PROCEDURA OPERATIVA

Gestione conto

Procedura emessa il 26/05/2021

Owner della procedura: Perspective Happiness and Services

SOMMARIO

1 OBIETTIVO DEL DOCUMENTO

Obiettivo del presente documento è illustrare il processo di gestione operativa del conto di pagamento con *focus* sul monitoraggio dell'operatività sul rapporto, la gestione dei blocchi e delle anomalie sul conto. 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

3.01 CONTI DI PAGAMENTO

3.01.01 GESTIONE CONTO

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:

- **AML** (*Anti Money Laundering*): dicitura inglese (in italiano Antiriciclaggio) con cui si intende l'azione preventiva e la lotta al riciclaggio di beni, denaro o altre utilità in genere. L'attività di riciclaggio in sé e per sé consiste nell'investire capitali provenienti da reato all'interno di attività lecite, così da rendere difficoltosa la loro identificazione. Attraverso questo meccanismo, ogni bene frutto di attività illecita (traffico di stupefacenti, evasione fiscale, rapina, sequestro o qualsivoglia reato non colposo) viene "ripulito" dal suo alone di illiceità e reintrodotto nel circolo economico attraverso sbocchi perfettamente legali.
- **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.
- **Operazione sospetta:** ogni attività atta, per sua natura, ad avere una connessione con il riciclaggio o con il finanziamento del terrorismo e, in particolare, le operazioni complesse di importo particolarmente rilevante o insolitamente elevato, nonché tutti gli schemi insoliti di operazione che non hanno uno scopo economico evidente o che non hanno uno scopo chiaramente lecito.
- **Unità di Informazione Finanziaria per l'Italia -UIF**: l'unità, attiva presso la Banca d'Italia, riceve e acquisisce informazioni riguardanti ipotesi di riciclaggio e di finanziamento del terrorismo, ne effettua l'analisi finanziaria e, su tali basi, ne valuta la rilevanza ai fini della trasmissione agli organi investigativi (Nucleo speciale di polizia valutaria della Guardia di Finanza - NSPV e Direzione investigativa antimafia-DIA) e della collaborazione con l'Autorità Giudiziaria.
- ***Claim*:** è una istanza di verifica aperta sull'applicazione di CRM per tracciare una problematica verificatasi sulla posizione di un cliente.
- ***Incident***: ogni evento o serie di eventi collegati, non pianificati dalla Società che interessa le sue risorse informatiche e che ha o probabilmente avrà un impatto sull' integrità, disponibilità, riservatezza, autenticità e/o continuità dei servizi o dei processi dell'IMEL oppure che implica la violazione o l'imminente minaccia delle norme in materia di sicurezza delle informazioni (es.: frodi informatiche, attacchi attraverso *internet*, malfunzionamenti e disservizi).

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)

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 al monitoraggio dell'operatività del conto e dalla *Perspectvie Augmented Intelligence* per la gestione di alcune anomalie relative al conto di pagamento Flowe.

3.2. 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 e le carte associate al cliente, nonché di inviargli notifiche via sms, *e-mail*, *push* in APP.

Nell'ambito della presente procedura l'applicazione consente:

- la consultazione dei documenti inoltrati dal cliente in fase di richiesta apertura del rapporto ed il contratto sottoscritto;
- la gestione del blocco App (apposizione e rimozione);
- la gestione di "*claim*" dedicati al fine di tracciare la problematica sul cliente ed ingaggiare gli operatori del *team Operations* per l'avvio delle attività di analisi.

3.3. 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 Services*:

- in caso di identificazione di un'operazione anomala, 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);
- l'analisi ed eventualmente la risoluzione manualmente alcune anomalie sui conti di pagamento (es.: pre-autorizzate generate in maniera errata).

3.4. GESTIONALE ANTIRICICLAGGIO - FCM

Il modulo *Financial Crime Mitigation* (FCM) dell'*outsourcer* Temenos, di seguito denominato anche "Gestionale Antiriciclaggio", permette lo svolgimento di una serie di attività e controlli ai fini AML supportando la Società dalla fase di acquisizione del cliente e per tutta la durata del rapporto.

Nello specifico, nell'ambito del sottoprocesso di monitoraggio dell'operatività del conto, il modulo consente di:

- monitorare l'operatività svolta sui conti di pagamento Flowe, identificando l'eventuale operatività sospetta ai fini AML (c.d. "*alert*");
- storicizzare l'operatività sospetta identificata, mediante il censimento di un "*Case*", che permette di tracciare le analisi svolte, le comunicazioni con il cliente e le eventuali azioni intraprese dalla Società al fine di adempiere agli obblighi in materia di antiriciclaggio.

3.5. 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 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. STRUMENTO DI TICKETING DEVOPS

Lo Strumento di *Ticketing* Devops viene utilizzato dagli operatori della *Perspective Happiness and Service* per la tracciatura delle anomalie riscontrate nella gestione della *Power Platform* e per ingaggiare gli operatori della *Perspective Augmented Intelligence* nel processo di gestione delle anomalie sui conti di pagamento.

3.7. POWER BI

Flowe si avvale dell'applicazione Microsoft PowerBI per estratte le fonti di dati in formati differenti e interattivi necessari alle analisi delle operazioni anomale o sospette.

3.8. LIVE MONITORING DASHBOARD – POWER BI

Flowe si avvale della *dashboard* "Live Monitoring" costruita tramite Microsoft PowerBI, al fine 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.

3.9. TRANSACTION DASHBOARD - POWER BI

Flowe si avvale della *dashboard* "Transaction" costruita tramite Microsoft PowerBI per estrarre le fonti di dati in formati differenti e interattivi necessari alle analisi delle operazioni potenzialmente fraudolente agite dalla clientela Flowe.

3.10. WORKFLOW AML

Il "*workflow* AML" è l'applicazione messa a disposizione dall'*outsourcer* Banca Mediolanum per la gestione del processo di Segnalazione delle Operazioni Sospette.

L'applicazione viene utilizzata dagli operatori della *Perspective Happiness and Service* per raccogliere tutti i dati e documenti inerenti l'operazione da valutare ai fini della trasmissione alla UIF.

4 ATTORI, RUOLI E RESPONSABILITÀ

Di seguito sono indicati i principali attori, coinvolti nel processo di rendicontazione del conto di pagamento Flowe e 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 dei *team Account Monitoring* and Fraud Management e AML and KYC di:

- ricevere e verificare le segnalazioni di operazioni anomale o sospette segnalate
- effettuare gli approfondimenti sulle operazioni anomale o sospette rilevate;
- avviare l'iter di Adeguata Verifica Rafforzata;
- raccogliere i dati e le informazioni da inoltrare per l'avvio del processo di valutazione di Segnalazione Operazione Sospetta;
- raccogliere l'autorizzazione alla chiusura del rapporto.

Gli operatori del *team AML and KYC* si occupano, inoltre, di aggiornare sul Gestionale Antiriciclaggio il profilo di rischio AML del cliente.

Nell'ambito del sottoprocesso di gestione delle anomalie sui conti di pagamento, la *Perspective Happiness and Service*, per il tramite del *team Operations* analizza e gestisce (eventualmente con il supporto della *Perspective Augmented Intelligence* o degli *outsourcer* impattati) le problematiche segnalate dalla clientela o emerse a fronte delle attività di monitoraggio operativo dei rapporti.

4.2. PERSPECTIVE AUGMENTED INTELLIGENCE

La *Perspective Augmented Intelligence*, nell'ambito del presente processo viene ingaggiata dagli operatori del *team Operations* nelle attività di analisi tecnica e risoluzione di anomalie che possono avere impatto sulle procedure inerenti i conti ed i servizi di pagamento della *Platform*.

4.3. DELEGATO ALLA SEGNALAZIONE DI OPERAZIONI SOSPETTE

Alla data di stesura del presente documento, il Responsabile della Funzione Antiriciclaggio di Flowe è stato nominato (con delibera del Consiglio di Amministrazione) anche Delegato all'invio delle segnalazioni di Operazioni Sospette (di seguito anche "Delegato SOS").

Nell'ambito del presente processo:

- valuta, alla luce di tutti gli elementi disponibili, le operazioni sospette rilevate dalla *Perspective Happiness and Service* ovvero di cui sia venuto a conoscenza nell'ambito della propria attività;
- assicura la trasmissione all'UIF delle segnalazioni ritenute fondate;
- decide l'archiviazione, fornendo evidenza delle relative motivazioni, le segnalazioni ritenute non fondate e le comunica alla *Perspective Happiness and Services*;
- valuta se, a fronte delle segnalazioni di operazioni sospette a lui pervenute, innalzare o diminuire il profilo di rischio dei soggetti correlati all'operatività analizzata, indipendentemente dall'esito conclusivo delle stesse, tenendo traccia delle motivazioni sottostanti;
- effettua verifiche, anche a campione, sulla congruità delle valutazioni effettuate dalla *Perspective Happiness and Service* sull'operatività della clientela;
- presta consulenza alle strutture operative in merito alle procedure da adottare per la segnalazione di eventuali operazioni sospette ed all'eventuale astensione dal compimento delle operazioni;
- gestisce, per quanto di competenza, i rapporti con l'UIF e corrisponde tempestivamente alle eventuali richieste di approfondimento provenienti dalla medesima.

4.4. OUTSOURCERS

4.4.1. Banca Mediolanum – Ufficio Atti Giudiziari

Nell'ambito del presente processo, Banca Mediolanum attraverso l'Ufficio Atti Giudiziari assiste

Flowe nella gestione degli Atti Giudiziari (richieste accertamento provenienti dall'Autorità Giudiziaria e Fiscale, richieste provenienti dagli organi fallimentari, adempimenti relativi agli atti di pignoramento o sequestro presso terzi); tali attività rappresentano un *input* all'avvio del processo di monitoraggio dell'operatività del conto di pagamento.

4.4.2. Banca Mediolanum – Team Operations Flowe

Nell'ambito del presente processo Banca Mediolanum attraverso il *Team Operations Flowe* del *Settore Product Operations* si occupa di effettuare un controllo costante sulle liste utilizzate dal Gestionale Antiriciclaggio (quali ad esempio black-list, liste PEP, liste PIL, liste appalti) sui clienti di Flowe (c.d. "Ricertificazioni").
In caso di *check* andato a buon fine (falso positivo) il team non intraprende alcuna azione. Qualora l'esito sia *ko* (positivo certificato) il *team* effettua ulteriori azioni, quali, ad esempio, l'innalzamento del profilo di rischio del cliente e/o la richiesta di moduli AVR e – se PEP – l'avvio dell'*iter* di approvazione al mantenimento del rapporto.

4.4.3. Banca Mediolanum – Analisi AML

Nell'ambito del presente processo, Banca Mediolanum attraverso l'Unità Analisi AML si occupa di analizzare ed istruire le segnalazioni ricevute, attraverso il workflow AML, dagli operatori della *Perspective Happiness and Service* ed inerenti presunte operazioni sospette da sottoporre al Delegato alla Segnalazione di Operazioni Sospette di Flowe, per la valutazione delle eventuali segnalazioni alla UIF. In caso di conferma, da parte del Delegato SOS, l'Unità si occupa delle attività di segnalazione secondo le modalità previste dalla normativa antiriciclaggio

L'Unità conduce, in raccordo con il Delegato alla Segnalazione di Operazioni Sospette di Flowe, le verifiche sulla funzionalità del processo di segnalazione e sulla congruità delle valutazioni effettuate dalla *Perspective Happiness and Services* sull'operatività della clientela.

4.4.4. Temenos

Nell'ambito del presente processo, l'*outsourcer* Temenos supporta Flowe nelle attività di analisi tecnica e risoluzione di anomalie che possono avere impatto sulle procedure inerenti i conti ed i servizi di pagamento del sistema di *Core Banking*.

5 PROCESSO DI GESTIONE DEL CONTO DI PAGAMENTO

Il processo di gestione del conto di pagamento Flowe si compone dei seguenti tre sottoprocessi:

1. Monitoraggio dell'operatività del conto;
2. Gestione dei blocchi;
3. Gestione delle anomalie sui conti di pagamento.

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 OPERATIVITÀ CONTO

Il processo di monitoraggio dell'operatività dei conti di pagamento Flowe rappresenta l'insieme delle attività e dei presidi posti in essere dalla Società con lo scopo di identificare operazioni sospette ai fini Antiriciclaggio o che evidenzino un utilizzo del rapporto non coerente con i principi della Società; a tal proposito, con il supporto della Funzione Antiriciclaggio di Flowe sono stati definiti e sviluppati appositi algoritmi che sulla base delle regole definite, giornalmente intercettano potenziali eventi che gli operatori della *Perspective Happiness and Service* analizzano e valutano al fine di identificare possibili comportamenti sospetti ai fini antiriciclaggio e antifrode.

5.1.1. Identificazione operazioni anomale

I due principali strumenti a supporto dell'identificazione di operazioni anomale relative all'utilizzo del conto di pagamento sono:

- Il Gestionale Antiriciclaggio - FCM: il sistema evidenzia, attraverso la creazione di "*alert*", la registrazione di operatività anomala (rispetto alle regole definite) in un determinato arco temporale (es.: una settimana); tali "*alert*" sono visualizzati nella sezione dedicata del gestionale e sono presi in carico ed analizzati dagli operatori del *team AML and KYC*;
- La *dashboard* Live Monitoring costruita tramite Microsoft PowerBI, al fine di identificare operazioni anomale relative all'utilizzo del conto di pagamento. La *dashboard* Live Monitoring prevede due tipologie di analisi su un arco temporale di 72h dal momento dell'apertura del report. 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.

Le attività di analisi delle operazioni registrate sul conto del Cliente possono essere avviate anche a seguito di:

- segnalazioni ricevute dall'Ufficio Atti Giudiziari dell'*outsourcer* Banca Mediolanum, quali ad esempio richieste di accertamento provenienti dall'Autorità Giudiziaria e Fiscale, richieste provenienti dagli organi fallimentari. Tali casistiche sono gestite dal *team AML and KYC*;
- richiami ricevuti da altri intermediari attraverso i canali interbancari SEPA (CAMT.056) e SWIFT (MT999). Per l'approfondimento dell'operatività gestita in caso di richiamo di un bonifico si rimanda a quanto descritto nella specifica procedura operativa "*Gestione pagamenti SCT*";
- registrazione di un reclamo da parte di un cliente.

Le ultime due casistiche sono gestite dal *team Account Monitoring and Fraud Management*.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica operatività anomala sul conto di pagamento A fronte della rilevazione di anomalie rispetto alle regole settate, il sistema FCM evidenzia degli "*alert*" (viene evidenziato un alert per ciascuna regola non rispettata). Al momento sono attive in produzione 15 regole.	Automatico	Giornaliero	Gestionale Antiriciclaggio-FCM
Verifica presenza *alert* in FCM L'operatore del *team AML and KYC* verifica i dettagli dell'*alert* e valuta se prendere in carico la posizione del cliente per l'analisi sulle operazioni rilevate	Manuale	Giornaliero	Gestionale Antiriciclaggio-FCM
Verifica operatività anomala sul conto di pagamento A fronte della rilevazione delle operazioni che hanno superato le regole impostate il sistema genera una lista di conti da verificare agli operatori del *team Account Monitoring and Fraud Management* una *e-mail* di notifica	Automatico	Ogni due ore (durante le ore lavorative)	dashboard Live Monitoring
Verifica anomalie segnalate dalla *dashboard* Live Monitoring L'operatore del *team Account Monitoring and Fraud Management* verifica il tipo di anomalia segnalata e valuta se prendere in carico la posizione del cliente per l'analisi sulle operazioni rilevate	Manuale	Giornaliero	dashboard Live Monitoring

5.1.2. Indagini su operazioni

A fronte della rilevazione, da parte dei predetti sistemi, di evidenze di operatività anomala o sospetta, gli operatori dei *team AML and KYC ed Account Monitoring and Fraud Management* (ciascuno per gli ambiti di competenza) prendono in carico l'operazione segnalata e, attraverso la consultazione degli applicativi aziendali dedicati, avviano le attività di analisi che sono relative l'intera posizione del cliente. Tali approfondimenti riguardano:

- il *set* documentale utilizzato dal cliente in fase di *onboarding*: l'operatore, tramite la specifica sezione di Fanbase, consulta i documenti inoltrati dal cliente in fase di richiesta apertura del rapporto (i documenti identificativi e il video selfie) ed il contratto sottoscritto;
- la movimentazione sul conto: l'operatore, tramite la *dashboard* "Transazioni" di PowerBI, estrae e verifica la movimentazione inerente le operazioni legate al conto di pagamento del cliente (a tal fine vengono estratti sia i movimenti relativi ai servizi di pagamento elettronico, quali ad esempio SCT e SDD, che quelli di *card authorization* e *card clearing*). Qualora sia necessario effettuare un'analisi più dettagliata sulle singole operazioni estratte, l'operatore utilizza il sistema T24 per l'approfondimento sugli SCT e SDD e SIA Crystal Gate per le indagini sulla movimentazione legata alla carta di pagamento.

Qualora, a fronte degli approfondimenti e delle indagini eseguite, l'operazione venga identificata come "non sospetta", non viene effettuata alcuna azione ed il processo termina.

Se, invece, a fronte di elementi oggettivi l'operazione viene valutata come "sospetta (ad esempio riscontro di documenti identificativi contraffatti o incongruenza tra video selfie e documento identificativo o nome del beneficiario di SCT in ingresso diverso dal nome del titolare del conto), l'operatore della *Perspective Happiness and Service* che ha condotto le analisi procede con:

- il blocco preventivo a livello di app, carte e conto;
- l'apertura di un *Case* su FCM contenente la descrizione degli elementi valutati;
- l'invio al cliente della modulistica di Adeguata Verifica Rafforzata (AVR).

Se l'operazione viene valutata come sospetta, ma non si hanno elementi oggettivi per procedere con il blocco preventivo dell'operatività del cliente, l'operatore procede solo con l'apertura del *Case* e l'invio dell''AVR; in questo caso, il blocco è eventualmente apposto a fronte dall'esito della valutazione dell'AVR.

CONTROLLO	**TIPO CONTROLLO**	**FREQUENZA CONTROLLO**	**APPLICATIVO**
Verifica documentazione fornita in *onboarding* L'operatore verifica: • 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	Manuale	Ad evento	Fanbase; Piattaforma FCM

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
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; Dashboard Transazioni PowerBI

5.1.3. Adeguata Verifica Rafforzata (AVR)

Invio AVR

Nei casi in cui, a seguito dell'analisi sull'operatività del conto del cliente vi siano i presupposti per avviare l'*iter* di Adeguata Verifica Rafforzata e raccogliere tutte le informazioni necessarie per la valutazione dell'operazione anomala o sospetta, l'operatore del *team AML and KYC* o del *team Account Monitoring and Fraud Management* (per competenza in base all'*input* della segnalazione) predispone ed invia al cliente una *e-mail* contenente la richiesta di compilazione e sottoscrizione del modulo dedicato e, se necessario, ulteriori richieste di chiarimento e/o documentazione attestante il la natura delle operazioni rilevate sul conto o la sua identità.

Valutazione AVR

Nel caso in cui il Cliente fornisca, in risposta alla *e-mail* di AVR, valide spiegazioni che giustifichino che lo stesso non abbia intrapreso un comportamento illecito e che confermino che il suo comportamento sia in linea con le normative vigenti in materia di Antiriciclaggio e con i principi della Società, l'operatore chiude il *Case* sul Gestionale Antiriciclaggio – FCM senza aggiornare il profilo di rischio AML del cliente).

Laddove, nonostante le spiegazioni fornite dal cliente, l'operatore ritenga che lo stesso abbia compiuto un'operazione ritenuta illecita o non coerente rispetto ai principi della Società oppure nel caso in cui il cliente non risponda all' AVR entro i termini previsti, l'operatore procede con:

- il blocco della posizione del cliente (se non già preventivamente apposto, cfr. parag. 5.1.2);
- l'invio delle informazioni afferenti l'operazione sospetta, identificata all'*Unità Analisi AML* dell'*outsourcer* Banca Mediolanum (cfr. parag. 5.1.4);
- l'aggiornamento, se richiesto dal Delegato SOS o previsto dalla casistica in oggetto, del profilo di rischio AML del cliente (cfr. parag. 5.1.45);
- l'avvio del processo di valutazione di recesso da parte della Società dal contratto di conto (cfr. parag. 5.1.6);
- ed infine, l'integrazione e la chiusura del "C*ase*" (cfr. parag. 5.1.7).

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica risposta AVR entro le tempistiche stabilite dalla Funzione Antiriciclaggio	Manuale	Ad Evento	Piattaforma FCM
Verifiche completezza e coerenza delle informazioni fornite dal Cliente	Manuale	Ad Evento	Piattaforma FCM

5.1.4. Segnalazione Operazione Sospetta (SOS)

Nel caso di operazione sospetta ritenuta illecita ai fini antiriciclaggio, l'operatore che ha gestito le attività di analisi raccoglie tutte le informazioni necessarie per valutare l'avvio dell'iter di invio della SOS alla Unità di Informazione Finanziaria (UIF) della Banca d'Italia.

L'operatore raccoglie tutti i dati e le informazioni necessari ad avviare il processo di segnalazione e, tramite l'applicativo *Workflow AML*, inserisce all'interno del *dossier* dedicato:

- il contratto di apertura del conto Flowe sottoscritto dal cliente;
- il dettaglio della movimentazione sospetta;
- la scheda contenente i dati anagrafici del cliente ed i riferimenti del conto di pagamento Flowe;
- se presente, eventuali documenti attesta (es.: il provvedimento dell'Autorità Giudiziaria).

Una volta completo, il *dossier* viene automaticamente inoltrato, tramite il *workflow AML*, all'*Unità Analisi AML* dell'*outsourcer* banca Mediolanum che analizza ed istruisce la presunta operazione sospetta inoltrata dagli operatori della *Perspective Happiness and Service* e la sottopone al Delegato alla Segnalazione di Operazioni Sospette di Flowe, per la valutazione in merito all'eventuale trasmissione alla UIF delle segnalazioni ritenute fondate. In caso di conferma

da parte del Delegato SOS, l'Unità si occupa delle attività di segnalazione delle operazioni secondo le modalità previste dalla normativa antiriciclaggio.

Il Delegato SOS può valutare se, a fronte delle segnalazioni di operazioni sospette pervenutegli, innalzare o diminuire il profilo di rischio dei soggetti correlati all'operatività analizzata, indipendentemente dall'esito conclusivo delle stesse, tenendo traccia delle motivazioni sottostanti.

5.1.5. Aggiornamento profilo rischio AML cliente

A fronte delle valutazioni effettuate dal Delegato SOS ed in base alla casistica in corso di analisi, se necessario si procede con la registrazione dell'innalzamento del profilo di rischio del cliente.

A titolo esemplificativo e non esaustivo, si procede con l'aggiornamento del profilo di rischio quando sono presenti provvedimenti da parte dell'Autorità Giudiziaria oppure quando, a fronte delle verifiche effettuate, vi sono delle variazioni sulla posizione personale del cliente.

L'aggiornamento del profilo di rischio AML del cliente viene gestito manualmente dagli operatori del *team AML and KYC* attraverso il Gestionale Antiriciclaggio FCM.

5.1.6. Recesso dal contratto

Le operazioni ritenute illecite o non coerenti rispetto ai principi della Società sono oggetto di valutazione da parte del responsabile della *Perspective Happiness and Service* (supportato da eventuale parere della Funzione Antiriciclaggio), per il successivo recesso dal contratto con il cliente.

L'operatore che ha seguito l'analisi dell'operazione, una volta ricevuta autorizzazione a chiudere il rapporto, predispone ed invia al cliente (tramite *e-mail*), la comunicazione di recesso unilaterale dal contratto.

In seguito, la posizione viene inoltrata agli operatori dedicati alle attività di *Operations* per la chiusura del conto e dei relativi servizi collegati; per maggiori approfondimenti si rimanda alla procedura operativa di "*Estinzione del conto di pagamento Flowe*".

5.1.7. Integrazione e chiusura del "Case"

A completamento di tutte le predette attività, l'operatore chiude il "*Case*" avendo cura di integrare la descrizione delle verifiche effettuate ed allega la documentazione e le comunicazioni intercorse tra la Società ed infine il cliente e se disposto, il recesso dal contratto.

5.2. GESTIONE DEI BLOCCHI

La Società, a seguito delle analisi sull'operatività del conto di pagamento e valutazione di comportamenti ritenuti fraudolenti o illeciti o di evidenze sulla documentazione fornita dal cliente durante il processo di *onboarding* ed apertura del conto, può disporre diverse tipologie di blocchi agli strumenti e "prodotti" del cliente.

Nei successivi paragrafi sono riportati, per ciascuna tipologia di blocco:

- una descrizione delle casistiche in cui vengono apposti;
- gli operatori autorizzati a disporre tali blocchi e gli strumenti utilizzati.

5.2.1. Blocco App

Il Blocco "App" è un blocco cautelativo che impedisce al Cliente di accedere all'App scaricata sul dispositivo mobile con cui si è registrato in fase di apertura del conto. Tale blocco può essere apposto a fini preventivi:

- dagli operatori dei *team AML and KYC* e *Account Monitoring and Fraud Management* → per tutti i soggetti valutati come sospetti o oggettivamente fraudolenti/illeciti a fronte di analisi sulla movimentazione e della documentazione;
- dagli operatori del *team Operations* → a seguito della ricezione della richiesta del cliente di chiusura del conto di pagamento.

L'inibizione all'accesso in App è gestita attraverso la *Power App Fanbase*: dopo aver selezionato il cliente da bloccare, l'operatore crea, nella sezione dedicata (*History*), un "*claim*" di tipo "*Block User*", inserisce le note sulle motivazioni che giustificano il blocco apposto e seleziona il *flag* che attiva il blocco ("*Block on sign In*").

CONTROLLO	**TIPO CONTROLLO**	**FREQUENZA CONTROLLO**	**APPLICATIVO**
Verifica apposizione blocco L'operatore verifica, attraverso la sezione dedicata, la corretta ed avvenuta apposizione del blocco sul cliente in oggetto	Manuale	Ad Evento	Fanbase

5.2.2. Blocco carta

Il blocco "carta" impedisce al Cliente l'utilizzo della carta (sia fisica che virtuale) e di effettuare tutte le operazioni ad essa collegata.

Tale blocco può essere apposto a fini preventivi:

- dagli operatori dei *team AML and KYC* e *Account Monitoring and Fraud Management* → per tutti i soggetti valutati come sospetti o oggettivamente fraudolenti/illeciti a fronte di analisi sulla movimentazione e della documentazione;
- dagli operatori del *team Operations* → a seguito della ricezione della richiesta, del cliente, di chiusura del conto di pagamento.

Le attività di sospensione dell'utilizzo della carta sono gestite attraverso il Gestionale Carte – SIA Cristal Gate: dopo aver selezionato cliente da bloccare, l'operatore seleziona la funzionalità dedicata ("*Change Account Status*" - *Generic Bank Block* "KD") ed il sistema, automaticamente, applica il blocco solo alla carta di debito attiva in quel momento.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica apposizione blocco L'operatore verifica, attraverso la sezione dedicata, la corretta ed avvenuta apposizione del blocco sul cliente in oggetto	Manuale	Ad Evento	Gestionale Carte-SIA Cristal Gate

5.2.3. Blocco conto di pagamento

Il blocco del conto di pagamento impedisce al cliente di disporre delle somme presenti sul conto. In questo caso il Cliente può accedere all'App ed utilizzare la carta di debito ma tutte le operazioni disposte sono automaticamente rifiutate dal Sistema di *Core Banking* in quanto il conto risulta di fatto inibito; in generale, tale blocco viene apposto dagli operatori dei *team AML and KYC* e *Account Monitoring and Fraud Management* a fronte di identificazione di operazioni o posizioni sospette, successivamente ai blocchi APP e carta.

Il blocco sul conto di pagamento viene disposto attraverso il Sistema di Core Banking T24; dopo aver selezionato cliente da bloccare, l'operatore inserisce:

- la tipologia di blocco (c.d. "*Posting Restriction*"): solo in addebito[1], solo in accredito, in accredito e in addebito;
- la motivazione del blocco;
- la data di disposizione.

Un secondo operatore della *Perspective Happiness and Services* dotato di adeguati poteri autorizzativi, accede alla posizione del cliente ed approva la disposizione precedentemente inserita.

Si specifica infine che il blocco della "posizione cliente", corrisponde ad un blocco apposto a livello di App, carta e conto ed è previsto a seguito di:

- identificazione di potenziali frodi o frodi accertate agite dal cliente;
- monitoraggio della clientela in essere ai fini Antiriciclaggio che abbia portato a identificare operazioni o soggetti non conformi/idonei con la normativa AML o i principi della Società;
- ricezione della segnalazione di decesso del cliente a fronte della quale, come previsto dalla normativa la Società, in attesa della ricezione della documentazione di successione da parte degli eredi, blocca l'operatività del conto di pagamento (e di tutti i servizi ad esso collegati) intestato alla persona deceduta.

[1] Ad esempio, nel caso in cui ci sia necessità di effettuare un richiamo interbancario (CAMT.056) per un'operazione in addebito sul conto da bloccare l'operatore, per garantire il corretto processamento dell'operazione, dispone il blocco solamente in addebito, lasciando la regolare operatività di accredito sul conto stesso.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica apposizione blocco L'operatore *Happiness and Services* con profilo dedicato accede alla posizione del cliente da bloccare, verifica i dati precedentemente inseriti e conferma la disposizione di blocco.	Manuale	Ad Evento	T24

5.2.4. Blocco clienti inattivi

Nella Piattaforma di *Core-Banking* (T24) è stata impostato un controllo automatico che giornalmente verifica se ciascun cliente ha eseguito almeno una transazione negli ultimi 12 mesi (questa soglia è stata modificata il 17.05.2021, precedentemente la soglia era impostata a 6 mesi dato che Flowe aveva lanciato la propria operatività da pochi mesi). Se il cliente non ha eseguito alcuna transazione nei precedenti 12 mesi viene automaticamente settato da T24 lo *status* di "*Inactive*". I clienti *Inactive* sono completamente bloccati (sia per operazioni in ingresso che in uscita) per evitare fenomeni di Frode.

Un cliente *Inactive* per poter tornare a utilizzare il conto deve contattare l'operatore del *team Customer Interaction* e chiedere di essere riattivato secondo i seguenti *step*:

- il Cliente con conto bloccato che non riesce ad effettuare bonifici oppure che non ha ricevuto un bonifico effettua l'accesso all'app con *passcode* e procede con l'apertura della *chat* con BOT, segnalando il problema riscontrato. In questo caso sarà trasferito all'operatore;
- l'operatore del *team Customer Interaction* riceve la richiesta del cliente identificato e verificato che il conto risulta "*inactive*" procede con la riattivazione del conto in T24.

5.3. GESTIONE DELLE ANOMALIE SUI CONTI DI PAGAMENTO

L'operatività svolta dai clienti sul conto di pagamento Flowe viene gestita in modo automatizzato dal *Sistema di Core Banking*.

Nei seguenti paragrafi sono descritte le attività gestite dagli operatori del *team Operations* in caso di rilevazione, da parte della clientela, di anomalie che influiscono sulla corretta elaborazione delle operazioni svolte sul conto e per le quali si rende necessario una verifica ed eventuale azione di risoluzione.

5.3.1. Identificazione anomalia sul conto

Le anomalie sui conti di pagamento possono essere:

- segnalate dalla clientela tramite *chat* o *e-mail* (per i dettagli si faccia riferimento a quanto

descritto nei processi "*Customer Care*");

oppure

- identificate a seguito delle attività di monitoraggio operativo poste in essere dalla *Perspective Happiness and Service*; rientrano in questa tipologia, ad esempio, le evidenze che emergono durante i controlli massivi svolti per verificare le operazioni della clientela o a seguito di segnalazioni degli outsourcer (es.: SIA, Temenos) relative a problematiche di sistema che hanno comportato anomalie sull'operatività del conto.

Qualora l'anomalia identificata non riguardi un solo cliente, l'operatore della *Perspective Happiness and Service* che ha rilevato la problematica apre un "*claim*" in Fanbase, in modo da avviare le attività di analisi da parte degli operatori del *team Operations*; in caso di anomalia "massiva" l'operatore del *team Operations* procede alla registrazione dell'*incident* nell'apposito Strumento di *Ticketing* (di Temenos/SIA) riportando una descrizione di quanto rilevato.

CONTROLLO	**TIPO CONTROLLO**	**FREQUENZA CONTROLLO**	**APPLICATIVO**
Verifica presenza anomalia massiva o già nota L'operatore che prende in carico la segnalazione verifica che non rappresenti un'anomalia massiva o un "bug" noto e già tracciati; in caso di controllo positivo, ingaggia il *team Customer Interaction* al fine di notificare al cliente che sono in corso le attività di sistemazione della problematica. Al contrario, l'operatore *Happiness and Service* apre un "*claim*" che viene preso in carico dall'operatore di Operations.	Manuale	Ad evento	P0; Fanbase; Strumento di Ticketing Devops

5.3.2. Analisi problematica

L'operatore del *team Operations*, una volta ricevuta l'assegnazione dell'anomalia (attraverso "*claim*" dedicato"), effettua gli approfondimenti e le analisi necessarie alla gestione e risoluzione della problematica. Se necessario, in base al tipo di problematica, l'operatore coinvolge l'outsourcer dell'applicazione impattata dall'anomalia.

Per maggiori dettagli sul processo di gestione degli incidenti gravi si faccia riferimento alla procedura di Flowe "*Incident Management*".

Si riporta di seguito un elenco esemplificativo e non esaustivo delle possibili anomalie relative la gestione del conto:

- anomalie di gestione delle "pre-autorizzate" (*Card*);
- anomalie di gestione dei pagamenti (SCT, SDD, SEDA, *Money Transfer* e *Top-Up*); per il

dettaglio delle attività eseguite in caso di anomalie sugli strumenti di pagamento, si faccia riferimento ai contenuti dei relativi processi di gestione;

- anomalie sui *Drop*;
- anomalie sulla gestione della *fee* mensile applicata ai clienti intestatari di conto per i quali è previsto il pagamento del canone;
- anomalie legate alla *transaction list* (es.: bug generici relativi alla visualizzazione delle transazioni in APP).

L'operatore dedicato alle attività di *Operations* verifica, in base al tipo di anomalia, se risolvibile in autonomia o se necessario l'intervento tecnico degli operatori della *Perspective Augmented Intelligence* o del fornitore della componente interessata dalla problematica.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica tipologia di anomalia L'operatore effettua l'analisi della problematica, effettuando delle prove e dei test propedeutici all'identificazione della causa e delle possibili modalità di risoluzione.	Manuale	Ad evento	T24, Gestionale Carte - SIA Cristal Gate, Fanbase, Strumento di Ticketing Devops, Dashboard relativa al clearing delle transazioni carta

5.3.3. Gestione e risoluzione anomalia

Anomalie risolvibili in autonomia da operatore del team Operations

Se l'anomalia riscontrata è risolvibile in autonomia dall'operatore del *team Operations* (es.: una pre-autorizzata formatasi erroneamente sul conto del cliente), quest'ultimo procede con le attività di sistemazione sui vari applicativi (es.: "*reverse*" manuale sul *Sistema di Core Banking*).

A seguito delle attività tecniche di gestione e conseguente chiusura del "*claim*" dedicato, prima di comunicare al cliente il rientro della problematica, l'operatore del *team Operations* effettua le verifiche necessarie ad attestare l'avvenuta risoluzione dell'anomalia.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica avvenuta risoluzione dell'anomalia sul conto del cliente Ad esempio, in caso di creazione errata di una "pre-autorizzata" sul	Manuale	Ad evento	T24, Gestionale Carte – SIA Cristal Gate, Fanbase

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
conto del cliente l'operatore verifica, attraverso T24, che a seguito delle attività di risoluzione: • il movimento non sia più presente sul conto; • il saldo disponibile del conto non tenga più in considerazione la pre-autorizzata.			

Anomalie per cui è necessario l'intervento della Perspective Augmented Intelligence

Qualora la problematica riscontrata sul conto di pagamento del cliente necessiti, ai fini della risoluzione, l'intervento di un operatore della *Perspective Augmented Intelligence*, l'operatore del *team Operations* apre un *ticket* contenente tutte le specifiche relative alla posizione del cliente e all'anomalia riscontrata sullo strumento di *Ticketing* DevOps.

A titolo di esempio si riportano alcuni esempi di anomalia gestite dalla *Perspective Augmented Intelligence*:

- anomalie relative la funzionalità di "*Account Top-Up*" (es.: mancata ricarica con carta di pagamento su conto *Inactive);*
- anomalie generiche che interessano le notifiche 3-D Secure, notifica *Smart Agent*.

A seguito delle attività tecniche di gestione e conseguente chiusura del ticket dedicato, prima di chiudere il "*claim*" e comunicare al cliente il rientro della problematica, l'operatore del *team Operations* effettua le verifiche necessarie ad attestare l'avvenuta risoluzione dell'anomalia.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica avvenuta risoluzione dell'anomalia sul conto del cliente In caso di anomalie sulle ricariche con carta (Top-Up), l'operatore verifica che la ricarica con carta rimasta bloccata e poi ri-processata dall'operatore della *Perspective Augmented Intelligence* sia stata correttamente registrata sul conto del cliente; l'operatore verifica inoltre la correttezza dei dati dell'operazione (data, importo e	Manuale	Ad evento	P0, T24, Fanbase, Strumento di Ticketing Devops

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
transaction type). In caso di anomalie che interessano la parte *transaction list* di APP, l'operatore verifica che l'operatore della *Perspective Augmented Intelligence*, a seguito delle attività tecniche di risoluzione, abbia correttamente modificato, eliminato o aggiornato la transazione anomala e che la *transaction list* visualizzata in App sia esattamente allineata con quanto presente in T24.			

Anomalie per cui è necessario l'intervento del fornitore

In caso di anomalie per cui è necessario il coinvolgimento del fornitore della componente impattata, l'operatore della *Perspective Happiness and Service* addetto alle attività di *Operations* inoltra (tramite *e-mail* o tramite strumento di *ticketing*, in base al fornitore impattato) i dettagli della segnalazione al *team* dedicato del fornitore che avvia un'ulteriore verifica finalizzata alla gestione e risoluzione dell'anomalia.

Rientrano in questa casistica le anomalie massive relative a procedure *standard* dei conti di pagamento ed i problemi sulle parametrizzazioni del sistema di *Core Banking*.

A seguito ricezione della notifica di avvenuto completamento delle attività tecniche di risoluzione, prima di chiudere il "*claim*" e comunicare al cliente il rientro della problematica, l'operatore del *team Operations* effettua le verifiche necessarie ad attestare l'avvenuta risoluzione dell'anomalia.

In caso di esito positivo delle verifiche, l'operatore conferma al fornitore che è possibile rilasciare in produzione gli interventi tecnici; al contrario, in caso di riscontro di ulteriori problematiche, l'operatore richiede al fornitore di procedere con eventuali ulteriori verifiche o attività tecnici.

Per tutte le casistiche di anomalia (indipendentemente dalla modalità di intervento), a completamento delle attività di verifica dell'avvenuta gestione della problematica, l'operatore chiude su Fanbase il "*claim*" associato alla posizione del cliente. Tale attività genera una notifica automatica all'operatore dedicato alle attività di *Customer Interaction* che procede con la comunicazione al cliente dell'avvenuta risoluzione del problema.

6 NORMATIVA

6.1. NORMATIVA INTERNA

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

- *Regolamento del processo di "Segnalazione Operazioni Sospette (SOS)";*
- *Procedura Operativa "Gestione pagamenti SCT";*
- *Procedura Operativa "Gestione dei reclami";*
- *Procedura Operativa "Incident Management";*
- *Procedura Operativa "Estinzione conto".*

6.2. NORMATIVA ESTERNA

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

- *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 tramite promulgazione del D.Lgs. 6/10/2019 n. 125;*
- *le disposizioni attuative del Decreto Antiriciclaggio, emanate dalle Autorità di Vigilanza di Settore e tempo per tempo vigenti.*
- *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;*
- *Direttiva PAD. Trasparenza e comparabilità delle spese relative al conto di pagamento. Terminologia standardizzata europea;*
- *Direttiva (UE) 2015/2366 PSD2 – (Payment Services Directive 2);*
- *Decreto legislativo 1° settembre 1993, numero 385. Testo unico delle leggi in materia Bancaria e Creditizia.*

Completano il quadro di riferimento a livello nazionale, i decreti del Ministro dell'Economia e delle Finanze (MEF) e gli schemi rappresentativi di comportamenti anomali emanati dalla UIF