PROCEDURA OPERATIVA

Monitoraggio e gestione delle frodi subite dalla clientela (Ambito monetica)

Procedura emessa il 30/08/2021

Owner della procedura: Perspective Happiness and Services

1 OBIETTIVO DEL DOCUMENTO 3
1.1. AMBITO DI APPLICAZIONE 3
1.2. AGGIORNAMENTO DEL DOCUMENTO 3
2 DEFINIZIONI 4
3 STRUMENTI A SUPPORTO DEL PROCESSO 5
3.1. APP FLOWE 5
3.2. PLATFORM – POWER PLATFORM – P0 (PZERO) 5
3.3. FANBASE – POWER PLATFORM 6
3.4. SPRINKLR 6
3.5. SISTEMA DI CORE BANKING - T24 6
3.6. GESTIONALE CARTE – SIA CRISTAL GATE (GUI) 6
3.7. FALCON 6
4 ATTORI, RUOLI E RESPONSABILITÀ 7
4.1. PERSPECTIVE HAPPINESS AND SERVICE 7
4.2. OUTSOURCERS 8
4.2.1. Banca Mediolanum – Funzione Risk Management 8
4.2.2. SIA 8
4.3. ALTRI ATTORI COINVOLTI 8
4.3.1. Mastercard 8
5 PROCESSO DI MONITORAGGIO E GESTIONE DELLE FRODI SUBITE DAI CLIENTI (AMBITO MONETICA) 8
5.1. MONITORAGGIO ANTIFRODE DELLE OPERAZIONI DISPOSTE CON CARTA 9
5.1.1. Definizione ed aggiornamento regole antifrode 9
5.1.2. Elaborazione dati operazione 9
5.1.3. Contatto e gestione cliente 10
5.1.4. Monitoraggio operatività elevata 10
5.2. GESTIONE DEI DISCONOSCIMENTI 11
5.2.1. Raccolta segnalazione e verifiche preliminari 11
5.2.2. Analisi e classificazione evento 12
5.2.3. Comunicazione al cliente 16

5.2.4. Archiviazione dati e predisposizione reportistica 17
6 NORMATIVA 17
6.1. NORMATIVA INTERNA 17
6.2. NORMATIVA ESTERNA 17

1 OBIETTIVO DEL DOCUMENTO

Obiettivo del presente documento è illustrare il processo di monitoraggio e gestione degli eventi fraudolenti subiti dalla clientela Flowe con riferimento alle operazioni disposte tramite la carta di pagamento (sia fisica che virtuale).

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

3.13.04 MONITORAGGIO E GESTIONE FRODI SUBITE DAI CLIENTI (AMBITO MONETICA)

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:

- ***Merchant*:** esercente convenzionato presso il quale viene effettuato il pagamento abilitato ad accogliere compensi tramite carta.
- **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.
- **Disputa:** contestazione di un'operazione di pagamento avvenuta con carta per cui il cliente richiede il rimborso per presunta frode.
- ***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.
- ***3D Secure Code*:** protocollo *standard* sicuro per i pagamenti *online* effettuati con carta adottato dai principali circuiti, tale strumento è utile per aumentare il livello di sicurezza della transazione in quanto permette al *merchant* di verificare che la persona che effettua il pagamento online sia effettivamente il titolare della carta richiedendo un ulteriore passaggio in fase di autorizzazione del pagamento.
- **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.
- ***Chargeback*:** procedura con la quale vengono gestiti i movimenti relativi a contestazioni da parte dei titolari di carte. Utilizzato sui circuiti internazionali, tale meccanismo è generalmente attivato quando il titolare di una carta chiede alla società emittente lo storno (cioè, il rimborso) di una transazione già avvenuta.
- **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:

- attraverso la funzionalità *SmartAgent*, la possibilità per il cliente di confermare o disconoscere le operazioni effettuate tramite carta ed identificate, dal sistema antifrode, come "sospette";
- disattivare, in caso di sospetta frode subita, la carta di pagamento;
- interagire, tramite il canale chat, con l'operatore del *team Customer Care* per disconoscere un'operazione di pagamento effettuata tramite carta.

All'interno dell'App, è integrata una funzionalità che permette al cliente di attivare il *3DSecureCode* al fine di autorizzare in sicurezza i pagamenti *online* effettuati con carta di debito a favore degli esercenti aderenti a tale protocollo di sicurezza. Il servizio prevede, in fase di autorizzazione, l'invio tramite notifica "*push*" sul dispositivo del cliente di un OTP (*One Time Password*) valido per l'autorizzazione dello specifico pagamento. Tale presidio permette di ridurre:

- la possibilità di utilizzo fraudolento delle carte, grazie all'autenticazione al momento effettivo della transazione;
- le controversie ed i *chargeback* da trattare.

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 delle *Perspective Happiness and Service* nello svolgimento delle attività legate alla gestione dei disconoscimenti delle operazioni disposte tramite carta.

La *Platform*, inoltre, mette a disposizione i servizi necessari alla ricezione dei dati relativi agli "*alert*" evidenziati dal sistema Falcon e notificati in App attraverso la funzionalità *SmartAgent*.

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 viene utilizzata per la storicizzazione della documentazione inerente le pratiche di disconoscimento avanzate dai clienti Flowe.

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, ai fini delle analisi relativi ai disconoscimenti, i dettagli dei movimenti relativi alla carta sospetta.

3.6. GESTIONALE CARTE – SIA CRISTAL GATE (GUI)

Flowe si avvale della piattaforma di *card management* SIA CRISTAL GATE (di seguito indicato come Gestionale carte) fornita dall'*outsourcer* SIA per consultare le informazioni relative alla carta ed ai relativi movimenti e gestire l'apposizione e la rimozione dei relativi blocchi.

3.7. FALCON

Falcon è il sistema di prevenzione delle frodi sulle operazioni di pagamento effettuate tramite carta di debito (su circuito internazionale) dell'*outsourcer* SIA.

Attraverso l'analisi dei dati in *real time* e l'integrazione con le logiche di autorizzazione del *card management*, il sistema Falcon permette di:

- definire e gestire, in maniera dinamica, le regole dell'impianto per l'analisi del transato collegato alla carta. Sulla base di tali regole, il sistema elabora un punteggio di rischio da attribuire a ogni autorizzazione e innesca un'azione, quale ad esempio approvare l'autorizzazione, aprire un "*case*" per un'ulteriore analisi o bloccare la carta, restituendo al sistema autorizzativo uno specifico codice;
- gestire i "*case*" generati dalle regole definite. Il "*case*" è l'insieme delle informazioni inerenti la carta oggetto di sospetta frode. A fronte delle attività di analisi e valutazione, è possibile confermare nell'applicativo l'eventuale esistenza di una frode.
- accedere, ai fini delle valutazioni sui disconoscimenti avanzati dalla clientela, a liste contenenti le carte compromesse note, i *merchant* e gli indirizzi IP a rischio.

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 carta ed effettuare le verifiche preliminari sull'evento;
- qualora ci siano i presupposti per attivare la pratica di disputa, richiedere al cliente tutta la documentazione necessaria per l'ingaggio dell'*outsourcer* SIA;
- inoltrare la pratica a SIA per l'analisi e classificazione dell'evento fraudolento segnalato dal cliente;
- 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 le perdite operative e le frodi subite dalla clientela ("*Fraud Reporting*").

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

- definire ed aggiornare il sistema monitoraggio frodi sulle operazioni effettuate con carta di pagamento;
- analizzare i dati delle transazioni che hanno generato l'attivazione del blocco carta per operatività elevata e valutare le opportune azioni sul conto di pagamento associato;
- ricevere, da parte di SIA, le segnalazioni relative all'utilizzo di carte bloccate e valutare l'attivazione di ulteriori presidi antifrode.

4.2. OUTSOURCERS

4.2.1. 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.

4.2.2. SIA

Nell'ambito del presente processo, l'*outsourcer* SIA:

- nell'ambito del processo di monitoraggio antifrode delle operazioni con carta, in aggiunta alla gestione della componente tecnologica del sistema Falcon, gestisce i contatti telefonici con il titolare della carta, al fine di verificare la genuinità delle transazioni segnalate dagli strumenti di rilevazione delle frodi.
- nell'ambito del processo di disconoscimento, effettua le analisi e gli approfondimenti sulle pratiche di disputa avanzate dalla clientela Flowe. In caso di accertamento della frode subita dal cliente, effettua il *chargeback* dell'importo dell'operazione attraverso il c.d. "Rimborso salvo Buon fine" a favore del cliente. Al contrario, a seguito di rilevazione di elementi che non caratterizzano l'evento come fraudolento procede con le attività di recupero dell'importo eventualmente già accreditato.

4.3. ALTRI ATTORI COINVOLTI

4.3.1. Mastercard

La carta di pagamento emessa da Flowe è associata al circuito internazionale MasterCard (MasterCard *Prepaid*), operatore riconosciuto a livello internazionale e *partner* di riferimento di diverse istituzioni bancarie e soggetti vigilati.

Nell'ambito del presente processo, il circuito Mastercard viene ingaggiato da SIA durante la fase di analisi e classificazione dell'evento per effettuare ulteriori indagini ed approfondimenti sull'operazione volti ad accertare la frode subita dal cliente.

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

Il processo di monitoraggio e gestione degli eventi fraudolenti subiti dalla clientela Flowe con riferimento alle operazioni disposte tramite la carta di pagamento (sia fisica che virtuale) si compone dei seguenti sottoprocessi:

- monitoraggio, ai fini antifrode, delle operazioni disposte con carta;
- 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 CON CARTA

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 carta di pagamento; tale monitoraggio è completamente automatico e viene svolto attraverso il sistema antifrode Falcon messo a disposizione dall'outsourcer fornitore SIA.

5.1.1. Definizione ed aggiornamento regole antifrode

La *Perspective Happiness and Service* per il tramite del *team Account Monitoring and Fraud Management* è responsabile della definizione ed aggiornamento del sistema monitoraggio frodi sulle carte di pagamento. In particolare, valuta l'attivazione di nuove regole e/o l'aggiornamento dei parametri che caratterizzano il funzionamento delle stesse (es.: paesi, orari, importi) e si interfaccia con l'*outsourcer* per le attività tecniche di adeguamento del sistema informatico.

5.1.2. Elaborazione dati operazione

Il sistema Falcon elabora, in *real time*, tutte le operazioni (sia prelievi che pagamenti) effettuate dalla clientela con la carta (sia fisica che virtuale); in particolare, per ciascuna transazione, rileva il superamento delle soglie previste da ogni regola dell'impianto e innesca l'azione prevista:

- qualora non sia rilevata alcuna anomalia (rischio nullo o basso) à l'operazione viene autorizzata;
- se i dati dell'operazione superano i livelli di soglia stabiliti dalle regole antifrode à l'operazione viene declinata (al sistema autorizzativo viene restituito uno specifico codice);
- qualora l'operazione sia "sospetta" ovvero rientri in una delle regole prestabilite che determinano la rischiosità della stessa, il sistema crea, automaticamente, un "*alert*" (di seguito anche "*case*").

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica dei dati dell'operazione di pagamento rispetto ai parametri delle regole antifrode attive	Automatico	Continuativo	Falcon

5.1.3. Contatto e gestione cliente

Tutti gli *alert* evidenziati dal sistema Falcon sono comunicati al cliente attraverso la funzionalità *SmarAgent* presente nell' App Flowe; tale funzionalità, dopo aver ricevuto da Falcon i dati del "*case*" genera ed inoltra al cliente una notifica con l'obiettivo di accertare la genuinità della transazione.

Qualora il cliente risponda alla notifica confermando di aver disposto l'operazione "sospetta", il "*case*" viene automaticamente chiuso; al contrario, se il cliente disconosce l'operazione notificata, la sua posizione viene presa in carico e gestita con priorità dall'*outsourcer* SIA. L'operatore del *team* "presidio antifrode" di SIA, dopo aver contatto telefonicamente il cliente, blocca la carta di pagamento e comunica al cliente la possibilità di procedere, attraverso Flowe, con il disconoscimento dell'operazione e la richiesta di rimborso per frode subita.

L'*outsourcer* SIA effettua due tentativi di contatto al cliente, a distanza di due (2) ore; se al secondo contatto il cliente non risponde oppure risponde la segreteria telefonica oppure risponde un parente, il *case* viene esitato come "*Unable to Confirm Not Fraud*". Ove la regola lo prevede, la carta viene comunque posta in blocco cautelativo.

Il cliente può, in ogni caso, ricontattare successivamente il numero telefonico sul quale ha ricevuto la telefonata così da approfondire con un operatore dedicato di SIA le informazioni relative all'operazione sospetta.

5.1.4. Monitoraggio operatività elevata

Il sistema di monitoraggio antifrode delle operazioni disposte tramite carte di pagamento prevede, inoltre, l'apposizione di un blocco automatico (preventivo) da parte di SIA, in caso di superamento del numero e/ o dell'importo massimo di transazioni giornaliere previste (i valori massimi possono variare in base alle regole definite dalla Società, es.: in base al tipo di *merchant* coinvolto nell'operazione).

Giornalmente, l'*outsourcer* SIA invia, tramite *e-mail*, al *team Account Monitoring and Fraud Management* l'elenco delle posizioni sulle quali è stato apposto il blocco carta per operatività elevata.

L'operatore del *team Account Monitoring and Fraud Management*, per ciascun cliente presente nel report, analizza i dati delle transazioni che hanno generato l'attivazione del blocco verificando se necessario anche lo storico delle operazioni del cliente.

Qualora non emergano elementi di anomalia o di sospetto l'operatore elimina, attraverso la funzionalità del Gestionale Carte – SIA Cristal Gate, il blocco riattivando la piena operatività della carta. Al contrario, se dagli approfondimenti emergono operazioni sospette o anomalie rispetto al

tipo di operazione eseguita, l'operatore avvia l'iter di Adeguata Verifica Rafforzata (cfr. "*Procedura Operativa Gestione conto*"); in questo caso, durante il processo di verifica ed accertamento delle transazioni in oggetto, l'operatività tramite carta rimane bloccata a fini preventivi.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica numero/importo massimo giornaliero di operazioni disposte con carta	Automatico	Continuativo	Falcon
Verifica storico transazioni cliente	Manuale	Ad evento	SIA Cristal Gate (GUI); T24

Si specifica inoltre che, qualora il titolare di una carta bloccata (da Flowe[1] o da SIA automaticamente per operatività elevata) tenti di disporre un pagamento SIA inoltra, tramite *e-mail*, una segnalazione agli operatori del *team Account Monitoring and Fraud Management* che analizzano la posizione del cliente e l'operatività associata al conto di pagamento e verificano che effettivamente le transazioni siano state negate.

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 dello stesso, emergano ragionevoli dubbi per sospettare una frode agita dallo stesso Cliente; in caso di successiva decisione di mancato rimborso, la *Perspective Happiness and Service* coinvolge la Funzione *Compliance* per gestire le comunicazioni con Banca d'Italia.

5.2.1. Raccolta segnalazione e verifiche preliminari

Il cliente può disconoscere un'operazione disposta tramite carta di pagamento a seguito di ricezione di notifica attraverso la funzionalità *SmartAgent* (cfr. paragr. 5.1.3) oppure a fronte di verifica, svolta in autonomia, della lista movimenti del conto (presente in App).

Le attività di gestione dei disconoscimenti delle operazioni disposte tramite la carta di pagamento

[1] Per le casistiche e le modalità di blocco della carta di faccia riferimento alla "Procedura operativa Gestione conto" par. 5.2.2.

sono di competenza del *team Customer Interaction* che viene ingaggiato dal cliente 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;
- trasferimento, su canale *chat*, del contatto del cliente. In questo caso, il cliente interagisce prima con l'assistente virtuale il quale, dopo aver identificato l'argomento dedicato ("disputa", "disconoscimento", "rimborso") inoltra il contatto all'operatore;
- ricezione di una comunicazione alla casella e-mail dedicata ai reclami. In questo caso la segnalazione viene tracciata e gestita come un reclamo ufficiale (per ulteriori approfondimenti si rimanda al processo "Gestione Reclami").

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 ed, 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:

- comunica al cliente che, per sua tutela, è necessario procedere al blocco della carta;
- fornisce al cliente tutti i dati di dettaglio dell'operazione (es.: *merchant*, 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 *merchant* non familiare per il cliente);
- informa il Cliente circa le responsabilità e conseguenze derivanti da dichiarazioni mendaci;
- comunica le modalità di attivazione della procedura di disputa, il funzionamento della stessa e le tempistiche di rimborso.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica dati operazione tramite carta oggetto di disconoscimento da parte del cliente	Manuale	Ad evento	SIA Cristal Gate (GUI); T24

5.2.2. *Analisi e classificazione evento*

Raccolta ed analisi dati operazione

Nella fase di analisi e classificazione dell'evento, l'operatore verifica innanzitutto se l'operazione è stata disposta tramite POS fisico oppure *online* (tramite sito di *e-commerce*).

Nel primo caso, qualora l'operatore riscontrasse che l'utente non ha fatto quello che serviva per garantire la sicurezza e/o per proteggere le sue credenziali (PIN) non verrà effettuato alcun tipo di rimborso.

Diversamente (es clonazione), l'utente è responsabile esclusivamente nei limiti di 50 euro. A titolo esemplificativo se, a seguito di una clonazione il cliente rileva una spesa non autorizzata di 150 euro gli scenari che potrebbero prospettarsi sono i seguenti:

- Rimborso di 150 euro, se l'utente non aveva la possibilità di accorgersene o di comunicarcelo per colpa di una nostra anomalia
- Rimborso di 100 euro se poteva accorgersene prima o, semplicemente, lo ha comunicato in ritardo (in questo caso i 50 euro restano a suo carico).

Per quel che riguarda invece le disposizioni online, l'operatore richiede a SIA, tramite *e-mail*, di verificare il tipo di *merchant* coinvolto nella transazione; inoltre, l'operatore verifica sul *web* se, rispetto alla casistica in corso di analisi, sono presenti notizie o recensioni sul *merchant* o sulla piattaforma di *e-commerce* che evidenzino la presenza di eventi fraudolenti già accertati da altri intermediari.

Qualora, anche a seguito di ulteriore contatto con il cliente, l'operatore riscontri la regolarità dell'operazione e quindi l'assenza degli elementi necessari per procedere con il rimborso, 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. 5.2.3). 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 verifiche preliminari condotte, vi siano i presupposti per procedere con il disconoscimento oppure è necessario effettuare degli ulteriori approfondimenti, l'operatore richiede al cliente:

- se non già fatto in precedenza, di procedere in autonomia, attraverso la funzionalità presente in App, con la disattivazione della carta (temporanea o definitiva con eventuale ri-emissione). Tale azione rappresenta la misura preventiva volta a bloccare eventuali futuri tentativi di frode verso il cliente;
- di compilare, sottoscrivere ed inoltrare il modulo "*Claim Form*" necessario a formalizzare il disconoscimento dell'operazione.

Si precisa infine che le attività di analisi dell'evento sono avviate solo a seguito della contabilizzazione dell'operazione; se il pagamento è in stato approvato attraverso una "prenotata" sul conto (il cliente la riconosce perché in *transaction list* dell'app compare la dicitura PREAUTORIZZATA) l'operatore del *team Customer Interaction* spiega al cliente la necessità di attendere la contabilizzazione del movimento prima di attivare la pratica di disputa (a fronte del processo di *card clearing* l'operazione potrebbe essere annullata).

CONTROLLO	**TIPO CONTROLLO**	**FREQUENZA CONTROLLO**	**APPLICATIVO**
Verifica che l'operazione sia stata effettuata tramite POS fisico con inserimento PIN	Manuale	Ad evento	SIA Cristal Gate (GUI)

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
L'operatore verifica la modalità di disposizione dell'operazione qualora sia stata autorizzata attraverso l'inserimento del PIN, la richiesta di disconoscimento viene rifiutata in quanto si identifica un utilizzo improprio o negligente del dispositivo di pagamento e dei codici autorizzativi			
Verifica presenza notizie o recensioni sul *merchant* o sulla piattaforma di *e-commerce* utilizzata per il pagamento	Manuale	Ad Evento	Internet
Verifica *merchant* coinvolto nell'operazione In caso di operazione con carta disposta tramite sito di e-commerce, l'operatore richiede (tramite l'invio di una e-mail) di verificare verifica il *merchant* sia classificato come "*good merchant*" e che la piattaforma utilizzata per la finalizzazione degli acquisti richieda l'inserimento del *3DSecureCode*; in caso positivo, la richiesta di disconoscimento viene rifiutata in quanto si riconosce un utilizzo improprio o negligente del dispositivo di pagamento e dei codici autorizzativi.	Manuale	Ad Evento	DCMS

Gestione del modulo "Claim form"

A seguito della ricezione del modulo "*Claim form*" e degli eventuali allegati (es.: scontrini, fatture, denuncia all'autorità competente), l'operatore del *team Customer Interaction* verifica che sia stato compilato in tutte le sezioni richieste e che i dati inseriti e gli allegati presenti siano coerenti con le informazioni comunicate in precedenza. Qualora i dati nel "*Claim form*" siano mancanti o non corretti, l'operatore contatta il cliente per richiedere l'integrazione o la revisione del documento; in questo caso, qualora riscontri incoerenze rispetto alle comunicazioni precedentemente intercorse (tramite *e-mail* o *chat*) o assenza dei dettagli necessari a procedere con la disputa, l'operatore ricorda al cliente le responsabilità e le conseguenze derivanti da dichiarazioni mendaci.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica completezza e coerenza dei dati presenti nel "*Claim form*" con i dati relativi l'operazione di pagamento oggetto di disconoscimento e con le dichiarazioni rilasciate in precedenza tramite *e-mail* o in *chat*	Manuale	Ad evento	SIA Cristal Gate (GUI); caselle e-mail; Sprinklr

Inoltro pratica a SIA

Una volta ricevuto e verificato il modulo, l'operatore del *team Customer Interactions* raccoglie tutti i dati ed i documenti necessari a SIA per la gestione della pratica di disputa; a tal proposito, l'operatore invia a SIA i seguenti documenti:

- "*Claim Form*" compilato e sottoscritto dal cliente;
- eventuale documentazione allegata fornita dal cliente (es.: scontrini, ricevute);
- *File excel* "indice", contenente tutte le informazioni relative alla transazione;
- eventuale copia della denuncia presentata dal cliente all'autorità competente. A tal proposito, si precisa che la denuncia non è obbligatoria e necessaria ai fini del rimborso dell'importo dell'operazione;
- se necessario, le evidenze del movimento registrato sul sistema di *Core Banking*.

Tutta la documentazione viene raccolta in una cartella denominata "Caricamento GGMMAAA Flowe" e storicizzata su Fanbase, sotto la posizione del cliente.

L'operatore, inoltre, inserisce i dati della pratica nel file gestionale "Censimento dispute" presente nello *sharepoint* dedicato alle attività operative della *Perspective Happiness and Services*.

Valutazione SIA

L'outsourcer SIA, una volta ricevuta la pratica inerente l'operazione disconosciuta, avvia le verifiche di dettaglio volte ad accertare la frode subita dal cliente.

Qualora l'esito delle verifiche di SIA evidenzi l'assenza di presupposti per procedere con l'accoglimento della richiesta di rimborso (es.: l'operazione è stata autorizzata con il *3DSecureCode*), SIA chiude la pratica e l'operatore del *team Customer Interaction* si occupa dell'invio della comunicazione di diniego al cliente (cfr. paragr. 5.2.3).

Al contrario, se l'evento oggetto di disputa viene riconosciuto come frode subita dal cliente, l'*outsourcer* SIA procede con il *chargeback* dell'importo dell'operazione attraverso il c.d. "Rimborso salvo Buon fine" a favore del cliente. Il rimborso avviene attraverso il successivo ciclo di clearing delle transazioni carte, con conterrà in questo caso il riaccredito della transazione disconosciuta.

Valutazione circuito

Nel caso di valutazione positiva da parte di SIA è prevista, inoltre, un'ulteriore valutazione dell'evento da parte del circuito Mastercard volta a confermare le analisi svolte ed accertare l'evento fraudolento.

Qualora l'esito della valutazione di Mastercard sia positiva, cioè viene confermato la frode subita dal cliente, SIA conferma all'operatore del *team Customer Interaction* la chiusura della pratica di disputa; quest'ultimo comunica al cliente l'esito positivo della segnalazione.

Al contrario, qualora Mastercard evidenzi la presenza di elementi che non caratterizzano l'evento fraudolento e quindi l'impossibilità di accettare la richiesta di rimborso del cliente, SIA procede con le attività di recupero dell'importo accreditato (inviando un clearing di riaddebito della transazione) e alla notifica all'operatore del *team Customer Interaction* che si occupa della comunicazione verso il cliente.

Si specifica infine che SIA procede con il recupero dell'importo dell'operazione anche nel caso in cui, entro la data di scadenza della pratica, lo stesso *merchant*, su segnalazione del circuito, provveda a rimborsare l'importo dell'operazione al cliente; anche in questo caso la comunicazione al cliente viene gestita dal *team Customer Interaction* che, sulla base delle informazioni ricevute da SIA, fornisce al cliente tutte le spiegazioni relative alle verifiche effettuate.

5.2.3. Comunicazione al cliente

Comunicazione Salvo Buon Fine

In caso di riconoscimento, da parte di SIA o del circuito Mastercard, dell'operazione oggetto di disputa 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 entro la data di scadenza della pratica, le valutazioni saranno confermate, l'importato riconosciuto sarà considerato definitivo. In caso contrario, Flowe, per il tramite dell'*outsourcer* SIA 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 (dal *team Customer Interaction*, da SIA, dal circuito), 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 verifica preliminare, 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 da SIA o dal circuito a seguito dell'inoltro della documentazione completa, la comunicazione viene inviata alla casella e-mail del cliente da cui è stato ricevuto il modulo "*Claim Form*".

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.

5.2.4. *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 dispute" indicando l'esito della disputa ("Stato pratica", "Tipologia Pratica" e "Cronologia Eventi") 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 carte di debito";*

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;*
- *Decreto Legislativo 27 gennaio 2010, n. 11 e succ. modifiche;*
- *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);*

- *Guidelines EBA/2019/04 (Orientamenti sulla gestione dei rischi ICT e di sicurezza).*