PROCEDURA OPERATIVA

Procedura operativa di Monitoraggio e Gestione conto ai fini antifrode agita dai clienti

Procedura emessa il 13 Ottobre 2023

Owner della procedura: Perspective *Banking Services & Controls*

SOMMARIO

1 OBIETTIVO DEL DOCUMENTO

Obiettivo del presente documento è illustrare i processi di monitoraggio e gestione degli eventi fraudolenti agiti dai clienti Flowe nei confronti della stessa Società e di soggetti terzi.

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, i due processi in esame sono classificati 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

3.13.01 MONITORAGGIO E GESTIONE FRODI AGITE DAI CLIENTI VERSO LA SOCIETA'

3.13.02 MONITORAGGIO E GESTIONE FRODI AGITE DAI CLIENTI VERSO TERZI

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 Banking Services & Controls*.

2 DEFINIZIONI

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

- ***Perspective:*** Unità organizzativa di Flowe.
- ***CERTFin:*** Ente idstituito internamente a ad ABI per la prevenzione alle frodi e che funge anche da centrale dell'interscambio di informazioni continuativo tra istituti.
- **SCT (*Sepa Credit Transfer*)**: bonifico nazionale e transfrontaliero all'interno dei paesi dell'area SEPA.
- ***Instant SCT:*** bonifico istantaneo nazionale e transfrontaliero all'interno dell' area SEPA. A differenza degli SCT che vengono trasferiti tramite i canali SEPA, i bonifici Instant sono trasferiti tramite chiamate API dirette tra gli istituti controparte.
- ***Richiamo SEPA (CAMT.056):*** richiamo interbancario effettuato dall'ordinante di un bonifico tramite il canale SEPA per diverse ragioni, tra cui il fatto che quel bonifico è di tipo fraudolento o sospetto tale.
- ***Richiamo SWIFT:*** messaggio interbancario trasmesso tramite il canale SWIFT. A differenza del richiamo SEPA, il messaggio SWIFT è un messaggio testuale composto e inviato dall'ordinante.
- **Live monitoring - LM:** strumento di alerting a supporto delle funzioni ordinarie dell'ufficio Account Monitoring and Fraud Management.
- **Transaction Alert manager:** sezione dell'applicativo FCM dedicata agli *alert* generati dall'intercetto di una transazione da parte di una delle regole di screening impostate per gli SCT.
- **Sanction lists:** liste interne all'applicativo FCM contenenti nominativi di soggetti appartenenti a categorie a rischio (i.e. terrorismo, appalti, indesiderati ecc) utilizzate anche per lo screening degli SCT.
- **Input - profilo B0**: profilo base dell'operatore FCM. Attualmente assegnato al *Team Operations Flowe* di Banca Mediolanum.
- **Chief Service Senior - profilo L1:** profilo da supervisore assegnato al *Team AML* della *Perspective Happiness & Services*.
- **Head of Chief Service:** profilo del Responsabile della *Perspective Happiness & Services*.
- **Soggetto collegato:** cliente Flowe collegato per operatività al cliente Flowe principale oggetto di analisi.
- **Activity - Customer Security:** strumento di FanBase che permette di reportizzare l'alert generato sulla posizione del cliente, annotare tutto lo storico della pratica ed effetturare tutte le azioni necessarie (i.e. blocco accesso in app, blocco conto di pagamento, cancellazione device ecc)
- **Activity - Verification:** strumento di FanBase che permette a tutti i *team della perspective Happiness & Service*, di notificare un'anomalia su un cliente e di indirizzare la pratica al team competente.
- **Operazione sospetta**: operazione finanziaria che per connotazioni oggettive (caratteristiche, entità, natura) e in relazione alla posizione soggettiva del cliente (capacità economica e attività svolta) induce a sospettare una provenienza illecita delle somme utilizzate.

- **SOS - Segnalazione Operazione Sospetta**: segnalazione obbligatoria *all'Unità di Informazione Finanziaria* per qualsiasi attività – compiuta o tentata dal cliente – apparentemente finalizzata al compimento di operazioni fraudolente, di riciclaggio o di finanziamento del terrorismo.
- **Adeguata verifica rafforzata (di seguito anche AVR):** le misure rafforzate di adeguata verifica (ai sensi del D.Lgs. 231/2007) si applicano quando sussiste un elevato rischio di riciclaggio e di finanziamento del terrorismo, per effetto di specifiche previsioni normative o di una autonoma valutazione dell'intermediario. Le misure rafforzate di adeguata verifica della clientela vengono attuate: approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto; acquisendo informazioni aggiuntive sul cliente; intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale.
- **Riscontro Adeguato:** ricezione di tutta la documentazione richiesta a giustificare i sospetti sia sulla movimentazione che sugli altri elementi, purché idonea (non falsificata e completa di tutti gli elementi necessari)
- **Riscontro Parziale:** ricezione di parte della documentazione richiesta a giustificare i sospetti sia sulla movimentazione che sugli altri elementi, purché idonea (non falsificata). Si intende riscontro parziale anche il caso in cui riceviamo una giustificazione della movimentazione che per natura non richiede la presenza di un documento (es. prestito tra familiari)
- **Riscontro Non Adeguato:** ricezione di tutta o di parte della documentazione richiesta a giustificare i sospetti, ma con elementi oggettivi di manomissione/falsificazione degli stessi, o con elementi necessari mancanti (es. partita iva su una fattura). Si intende non adeguato anche un riscontro senza documentazione allegata, seppur la natura della transazione lo richieda (es. vendita)
- **Mancato riscontro:** mancata risposta alla richiesta inviata.

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. PLATFORM – POWER PLATFORM – P0 (PZERO)

P0 è la Piattaforma della Società (*full cloud* – Microsoft Azure) sulla quale è implementata la logica applicativa. Mediante la piattaforma è possibile integrare sistemi esterni.

3.2. FANBASE – POWER PLATFORM

Piattaforma applicativa sviluppata internamente alla Società basata su tecnologia *cloud* Microsoft Power Platform. Tale soluzione mette a disposizione degli operatori di *front e back office* funzionalità volte al supporto diretto e indiretto del cliente finale (*Customer Relationship Management*).

Fan Base è la *Power App* che supporta la *Perspective Banking Services & Controls – Team Account Monitoring & Fraud Management* - nello svolgimento delle attività di analisi della posizione oggetto di alert ricevuto dal team. A partire dall'ultimo trimestre 2021, tramite la

Power App, il *Team Account Monitoring & Fraud Management* ha a disposizione una *Activity* specifica che permette oltre alla tenuta della pratica, l'invio di e-mail di richieste documentali e tutte le comunicazioni necessarie alla gestione del rapporto con il cliente, nonché la tracciatura di tutte le attività effettuate sulla posizione del cliente consentendo un aggiornamento costante a tutta la *Perspective Banking Services & Controls*. Infine, tramite Fan Base è possibile appore blocchi all'utilizzo dell'App da parte del cliente, del blocco conto (*Posting Restrictions*) tramite API diretta verso Temenos e del blocco carta tramite API diretto verso il gestionale carte di SIA-NEXI, nei casi di seguito descritti in questa procedura.

3.3. PIATTAFORMA FCM – TEMENOS

Il modulo *Financial Crime Mitigation* (FCM) dell'*outsourcer* Temenos, permette lo svolgimento di una serie di controlli sul transato che hanno l'obiettivo di controllo preventivo e di mitigazione del rischio di frode, che sia subita o che sia agita dai clienti Flowe.

Nello specifico, il modulo è totalmente integrato con il core banking T24, dal quale recepisce una serie di messaggi, che permettono l'attivazione delle logiche sottostanti le regole implementate su FCM ai fini dei controlli di tipo antifrode. Tali regole sul transato implementate nel modulo hanno l'obiettivo di filtrare, o se previsto bloccare, l'esecuzione di bonifici in accredito e/o addebito. Dal secondo semestre del 2022, in virtù dello sviluppo della funzionalità dei bonifici instant, è stato rilasciato in produzione un nuovo modulo (SAP Module) che ha l'obiettivo di presidiare gli eventi in tempo reale. Il set di regole implementate sul SAP Module hanno lo scopo di negare transazioni istantanee, non revocabili e difficilmente richiamabili, nel caso vi siano dei rischi di frode subita o agita da parte dei clienti Flowe.

3.4. 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 Banking Services & Controls*:

- in caso di ricezione di una segnalazione di frode agita da un cliente Flowe o di identificazione di operatività anomala (sospetta frode agita), la raccolta delle informazioni di dettaglio relative le operazioni di pagamento (es.: SCT, SDD);
- la gestione del blocco del conto di pagamento (apposizione e rimozione)
- la gestione della messaggistica di richiamo interbancario
- la gestione di messaggistica di pagamento.

3.5. GESTIONALE CARTE –CRYSTAL GATE (GUI)

Flowe si avvale della piattaforma di *card management* CRYSTAL GATE (di seguito indicato come Gestionale carte) fornita dall'outsourcer NEXI per la consultazione di tutte le informazioni inerenti le operazioni effettuate tramite le carte di pagamento e per la gestione dei relativi blocchi (apposizione e rimozione).

3.6. LIVE MONITORING DASHBOARD – POWER BI

Flowe si avvale della *dashboard Live Monitoring* costruita tramite Microsoft PowerBI, alfine di identificare operazioni anomale relative all'utilizzo del conto di pagamento.

Le *dashboard* di PowerBI sono la rappresentazione puntuale e dettagliata di alcune categorie di dati, provenienti direttamente dal *database* di Flowe.

La *dashboard Live Monitoring* prevede due tipologie di analisi su un arco temporale di 72h dal momento dell'apertura del *report*. *Live Monitoring* evidenzia la movimentazione cumulativa di ogni conto di pagamento nell'arco temporale selezionato e segnala i conti che nel suddetto arco temporale presentano movimentazione in uscita maggiore o uguale al 90% delle entrate. Sempre all'interno dello stesso applicativo, tramite degli specifici filtri è possibile evidenziare i conti che riportano degli accrediti o addebiti sopra soglie definite dal *Team Account Monitoring & Fraud Management,* in accordo con il *Chief Banking Services & Controls* .

3.7. TRANSACTION DASHBOARD - POWER BI

Flowe si avvale della *dashboard Transcation* costruita tramite Microsoft PowerBI per analizzare tutte le transazioni in formati differenti e interattivi. Tale strumento supporta le analisi delle operazioni potenzialmente fraudolente agite dalla clientela Flowe.

3.8. CLEAFY

Flowe si avvale dell'applicativo *Cleafy Web Console* fornita da Cleafy come supporto alla prevenzione e rilevamento realtime di attività sospetta sull'utilizzo dell'app Flowe e sulle operazioni di bonifico.

Cleafy espone tutte le sessioni app e le analizza riportando ogni evento registrato tramite etichette (TAG). Ogni evento e quindi ogni TAG può essere utilizzato come elemento di innesco degli alert previsti dal impianto regole in vigore e redatto dal Responsabile del *Team Account Monitoring & Fraud Management*, in accordo con il *Chief Banking Services & Controls*.

4 ATTORI, RUOLI E RESPONSABILITÀ

Di seguito sono indicati i principali attori, coinvolti nel processo di monitoraggio e gestione dei conti ai fini antifrode.

4.1. PERSPECTIVE *BANKING SERVICES & CONTROLS*

La *Perspective Banking Services & Controls*, nell'ambito del processo di monitoraggio e gestione delle frodi agite dai clienti verso soggetti terzi, è responsabile per il tramite del *team Account Monitoring and Fraud Management* di:

- ricevere e verificare le segnalazioni relative a frodi agite da clienti Flowe e ricevute tramite reclamo o comunicazione di altro Istituto;
- effettuare gli approfondimenti sulle operazioni "potenzialmente sospette" (potenziali frodi relative ad utilizzo del conto) rilevate dagli strumenti di monitoraggio dei conti;

- avviare l'*iter* di richiesta documentazione a supporto delle analisi per la valutazione della pratica ai fini antifrode;
- raccogliere i dati e le informazioni da inoltrare per l'avvio del processo di valutazione di Segnalazione Operazione Sospetta;
- disporre la chiusura del rapporto tramite l'approvazione da parte del *Chief Banking Services & Controls o dell'Head of Controls & Regulatory Reporting*.

La *Perspective Banking Services & Controls*, nell'ambito del processo di monitoraggio e gestione delle frodi agite dai clienti verso la Società è responsabile, per il tramite del *team Account Monitoring and Fraud Management*, di presidiare il corretto funzionamento di tutti gli strumenti a propria disposizione per la generazione di alert, il relativo sviluppo e il costante aggiornamento degli impianti regole ad essi relativi in linea con il variare delle esigenze.

4.2. OUTSOURCER

4.2.1 Banca Mediolanum- Team Operations Flowe

Nell'ambito del presente processo il *Team Operations Flowe* del *Settore Product Operations* di Banca Mediolanum, nell'ottica di fornire supporto al *team Account Monitoring and Fraud Management* della *Perspective Banking Services & Controls*, si occupa di:

- effettuare un primo controllo degli alert generati dalle regole sul transato SCT generate in FCM procedendo con la valutazione dell'alert al livello approvativo *Input – B0*. Laddove necessario, richiedere i dovuti approfondimenti al *team Account Monitoring and Fraud Management* della *Perspective Banking Services & Controls*, che valuta se avviare il processo di verifica sulla posizione del cliente associato alla transazione oggetto di alert.
- effettuare una prima analisi a supporto del *team Account Monitoring and Fraud Management* della *Perspective Banking Services & Controls* in merito alle segnalazioni periodiche prodotte dal Contact Center di SIA, relative alle carte di pagamento poste in uno stato di blocco per Operatività Elevata. Laddove necessario, richiedere i dovuti approfondimenti al *team Account Monitoring and Fraud Management* della *Perspective Banking Services & Controls*, che valuta se avviare il processo di verifica sulla posizione del cliente titolare della carta di pagamento posta in stato di blocco.

Supportare nella gestione dei richiami interbancari il *team Account Monitoring and Fraud Management*. Nello specifico il team Operations Flowe, gestisce la fase di ricezione e registrazione dei messaggi CAMT.056 inviati verso Flowe, ingaggiando il Team Account Monitoring and Fraud Management per la gestione degli stessi. Successivamente a fronte dell'esito stabilito dal Team Account Monitoring and Fraud Management, il team Operations Flowe procede a inviare la riposta di rifiuto o accettazione del richiamo CAMT.056. Nel caso di necessità di invio di un richiamo interbancario disposto da Flowe verso altro istituto, il team Operations Flowe, su ingaggio del team Account Monitoring and Fraud Management, procede all'invio e alla registrazione dell'eventuale risposta ricevuta.

4.2.2 Temenos

Flowe si avvale dell'*outosourcer* Temenos - applicativo di *Core Banking* T24 – per gestire i processi "*core*" della Società per la gestione delle operazioni di pagamento e la relativa messaggistica interbancaria. L'outsourcer fornisce anche il modulo *Financial Crime Mitigation* (FCM) per lo svolgimento di una serie di attività e controlli ai fini AML e di antifrode supportando la Società dalla fase di acquisizione del cliente e per tutta la durata del rapporto.

4.2.3 NEXI - SIA

Flowe si avvale dell'*outosourcer* NEXI per la consultazione delle informazioni della carta associata al cliente – tipologia di carta (fisica o virtuale), dettagli dell'intestatario della carta (luogo di spedizione, dati anagrafici e residenza). La piattaforma Crystal Gate (GUI) permette inoltre, di impostare eventuali blocchi temporanei nonché di avere evidenza di tutti i dettagli delle operazioni della carta (di debito e prepagata).

4.2.4 Intesa SanPaolo

Flowe si avvale dell'*outsourcer* Intesa SanPaolo per la gestione della messaggistica interbancaria .Tramite l'ufficio *Agency Service* di Intesa SanPaolo il team *Account Monitoring and Fraud Management* della *Perspective Banking Services & Controls* riceve e invia le comunicazioni tramite il canale SWIFT a supporto dei processi di seguito riportati.

5 PROCESSO DI MONITORAGGIO E GESTIONE DELLE FRODI AGITE DAI CLIENTI VERSO LA SOCIETA'

Il processo di monitoraggio e gestione degli eventi fraudolenti agiti dai clienti nei confronti della stessa Società si compone, alla data di stesura del presente documento, del seguente sottoprocesso:

- Frodi perpetrate dai clienti in fase di *onboarding*

5.1. FRODI PERPETRATE DAI CLIENTI IN FASE DI ONBOARDING

Al fine di prevenire il tentativo di molteplici *onboarding* da parte di un medesimo soggetto attraverso l'utilizzo di documenti identificativi contraffatti (per esempio, ai fini di attività finanziaria illecita, che sia di frode o che sia di riciclaggio), Flowe ha adottato strumenti e modalità operative attraverso le quali verifica, durante il processo di *onboarding* del cliente l'univocità del soggetto oltre che la validità e la veridicità del documento di riconoscimento utilizzato per l'apertura del conto a distanza. Per la descrizione del processo di verifica in fase di onboarding si rimanda alla *sezione 5.1.4. Identificazione del cliente*, della procedura operativa *Onboarding cliente ed apertura conto di pagamento*.

Anche il team *Account Monitoring and Fraud Management*, come in seguito descritto, si occupa dell'analisi delle modalità di *onboarding* dei clienti, tramite la presa visione di eventuali *alert* lavorati dal team AML, e la verifica del set documentale presentato dal cliente per l'attivazione del conto.

6 PROCESSO DI MONITORAGGIO E GESTIONE DELLE SOSPETTE FRODI AGITE DAI CLIENTI VERSO TERZI

Il processo di monitoraggio e gestione degli eventi fraudolenti agiti dalla clientela nei confronti di soggetti terzi, viene di seguito mappata nelle seguenti modalità:

- la descrizione del controllo effettuato;
- 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.

6.1. IDENTIFICAZIONE OPERAZIONE "ANOMALA" (SOSPETTA FRODE)

Flowe, in qualità di IMEL autorizzato da Banca d'Italia, nell'ambito del monitoraggio continuo dei propri clienti, si è dotata di una procedura operativa finalizzata a gestire e intervenire nei confronti della clientela che utilizza il conto di pagamento per agire in maniera fraudolenta nei confronti di terzi.

Dalla gestione di tali eventi è possibile per Flowe trarre informazioni utili all'individuazione di nuovi fenomeni fraudolenti per definire e attuare le misure di prevenzione necessarie al fine del miglioramento continuo del livello di sicurezza fornito ai propri clienti.

6.1.1 Monitoraggio Interno

Gli eventi di possibile frode agita da un cliente Flowe possono essere identificati direttamente da Flowe, attraverso le attività di monitoraggio del *team Account Monitoring and Fraud Management* della *Perspective Banking Services & Controls*.Il *team Account Monitoring and Fraud Management*, nell'ambito delle attività di monitoraggio dei conti di pagamento ai fini di attività antifrode, fissa delle regole sulle singole transazioni e della movimentazione giornaliera dei singoli conti.

Attraverso l'utilizzo della *dashboard Live Monitoring* di PowerBI, più volte al giorno vengono individuati i rapporti caratterizzati da una movimentazione di importo rilevante ai fini delle soglie impostate dal *team Account Monitoring and Fraud Management*. Tali rapporti sono oggetto di analisi ed approfondimento.

La dashboard *Live Monitoring* permette di identificare i conti di pagamento con un transato totale (entrate e uscite) di importo rilevante ai fini dell'analisi antifrode e i conti che riportano una movimentazione in uscita maggiore o uguale al 90% delle entrate. L'arco temporale oggetto di analisi varia a seconda della temporalità delle estrazioni e non supera mai i 5 giorni di calendario. L'operatore *Account Monitoring and Fraud Management* seleziona l'arco temporale interessato ed effettua un controllo puntuale di ogni posizione scaricando prima la lista dei conti che presentano la fattispecie sopra-riportata e successivamente tramite l'isolamento di ogni conto effettua un'analisi dettagliata prevista dalla sezione 6.2 della presente procedura. In caso di False Hit, l'operatore chiude l'analisi indicando il motivo della valutazione positiva del caso all'interno del file dedicato alle estrazioni Live Monitoring. In caso di True Hit, l'operatore indica il motivo della valutazione negativa all'interno del file dedicato e contestualmente apre una activity di Customer

Security in FanBase. Al suo interno riassume l'esito delle analisi effettuate e avvia tutte le azioni previste nella sezione 6.2.4 "Esito negativo delle indagini" di questa procedura.

Il *team Account Monitoring and Fraud Management* si avvale di FCM per l'identificazione sia dei bonifici ordinari (Standard SCT) che dei bonifici istantanei , e in accredito e in addebito, di importo maggiore o uguale a 250€.

- Bonifici in accredito riportanti nome beneficiario diverso dal titolare del conto di destinazione
- Bonifici in accredito e addebito con IBAN e BIC controparti inserite in *blacklist*
- Bonifici in accredito e addebito con controparti inserite in *sanction lists*.

Questo processo è effettuato da parte di operatori con due livelli autorizzativi differenti: l'operatore del team *Operations Flowe* verifica l'alert generato dal sistema di *Screening* di FCM e valuta al livello input, la transazione su cui è scattato alert secondo le regole precedentemente descritte. Se il bonifico è stato intercettato correttamente l'operatore del team *Operations Flowe*, valuta l'alert come True Hit, specificando nella sezione dedicata la motivazione. Valuta invece come False Hit nei casi in cui il bonifico è stato intercettato correttamente da un punto di vista formale dal motore di screening, ma nella sostanza i bonifici non sono passibili di rifiuto/cancellazione (ad esempio non esaustivo, refuso nel nome beneficiario). L'operatore del team *Account Monitoring and Fraud Management* dopo le analisi previste di seguito, a fronte dell'esito di queste ultime, decide se confermare o convertire la valutazione inserita in input. Se l'operatore del team *Account Monitoring and Fraud Management (chief)*, valuta l'alert come False Hit il bonifico è correttamente processato; se valuta l'alert come True Hit il bonifico è rifiutato, se in accredito, o cancellato, se in addebito. In quest'ultimo caso, l'operatore del team *Account Monitoring and Fraud Management* apre una *activity* di *Customer Security* in *FanBase*. Al suo interno riassume l'esito delle analisi effettuate e avvia tutte le azioni previste nella sezione 6.2.4 "Esito negativo delle indagini" di questa procedura.

Il team Account Monitoring e Fraud Management si avvale dal mese di ottobre 2022, dello strumento FCM SAP Module. Tale funzionalità dell'applicativo FCM è stato sviluppata per poter far fronte alle nuove necessità in tema di prevenzione, mitigazione e rilevamento dei possibili eventi fraudolenti, perpetrati dai clienti Flowe tramite l'utilizzo di addebiti istantanei (SCT Instant). FCM SAP Module permette di intercettare e non completare le disposizioni di bonifico istantaneo che eccedono il limite di 15.000€. Oltre a questa regola, è stato stabilito che se le operazioni di accredito delle ultime 48 ore superano l'importo cumulato di 1.500€, qualunque operazione di bonifico istantaneo che per importo fa eccedere il 95% di questa somma, debba essere rifiutata. Qualsiasi evento generato dall'applicativo FCM SAP Module crea subito in automatico una Customer Security su Fanbase assegnata al team, che viene lavorata dall'operatore secondo quanto descritto nella sezione 6.2 "Indagini sull'operazione anomala (sospetta frode)" di questa procedura. Non è prevista alcuna operazione manuale da parte dell'operatore del team Account Monitoring and Fraud Management, se non nel caso in cui l'evento viene valutato come False Hit e viene valutata la possibilità di concedere al cliente la Whitelist, ovvero la possibilità di replicare la medesima operazione, con medesimi IBAN controparte e importo rispetto a quella intercettata dall'applicativo in precedenza. Tale possibilità è concessa al cliente in un periodo di tempo che va dal momento dell'attività svolta dall'operatore fino alla prima mezzanotte successiva.

Il team Account Monitoring and Fraud Management sempre dal mese di ottobre 2022, si avvale anche dell'applicativo Cleafy, a completamento del proprio pacchetto applicativo definibile anche come "Motore Antifrode". Cleafy permette di visualizzare le sessioni di utilizzo dell'app Flowe da parte di ogni cliente e in particolare evidenzia le operazioni di

bonifico standard e bonifico istantaneo effettuate dai clienti, tramite l'utilizzo della specifica funzionalità all'interno della propria app Flowe. Ad ogni evento rilevato dall'applicativo Cleafy, è associata un'etichetta (TAG). L'impianto regole non è altro che la combinazione di può eventi, individuati tramite gli specifici TAG che se presenti all'interno di una sessione app, generano un evento di sospetto che può suddividersi in Alert Rosso o Alert Giallo a seconda della sua gravità. Se una sessione o l'evento riporta un Alert Giallo l'operazione di bonifico ordinario o istantaneo associata, viene completata ma viene generato un alert all'interno della sezione dedicata di FCM. Se invece vi è un Aler Rosso, l'operazione di bonifico ordinario o istantaneo associata, viene bloccata e viene generato un alert all'interno della sezione dedicata di FCM. In entrambi i casi, l'operatore del team Account Monitoring e Fraud Management procede ad aprire una Activity di tipo Customer Security su FanBase e a procedere secondo quanto definito nella sezione 6.2 "Indagini sull'operazione anomala (sospetta frode)" della presente procedura.

6.1.2. Segnalazioni interne da altre strutture

Il team *Account Monitoring and Fraud Management* può essere ingaggiato anche da segnalazioni provenienti da altre strutture, come ad esempio il team *Customer Interaction* o il team *Operations*. Il team viene ingaggiato tramite *FanBase*, con l'apertura di una *activity Customer Security* assegnato al team stesso. L'operatore che prende in carico il caso attua tutte le procedure previste anche per tutti gli altri tipi di segnalazione.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica presenza conti che riportano un transato, sul *periodo* temporale in analisi (impostabile sulla dashboard in funzione dell'esigenza), superiore ai 3.000€, per SCT IN e SCT OUT)	Manuale	Tre volte al giorno	Dashboard Live Monitoring PowerBI
Verifica presenza conti che riportano un transato, sul periodo temporale in analisi (impostabile sulla dashboard in funzione dell'esigenza), superiore ai 2.000€, per Incoming Instant Transfer.	Manuale	Tre volte al giorno	Dashboard Live Monitoring PowerBI
Verifica operatività anomala sul conto di	Manuale	Tre volte al giorno	Dashboard Live Monitoring

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
pagamento. Verifica presenza conti che riportano totale di uscite maggiore o uguale al 90% delle entrate, sul *periodo* temporale in analisi (impostabile sulla dashboard in funzione dell'esigenza), per SCT IN e tutte le categorie di transazioni in uscita (SCT OUT, *MoneyTransfer* OUT, *Card Authorization*) per un totale entrate di minimo 400€.			PowerBI
Verifica presenza conti che riportano totale di uscite maggiore o uguale al 90% delle entrate, sul *periodo* temporale in analisi (impostabile sulla dashboard in funzione dell'esigenza), per ricarica conto tramite VPos TopUp e tutte le categorie di transazioni in uscita (SCT OUT, *MoneyTransfer* OUT, *Card Authorization*) per un totale entrate di minimo 900€. SIA PAY per conto di Flowe blocca le ricariche Vpos che nell'arco temporale delle 24h superano l'importo cumulativo di 1.500€ e/o delle 3 ricariche completate. Tale presidio non è gestito da Flowe ed il team Account Monitoring & Fraud Management non riceve alcuna notifica a riguardo.	Manuale	Tre volte al giorno	Dashboard Live Monitoring PowerBI

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica presenza conti che riportano totale di uscite maggiore o uguale al 90% delle entrate, sul *periodo* temporale in analisi (impostabile sulla dashboard in funzione dell'esigenza), per Instante Incoming Transfer e tutte le categorie di transazioni in uscita (SCT OUT, *MoneyTransfer* OUT, *Card Authorization*) per un totale entrate di minimo 400€.	Manuale	Tre volte al giorno	Dashboard Live Monitoring PowerBI
Controllo corrispondenza tra beneficiario e titolare del conto beneficiario. SCT IN di importo maggiore uguale a 250€. L'operatore del *team Operation Flowe compie una prevalutazione dell'*alert *generato da FCM* in caso di non corrispondenza tra il nominativo del beneficiario del bonifico in entrata e quello del titolare del conto. *L'operatore Account Monitoring and Fraud Management* valuta tali alert effettuando tutte le analisi previste sulla posizione del cliente per poter decidere se accreditare correttamente la transazione o rifiutarla. FCM valuta automaticamente tutti i bonifici che riportano corrispondenza tra	Manuale/Automatico	Giornaliero	FCM, Transaction Dashboard PowerBI, T24

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
titolare del conto, beneficiario della transazione.			
Controllo bonifici in accredito e addebito con IBAN e BIC controparti inserite in blacklist di importo maggiore uguale a 250€. L'operatore del *team Operation Flowe compie una prevalutazione dell'alert generato da FCM. L'operatore Account Monitoring and Fraud Management* valuta tali alert effettuando tutte le analisi previste sulla posizione del cliente per poter decidere se accreditare/addebitare correttamente la transazione o rifiutarla/cancellarla	Manuale/Automatico	Giornaliero	FCM, Transaction Dashboard PowerBI, T24
Controllo bonifici in accredito e addebito con controparti inserite in sanction lists di importo maggiore uguale a 250€. L'operatore del *team Operation Flowe compie una prevalutazione dell'alert generato da FCM. L'operatore Account Monitoring and Fraud Management* valuta tali alert effettuando tutte le analisi previste sulla posizione del cliente per poter decidere se accreditare/addebitare correttamente la	Manuale/Automatico	Giornaliero	FCM, Transaction Dashboard PowerBI, T24

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
transazione o rifiutarla/cancellarla			
Controllo e blocco bonifici istantanei in addebito di importo superiore ai 15.000€ Viene generata in automatico una activity di tipo Customer Security in FanBase	Automatico	Nel Continuum	FCM, Fanbase
Controllo e blocco bonifici istantanei in addebito che per importo eccedono il 95% degli importi accreditati sullo specifico conto nelle ultime 48 ore (minimo 1.500€) Viene generata in automatico una activity di tipo Customer Security in Fanbase per ogni operazione bloccata	Automatico	Nel Continuum	FCM, Fanbase
Controllo e blocco per Alert Rosso di bonifici istantanei effettuati verso istituti considerati ad alto rischio, oltre a determinati importi. Una volta generato l'alert, viene storicizzato nella specifica sezione di FCM Istituti ad alto rischio e relativi limiti di importo per ognuno di essi sono stabiliti a fronte di analisi statistica condotta dal team Account Monitoring and Fraud Management	Automatico	Nel Continuum	Cleafy, FCM

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Controllo e blocco per Alert Rosso di bonifici istantanei effettuati verso specifici IBAN inseriti nella lista Blacklist all'interno dell'applicativo Cleafy. Una volta generato l'alert, viene storicizzato nella specifica sezione di FCM	Automatico	Nel Continuum	Cleafy, FCM
Controllo e generazione di Alert Giallo in caso di bonifici ordinari e istantanei, all'interno di una sessione app che presenta eventi anomali o definiti di sospetto dal team Account Monitoring and Fraud Management. Una volta generato l'alert, viene storicizzato nella specifica sezione di FCM	Automatico	Nel Continuum	Cleafy, FCM

6.1.3. Segnalazione da Altri istituti / CERTFin

Flowe in quanto istituto aderente al CERTFin – CERT Finanziario Italiano, riceve ed invia segnalazioni di IBAN sospetti come fraudolenti da e a tutti gli aderenti, nonché la maggioranza degli istituti finanziari italiani. Flowe collabora inoltre attivamente alla prevenzione delle frodi tramite un contatto continuo e denso con tutti gli istituti finanziari in autonomia.

CERTFin invia più volte al giorno a Flowe liste di IBAN italiani e no, segnalati dagli aderenti come sospetti fraudolenti, tramite la casella mail presidio.antifrode@flowe.com. L'operatore Account Monitoring and Fraud Management copia la lista di IBAN contenuta all'interno di ogni comunicazione all'interno del repository dedicata. Se all'interno della lista vi è un conto Flowe, l'operatore attiva immediatamente la verifica prevista per tutti i casi di sospetta frode descritta in questa procedura e se necessario procede all'apposizione del blocco preventivo dell'operatività di tale conto.

Tramite la casella mail dedicata, censita nella rubrica del CERTFin, il team Account Monitoring and Fraud Management può ricevere le segnalazioni che gli altri istituti inviano in autonomia per indicare operazioni di sospetta frode agita dai clienti Flowe. Alla ricezione

di tali comunicazioni, l'operatore del team attiva immediatamente tutte le azioni previste per l'analisi descritte nella sezione 6.2 di questa procedura e se necessario procede all'apposizione del blocco preventivo dell'operatività del conto.

L'operatore del team Account Monitoring and Fraud Management sia in caso di valutazione come False Hit che, come True Hit, apre una activity di Customer Security in FanBase. Al suo interno riassume l'esito delle analisi effettuate e avvia tutte le azioni previste nella sezione 6.2 di questa procedura.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica presenza, nelle caselle di posta elettronica aziendale dedicate ai reclami, di segnalazioni (da parte di clienti o altri soggetti) relativi ad eventi fraudolenti agiti da clienti Flowe	Manuale	Giornaliero	Casella di posta elettronica Office 365; Legal mail
Verifica presenza, nella casella di posta elettronica presidio.antifrode@flowe.com, di segnalazioni da parte di altri istituti relativi ad eventi fraudolenti agiti da clienti Flowe	Manuale	Giornaliero	Casella di posta elettronica Office 365
Verifica presenza, nella sezione di T24, di richieste di richiami di SCT da parte di altri istituti.	Manuale	Giornaliero	T24

6.1.4 Segnalazione per richiamo interbancario

Utilizzando i canali di messaggistica interbancaria SEPA e SWIFT, gli istituti hanno l'onere e la facoltà di richiamare operazioni di Credit Transfer, nel caso in cui queste siano di natura fraudolenta, su richiesta dei propri clienti (parte offesa). Flowe gestisce direttamente i richiami interbancari SEPA (CAMT.056) tramite il core banking T24, mentre la messaggistica SWIFT è gestita indirettamente tramite l'ausilio del servizio Agency Services offerto da Intesa San Paolo.

Come indicato in precedenza per la gestione dei richiami interbancari provenienti dal circuito SEPA (CAMT.056), il team Account Monitoring and Fraud Management si avvale del supporto del Team Operations Flowe di Banca Mediolanum.

Alla ricezione di un richiamo interbancario CAMT.056 tramite il modulo preposto del core banking T24, l'operatore del team Operations Floweapre una activity Customer Security di tipo Richiamo da Parte di Terzi assegnandola al team Account Monitoring and Fraud Management. L'operatore di quest'ultimo, attiva tutte le indagini necessarie e previste dalla sezione 6.2 della presente procedura per poter confermare o meno l'apposizione del blocco preventivo del conto oggetto di richiamo, alla verifica di quale sia la capienza dello stesso e quindi il blocco delle somme relative all'operazione in accredito sospetta. Attenendosi alla normativa EBA, Flowe processa entro 10 giorni lavorativi la risposta al

richiamo interbancario relativo ad un bonifico SCT ordinario, mentre per quanto riguarda i bonifici SCT istantanei la scadenza normativa è di 15 giorni lavorativi.L'operatore del team Account Monitoring and Fraud Management sia in caso di valutazione come False Hit che, come True Hit, sempre tramite la stessa activity di Customer Security in FanBase, ingaggia il team Operations Flowe per procedere all'invio della risposta negativa (CAMT.029) o positiva (PACS.004) tramite il core banking T24.

Relativamente invece ai richiami interbancari pervenuti tramite il canale SWIFT, questi messaggi vengono inviati da Intesa SanPaolo Agency Services attraverso una mail alla casella presidio.antifrode@flowe.com. Una volta ricevuto il messaggio l'operatore del team Account Monitoring and Fraud Management, al fine di intervenire prontamente all'eventuale blocco delle somme oggetto di richiamo, dopo aver registrato l'evento tramite apertura di activity Customer Security, attiva tutte le verifiche previste nella sezione 6.2 di questa procedura. L'esito verrà inviato tramite risposta alla mail di ingaggio e sarà poi onere di Intesa SanPaolo Agency Services, farlo pervenire all'istituto ordinante.

6.1.5 Segnalazione per reclamo da parte di non clienti per sospetta frode

Il team Account Monitoring and Fraud Management viene ingaggiato dal team Claims & Customer Communication Legal Check tramite apertura di activity in Fanbase. L'operatore Account Monitoring and Fraud Management che prende in carico la pratica individua la posizione oggetto del reclamo e dispone tutte le verifiche previste nella sezione 6.2. della presente procedura. A valle delle analisi approfondite e dettagliate sulla posizione individuata, l'operatore redige l'istruttoria di risposta, indicando tutti gli eventi salienti relativi alla transazione di sospetta frode e la situazione del conto individuato.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica presenza, nella casella di posta elettronica presidio.antifrode@flowe.com, di segnalazioni da parte di CERTFin o di altri istituti relativi ad eventi fraudolenti agiti da clienti Flowe.	Manuale	Giornaliero	Casella di posta elettronica Office 365
Verifica presenza, nella sezione di T24, di richieste di richiami di standard SCT e Incoming Instant SCT da parte di altri istituti.	Manuale	Giornaliero	T24, Fanbase
Verifica presenza, nella casella di posta elettronica presidio.antifrode@flowe.com, di comunicazioni provenienti da Agency Services di Intesa SanPaolo relative a messaggistica SWIFT contente segnalazione di operazioni di sospetta frode agita	Manuale	Giornaliero	Casella di posta elettronica Office 365

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
da clienti Flowe, provenienti da altri isituti.			
Verifica presenza, di activities in Fanbase aperte dal team Claims, per operazioni di sospetta frode agite da clienti Flowe.	Manuale	Giornaliero	Casella di posta elettronica Office 365; Legal mail, Fanbase

6.2. INDAGINI SU OPERAZIONE "ANOMALA" (SOSPETTA FRODE)

Per qualsiasi casistica indicata nella sezione 6.1 della presente procedura, l'operatore del team Account Monitoring and Fraud Management che prende in carico il caso effettua una serie di indagini ai fini di poter valutare la posizione e intraprendere tutte le azioni necessarie sul conto oggetto della segnalazione.

6.2.1 Indagine sulla movimentazione del conto

L' operatore del *team Account Monitoring and Fraud Management* tramite l'utilizzo degli applicativi a sua disposizione, analizza l'operazione oggetto di segnalazione in tutte le sue caratteristiche (tipologia, importo, causale, beneficiario). Ai fini di poter definire l'operazione come "anomala" e per quale motivo, l'operatore prende visione di una parte o tutta la movimentazione del conto di pagamento.

6.2.2 Indagine sul set documentale di registrazione

L' operatore del *team Account Monitoring and Fraud Management* oltre al controllo della movimentazione effettua un controllo dettagliato anche sul set documentale utilizzato dal titolare del conto ai fini dell'accensione dello stesso.

In particolare, l'operatore verifica la veridicità del documento d'identificazione utilizzato dal cliente, la congruenza tra l'immagine del video selfie di onboarding e la fototessera presente sul documento identificativo. Inoltre, viene presa visione delle dichiarazioni fatte dal cliente in fase di accensione conto rispetto alla propria situazione patrimoniale, il suo reddito annuo e la sua posizione professionale. Quest'ultima indagine è effettuata ai fini di una corretta identificazione del titolare del conto oggetto di segnalazione e per confermare la congruenza tra la movimentazione del conto e la posizione finanziaria del titolare.

6.2.3 Pre-Analisi con esito positivo delle indagini (False Hit)

A fronte della serie di indagini effettuate dall'operatore del *team Account Monitoring and Fraud Management*, in assenza di elementi probatori o oggettivi sulla movimentazione del conto o del set documentale di registrazione del titolare, la segnalazione viene valutata come False Hit in quanto non vi sono evidenze di evento fraudolento attuato da parte del cliente Flowe. In questi casi, l'evento segnalato viene archiviato secondo le modalità previste per ogni casistica di segnalazione precedentemente riportate, salvo che gli eventi analizzati non risultino essere sospetti di attività di riciclaggio. Per questi ultimi casi, si

veda la sezione 6.2.5. della presente procedura.

6.2.4 Pre-Analisi con esito negativo delle indagini (True Hit)

A fronte della serie di indagini effettuate dall'operatore del *team Account Monitoring and Fraud Management*, in presenza di elementi probatori o oggettivi sulla movimentazione del conto o del set documentale di registrazione del titolare, la segnalazione viene valutata come *True Hit* essendo in presenza di un sospetto evento fraudolento attuato da parte del cliente Flowe.

L'operatore apre activity di tipo *Customer Security* nella posizione del cliente in *FanBase* e dopo aver riportato tutte le evidenze emerse nelle indagini e i relativi elementi probatori e/o oggettivi nella sezione dedicata, valuta la gravità dell'evento di sospetta frode agita e se necessario attua immediatamente il blocco preventivo della posizione secondo le modalità indicate nella sezione dedicata della presente procedura.

In caso di *True Hit*, l'operatore deve inviare una comunicazione al titolare del conto. Tale comunicazione viene inviata direttamente dalla sezione dedicata della *Customer Security* aperta a seguito della prevalutazione negativa e può avere diverse finalità che verranno descritte nei dettagli nella sezione dedicata.

6.2.5 Contatto con il cliente sospetto

Le comunicazioni inviate in queste casistiche dal team Account Monitoring and Fraud Management hanno il fine di verificare insieme al cliente la natura delle operazioni valutate come sospette frodi agite dagli stessi.

L'operatore del *team Account Monitoring and Fraud Management* seleziona direttamente dalla finestra dedicata della *Customer Security* aperta a seguito della prevalutazione negativa, il template adeguato alla casistica in oggetto. Il template viene poi completato con l'inserimento delle operazioni sospette, la lista dei documenti richiesti ai fini della corretta valutazione e per la chiusura dell'indagine in corso ed infine la tempistica concessa al cliente per la produzione del riscontro.

L'esito del contatto con il cliente sospetto ha il fine ultimo di poter confermare i sospetti e quindi far mettere in pratica tutte le misure cautelative provvisorie e definitive sulla posizione analizzata oppure per archiviare come False Hit il caso.

Nel caso in cui le pre-analisi e le successive attività evidenziassero operazioni anomale, ma relative ad un utilizzo del conto non di natura fraudolenta, ma di sospetto riciclaggio, l'operatore del *team Account Monitoring and Fraud Management* dopo attenta valutazione apre in *FanBase un activity di tipo AML*, assegnata all'omologo team, allegando tutte le evidenze raccolte per l'avvio del AVR formale e del processo previsto dalla *"Procedura operativa del processo di adeguata verifica SOS e gestione conto"*.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica documentazione fornita in onboarding L'operatore verifica:	Manuale	Ad evento	FanBase

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
• la corrispondenza tra i contenuti del video *selfie* e la foto presente nel documento di identità; • la presenza di anomalie formali o altri elementi strutturali che possano indurre a riconoscere "compromissioni" del documento utilizzato in fase di identificazione; • che i dati antiriciclaggio forniti in fase di richiesta apertura (es.: professione, patrimonio e reddito annuo) siano coerenti con la movimentazione registrata sul conto.			
Verifica movimentazione conto riconducibile a schemi considerati "sospetti" A titolo di esempio (non esaustivo), l'operatore verifica che: • a fronte di movimenti di accredito si siano registrati, a distanza di breve tempo, movimenti in addebito dello stesso importo; • siano presenti movimenti ricorrenti verso coordinate bancarie o *merchant* riconducibili ad altri casi sospetti o appurati come frodi/truffe; • il nome del beneficiario del bonifico in accredito sia diverso dal nome dell'intestatario del conto di pagamento.	Manuale	Ad evento	T24; SIA Crystal Gate; FanBase; Dashboard Transazioni PowerBI
Verifiche completezza e coerenza delle informazioni fornite dal Cliente in risposta alla richiesta di approfondimento sulle transazioni oggetto di analisi/sulla movimentazione "anomala" del conto	Manuale	Ad Evento	FanBase e Casella di posta elettronica Office 365

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Ad esempio non esaustivo: documenti accertanti la natura della provvista; documenti che accertino la natura del rapporto tra ordinante della transazione e cliente Flowe beneficiario.			

6.3. BLOCCO PREVENTIVO DELL'OPERATIVITA'

Qualora a seguito delle pre-analisi e delle successive valutazioni sulle operazioni sospette ai fini delle verifiche di antifrode, l'evento venisse confermato come sospetta o accertata frode, l'operatore del *team Account Monitoring and Fraud Management* appone i blocchi preventivi.

In particolare, tali blocchi preventivi sono disposti nei casi di:

- evidenze oggettive sulla movimentazione del cliente (esempio non esaustivo, molteplici bonifici con nome beneficiario diverso dal titolare del conto e immediati addebiti per distrarre le somme accreditate)
- evidenze oggettive sul set documentale di registrazione (esempio non esaustivo, elementi oggettivi di falsità dei documenti identificativi)
- mancato riscontro alla richiesta documentale da parte del cliente entro le tempistiche indicate o riscontro non esaustivo ai fini della valutazione in essere sull'evento di sospetta frode agita.

6.3.1 Blocco Accesso in App (FANBASE)

Il blocco "accesso in App", effettuato mediante il gestionale Power Apps - Fan Base, è un blocco che impedisce al cliente di accedere all'App, scaricata sul dispositivo mobile, con cui si è registrato in fase di apertura del conto.

Il blocco preventivo è sempre seguito dall'invio di una comunicazione di notifica al titolare del conto. Tale comunicazione contiene inoltre nella maggior parte dei casi richieste di invio di documentazione ai fini di verifica delle operazioni oggetto di sospetta frode agita dai clienti. In casi particolari, nei quali il team necessita risposta urgente (entro poche ore dall'invio della richiesta documentale ai fini di verifica prevista da normativa), l'operatore del team Account Monitoring and Fraud Management invia anche SMS al numero censito, per sollecitare il cliente a visionare la casella mail censita alla quale è stata invitata la notifica.

Le comunicazioni di richiesta documentale ai fini di verifica delle operazioni sospette variano a seconda della segnalazione che ha generato il sospetto.

CONTROLLO	TIPO ATTIVITÀ	FREQUENZA ATTIVITÀ	APPLICATIVO
L'operatore del *Team Account Monitoring and Fraud Management* nella posizione del cliente crea un "*activity Customer Security*" riportando tutte le evidenze emerse nelle indagini e i relativi elementi probatori e/o oggettivi nella sezione dedicata	Manuale	Ad Evento	Power Apps
Tramite la specifica sezione Block User l'operatore appone il blocco preventivo di accesso in app ("*Block on sign In*")	Manuale	Ad Evento	Power Apps
Verifica la corretta ed avvenuta apposizione del blocco sul cliente in oggetto	Manuale	Ad Evento	Power Apps
L'operatore del *Team Account Monitoring and Fraud Management* invia tramite la sezione Send e-mail la richiesta documentale ai fini di verifica delle operazioni sospette utilizzando il template più adeguato alla casistica di segnalazione.	Manuale	Ad Evento	Power Apps

6.3.2 Blocco Operatività del Conto di pagamento (T24 - FanBase)

Il blocco "conto", effettuato mediante il gestionale PowerApps – Fanbase, che tramite una chiamata API genera medesimo blocco sul CoreBanking T24.Si tratta di un blocco che ha effetti sul conto di pagamento, apposto dal team *Account Monitoring and Fraud Management*, che impedisce al cliente di disporre delle somme presenti sul conto e di ricevere nuovi accrediti, nelle casistiche di blocco preventivo. In assenza di altri blocchi sulla posizione (accesso in app e carta) il cliente può accedere all'App ma tutte le operazioni tentate di addebito e accredito, anche quelle con carta, sono automaticamente rifiutate dal Sistema di *Core Banking* in quanto il conto risulta di fatto inibito.

Dato che il gestionale T24, per garantire un più alto livello di sicurezza del processo, prevede l'apposizione di blocco attraverso una doppia approvazione, anche il blocco effettuato tramite FanBase è stato sviluppato per prevedere che un primo operatore del team Account Monitoring and Fraud Management apponga il blocco dalla sezione dedicata di Fanbase, e che questa azione generi un messaggio di richiesta approvazione che deve essere eseguito da un secondo operatore

CONTROLLO	TIPO ATTIVITÀ	FREQUENZA ATTIVITÀ	APPLICATIVO
L'operatore del *Team Account Monitoring and Fraud Management* tramite la sezione Block User dell'activity Customer security in Fanbase, inserisce la tipologia di blocco c.d. "*Posting Restriction*": • solo in addebito (blocco 1) • solo in accredito (blocco 2) • totale (blocco 3)	Manuale	Ad Evento	T24, FanBase
Inserisce una breve descrizione della motivazione del blocco tramite utilizzo di parole chiave.	Manuale	Ad Evento	T24, Fanbase
Un secondo operatore del *Team Account Monitoring and Fraud Management* procede poi con approvazione del blocco precedentemente inserito	Manuale	Ad Evento	T24, Microsoft Outlook, Microsoft Teams

6.3.3 Blocco Operatività Carta (SIA Crystal Gate)

Il blocco "carta", effettuato mediante il gestionale PowerApps – FanBase, che tramite una chiamata API genera medesimo blocco sull'applicativo Crystal Gate (GUI) è un blocco che impedisce al cliente l'utilizzo della carta (sia fisica che virtuale) e di effettuare tutte le operazioni ad essa collegata.

Tramite l'applicativo PowerApps - FanBase, , l'operatore del *Team Account Monitoring and Fraud Management*, applica il blocco di tipo Bank sulla posizione del cliente. Tale blocco una volta apposto si estende alla carta di debito attiva abbinata a tale posizione e comporta la negazione diretta di qualsiasi autorizzativo tentato dal titolare. Viene selezionato il blocco di tipo Bank in quanto non può essere rimosso dal cliente tramite specifica funzionalità in APP a differenza del blocco di tipo Customer.

CONTROLLO	TIPO ATTIVITÀ	FREQUENZA ATTIVITÀ	APPLICATIVO
L'operatore del *Team Account Monitoring and Fraud Management* dalla sezione Block User dell'activity Customer Security appone il blocco di tipo Generic Bank Block Temporary (KD)	Manuale	Ad Evento	SIA Crystal Gate, FanBase
L'operatore del *Team Account Monitoring and Fraud Management* verifica la corretta ed avvenuta apposizione del blocco sul cliente in oggetto	Manuale	Ad Evento	SIA Crystal Gate, FanBase

6.4. POSSIBILI AZIONI AGGIUNTIVE

6.4.1 Storno dell'operazione SCT non completata (pre cut-off)

Il *team Account Monitoring and Fraud Management*, in presenza di accertata provvista fraudolenta, può valutare la possibilità di effettuare storno delle operazioni SCT ordinari in uscita disposte ai fini di distrazione di tali somme da parte del cliente Flowe valutato come frodatore. Questo è possibile solo nel caso in cui l'operazione risulta essere ancora non completata, ovvero che il cut-off successivo alla disposizione di bonifico ordinario non è ancora stato raggiunto, e in presenza di elementi oggettivi sull'accredito delle somme in oggetto; ad esempio non esaustivo, la presenza di una segnalazione da parte di altro istituto di evento fraudolento e la presenza della relativa denuncia.

Tale operazione viene effettuata a fronte di mancato riscontro o riscontro non esaustivo al contatto con il cliente attivato precedentemente alla disposizione di storno. Ad esempio non esaustivo, in presenza di richiamo interbancario (SEPA o SWIFT) pervenuto tra il momento della disposizione del bonifico ordinario e il successivo cut-off, come descritto nelle precedenti sessioni, il cliente viene immediatamente contattato per poter verificare la natura degli accrediti oggetto di richiamo. In questo caso specifico, i tempi di risposta richiesti al cliente sono in termini di ore e per questo motivo, oltre alla comunicazione mail, è sono previsti solleciti ricorrenti tramite l'invio di SMS al numero di telefono censito da parte del titolare del conto, ogni 30 minuti o meno a seconda dell'urgenza. In assenza di riscontro alla nostra comunicazione mail o per riscontro non esaustivo, viene valutata la possibilità di effettuare lo storno delle operazioni in addebito non ancora completata.

Per i dettagli in merito alla gestione degli storni sugli SCT fraudolenti in addebito disposti dai conti Flowe, si faccia riferimento alla "*Procedura Operativa Pagamenti SCT*".

6.4.2 Invio richiami interbancari SEPA / SWIFT in uscita

Qualora il cliente "frodatore", una volta ricevute le somme fraudolente sul conto di pagamento, abbia disposto uno o più SCT in uscita relativamente alla provvista fraudolenta e questi ultimi siano stati correttamente completati, il *team Account Monitoring and Fraud Management* può valutare la possibilità di inviare dei richiami interbancari per il recupero delle somme. Secondo il regolamento SEPA, i richiami interbancari *CAMT.056* possono essere inviati entro 13 mesi dalla data valuta addebito dell'operazione oggetto di richiamo. In questo caso il richiamo interbancario è di tipo *BANK - FRAD* (fraudolent); questa definizione indica che il richiamo è stato disposto su iniziativa dell'istituto in presenza di un sospetto evento fraudolento o di uno comprovato. Per l'inserimento del richiamo interbancario in uscita, il team Account Monitoring and Fraud Management si avvale del supporto del team Operations Flowe di Banca Mediolanum. Quest'ultimo viene ingaggiato tramite l'assegnazione di una activity Customer Security specifica, dove l'operatore del team Account Monitoring and Fraud Management riporta tutti gli elementi per poter procedere all'inserimento del richiamo tramite il core banking T24. In casi particolari, l'operatore del team *Account Monitoring and Fraud Management* a completamento dell'invio del richiamo interbancario *CAMT.056*, per una serie di istituti, principalmente esteri, ha la facoltà di valutare la predisposizione anche della richiesta di invio messaggio *MT199* (richiamo *SWIFT*) verso il servizio *Agency Service* di Intesa San Paolo, che invierà successivamente, per conto di Flowe il messaggio di richiamo all'istituto beneficiario della transazione.

Per i dettagli in merito alla gestione dei richiami *CAMT.056* in uscita sugli SCT fraudolenti in addebito disposti dai conti Flowe, si faccia riferimento alla "*Procedura Operativa Pagamenti SCT*".

6.4.3 Valutazione rimborso somme richiamate / reclamate.

Qualora, sul conto di pagamento del soggetto frodatore, siano disponibili delle somme, il team *Account Monitoring and Fraud Management* può valutare la possibilità del rimborso delle somme al soggetto frodato.

Per procedere con le attività di rimborso degli importi, il team verifica la presenza di molteplici elementi probatori e/o oggettivi di conferma dell'evento come fraudolento, a seguito della analisi effettuate e descritte nella sezione 6.2 della presente procedura. L'operatore, infine può procedere al rimborso delle somme richiamate/reclamate al c.d. "soggetto frodato" solo in presenza:

- della richiesta di richiamo interbancario dall'istituto dell'ordinante (soggetto Frodato);
- della copia di una o più denunce di eventi fraudolenti agiti da stesso correntista Flowe, ricevute da parte dell'autorità giudiziaria, dall'istituto controparte o di un soggetto inscritto all'albo degli Avvocati.

La decisione di rimborso è comunque subordinata alla presenza di quei due elementi sopra elencati e in casi più complessi tramite la conferma del Head of Controls & Regulatory Reporting e/o del responsabile della *perspective Banking Services & Controls* Laddove necessario si riserva la facoltà di confrontarsi con i referenti del *Team Contenzioso e Reclami*, della *Divisione Affari Legali* e della *Funzione Antiriciclaggio* dell'*outsourcer* Banca Mediolanum.

Una volta verificati i già menzionati elementi, l'operatore del *team Account Monitoring and Fraud Management verifica:*

- se il richiamo interbancario è ancora in corso di validità o se risulta essere oltre i 10 giorni (per bonifici SCT standard) o i 15 giorni (per bonifici SCT instant) lavorativi. Se tali tempistiche sono già decorse, la risposta al richiamo interbancario sarà già evasa, così come previsto dalle direttive interbancarie (*Rulebook EBA*)
- se la capienza del conto individuato come fraudolento possa permettere il rimborso totale o parziale delle somme richiamate.

Nel caso il richiamo risulta essere ancora in corso di validità e in presenza di somme per soddisfarlo totalmente, un operatore del *team Account Monitoring and Fraud Management* procede ad inserire l'accettazione dello stesso dalla sezione dedicata di T24 e un secondo operatore dello stesso team procede con l'approvazione.

Nel caso in cui le somme non sono sufficienti a soddisfare totalmente il richiamo interbancario, ma solo parzialmente o se il richiamo interbancario è stato già lavorato tramite rifiuto, in quanto decorsi i giorni lavorativi indicati dal *Rulebook EBA*, l'operatore del *team Account Monitoring and Fraud Management* trasferisce gli importi oggetto dell'operazione fraudolenta su un conto transitorio della Società[1] e poi dispone, attraverso l'applicazione di *Core Banking*, il/i bonifici SCT verso gli IBAN di origine delle somme (intestati ai soggetti coinvolti nella frode, i c.d. "soggetti frodati"). Per eseguire le operazioni di rimborso l'operatore del *team Account Monitoring and Fraud Management* con idonei poteri autorizzativi procede all'autorizzazione degli input precedentemente inseriti da un operatore dello stesso team.

In caso di presenza di più segnalazioni sulla stessa posizione, il rimborso viene eseguito nell'ordine di soddisfazione dei requisiti, i rimborsi sui soggetti che hanno inviato per primi reclamo e denuncia sono considerati "reclamanti privilegiati". Le attività di rimborso sono eseguite per tutti i soggetti che hanno avanzato segnalazione, fino ad esaurimento dei fondi sul rapporto.

Una volta completate le attività di rimborso ai soggetti frodati, l'operatore aggiorna le informazioni presenti nel *Activity* di FanBase.

CONTROLLO	**TIPO CONTROLLO**	**FREQUENZA CONTROLLO**	**APPLICATIVO**
Verifica presenza richiesta di richiamo da parte dell'istituto del soggetto frodato	Manuale	Ad evento	T24
Verifica veridicità e contenuti della denuncia presentata all'autorità giudiziaria	Manuale	Ad evento	na

[1] Il trasferimento delle somme non è diretto tra i rapporti impattati per tutelare i dati personali dei soggetti coinvolti.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica iscrizione all'Albo degli Avvocati del soggetto mittente della comunicazione	Manuale	Ad evento	Sito Internet Consiglio Nazionale Forense
Verifica saldo conto di pagamento cliente "frodatore"	Manuale	Ad evento	T24
Verifica data ricezione denuncia e richiamo per valutazione ordine e priorità di gestione dei rimborsi	Manuale	Ad evento	T24; Legal mail; Casella di posta elettronica Office 365

6.4.4 Segnalazione di operazione sospetta (SOS)

Nel caso l'operazione fraudolenta agita dal cliente sia ritenuta illecita anche ai fini antiriciclaggio, o in presenza di elementi oggettivi e probatori che accertino l'evento fraudolento oltre determinati parametri (per esempio non esaustivo, somme rilevanti o modus operandi continuativo nel tempo) l'operatore del *team Account Monitoring and Fraud Management* che ha gestito le attività di analisi, raccoglie tutte le informazioni necessarie per valutare l'avvio dell'iter di invio della SOS alla funzione Antiriciclaggio di Banca Mediolanum.

Per il dettaglio della gestione delle segnalazioni delle operazioni sospette, si faccia riferimento alla *sezione 12. "Procedura operativa del processo di segnalazione operazioni sospette (SOS)" della "Procedura operativa del Processo di adeguata verifica, SOS e gestione conto"*.

6.4.5 Inserimento in Greylist

In caso di permanenza di elementi di sospetto sull'utilizzo del conto da parte del cliente a titolo di esempio non esaustivo, in assenza di elementi per procedere al recesso d'ufficio del contratto a seguito di verifica conclusa con valutazione parzialmente positiva, o a seguito di invio di Segnalazione per Operatività Sospetta, il team Account Monitoring e Fraud Management valuta la possibilità di porre il conto in uno stato di monitoraggio attivo tramite l'inserimento dello stesso in *Greylist*.

L'inserimento di una posizione in *Greylist* consiste nell'introduzione del conto tramite i suoi parametri identificativi (numero conto, intestatario ecc.) all'interno di una specifica lista dell'applicativo FCM. Successivamente all'introduzione della posizione in monitoraggio attivo, per ogni SCT Standard e in accredito e in addebito sopra i 250€, FCM genera un alert che deve essere valutato entro la giornata lavorativa dagli operatori del team Account Monitoring e Fraud Management per poter accettarne l'accredito o completare l'addebito. Per quanto riguarda invece gli SCT Istantanei con importo superiore a 250€ vengono negati sia in addebito che in accredito, in quanto a differenza degli SCT Standard, non è possibile porre tali messaggi in uno stato di blocco temporaneo.

Il monitoraggio attivo tramite *Greylist* è previsto per un periodo di 60 giorni dall'attivazione. Al termine di tale periodo, la posizione verrà nuovamente analizzata al fine di un'eventuale valutazione positiva oppure di procedere con ulteriori azioni ad esempio non esaustivo, il recesso d'ufficio o l'invio di una SOS se non ancora effettuato.

6.4.6 Recesso dal contratto

In presenza di operazioni ritenute fraudolente[2] e quindi non coerenti rispetto ai principi della Società, per mancato, parziale o non esaustivo riscontro alla richiesta documentale ai fini di verifica dell'evento di sospetta frode, ed in presenza di elementi oggettivi di attività fraudolenta, l'operatore del *Team Account Monitoring and Fraud Management* può proporre all'Head of Controls & Regulatory Reporting della *Perspective Banking Services & Controls* la valutazione di recesso dal contratto con il cliente. A seconda della casistica, della gravità dell'evento fraudolento o del mero sospetto, né accertato, né confermato, il recesso di ufficio proposto può avere un decorso di 60 giorni dalla notifica oppure decorso immediato.

In presenza di elementi oggettivi sulla natura fraudolenta dell'operatività del conto, il recesso d'ufficio del contratto avviene con decorso immediato. A titolo di esempio non esaustivo, se sulla movimentazione sospetta è pervenuto richiamo interbancario e relativa denuncia ricevuta tramite i canali preposti.

Qualora il titolare del conto non fornisca riscontro (mancato) o fornisca riscontro non adeguato alla richiesta documentale ai fini della verifica, come previsto dalla normativa antiriciclaggio (d.lgs 231/2007, art.42 c.1), in assenza di elementi oggettivi sulla natura fraudolenta della movimentazione, il team Account Monitoring and Fraud Management procede all'apposizione del blocco della posizione e alla proposta di recesso con decorso a 60 giorni all'Head of Controls & Regulatory Reporting. Il blocco del conto permane fino al ricevimento di adeguato o totale riscontro alla richiesta documentale. In tal caso il Team Account Monitoring and Fraud Management procederà alla valutazione di quanto ricevuto ai fini della conferma del recesso.

Al contrario, qualora il titolare del conto fornisca riscontro parziale o che la documentazione fornita seppur idonea alla giustificazione della movimentazione, ma o faccia permanere i sospetti di frode agita, il Team Account Monitoring and Fraud Management procede all'inserimento della posizione all'interno della *Greylist* (si veda paragrafo 6.4.5) e all'invio della proposta di censimento del recesso d'ufficio con decorso a 60 giorni all'Head of Controls & Regulatory Reporting. Se accordata l'estinzione, nell'arco temporale tra il censimento e l'effettiva chiusura non è prevista la rimozione dalla *Greylist*. La stessa procedura è prevista in caso di riscontro parziale alla richiesta documentale ai fini della verifica.

Per quanto riguarda il processo di recesso dal contratto si rimanda alla sezione 13. "Recesso del conto" della *"Procedura operativa del Processo di adeguata verifica, SOS e gestione conto"*. Inoltre per maggiori approfondimenti si rimanda alla "*Procedura operativa Estinzione conto* ".

[2] Indipendentemente dal saldo del conto di pagamento e dall'esito delle attività di rimborso nei confronti dei soggetti frodati.

6.4.7 Conversione della tipologia di recesso

In alcuni casi, la decisione di recesso d'ufficio a 60 giorni può subire delle variazioni così come segue. Laddove non sia previsto il blocco dell'operatività durante tale arco temporale, nel caso in cui il titolare del conto presenti ulteriore movimentazione sospetta, il team Account Monitoring and Fraud Management valuta l'invio di ulteriore richiesta documentale ai fini della verifica. Qualora vi sia un mancato riscontro o riscontro non adeguato entro le tempistiche previste dalla comunicazione, ai sensi della normativa antiriciclaggio (d.lgs 231/2007, art.42 c.1), l'operatività della posizione viene bloccata. Tale blocco permane fino all'eventuale riscontro totale o parziale alla richiesta inviata oppure fino al raggiungimento del termine del periodo previsto per l'estinzione d'ufficio già concordata.

Qualora invece dovessero pervenire elementi oggettivi (si rimanda agli esempi del paragrafo 6.4.6 della presente procedura), sia relativamente alla movimentazione precedente al censimento del recesso d'ufficio a 60 giorni, sia per le operazioni successive, il Team Account Monitoring and Fraud Management procede alla conversione d'ufficio del recesso con decorso immediato.

Per quanto riguarda le modalità di attuazione di recesso immediato si rimanda alla sezione 13. "Recesso del conto" della *"Procedura operativa del Processo di adeguata verifica, SOS e gestione conto"*.

7 NORMATIVA

7.1 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 per la gestione del rischio di reputazione;
- Procedura operativa "Onboarding ed Apertura conto";
- Procedura operative "Gestione conto";
- Procedura Operativa "Gestione pagamenti SCT";
- Procedura Operativa Estinzione conto.

7.2 NORMATIVA ESTERNA

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

- 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;
- Direttiva (UE) 2015/2366 PSD2 – (Payment Services Directive 2);
- 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.