Regolamento del processo di Fraud Reporting

Regolamento di processo emesso il 31/03/2022

Owner: Perspective Happiness and Services

1 PREMESSA

L'art. 96, paragrafo 6 della "*Direttiva europea dedicata ai servizi di pagamento elettronico*" (PSD2) introduce l'obbligo, per i prestatori di servizi di pagamento, di raccogliere i dati relativi alle operazioni di pagamento fraudolente registrati, di classificarli secondo i criteri riportati all'interno delle Linee Guida EBA e dalle istruzioni operative di Banca d'Italia e di inoltrarli semestralmente alla stessa Banca d'Italia (c.d. «*Fraud Reporting*»).

Il presente Regolamento illustra i principi guida, l'architettura organizzativa e le interdipendenze alla base del processo attuato da Flowe per la predisposizione della reportistica periodica da inoltrare a Banca d'Italia ("*Fraud Reporting*").

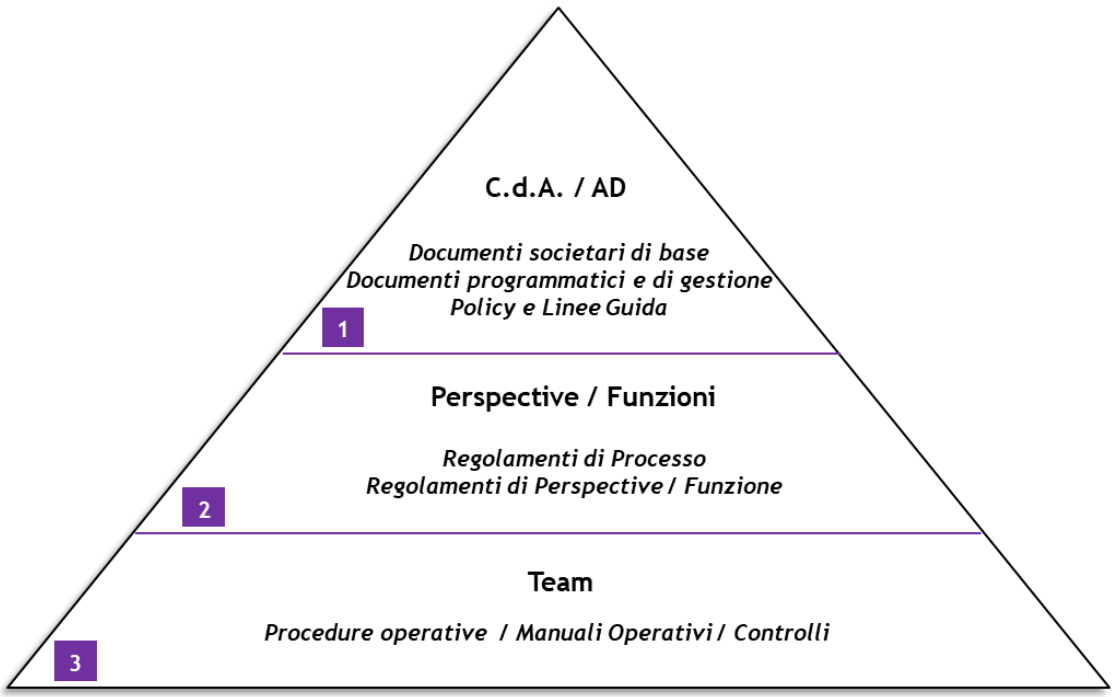
1.1. OBIETTIVO DEL DOCUMENTO

Il presente documento ha l'obiettivo di:

- descrivere le diverse fasi del processo di predisposizione ed invio alla Banca d'Italia della reportistica inerente le operazioni di pagamento elettronico e le relative frodi;
- richiamare ruoli e responsabilità degli attori coinvolti nel processo, in relazione all'assetto organizzativo, compiti e responsabilità disciplinati della Relazione sulla Struttura Organizzativa di Flowe.

Con riferimento alla "*Policy di Conglomerato sulle modalità di redazione, aggiornamento, approvazione e diffusione della Normativa Interna*", il presente documento si colloca al secondo livello della piramide documentale richiamata nello schema seguente.

Modello della normativa interna di riferimento



1.2. STRUTTURA DEL DOCUMENTO

Il Regolamento si compone complessivamente di 4 capitoli oltre al presente capitolo introduttivo.

Di seguito sono descritte sinteticamente le principali tematiche trattate in ogni capitolo:

Capitolo 2: Gli attori coinvolti

Obiettivo del Capitolo è descrivere e richiamare in modo chiaro ruoli e responsabilità degli attori coinvolti nel processo oggetto del presente documento, definendo le modalità di integrazione e coordinamento previste nei casi di processo di carattere interfunzionale.

Capitolo 3: Il processo

Obiettivo del Capitolo è descrivere gli aspetti di carattere organizzativo, il processo e le modalità di interazione con le altre entità organizzative o di società terze, interne o esterne alla Società, in relazione al processo oggetto di regolamentazione, gli strumenti utilizzati e gli *output* attesi dalle fasi in cui il processo è articolato.

Capitolo 4: Il contesto normativo esterno

Obiettivo del Capitolo è descrivere il quadro normativo esterno di riferimento nell'ambito rilevante per il processo oggetto di regolamentazione (es. normativa di primo e secondo livello)

Capitolo 5: Le policy e la normativa interna di riferimento

Obiettivo del Capitolo è descrivere le fonti informative interne alla Società (es. policy, procedure operative, regolamenti di processo) che presentano relazioni con il processo in esame.

2 GLI ATTORI COINVOLTI

Gli attori, ovvero le unità organizzative aziendali coinvolte a vario titolo nel processo di predisposizione ed invio del *Fraud Reporting* sono di seguito richiamati, con evidenza esclusivamente del ruolo specificatamente attribuito nel processo medesimo.

2.1. PERSPECTIVE HAPPINESS AND SERVICE

La *Perspective Happiness and Service*, in qualità di referente aziendale delle attività di predisposizione del "*Fraud Reporting*", definisce e pianifica le attività delle diverse unità organizzative coinvolte nel processo di predisposizione della reportistica in ambito, assicurando che i dati siano raccolti e validati in tempo utile alla scadenza dell'invio della segnalazione.

In particolare, nell'ambito del presente processo, è responsabile:

- attraverso il *team Customer Interaction*, di raccogliere e tracciare nei file gestionali dedicati, i dati relativi alle operazioni di pagamento fraudolente accertate (a fronte di disconoscimenti diretti da parte dei Clienti o intercettate durante le attività di monitoraggio);
- attraverso il *team Monitoraggio Segnalazioni* di:

- verificare che i dati statistici relativi al transato presenti nel *report, prodotto dal team Data Platform della Perspective Augmented Intelligence,* siano coerenti con i dati delle medesime transazioni registrate nell'applicativo di *Core Banking* T24; In caso di disallineamenti sarà cura del team *Operations* andare a correggerli ed integrarli;
- effettuare controlli a campione sulla corretta classificazione dei dati delle frodi, secondo la classificazione definita da Banca d'Italia;
- verificare, attraverso l'esecuzione della "macro" dedicata, il rispetto delle regole di convalida presenti nel template fornito da Banca d'Italia;
- intrattenere i rapporti con gli outsourcers che intervengono nel processo

Infine, il Responsabile della *Perspective*, si occupa di inoltrare all'*Ufficio Segnalazioni di Vigilanza* di Banca Mediolanum il *report* nel template previsto dalle disposizioni di Banca d'Italia (e comprensivo delle diverse ripartizioni dei dati richieste);

2.2. PERSPECTIVE AUGMENTED INTELLIGENCE

Nell'ambito del presente processo la *Perspective Augmented Intelligence*, attraverso il *team Data Platform*, si occupa delle attività tecniche di aggregazione, calcolo dei dati e alimentazione del template *excel* (Sezione "Data CT") necessarie alla produzione del report semestrale da inviare a Banca d'Italia.

2.3. ORGANIZZAZIONE FLOWE

Nell'ambito del presente processo Organizzazione Flowe si occupa di attivare, in caso di evoluzioni alle disposizioni normative in materia, segnalate dalla Funzione Compliance, la Perspective Happiness e Service, Augmented Intelligence e gli altri attori owner delle informazioni sui servizi di pagamento e sulle frodi, per le eventuali modifiche alle attività e/o agli strumenti di tracciatura dei dati.

2.4. OUTSOURCER

2.3.1. Banca Mediolanum – Ufficio Segnalazioni di Vigilanza

Nell'ambito del presente processo Banca Mediolanum, attraverso *l'Ufficio Segnalazioni di Vigilanza*, supporta Flowe nell'invio della reportistica di Fraud Reporting a Banca d'Italia.

In caso di flussi di ritorno dovuti, ad esempio, a eventuali anomalie, l'Ufficio ingaggia la *Perspective Happiness and Service* per la risoluzione delle stesse ed il successivo invio della versione revisionata.

2.3.2. Banca Mediolanum – Risk Management

Nell'ambito del presente processo la *Funzione Risk Management*, in *outsourcing* presso Banca Mediolanum, fornisce supporto al *team Customer Interaction* della *Perspective*

Happiness and Service nelle attività di raccolta, verifica e riconciliazione delle perdite rivenienti da frodi, oggetto di segnalazione all'interno del "*Fraud Reporting*".

2.3.3. SIA

Nell'ambito del presente processo SIA in qualità di "*Card processor*" di Flowe, raccoglie i dati relativi alle operazioni di pagamento effettuate tramite carta e genera il *Fraud report* per le componenti "prelievi" ("*Cash withdrawals*") e "pagamenti con carta" ("*Card Payments*").

3 PROCESSO DI FRAUD REPORTING

Facendo riferimento alla tassonomia dei processi aziendali, il processo in esame è classificato nell'ambito dei processi di *Operations* secondo l'alberatura dei processi adottati dalla Società, come di seguito riportato:

3.00 PROCESSI DI OPERATIONS

3.13 PREVENZIONE, GESTIONE E CONTROLLO FRODI

3.13.05 FRAUD REPORTING ALL'AUTORITA' DI VIGILANZA

Di seguito è riportata la rappresentazione del processo di predisposizione ed invio a Banca d'Italia della reportistica dedicata alle frodi ("*Fraud Reporting*") relative ai servizi di pagamento elettronico subite dai clienti.

3.1. RACCOLTA E CLASSIFICAZIONE DATI (TRANSAZIONI E FRODI)

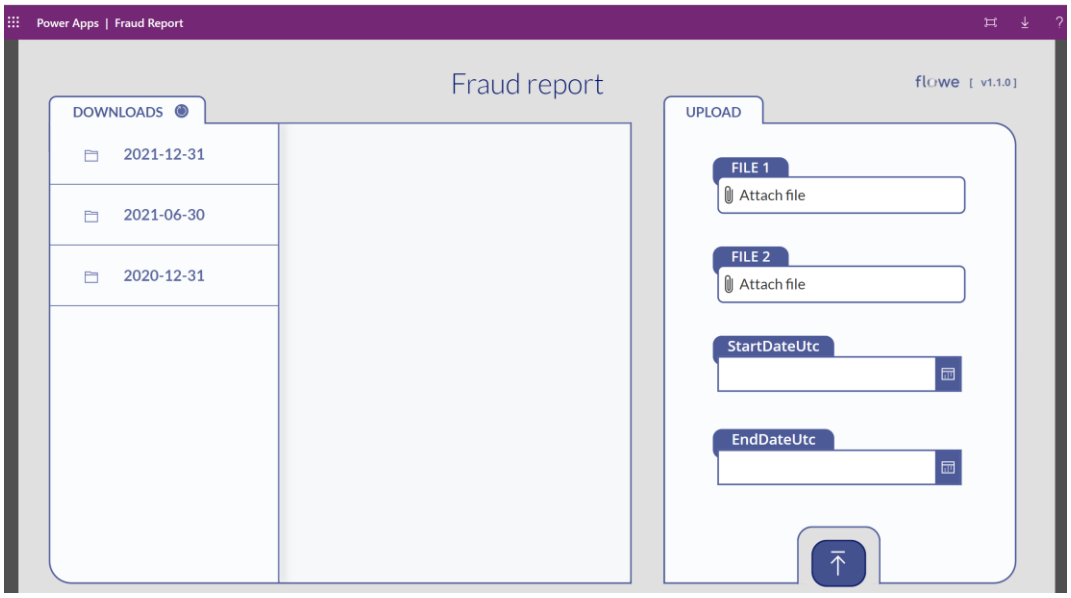
Si riportano di seguito, le unità organizzative *owner* della raccolta e classificazione dei dati relativi alle operazioni di pagamento disposte dalla clientela e delle operazioni fraudolente (e delle relative perdite) oggetto del "*Fraud Reporting*".

Per i dettagli in merito alle attività di censimento degli eventi di frode ed ai relativi dati registrati, si fa riferimento a quanto dettagliato nei processi relativi alla gestione degli eventi fraudolenti subiti dai clienti (ambito "pagamenti" ed ambito "monetica").

Se necessario, per la raccolta dei dati relativi alle perdite rivenienti da frodi, le unità organizzative "*data owner*" vengono supportate dalle unità organizzative della *Funzione Risk Management* di Banca Mediolanum.

3.2. AGGREGAZIONE DATI (TRANSAZIONI E FRODI)

Per quanto rigurarda i "*Credit transfer*" Entro i 2 mesi precedenti alla scadenza dell'invio della segnalazione (orientativamente a inizio febbraio per la segnalazione di aprile e inizio agosto per la segnalazione di ottobre), il *team Monitoraggio Segnalazioni della Perspective Happiness & Services* richiede l'avvio delle attività tecniche di estrazione ed aggregazione dei dati relativi alle operazioni di pagamento (procedura automatica) attraverso una dashboard messa a disposizione dal team *Data Platform* della *Perspective Augmented Intelligence*. I dati sono quindi estratti ed aggregati da procedure automatiche in gestione al team *Data Platform* della *Perspective Augmented Intelligence*



Sulla base dei servizi di pagamento "rilevanti" ai fini della predisposizione del *template Fraud Report* il team Operations della *Perspective Happiness and Service* predispone il file "*AvailableItemCode*", da caricare nella dashboard di cui sopra.

Di seguito il dettaglio di quanto previsto, e quanto non previsto, nell'estrazione in oggetto:

Credit Transfer	
IN SCOPE	**OUT OF SCOPE**
Trasferimento interno tra Flomes (in uscita)	Commissioni Flowe
Rimborso delle spese condivise	SDD
Transazioni Bazar	PISP
Bonifici bancari in uscita	Carte regalo Amazon
Transazioni con carta	Bollettini postali
	CBILL
	Ricariche telefoniche

Una volta caricato il file ed indicato il relativo periodo di competenza, la dashboard fornisce l'estrazione della lista delle transazioni registrate nel semestre di competenza ed esegue la procedura automatica di calcolo dei KPI relativi a somma ("*amount*") e numero ("*count*") delle transazioni di pagamento elettronico, suddivise in base ai vari criteri di classificazione indicati da Banca d'Italia, per la componente "Credit Transfer".

I suddetti criteri richiedono di classificare le operazioni in scope al Fraud Report nel seguente ordine:

- Totale Credit Transfer:
    a. Di cui avviati elettronicamente
    b. Di cui avviati tramite canale di pagamento remoto
        i. Di cui autenticati tramite autenticazione forte del cliente (SCA)
        ii. Di cui autenticati tramite autenticazione del cliente non forte
            1. Modico valore (art. 16 RTS)

Per quanto riguarda i dati relativi alle transazioni effettuate con carta, si specifica, infine che la componente del template del Fraud report contenente i dati relativi alle

transazioni effettuate con carta vengono forniti direttamente da SIA nel formato target. Infatti, per i dati relativi alle transazioni effettuate con carta, SIA fornisce i KPI da riportare nel Fraud Reporting calcolati e già verificati.

3.3. VERIFICA E VALIDAZIONE DATI

Una volta che è stato completato il caricamento e l'aggregazione di tutti i dati statistici oggetto della reportistica il team Monitoraggio Segnalazioni della Perspective Happiness and Service procede ad una validazione/correzione o integrazione del file prodotto attraverso una riconciliazione di quanto presente nel Core Banking T24.

Infine, gli operatori dei team *Account Monitoring & Fraud Management* e *Customer Interaction* integreranno il *fraud report* con le informazioni relative alle frodi conclamate che sono censite tempo per tempo nei due file:

1. "Censimento Frodi su Credit Transfer", contenente i dati sulle frodi subite dai clienti relative ai" Credit Transfers" (aggiornato dal team *Account Monitoring & Fraud Management)*

2. "Censimento Dispute", contenente le dispute richieste dai clienti Flowe relativamente alle transazioni con carta e la relativa tipologia; ai fini della predisposizione del Fraud Reporting vengono considerate solo quelle di tipo "Fraud" (aggiornato dal team *Customer Interaction)*

In questa fase, gli operatori del *team Monitoraggio Segnalazioni* della *Pespective Happiness & Services* confermano ed eventualmente completano, ove necessario, la colonna "*data availability*" (secondo le indicazioni fornite nelle istruzioni operative di Banca d'Italia) ed effettuano il controllo sull'avvenuta convalida dei dati attraverso l'esecuzione della "macro" messa a disposizione dalla stessa Banca d'Italia.

In caso di discrepanze o incongruenze dei dati, le attività di analisi della problematica e conseguente correzione dei dati vengono gestite dalla *Perspective Happiness and Service - team Operation*.

3.4. INVIO REPORT ALLA BANCA D'ITALIA

A seguito della conclusione delle attività di verifica e validazione dei dati, il Responsabile della *Perspective Happiness and Service* inoltra all'Ufficio Segnalazioni di Vigilanza di Banca Mediolanum il report, nel template previsto dalle istruzioni comunicate da Banca d'Italia (e comprensivo delle diverse ripartizioni dei dati richieste) che si occupa dell'inoltro all'Autorità di Vigilanza attraverso l'applicazione "Infostat".

I dati statistici sulle frodi subite dai clienti in merito alle operazioni di pagamento elettronico sono trasmessi alla Banca d'Italia ogni sei mesi (per il periodo di riferimento Gennaio-Giugno il *report* deve essere inviato entro fine settembre; per il periodo di riferimento Luglio-Dicembre il *report* deve essere inviato entro fine marzo.

Qualora ci siano da notificare alla Banca d'Italia modifiche su transazione o frodi già trasmesse, la *Perspective Happiness and Service* si occupa anche delle attività di modifica di "*Fraud Reporting*" già inviati, coinvolgendo eventualmente se necessario gli *outsourcer* citati.

4 LA NORMATIVA ESTERNA DI RIFERIMENTO

Nel presente capitolo si richiama il contesto normativo nel quale opera il presente Regolamento di processo.

Si riportano di seguito i principali riferimenti normativi:

- *Direttiva (UE) 2015/2366 PSD2 – (Payment Services Directive 2);*
- *Decreto Legislativo 15 dicembre 2017, n. 218 e succ. modifiche;*
- *Decreto Legislativo 27 gennaio 2010, n. 11 e succ. modifiche;*
- *Regulatory Technical Standards on strong customer authentication and secure communication under PSD2;*
- *Guidelines on fraud reporting (EBA GL-2018-05);*
- *Orientamenti recanti modifica agli orientamenti EBA GL-2018-05 (EBA/GL/2020/01);*
- *Handbook for the reporting of payments and fraud statistics under EBA GL on fraud reporting under PSD2 (EBA/GL/2018/05) – Banca d 'Italia.*

5 LE POLICY E LA NORMATIVA INTERNA DI RIFERMENTO

Si riepilogano le fonti informative interne alla Società che presentano relazioni con il processo in esame:

- *Policy di Gestione del Fraud Reporting;*
- *Policy per il controllo e la gestione dei Rischi Operativi;*
- *Policy la gestione del Rischio Reputazionale;*
- *Procedura operativa di monitoraggio e gestione delle frodi subite dalla clientela (Ambito pagamenti);*
- *Procedura operativa di monitoraggio e gestione delle frodi subite dalla clientela (Ambito monetica).*