# PROCEDURA OPERATIVA

# Monitoraggio e gestione delle frodi subite dalla clientela (Ambito pagamenti)

Procedura emessa il 31/03/2022

Owner della procedura: Perspective Happiness and Services

# 1 OBIETTIVO DEL DOCUMENTO

Obiettivo del presente documento è illustrare il processo di monitoraggio e gestione degli eventi fraudolenti subiti dalla clientela con riferimento alle operazioni di pagamento disposte tramite l'App Flowe o le c.d "Terze Parti".

In particolare, la procedura descrive:

- le attività operative e la sequenza logica con cui sono eseguite;
- il ruolo e la responsabilità degli attori coinvolti a vario titolo nel processo;
- i dettagli dei controlli di primo livello effettuati;
- gli strumenti a supporto dell'operatività.

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

3.00 PROCESSI DI OPERATIONS

3.13 PREVENZIONE, GESTIONE E CONTROLLO FRODI

3.13.03 MONITORAGGIO E GESTIONE FRODI SUBITE DAI CLIENTI SU DISPOSIZIONI DI PAGAMENTO

## 1.1. AMBITO DI APPLICAZIONE

La presente procedura si applica a Flowe S.p.A. Società Benefit.

## 1.2. AGGIORNAMENTO DEL DOCUMENTO

L'aggiornamento e la revisione del presente documento sono di responsabilità della *Perspective Happiness and Service*.

## 2 DEFINIZIONI

Si riportano di seguito alcune definizioni e concetti di base utilizzati all'interno della procedura operativa:

- **Terze Parti**: Le Terze Parti (*Third Party Provider*) sono soggetti non bancari che possono essere autorizzati dai clienti per gestire le proprie finanze e le operazioni di pagamento. Sono classificati in: PISP, AISP E CISP.
    - PISP (*PAYMENT INITIATION SERVICE PROVIDERS*): sono soggetti che, su espressa autorizzazione del cliente, prestano il servizio di disposizione di ordini di pagamento. Fungono da tramite tra la banca e il titolare del conto di pagamento accessibile online e avviano il pagamento a favore di un terzo soggetto.
    - AISP (*ACCOUNT INFORMATION SERVICES PROVIDERS*), sono operatori che consentono al titolare di conti accessibili *online* di ottenere un'informativa completa relativa ai servizi di pagamento dei rapporti a lui intestati. Ad esempio, il cliente utilizza l'AISP per avere una visione di insieme della propria situazione finanziaria, analizzare le sue abitudini di spesa e le esigenze finanziarie future.
    - CISP (*CARD ISSUER SERVICE PROVIDERS*), sono soggetti che emettono carte di pagamento, regolate su un conto di pagamento *online* di un istituto di credito diverso da quello che ha emesso la carta.
- ***Strong Customer Authentication* - SCA:** è una misura di sicurezza basata sull'autenticazione a due fattori che risultano strettamente legati al cliente. L'identità dei clienti secondo la normativa PSD2 deve essere identificata usando almeno 2 dei metodi indicati di seguito:
    - elementi di proprietà del cliente (ad es. telefono o *tablet*);
    - elementi caratteristici del cliente (ad es. riconoscimento facciale o impronta digitale);
    - elementi di utilizzo elettronico del cliente (ad es. PIN o *password*).

  La SCA ha lo scopo di impedire o ridurre al massimo le azioni fraudolente da parte di soggetti terzi non autorizzati.
- **Disconoscimento:** segnalazione da parte del cliente di operazioni che non riconosce, ad esempio un addebito sul conto effettuato più volte, di importo superiore a quanto realmente speso o un'operazione non autorizzata o mai effettuata in quanto riconosciuta come potenziale frode.
- **Rimborso Salvo Buon Fine**: rimborso erogato in favore del cliente in modo non definitivo; tale rimborso in una fase successiva sarà confermato o annullato previa restituzione dello stesso.
- ***Claim*:** è una istanza di verifica aperta sull'applicazione di CRM per tracciare una problematica verificatasi sulla posizione di un cliente.
- ***Phishing*:** Truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di *home banking*, ecc.), motivando tale richiesta con ragioni di ordine tecnico.
- **Arbitro Bancario Finanziario - ABF:** l'arbitro Bancario Finanziario - anche ABF - è un sistema di risoluzione stragiudiziale di controversie previsto dalla legge italiana il cui funzionamento è affidato a Banca d'Italia. Il cliente ha la possibilità di rivolgersi all'ABF dopo aver cercato di risolvere la controversia inviando un reclamo scritto all'intermediario senza ricevere riscontro entro il termine previsto dalla normativa o se non è soddisfatto del riscontro.

# 3 STRUMENTI A SUPPORTO DEL PROCESSO

L'infrastruttura tecnologica di cui si è dotata Flowe per supportare il processo in oggetto include gli strumenti informatici di seguito descritti.

## 3.1. APP FLOWE

L'App Flowe è il canale distributivo con cui operano i clienti della Società, versione IOS e Android, per l'apertura e la gestione del conto di pagamento e della carta ad esso associata.

L'App Flowe nell'ambito della procedura operativa prevede un sistema *chatBot* per fornire ai clienti supporto istantaneo anche al fine di segnalare alla Società disconoscimenti di operazioni di pagamento.

All'interno dell'App sono inoltre integrati i presidi, previsti anche in ottemperanza alla Direttiva PSD2, finalizzati a ridurre le frodi nei confronti dei clienti e a rendere più sicuri i pagamenti (*Strong Customer Authentication* e *Dynamic Linking*).

## 3.2. PLATFORM – POWER PLATFORM – P0 (PZERO)

La piattaforma proprietaria di Flowe (di seguito indicata come Platform o P0) è il cuore della soluzione informatica della Società in cui avviene l'autenticazione sicura del cliente (*Network gateway* ed *Identity provider*), sono salvati i dati anagrafici e finanziari (nei vari *databases*), sono sviluppati collegamenti e funzionalità per i clienti e necessari alla gestione (API), sono attivati i "contatti" con gli enti esterni (*Event bus*/API), il tutto attraverso applicazioni di micro-servizi opportunamente configurate (*Microservices and Orchestrator*), indipendenti dalla versione, scalabili ed incentrati sul cliente, che comunicano tra loro tramite protocolli *standard* ed interfacce definite.

Nella *Platform* sono storicizzati i dati afferenti alla posizione dei clienti e le operazioni effettuate dagli stessi; questi dati vengono utilizzati dagli operatori della *Perspective Happiness and Service* nello svolgimento delle attività legate alla gestione dei disconoscimenti delle operazioni di pagamento disposte tramite l'App.

## 3.3. FANBASE – POWER PLATFORM

Fanbase è la *power app* utilizzata dagli operatori della *Perspective Happiness and Service* per la gestione delle diverse attività di *front* e *back office* inerenti la clientela.

Rappresenta l'applicazione per il *Customer Relationship Management* (CRM) e consente la visualizzazione della scheda cliente, la modifica di alcuni dati, la possibilità di inserire il blocco di accesso all'APP, nonché di inviargli notifiche via sms, e-mail, *push* in APP.

Nell'ambito della presente procedura l'applicazione consente:

- di storicizzare, tutti i contatti, le azioni o le istanze di verifica eseguite sul cliente a seguito di segnalazione di disconoscimento di un'operazione di pagamento;
- la gestione del blocco App (apposizione e rimozione), necessario al fine di prevenire ulteriori eventi fraudolenti nei confronti del cliente.

### 3.4. SPRINKLR

Sprinklr è un sistema in *Cloud* utilizzato da Flowe per la gestione e la tracciatura dei contatti dei clienti tramite *chat*.

Nell'ambito della presente procedura, l'applicazione viene utilizzata dagli operatori del *team Customer Interaction* della *Perspective Happiness and Service* per la ricezione, tramite *chat*, delle segnalazioni di disconoscimento ed il recupero, in fase di analisi della segnalazione, dei contenuti delle conversazioni con i clienti.

### 3.5. SISTEMA DI CORE BANKING - T24

Flowe si avvale del modulo T24, di seguito indicato anche come Sistema di *Core Banking*, dell'*outsourcer* Temenos, applicativo tramite il quale vengono gestiti i processi "*core*" della Società per la gestione delle operazioni di pagamento.

Nell'ambito della presente procedura l'applicazione consente agli operatori della *Perspective Happiness and Service* di recuperare i dettagli delle operazioni di pagamento oggetto di disconoscimento.

## 4 ATTORI, RUOLI E RESPONSABILITÀ

Di seguito sono indicati i principali attori, coinvolti nel processo di monitoraggio e gestione delle frodi subiti in ambito monetica ed i relativi ruoli e responsabilità nell'ambito delle attività descritte.

### 4.1. PERSPECTIVE HAPPINESS AND SERVICE

La *Perspective Happiness and Service*, nell'ambito del presente processo, è responsabile per il tramite del *team Customer Interaction* di:

- ricevere le richieste di disconoscimento delle operazioni disposte tramite l'App Flowe o le Terze Parti ed effettuare le verifiche preliminari sull'evento;
- qualora ci siano i presupposti per approfondire la segnalazione del cliente, inoltrare la pratica al *Team Account Monitoring and Fraud Management*;
- gestire le comunicazioni, sia in caso di diniego che di accertamento della frode, verso il cliente;
- raccogliere ed archiviare tutti i dati ed i documenti relativi ai disconoscimenti ai fini della produzione della reportistica periodica relativa alle perdite operative e alle frodi subite dalla clientela ("*Fraud Reporting*").

per il tramite del *team Account Monitoring and Fraud Management* di:

- prendere in carico ed analizzare le transazioni segnalate dalla *dashboard* "*Live Monitoring*";

- effettuare le analisi e gli approfondimenti volti ad accertare che l'operazione di pagamento segnalata (no monetica) rappresenti un evento fraudolento subito dal cliente;
- gestire il rimborso "Salvo Buon Fine" dell'importo relativo all'operazione potenzialmente oggetto di frode e di richiamo dell'operazione;
- apporre e/o rimuovere il blocco App, al fine di prevenire ulteriori eventi fraudolenti nei confronti del cliente.
- ingaggiare la *Perspective Augmented Intelligence* per effettuare con le indagini tecniche sull'evento segnalato dal cliente;
- classificare l'evento come "frode conclamata" o "frode non accertata";
- integrare la pratica di disconoscimento su *Fanbase* con tutte le evidenze emerse dall'istruttoria e dall'analisi tecnica dell'evento segnalato dal cliente;
- qualora dalle indagini tecniche non emergano elementi per ritenere accertata la segnalazione di frode, attivare l'*iter* di recupero della somma precedentemente accreditata.

Infine, per il tramite del *team Operations*, la *Perspective* effettua, qualora vi siano le condizioni, le attività di storno dell'operazione oggetto della segnalazione di disconoscimento.

### 4.2. PERSPECTIVE AUGMENTED INTELLIGENCE

La *Perspective Augmented Intelligence* nell'ambito del presente processo è responsabile delle attività di anali tecniche volte a accertare la segnalazione come "frode conclamata" ed a definire eventuali azioni di rafforzamento dei presidi di sicurezza informatica.

### 4.3. OUTSOURCER

#### *4.3.1. Banca Mediolanum – Funzione Risk Management*

La Funzione *Risk Management* di Banca Mediolanum si occupa delle attività previste a livello regolamentare e gestionale per l'identificazione, la misurazione, la mitigazione e la reportistica dei rischi operativi. Nell'ambito di tale *framework*, svolge attività di verifica, raccolta e riconciliazione delle perdite rivenienti dagli eventi di frode subiti della clientela oggetto di reporting periodico «interno» alle funzioni aziendali (es.: Comitato Rischi della Capogruppo e CdA) ed «esterno» alle Autorità di Vigilanza.

## 5 PROCESSO DI MONITORAGGIO E GESTIONE DELLE FRODI SUBITE DAI CLIENTI (AMBITO PAGAMENTI)

Il processo di monitoraggio e gestione degli eventi fraudolenti subiti dalla clientela Flowe con riferimento alle operazioni di pagamento (no monetica) si compone dei seguenti sottoprocessi:

- monitoraggio, ai fini antifrode, delle operazioni di pagamento disposte tramite l'App Flowe o le Terze Parti;
- gestione dei disconoscimenti.

Per ciascun sottoprocesso, di seguito è riportata una descrizione delle attività svolte dagli attori coinvolti, unitamente a:

- la descrizione del controllo effettuata;
- il tipo di controllo (automatico, manuale);
- la frequenza del controllo;
- lo strumento informatico (c.d. applicativo) a supporto delle attività operative svolte e dei controlli eseguiti.

### 5.1. MONITORAGGIO ANTIFRODE DELLE OPERAZIONI DISPOSTE DALLA CLIENTELA

La Direttiva europea 2015/2366 sui servizi di pagamento elettronico (di seguito anche "Direttiva PSD2"), include, tra i suoi obiettivi, l'aumento del livello di sicurezza dei servizi di pagamento elettronico ed il presidio e il governo dei rischi informatici in relazione ai sistemi di pagamento.

Flowe, in qualità di IMEL autorizzato da Banca d'Italia, ha adottato una serie di regole, strumenti e presidi volti a monitorare l'operatività della clientela effettuata tramite l'App; tale monitoraggio è completamente automatico e viene svolto attraverso i seguenti sistemi:

- Gestionale Antiriciclaggio - FCM: il sistema evidenzia, attraverso la creazione di "*alert*", la registrazione di operatività anomala (rispetto alle regole definite) in un determinato arco temporale (es.: una settimana); tali "*alert*" sono visualizzati nella sezione dedicata del gestionale e sono presi in carico ed analizzati dagli operatori del *team AML and KYC*;
- Live Monitoring Dashboard - PowerBI: Flowe si avvale della *dashboard Live Monitoring* costruita tramite Microsoft PowerBI, basata sulle transazioni NRT presenti sul *database*. al fine di identificare operazioni anomale relative all'utilizzo del conto di pagamento. La *dashboard Live Monitoring* prevede due tipologie di analisi su un arco temporale di 72h dal momento dell'apertura del *report*, ovvero: evidenzia la movimentazione cumulativa di ogni conto di pagamento nell'arco temporale selezionato; segnala i conti che nel suddetto arco temporale presentano movimentazione in uscita maggiore o uguale al 90% delle entrate. Gli operatori del team *Account Monitoring and Fraud Management* eseguono tre volte al giorno estrazione manuale dei conti impattati dagli alert relativi ai parametri di cui sopra.
- Per il dettaglio dell'operatività prevista a seguito della rilevazione, da parte dei predetti sistemi, di alert relativi ad operazioni di pagamento "anomale" si faccia riferimento a quanto descritto nella "*procedura operativa gestione conto*".

Inoltre, coerentemente a quanto previsto dalla Direttiva PSD2, all'interno dell'App Flowe sono presenti tutti i presidi volti a garantire il livello di sicurezza dei pagamenti elettronici. Tali presidi sono rappresentata dalla "*Strong Customer Authentication*" (di seguito anche "SCA") e dal "*Dynamic Linking*".

**Strong Customer Authentication ("SCA")**

In fase di disposizione di un'operazione di pagamento, al fine di accertare l'identità del cliente, è prevista la verifica (automatica) di almeno due fattori di diversa tipologia. Tali fattori sono combinati in modo dinamico legando ciascuna transazione ad un importo e un beneficiario specifico, certificandone dunque l'unicità.

La SCA può non essere stata utilizzata e, dunque, non registrata a sistema nei casi di esenzione previsti dalle attuali linee guida EBA ovvero:

- pagamenti verso "*Trusted beneficiaries*" (*White List*);
- pagamenti presso "*Unattended terminals*" per il trasporto e il parcheggio;

**Dynamic Linking**

Al fine di garantire la sicurezza delle operazioni disposte dai clienti è obbligatorio l'utilizzo di una *One Time Password* (OTP) "*dynamic linking*" per autorizzare le operazioni dispositive o variazioni di configurazioni legate alla sicurezza.

La Direttiva PSD2 prevede che la sicurezza delle operazioni di pagamento sia rafforzata da meccanismi di collegamento dinamico ("*dynamic linking*") che contengano almeno i riferimenti ad importo e beneficiario specifico al fine di garantire che l'autorizzazione per una transazione a distanza non venga utilizzata per altri scopi rispetto a quanto originariamente previsto dal pagatore.

## 5.2. GESTIONE DEI DISCONOSCIMENTI

La Direttiva PSD2 prevede che in caso di disconoscimento di un'operazione di pagamento (da parte del cliente), il prestatore di servizi di pagamento del pagatore (Flowe) sia tenuto a rimborsare l'importo dell'operazione di pagamento non autorizzata, immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui prende atto dell'operazione o riceve una notifica in merito.

Tale obbligo viene meno nel caso in cui, sulla base delle informazioni e dei documenti raccolti o delle analisi effettuate sulla posizione del cliente, emergano ragionevoli dubbi per sospettare una frode agita dallo stesso. Nel caso in cui Flowe dovesse riscontrare una frode da parte di un cliente ai danni della stessa Società, la *Perspective Happiness and Service* coinvolge la Funzione *Compliance* per gestire le comunicazioni con Banca d'Italia.

### *5.2.1. Raccolta segnalazione*

Le attività di gestione dei disconoscimenti delle operazioni di pagamento disposte dai clienti tramite App o il canale Terze Parti sono di competenza del *team Customer Interaction* che può essere ingaggiato attraverso le seguenti modalità:

- ricezione di una comunicazione dedicata alla casella *e-mail* istituzionale info@flowe.com;
- ricezione di una comunicazione alla casella PEC istituzionale o di una raccomandata A/R;
- ricezione di una comunicazione alla casella e-mail dedicata ai reclami. In questo caso la segnalazione viene tracciata e gestita come un reclamo ufficiale (cfr. "*Procedura Operativa Gestione Reclami*");

- trasferimento, su canale chat, del contatto del cliente. In questo caso, il cliente interagisce prima con l'assistente virtuale il quale, in base all'argomento identificato fornisce al cliente le istruzioni operative per gestire l'evento (es.: furto/smarrimento dei codici, furto/smarrimento delle credenziali, informazioni relative ad un movimento di addebito collegato ad un pagamento non riconosciuto).

Qualora, a fronte delle informazioni fornite dall'operatore del *team Customer Interaction* (in caso di segnalazione inviata tramite *e-mail*), il cliente recuperi tutte le informazioni necessarie a ritenere chiusa la segnalazione (es.: chiarezza e completezza delle istruzioni ricevute, riconoscimento della regolarità dell'operazione considerata "anomala"), il processo termina. In questo caso, i contenuti della conversazione intervenuta con il cliente sono storicizzati nel sistema Sprinklr e l'assistente virtuale o l'operatore *Customer Interaction* comunicano al cliente stesso che la segnalazione è stata evasa e che la Società non effettuerà ulteriori verifiche in merito.

Al contrario, qualora il cliente confermi la volontà di procedere con il disconoscimento di un'operazione di pagamento o abbia necessità di ricevere maggiori dettagli, la segnalazione viene presa in carico da un operatore *Customer Interaction* per le verifiche preliminari necessarie ad istruire la pratica di disconoscimento.

Si precisa, infine, che in caso di furto o smarrimento del dispositivo mobile sul quale è installata l'App, è fornita al cliente la possibilità - sul Sito istituzionale della Società - di rivolgersi all'assistente virtuale "WAI" attivabile tramite il canale chat o, in caso di orario di servizio attivo, al team Customer Interaction, per ricevere i riferimenti e le attività a suo carico da espletare in queste circostanze.

| **CONTROLLO** | **TIPO CONTROLLO** | **FREQUENZA CONTROLLO** | **APPLICATIVO** |
|---|---|---|---|
| Verifica tipologia di segnalazione cliente<br><br>L'assistente virtuale o l'operatore Customer Interaction verifica i contenuti della segnalazione del cliente. In caso di:<br>• Furto/smarrimento codici (anche a seguito di attacco di phishing): viene suggerito al cliente di modificare in autonomia, nell'area personale dell'App, il *passcode* di accesso, il *security code* e di disattivare la carta eventualmente associata al conto (per poi richiederne un'altra con un nuovo PAN);<br>• Furto/smarrimento credenziali: sono illustrate al cliente le modalità per recuperare e/o modificare in autonomia, nell'area personale dell'App, | Automatico<br><br>Manuale, se la segnalazione perviene tramite il canale e-mail o PEC/raccomandata | Ad evento | Microsoft LUIS |

| CONTROLLO | TIPO CONTROLLO | FREQUENZA CONTROLLO | APPLICATIVO |
|---|---|---|---|
| l'username (corrisponde al numero di cellulare) e il *passcode* (codice numerico di 5 cifre) per accedere all'App Flowe;<br>• Furto/smarrimento *device*: in base al tipo di *device* del cliente (IOS o Android), vengono fornite le modalità per bloccare le carte associate al conto di pagamento. Se il cliente utilizza anche altre applicazioni che permettono di effettuare pagamenti attraverso la carta virtuale, viene suggerito al cliente di rimuovere la carta anche da tali strumenti;<br>• Furto/smarrimento carta: viene suggerito al cliente di bloccare temporaneamente, in autonomia attraverso l'App la carta ("*freeze*") e di valutare successivamente la disattivazione e la richiesta di una nuova;<br>• Disconoscimento operazione di pagamento: vengono sottoposte al cliente una serie di domande volte a ricostruire le circostanze a cui afferisce l'operazione contestata. Se il Cliente riconosce l'operazione, il processo termina; al contrario, l'operatore Customer Interaction prende in carico la segnalazione ed avvia le verifiche necessarie ad istruire la pratica di disconoscimento. | | | |

### 5.2.2. *Verifiche preliminari*

L'operatore del *Team Customer Interaction* che prende in carico la segnalazione, verifica i dati relativi all'operazione oggetto di disconoscimento con quanto registrato negli applicativi di

riferimento e, in caso di necessità di approfondimenti o chiarimenti, contatta il cliente per verificare la natura delle operazioni in oggetto.

Durante le attività di verifiche preliminare, l'operatore:

- fornisce al cliente tutti i dati di dettaglio dell'operazione (es.: beneficiario, giorno ed ora della transazione) in maniera tale da accertare con lo stesso se si tratta di un effettivo disconoscimento. In questa fase, l'operatore supporta il cliente nell'identificazione degli elementi necessari a ricondurre quest'ultimo all'esperienza di pagamento vissuta ed a riconoscere la transazione (es.: nome del beneficiario non familiare per il cliente);
- consiglia al cliente di procedere in autonomia, attraverso la funzionalità presente in App, con il reset delle credenziali di accesso all'App e dei codici dispositivi;
- informa il cliente circa le responsabilità e conseguenze derivanti da dichiarazioni mendaci;
- comunica al cliente le modalità e le condizioni che regolano la disposizione del rimborso "Salvo Buon Fine" e la necessità, in caso di accertamento della genuinità dell'operazione di pagamento, di restituire l'importo a Flowe.

L'operatore del *team Customer Interaction*, inoltre, verifica se l'operazione oggetto di disconoscimento è disposta tramite l'App di Flowe o tramite le Terze Parti. Se l'operazione è stata disposta tramite l'App Flowe procede, con l'invio al cliente, tramite Fanbase, di una notifica "*out of band*"; la comunicazione contiene i dati dell'operazione di pagamento oggetto della segnalazione (beneficiario, iban, causale ed importo e data di addebito) che il cliente deve confermare direttamente in App. Al ricevimento della conferma da parte del cliente (tramite *security code*/dati biometrici) l'operatore *Customer Interaction*, se possibile in termini di caratteristiche e tempistiche dell'operazione, inserisce un Claim sulla posizione del cliente per richiedere l'esecuzione delle attività di storno sul conto del cliente (cfr. "*Procedura Operativa Pagamenti SCT*"); per garantire che la richiesta di storno sia gestita con urgenza, l'operatore inoltra anche una *e-mail* al *team Operations* con il riferimento all'operazione da stornare.

Al contrario, se l'operazione non è stornabile ma, in base ai dati raccolti e alle verifiche preliminari condotte, vi siano i presupposti per procedere con il disconoscimento oppure è necessario effettuare degli ulteriori approfondimenti, l'operatore apre un *claim* sulla posizione del cliente per richiedere l'avvio delle analisi e degli approfondimenti da parte del *team Account Monitoring and Fraud Management*.

In questo caso viene chiesto al cliente:

- se non già fatto in precedenza, di procedere in autonomia, attraverso la funzionalità presente in App, con il reset delle credenziali di accesso all'App e dei codici dispositivi;
- di inoltrare, la copia della denuncia presentata presso le autorità competenti. Tale documento sarà inviato, in fase di richiamo dell'operazione, all'istituto beneficiario.

| CONTROLLO | TIPO CONTROLLO | FREQUENZA CONTROLLO | APPLICATIVO |
|---|---|---|---|
| Verifica tipologia e dettagli transazione oggetto di disconoscimento<br>L'operatore verifica, attraverso gli applicativi dedicati, le | Manuale | Ad evento | P0, T24 |

| CONTROLLO | TIPO CONTROLLO | FREQUENZA CONTROLLO | APPLICATIVO |
|---|---|---|---|
| caratteristiche dell'operazione di pagamento oggetto di segnalazione (es.: importo, beneficiario,) al fine di determinare se vi siano i presupposti per sospettare una frode (es.: presenza di altri pagamenti – non disconosciuti- verso lo stesso beneficiario) | | | |
| Verifica canale da cui è stata disposta l'operazione (App Flowe vs Terze Parti)<br>L'operatore verifica il canale utilizzato dal cliente per disporre l'operazione di pagamento; in caso di operazione disposta tramite il canale Terze Parti, non è possibile procedere con lo storno in quanto le disposizioni di pagamenti inizializzate per il tramite delle Terze Parti sono irrevocabili (cfr. art. 80 della Direttiva PSD2) | Manuale | Ad evento | P0 Log, T24 |
| Verifica data ed orario regolamento operazione<br>Se l'operazione è in corso (non è stata ancora processata dal sistema), l'operatore avvia, per il tramite del *team Operations*, la procedura di storno. Al contrario, si prosegue con le attività di analisi dell'evento al fine di valutare il richiamo dell'operazione. | Manuale | Ad evento | T24 |

### *5.2.3. Analisi e classificazione evento*

L'operatore del *team Account Monitoring and Fraud Management* che prende in carico il *claim* effettua tutti gli approfondimenti volti ad accertare che l'operazione segnalata rappresenti un evento fraudolento subito dal cliente.

L'operatore verifica, attraverso gli applicativi aziendali, le informazioni legate al *device* sul quale è installata l'App Flowe ed ai codici di sicurezza associati al cliente, ed i dati legati all'operazione (es.: importo e beneficiario dell'operazione).

Sulla base delle evidenze delle verifiche, l'operatore valuta se apporre, attraverso *Fanbase*, il blocco App in modo da minimizzare il rischio di ulteriori operatività indesiderate.

| CONTROLLO | TIPO CONTROLLO | FREQUENZA CONTROLLO | APPLICATIVO |
|---|---|---|---|
| Verifica presenza recenti modifiche alle credenziali e ai codici di sicurezza<br>L'operatore verifica se, negli ultimi sette (7) giorni, il cliente ha:<br>• certificato un nuovo *device* mobile;<br>• certificato un nuovo indirizzo *e-mail*;<br>• modificato il numero di cellulare in anagrafica;<br>• resettato/modificato i codici di sicurezza (es.: *passcode*/*security code*).<br>La presenza di almeno uno di tali elementi, in aggiunta alle dichiarazioni raccolte dal cliente, può rappresentare un ragionevole presupposto per ritenere l'operazione una potenziale frode subita dallo stesso cliente. | Manuale | Ad evento | P0, Fanbase |
| Verifica coordinate del beneficiario operazione<br>L'operatore verifica, ad esempio, se le coordinate del beneficiario dell'operazione segnalata sono state oggetto di altre segnalazioni fraudolente. | Manuale | Ad evento | T24 |

Qualora, anche a seguito di ulteriore contatto con il cliente, l'operatore del *team Account Monitoring and Fraud Management* riscontri la regolarità dell'operazione disposta e quindi l'assenza degli elementi necessari per procedere con il rimborso chiude il *claim* integrando le informazioni relative all'istruttoria gestita. L'operatore del *team Customer Interaction* comunica al cliente che non vi sono i presupposti per procedere con la valutazione del disconoscimento e che la Società non effettuerà ulteriori verifiche o approfondimenti in merito (cfr. parag. 5.2.4). Nel caso in cui Flowe dovesse riscontrare una frode da parte di un cliente ai danni della stessa Società, la *Perspective Happiness and Service* coinvolge la Funzione *Compliance* per gestire le comunicazioni con Banca d'Italia.

Al contrario, se sulla base dei dati raccolti e delle analisi condotte, vi siano i presupposti per accettare il disconoscimento oppure è necessario effettuare degli ulteriori approfondimenti prima di ritenere la frode "accertata", l'operatore del *team Account Monitoring and Fraud Management*

dispone il rimborso Salvo Buon Fine a favore del cliente. L'accredito dell'importo dell'operazione contestata è gestito attraverso il sistema di *Core Banking* e coerentemente con quanto previsto dalla Direttiva PSD2, entro la fine della giornata operativa successiva alla ricezione della segnalazione.

L'operatore *Account Monitoring and Fraud Management* che ha gestito la segnalazione inserisce, tramite la sezione apposita in T24, tutti i dati dell'operazione e registra la richiesta di esecuzione; per processare l'operazione è necessaria l'autorizzazione da parte di un operatore diverso da quello che ha inserito a sistema l'operazione (logica *4eyes*). Pertanto, un secondo *user Account Monitoring and Fraud Management*, avente adeguati poteri autorizzativi, confermerà la disposizione. Anche in questo caso il *claim* viene aggiornato con le informazioni necessarie alla comunicazione al cliente (da parte dell'operatore *Customer Interaction*), dell'avvenuto rimborso (cfr. parag. 5.2.4).

Per tutte le segnalazioni di disconoscimento per le quali si procede con un rimborso Salvo Buon Fine, l'operatore *Account Monitoring and Fraud Management* procede inoltre con:

- l'inoltro, tramite *e-mail*, di una comunicazione alla *Perspective Augmented Intelligence* contenente tutti i dettagli delle informazioni raccolte e delle analisi svolte al fine di proseguire con le indagini volte a accertare la segnalazione come "frode conclamata";
- l'esecuzione delle attività collegate alla gestione dei richiami (cfr. "*Procedura Operativa Gestione Pagamenti SCT*").

### *5.2.4. Comunicazione al cliente*

**Comunicazione Salvo Buon Fine**

In caso di riconoscimento dell'operazione oggetto di disconoscimento come frode subita dal cliente, l'operatore del *team Customer Interaction* comunica, tramite e-mail, l'avvenuto rimborso "Salvo Buon Fine".

La comunicazione contiene la specifica che, se a fronte delle analisi in corso, le valutazioni saranno confermate, l'importo riconosciuto sarà considerato definitivo. In caso contrario, Flowe, procederà in autonomia con il recupero della somma sul conto di pagamento del cliente.

**Comunicazione di diniego**

Nel caso in cui, sulla base delle valutazioni effettuate (dai *team Customer Interaction* o *Account Monitoring and Fraud Management*) si ritenga che l'operazione oggetto di disconoscimento non rappresenti una frode subita dal cliente, l'operatore del *team Customer Interaction* comunica al cliente il diniego della pratica.

Se gli elementi per rifiutare la pratica sono chiari già nella fase di verifiche preliminari, l'operatore comunica il diniego attraverso lo stesso canale da cui è pervenuta la segnalazione (*e-mail*, PEC o *chat*); qualora invece il diniego sia stato elaborato dal *team Account Monitoring and Fraud Management* in fase di analisi dell'evento, la comunicazione viene inviata alla casella *e-mail* del cliente censita in anagrafica.

Infine, qualora la segnalazione di disconoscimento sia pervenuta attraverso un reclamo, il riscontro viene fornito attraverso il canale utilizzato dal cliente per la comunicazione (es.: *e-mail* o PEC); in caso di ricezione di una raccomandata A/R, viene fornito riscontro al cliente tramite una *e-mail* all'indirizzo censito in anagrafica.

In tutti i casi, la comunicazione di diniego illustra al cliente in maniera chiara ed esauriente le motivazioni alla base del rifiuto della segnalazione; in caso di disconoscimento pervenuto tramite reclamo, sono inoltre presenti le informazioni in merito alla possibilità di aderire all'Arbitro Bancario Finanziario o ad altre forme di risoluzione stragiudiziale delle controversie.

#### *5.2.5. Indagini per accertamento frode*

Gli operatori della *Perspective Augmented Intelligence* avviano, se necessario anche con il supporto dei fornitori delle applicazioni informatiche impattate dall'evento segnalato, gli approfondimenti tecnici volti a confermare l'attacco fraudolento subito dal cliente ed a definire eventuali azioni di rafforzamento dei presidi di sicurezza informatica.

In questa fase, l'operatore verifica, se necessario anche per il tramite dell'*outsourcer* Temenos, il metodo di autenticazione utilizzato dal cliente, l'indirizzo IP ed in caso di operazione disposta per il tramite di una Terza Parte, la presenza del consenso dedicato ad operare.

Nel caso di mancata autenticazione forte (SCA), sono avviate le analisi tecniche volte ad identificarne la causa ed a correggere eventuali anomalie.

Qualora si ritenga che la segnalazione sia il frutto di un potenziale intervento malevolo da parte di *hacker* sull'App del cliente, l'operatore *Augmented Intelligence* si confronta con il *team Account Monitoring and Fraud Management* per l'apposizione del blocco App.

| **CONTROLLO** | **TIPO CONTROLLO** | **FREQUENZA CONTROLLO** | **APPLICATIVO** |
|---|---|---|---|
| Verifica metodo di autenticazione<br>L'operatore verifica che l'operazione in esame sia stata effettuata tramite la Strong Customer Authentication (SCA). Qualora l'informazione non sia stata tracciata oppure non autorizzata secondo gli *standard* di sicurezza previsti dalla normativa, sono avviate le analisi tecniche necessarie a risolvere l'anomalia | Manuale | Ad evento | P0 |
| Verifica IP *address*<br>L'operatore verifica la geolocalizzazione dell'App rispetto al luogo in cui è stata disposta l'operazione di pagamento disconosciuta dal cliente (IP *address*) | Manuale | Ad evento | P0 |
| Verifica presenza consenso Terze Parti<br>In caso di operazione disposta tramite le Terze Parti l'operatore | Manuale | Ad evento | P0 |

| CONTROLLO | TIPO CONTROLLO | FREQUENZA CONTROLLO | APPLICATIVO |
|---|---|---|---|
| verifica inoltre, la presenza del consenso dedicato e il canale utilizzato dal cliente per fornirlo. | | | |

Sulla base delle evidenze delle analisi condotte dalla *Perspective Augmented Intelligence*, il *team Account Monitoring and Fraud Management* valuta se classificare l'evento come "frode conclamata" o "frode non accertata".

In caso di frode conclamata, l'operatore *Account Monitoring and Fraud Management*, integra il claim con le informazioni raccolte in maniera tale da notificare al *team Customer Interaction* che è possibile informare il cliente sull'esito finale del disconoscimento ed archiviare la pratica. Qualora, a titolo preventivo sia stato apposto il blocco App, l'operatore *Account Monitoring and Fraud Management* procede con la rimozione attraverso l'apposita funzionalità di *Fanbase*.

In caso contrario, qualora dalle indagini tecniche non emergano elementi per ritenere accertata la segnalazione di frode, l'operatore *Account Monitoring and Fraud Management* procede con l'iter di recupero della somma precedentemente accreditata. Se il conto del cliente è capiente (saldo disponibile maggiore o uguale dell'importo oggetto del rimborso Saldo Buon Fine), l'operatore *Account Monitoring* integra il claim con le informazioni necessarie all'operatore del *team Operations* per eseguire la contabilizzazione dell'addebito della somma dovuta dal cliente; per garantire che la richiesta sia gestita con urgenza, l'operatore inoltra anche una *e-mail* al *team Operations* con il riferimento alla posizione da gestire.

Se il conto del cliente non è capiente, l'operatore *Account Monitoring and Fraud Management* appone una prenotata al fine di bloccare i fondi sul conto del cliente.

L'operatore *Customer Interaction*, ingaggiato tramite l'inoltro del *claim* in *Fanbase*, notifica al cliente la necessità di restituire le somme ricevute a titolo di Rimborso Salvo Buon Fine e richiede allo stesso di accreditare il proprio conto per l'importo necessario.

Se dopo 3 mesi il cliente non ha ancora ricaricato il conto, il *team BackOffice Operations* metterà la cifra dovuta a perdita e procederà con la richiesta di estinzione unilaterale del conto.

In caso di importi molto elevati si valuterà con l'*Ufficio Contenzioso* di Banca Mediolanum Bmed se aprire un esposto.

Anche in questo caso, qualora a titolo preventivo sia stato apposto il blocco App, l'operatore *Account Monitoring and Fraud Management* procede con la rimozione attraverso l'apposita funzionalità di *Fanbase*.

#### *5.2.6. Archiviazione dati e predisposizione reportistica*

A conclusione delle attività di gestione del disconoscimento, l'operatore del *team Customer Interaction*:

- integra e modifica lo stato della pratica in *FanBase* (da "*In progress*" a "*Closed*");
- completa i dati all'interno del file gestionale "Censimento Frodi su *Credit Transfer*" (es.: Nome e Cognome, Tipologia operazione disconosciuta, Data apertura pratica, Customer ID, Numero

di conto, Importo contestato, Data addebito importo, Beneficiario operazione, Stato Pratica, Cronologia eventi, Canale contatto) utilizzato per la predisposizione della reportistica dedicata alle frodi registrate sui servizi di pagamento elettronico da inoltrare semestralmente alla Banca d'Italia.

Mensilmente, la *Funzione Risk Management* dell'*outsourcer* Banca Mediolanum accede allo *sharepoint* della *Perspective Happiness and Services* ed estrae (da tale file) i dati relativi ai rimborsi riconosciuti alla clientela oggetto di eventi fraudolenti necessari a calcolare il valore delle perdite operative sostenute dalla società.

# 6 NORMATIVA

## 6.1. NORMATIVA INTERNA

Nel presente capitolo si richiama il contesto normativo di riferimento per le attività della procedura in oggetto.

- *Policy per il controllo e la gestione dei Rischi Operativi;*
- *Policy la gestione del Rischio Reputazionale;*
- *Regolamento del processo di "Fraud Reporting";*
- *Procedura di "Gestione del conto";*
- *Procedura di Gestione dei pagamenti SCT.*
- *Procedura Operativa Gestione Reclami*

## 6.2. NORMATIVA ESTERNA

La cornice legislativa a cui fa riferimento la presente procedura è rappresentata dai seguenti documenti:

- *Direttiva (UE) 2015/2366 PSD2 – (Payment Services Directive 2);*
- *Decreto Legislativo 15 dicembre 2017, n. 218 e successive modifiche e integrazioni;*
- *Decreto Legislativo 27 gennaio 2010, n. 11 e successive Modifiche e integrazioni;*
- *Regulatory Technical Standards on strong customer authentication and secure communication under PSD2;*
- *Orientamenti recanti modifica agli orientamenti EBA GL-2018-05 (EBA/GL/2020/01).*
- *Provvedimento Della Banca d'Italia de 23 luglio 2019, Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica e successivi aggiornamenti;*
- *D. Lgs. 22/6/2007, n. 109 e successive modifiche ed integrazioni, recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo internazionale;*
- *D. Lgs. 21/11/2007, n. 231 e successive modifiche ed integrazioni, recante l'attuazione della*

*Direttiva 2018/843/CE;*

- *Disposizioni di Trasparenza delle operazioni e dei Servizi Bancari e Finanziari - Correttezza delle relazioni tra intermediari e clienti del 29 luglio 2009 e successive modifiche e integrazioni*