di testo libero.

Personale interessato: indicare se l'incidente ha avuto effetti sul personale del PSP e, in caso affermativo, fornire dettagli nel campo di testo libero.

B 5 – Mitigazione degli incidenti

Quali azioni/misure sono state adottate finora o sono previste per il ripristino in caso di incidente?: fornire informazioni dettagliate sulle azioni intraprese o pianificate per affrontare temporaneamente l'incidente.

Sono stati attivati i piani di continuità operativa e/o il piano di Disaster Recovery?: indicare se sono stati attivati o meno e, in caso affermativo, fornire i dettagli principali di ciò che è accaduto (ossia specificare quando sono stati attivatie in cosa consistevano tali piani).

Il PSP ha annullato o attenuato l'intensità di alcune misure di controllo a causa dell'incidente?: indicare se il PSP ha dovuto ignorare alcune misure di controllo (ad esempio, interrompendo l'applicazione del principio del doppio controllo) per affrontare l'incidente e, in caso affermativo, fornire dettagli relativi alle motivazioni alla base dell'attenuazione o dell'annullamento delle misure di controllo.

C – Rapporto finale

C 1 – Informazioni generali

Aggiornamento delle informazioni del rapporto intermedio (sintesi): fornire ulteriori informazioni sulle azioni intraprese per ripristinare l'attività a seguito dell'incidente e per evitare che questo si ripeta, sull'analisi delle cause all'origine, sulle lezioni apprese, ecc.

Data e ora di chiusura dell'incidente: indicare la data e l'ora in cui l'incidente è stato considerato chiuso.

Le misure di controllo originali sono stati ripristinate?: laddove il PSP abbia dovuto annullare o attenuare l'intensità di alcune misure di controllo a causa dell'incidente, indicare se le misure di controllo sono nuovamente attive e fornire ulteriori informazioni nel campo di testo libero.

C 2 – Analisi delle cause all'origine e follow-up

Quale è stata la causa all'origine dell'incidente, se già nota?: spiegare qual è la causa all'origine dell'incidente o, se non ancora nota, le conclusioni preliminari tratte dall'analisi delle cause all'origine dell'incidente. I PSP possono allegare un file con informazioni dettagliate se ritenuto necessario.

Principali azioni correttive/misure adottate o pianificate per impedire che l'incidente si verifichi nuovamente in futuro, se già note: descrivere le principali azioni intraprese o previste per evitare il ripetersi dell'incidente in futuro.

C 3 – Informazioni aggiuntive

L'incidente è stato condiviso con altri PSP a scopo informativo?: indicare quali PSP sono stati contattati, formalmente o informalmente, per essere informati in merito all'incidente; riportare i dettagli dei PSP informati, le informazioni che sono state condivise e le motivazioni alla base della condivisione di tali informazioni.

È stata intrapresa un'azione legale nei confronti del PSP?: indicare se, al momento della compilazione del rapporto finale, il PSP è soggetto a qualunque azione legale (ad esempio, se è stato citato in tribunale o ha perso la sua licenza) a seguito dell'incidente.