

– PARTE SPECIALE U –

**REATI FRODE E FALSIFICAZIONE DI STRUMENTI DI
PAGAMENTO DIVERSI DAI CONTANTI e
TRASFERIMENTO FRAUDOLENTO DI VALORI**

DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E DI TRASFERIMENTO FRAUDOLENTO DI VALORI

1. Delitti in materia di strumenti di pagamento diversi dai contanti 25 octies-1 del d.lgs. 231/2001

Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti,
previsto dall'art 493-ter c.p.

Tale reato è costituito dalla condotta di chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi o comunque ogni altro strumento di pagamento diverso dai contanti. È altresì punibile chiunque, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici
diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti,
previsto dall'art. 493-quater c.p.

Tale reato è costituito dalla condotta di chiunque, salvo che il fatto costituisca più grave reato, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è sempre ordinata la confisca delle apparecchiature, dei dispositivi o dei programmi informatici predetti, nonché la confisca del profitto o del prodotto del reato ovvero, quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, previsto dall'art. 640-ter

Tale reato è costituito dalla condotta di chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.

Trasferimento fraudolento di valori (art. 512-bis)

Salvo che il fatto costituisca più grave reato chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648 648-bis e 648-ter è punito con la reclusione da due a sei anni.

La stessa pena di cui al primo comma si applica a chi, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni.

Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1, comma 2)

Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente differenti sanzioni pecuniarie in conformità al numero di anni di reclusione previsti per il delitto commesso.

2. Le attività individuate come potenzialmente sensibili ai fini del d.lgs. 231/2001 con riferimento ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio

L'analisi delle attività aziendali ha consentito di individuare i processi nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-octies 1 del D. Lgs. 231/2001. In particolari i processi sensibili sono i seguenti:

Ufficio Marketing

1. **Gestione della domanda e gestione portafoglio progetti**, in relazione al quale sono state rilevate le seguenti attività sensibili:
 - a. distribuzione, ai clienti, di apparecchiature / dispositivi per effettuare pagamenti digitali alterati fraudolentemente al fine di trarre un vantaggio per la Banca o al fine di permettere al cliente di effettuare delle truffe (al fine di trarre un vantaggio, ad esempio di natura commerciale) e/o alterazione di un sistema informatico o telematico che produce un trasferimento di valuta virtuale;

Ufficio Back Office

2. **Incassi e pagamenti**, in relazione al quale sono state rilevate le seguenti attività sensibili:
 - a. utilizzo di sistemi di pagamento alterati fraudolentemente al fine di trarre un vantaggio indebito per la Banca in sede di gestione dell'erogazione delle pensioni;
 - b. utilizzo sistemi di pagamento alterati fraudolentemente al fine di trarre un vantaggio indebito per la società in sede di gestione dei pagamenti nell'ambito dell'attività di gestione bonifici estero;
 - c. utilizzo di sistemi di pagamento alterati fraudolentemente al fine di trarre un vantaggio indebito per la Banca in sede di gestione dei pagamenti nell'ambito dell'attività di gestione bonifici area euro;
 - d. trasferimento fraudolento di valori anche se il sistema di pagamento non è alterato attraverso ad es. intestazione fittizia in assenza di specifica documentazione di supporto ovvero a soggetti non facoltizzati (ad es. intestazione di un cc al coniuge di un soggetto sottoposto a sequestro preventivo o confisca, al fine di trarre un vantaggio indebito per la Banca) attribuendo fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità (titoli...) al fine di eludere le disposizioni di legge in materia di misure di prevenzione

patrimoniali o di contrabbando, le disposizioni antimafia ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-ter;

- e. con riferimento alle carte di credito, vendita o distribuzione ai clienti di apparecchiature e dispositivi per effettuare pagamenti digitali alterati fraudolentemente al fine di trarre vantaggio per la Banca (ad esempio mediante un meccanismo fraudolento del conteggio degli interessi) e/o alterazione di un sistema informatico o telematico che produce un trasferimento di valuta virtuale al fine di trarre vantaggio, per la Società (ad es. mediante un meccanismo fraudolento del conteggio degli interessi);
- f. con riferimento alle carte di debito, vendita o distribuzione ai clienti di apparecchiature e dispositivi per effettuare pagamenti digitali alterati fraudolentemente al fine di trarre vantaggio per la Banca (ad esempio mediante un meccanismo fraudolento del conteggio delle commissioni) e/o alterazione di un sistema informatico o telematico che produce un trasferimento di valuta virtuale al fine di trarre vantaggio, per la Banca (ad esempio mediante un meccanismo fraudolento del conteggio delle commissioni);
- g. con riferimento alle carte prepagate, vendita o distribuzione ai clienti di apparecchiature e dispositivi per effettuare pagamenti digitali alterati fraudolentemente al fine di trarre vantaggio per la Banca (ad esempio mediante un meccanismo fraudolento del conteggio delle commissioni) e/o alterazione di un sistema informatico o telematico che produce un trasferimento di valuta virtuale al fine di trarre vantaggio, per la Società (ad esempio mediante un meccanismo fraudolento del conteggio delle commissioni).
- h. Trasferimento all'estero di denaro, beni o altre utilità provenienti da delitto, ovvero compimento in relazione ad essi di altre operazioni, in modo da ostacolare operazioni di sequestro preventivo/sequestro/confisca.
- i. Utilizzo di applicativi di tesoreria alterati fraudolentemente al fine di trarre un vantaggio indebito per la società in sede di gestione dei pagamenti nell'ambito dell'attività di gestione bonifici estero.
- j. Trasferimento fraudolento di denaro, beni o altre utilità mediante operazioni con assegni al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, o in materia di documentazione antimafia ovvero di agevolare la commissione di uno dei reati di riciclaggio.
- k. Trasferimento fraudolento di denaro, beni o altre utilità mediante operazioni di bonifico al fine di eludere le disposizioni di legge in

materia di misure di prevenzione patrimoniali o di contrabbando, o le disposizioni antimafia, ovvero di agevolare la commissione di uno dei reati di

Ufficio Tesoreria

3. **Gestione Servizi di investimento**, in relazione al quale potrebbe sussistere il rischio di trasferimento fraudolento di denaro, beni o altre utilità mediante operazioni di investimento o in fase di apertura di posizioni di investimento.

Ufficio Antiriciclaggio

4. **Antiriciclaggio**, in relazione al quale sono state rilevate le seguenti attività sensibili:
 - a. nell'ambito di un più ampio disegno criminoso e non esercitando correttamente le sue funzioni, la Funzione Antiriciclaggio potrebbe concorrere ad attribuire fittiziamente a persone diverse dal titolare effettivo la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, o disposizioni in materia antimafia, ovvero di agevolare la commissione di uno dei delitti di cui agli artt. 648, 648 bis e 648 ter (es. omessa segnalazione di operazioni sospette e approvazione dell'operatività di un cliente per trasferire fittiziamente beni ad altri, al fine di elidere l'applicazione della confisca e degli altri mezzi di prevenzione patrimoniale, ovvero al fine di agevolare la commissione dei delitti di ricettazione, riciclaggio e autoriciclaggio).
 - b. La Funzione Antiriciclaggio, nella gestione delle proprie attività, potrebbe agevolare fraudolentemente il trasferimento di denaro, beni o altre utilità provenienti da delitto, ovvero il compimento in relazione ad essi di altre operazioni, in modo da ostacolare operazioni di sequestro preventivo/sequestro/confisca. La Funzione Antiriciclaggio potrebbe favorire l'approvazione dolosa dell'operatività di un cliente a seguito della gestione non corretta delle operazioni di adeguata verifica ordinaria / semplificata / rafforzata per agevolare lo stesso in operazioni di trasferimento di beni, valori o denaro al fine di eludere l'applicazione della confisca e degli altri mezzi di prevenzione patrimoniale, o le disposizioni antimafia, ovvero al fine di agevolare la commissione dei delitti di ricettazione, riciclaggio e autoriciclaggio.

Ufficio Economato

5. **Nella fase di acquisti beni e servizi**, la Banca potrebbe porre in essere operazioni di interposizione reale o fittizia, attraverso una serie di manipolazioni

e falsificazioni che ostacolano la tracciabilità del denaro e dei beni, con lo scopo di eludere l'applicazione delle norme in materia di prevenzione patrimoniale o di contrabbando, o le disposizioni antimafia, o di agevolare la commissione dei reati di ricettazione, riciclaggio o impiego di beni di provenienza illecita.

Area Crediti

6. **Nella fase di concessione credito alla clientela**, la Banca potrebbe porre in essere dolosamente attività che facilitano l'occultamento o il trasferimento di beni illeciti al fine di eludere misure di prevenzione patrimoniali o disposizioni antimafia.

3. Il sistema dei controlli e i presidi a mitigazione dei rischi reato

Per ognuna delle attività sensibili identificate sono stati individuati i sistemi dei controlli e i presidi in essere a mitigazione dei rischi reato in riferimento ai reati di frode e falsificazione di strumenti di pagamento diversi dai contanti nonché di Trasferimento fraudolento di valori, previsto dall'art. 512-bis c.p.

Per tutti

Presidi trasversali a tutti i processi interessati

- I processi della Banca sono assoggettati, oltre che ai controlli di linea, formalizzati e tracciati attraverso la piattaforma CSD, a controlli di secondo e terzo livello da parte della FAC (funzioni aziendali di controllo), esternalizzate alla Capogruppo, e dai referenti interni delle FAC medesime.
- Il Regolamento Generale descrive i principali compiti di ciascuna unità organizzativa. Il documento Deleghe di Potere disciplina le deleghe di firma e di spesa sia in ordine alla concessione del credito sia con riferimento all'operatività su prodotti bancari e finanziari. Il sistema delle utenze informatiche ricalca il sistema delle deleghe di potere. La coerenza tra il documento Deleghe e le abilitazioni nel sistema informatico della Banca è assoggettato a controlli periodici ed in occasione di modifica delle deleghe assegnate.
- E' stato adottato e viene periodicamente aggiornato il Codice Etico;
- Il personale della Banca e gli esponenti aziendali usufruiscono, nel continuo, di percorsi formativi riferiti sia di natura tecnico/operativo correlati ai

processi aziendali, sia di natura trasversale (ad. es. Whistleblowing, D.lgs. 231/01);

- Le Succursali sono assoggettate ai controlli periodici dell'Ufficio Controlli Permanenti che, sulla base del Piano annuale, provvede a visite ispettive in loco presso le Succursali e, su richiesta della Direzione, presso le Aree e gli Uffici di Direzione.
- Le operazioni dei dipendenti sono oggetto di controllo periodico da parte dell'Ufficio Controlli Permanenti.
- Il sistema informativo è gestito in full outsourcing da parte di Allitude S.p.A. con conseguenti possibilità di intervento estremamente limitate da parte della Banca.
- La Banca ha recepito il corpus normativo emanato dalla Capogruppo (Policy, Regolamenti e Procedure) in relazione a tutti gli ambiti della normativa antiriciclaggio (adeguata verifica, monitoraggio dell'operatività dei clienti, segnalazione di operazioni sospette). Vengono inoltre emanate dalla Cassa e rese accessibili a tutto il personale disposizioni operative in merito a specifici ambiti operativi riferiti al processo.
- È stato adottato l'applicativo Transaction Monitoring (Modulo SAS AML di Transaction & Monitoring), integrato nel sistema gestionale della Cassa, dedicato al controllo sulla movimentazione della clientela e alla contestuale individuazione di operazioni suscettibili di sospetto di riciclaggio o di finanziamento del terrorismo. La gestione degli alert generati dalla procedura avviene da parte di figure specificamente individuate (ad. es. settorista AML); è previsto il coinvolgimento del Referente AML e del suo staff che hanno visibilità su tutti gli alert generati e vengono coinvolti nella gestione di quelli che gli vengono loro trasferiti; l'Ufficio Presidi AML di Capogruppo ha la visibilità di tutti gli alert, ne gestisce alcune specifiche tipologie nonché quelli oggetto di trasferimento. L'intero processo è tracciato in un apposito workflow.
- Sono in essere automatismi e controlli finalizzati a verificare la corrispondenza del cliente e dei soggetti collegati al cliente con legami anagrafici di delega, rappresentanza e titolarità effettiva.
- In fase di on boarding del cliente è previsto il controllo incrociato con le liste (black list, sanction list, PEC/Crime) aggiornate nel continuo dal provider esterno individuato a livello di Gruppo; i dati presenti nelle liste vengono incrociati quotidianamente con le anagrafiche censite dalla banca. Vengono prodotte delle evidenze da gestire al fine di verificare se si tratti di match effettivi o di falsi positivi. La corretta esitazione dei match è oggetto

di controlli di primo e secondo livello.

- Il censimento anagrafico del cliente, al quale sono correlati i prodotti allo stesso vendibili ed al quale sono associati i parametri sulla base dei quali avviene il transaction monitoring, è caratterizzato da specifici vicoli procedurali (ad. es. ad ogni tipologia di controparte è associato un set minimo di dati ed informazioni da acquisire e da documentare mediante archiviazione ottica in procedura) che si concretizzano in un valido presidio in ordine alla corretta identificazione della clientela.
- Per i servizi esternalizzati viene seguito, con il coinvolgimento della Capogruppo, uno specifico processo, articolato in varie fasi e disciplinato dalla normativa emanata a livello di Gruppo e recepita dalla Cassa. È prevalente il ricorso alle esternalizzazioni infra gruppo.
- I clienti, attraverso l'invio degli estratti conto e degli scalari, della documentazione periodica prevista ai sensi della normativa sulla trasparenza bancaria e mediante l'accesso alla piattaforma In Bank (qualora attivata) hanno accesso nel continuo alla movimentazione dei propri rapporti e dispongono pertanto degli strumenti per rilevare eventuali anomalie.
- Presso la Cassa è presente l'Ufficio Reclami che gestisce i reclami, le lamentele, gli esposti ed i ricorsi (ABF, ACF, Ivass) della clientela in coerenza con la normativa esterna ed interna (Regolamento/Procedura/Controlli di Primo livello) e mediante l'utilizzo di un work flow, condiviso con la Capogruppo, nel quale vengono tracciate le fasi del processo.

Ufficio Marketing

Processo Gestione della domanda e gestione portafoglio progetti

- Il processo di sviluppo e gestione di nuovi prodotti avviene nell'ambito della cornice regolamentare emanata a livello di Gruppo con il coinvolgimento delle funzioni operative e di controllo della Capogruppo; tali regolamenti (ad. es. Regolamento sulla Trasparenza delle Operazioni e dei Servizi Finanziari, Regolamento di Gruppo in materia di nuovi prodotti) sono stati recepiti dalla Banca, pubblicati nella intranet aziendale e sono consultabili da tutto il personale;
- Dal punto di vista contabile, la creazione di nuovi conti, destinati alla contabilizzazione di eventuali proventi a favore della banca derivanti dalla fraudolenta alterazione di dispositivi o da attività comunque illecite, segue un iter formalizzato e rafforzato; sono inoltre previste le verifiche da parte del Collegio Sindacale e della società di revisione in merito alle voci di bilancio.

Ufficio Back Office

Processo Incassi e pagamenti

Pagamento pensioni

- La creazione e gestione delle relative utenze avviene attraverso il portale Buonconsiglio, gestito dalla Capogruppo Cassa Centrale, nel quale vengono inseriti i dati del titolare della pensione e l'IBAN del cc da accreditare. Il servizio prevede l'apertura di un rapporto di c/c intestato al beneficiario su cui appoggiare la pensione. Il contratto con l'Ente Previdenziale è sottoscritto dalla Capogruppo con adesione delle Banche Affiliate.
- In caso di decesso, l'INPS informa la Banca e l'Ufficio Back Office/CCB che procede alla restituzione delle rate non dovute, dopo aver informato la Succursale competente. Quest'ultima, qualora venga informata direttamente del decesso, dispone il blocco del conto e avvisa l'Ufficio Back Office per la restituzione, al competente Ente Previdenziale, dei ratei non dovuti.
- La piattaforma Buonconsiglio, per il tramite della Capogruppo, effettua un controllo informatico tra intestatario del conto e generalità del beneficiario del trattamento pensionistico. In caso di discordanza, la Capogruppo avvisa la Succursale ai fini della corretta intestazione del c/c al beneficiario del trattamento pensionistico. L'Ufficio Back Office gestisce i flussi disposti dagli enti competenti.
- Gli applicativi attraverso i quali avviene il pagamento dei trattamenti pensionistici sono gestiti in full outsourcing attraverso la Capogruppo e l'outsourcer informatico Allitude S.p.A.

Ufficio Back Office

Gestione bonifici area euro ed estero

Oltre ai presidi trasversali ed a quelli indicati con specifico riferimento al processo Antiriciclaggio, risultano in essere i seguenti presidi:

- Il processo di gestione dei bonifici in entrata ed uscita è contenuto nel Regolamento Incassi e Pagamenti e nelle Disposizioni attuative del processo.
- Il soggetto che inserisce il bonifico non può partecipare all'iter autorizzativo.
- L'autorizzazione all'invio bonifici in uscita, come previsto dal documento "Deleghe di potere" avviene in due fasi: 1. (Eccetto per i bonifici SCT disposti allo sportello, Prima autorizzazione: quale attività di controllo di merito; 2. Seconda autorizzazione: di tipo tecnico/informatico che ha lo scopo di verificare l'avvenuto rilascio dell'autorizzazione di merito (ove richiesta), di

controllare la correttezza formale dei messaggi da inviare e di disporre l'immissione in Rete.

- I soggetti abilitati alla prima ed alla seconda autorizzazione ed i limiti di importo/tipologia di bonifico al di sotto dei quali sono previste esenzioni sono stabiliti dalle Deleghe di Potere.
- Relativamente al servizio di tramitazione nel regolamento dei sistemi di pagamento (Target2, EBA, SEPA), è stato adottato un sistema informativo dotato di diagnostici on line sia per il riscontro delle generalità dei nominativi e dei soggetti sia per il riscontro delle disposizioni in entrata e in uscita, riconducibili alla propria operatività.
- Una volta completato l'iter autorizzativo, il bonifico viene immesso nella rete interbancaria attraverso la Capogruppo ed i suoi dati non risultano modificabili.
- I bonifici possono essere disposti da In bank, da parte dei soggetti già clienti, oppure da sportello, anche da clienti occasionali. Sia l'instaurazione del rapporto continuativo che l'operazione occasionale sono assoggettati al processo di adeguata verifica ai fini AML in conformità con la regolamentazione interna ed esterna.
- Per i bonifici disposti allo sportello, al cliente viene rilasciata la contabile dell'operazione, siglata dall'operatore.
- Sia per i bonifici in ingresso che per i bonifici in uscita è previsto il controllo automatico con le liste (black list, embargo etc). In presenza di match è necessario provvedere all'esitazione, previo svolgimento delle necessarie attività di verifica. Per i bonifici in ingresso o uscita da/verso paesi assoggettati ad embargo o a regimi sanzionatori, la Succursale viene avvisata a mezzo mail dall'Ufficio Back Office in merito al blocco; quindi, si interfaccia con il cliente per acquisire le informazioni e i documenti necessari al fine di lavorare la disposizione. Qualora tale fase di approfondimento abbia esito negativo, la disposizione viene respinta.
- Per i bonifici verso/da paesi ad alto rischio è previsto uno specifico iter, che si compone di una fase istruttoria e di una fase autorizzativa, gestite da soggetti diversi e tracciate nel sistema informativo.
- I rapporti con clienti residenti in paesi ad alto rischio devono essere autorizzati dalla Direzione Generale della Banca e sono assoggettati ad un processo di adeguata verifica rafforzata.
- Esiste un servizio esterno gestito dall'outsourcer informatico Allitude S.p.A. che, in presenza di bonifico che, in base alle impostazioni dell'algoritmo sottostante, risulta potenzialmente a rischio frode, verifica chiamando

direttamente il cliente, entro 2 h dall'inserimento della disposizione da In Bank, se è stato effettivamente disposto dal cliente stesso. Le risultanze dell'interlocuzione con il cliente vengono inviate a mezzo mail all'Ufficio Back Office della banca che gestisce l'operazione a seconda delle casistiche.

- I bonifici disguidati (incompleti, su conti estinti etc) vengono gestiti con un approccio caso per caso dall'Ufficio Back Office.
- La Banca ha aderito al servizio di verifica del beneficiario (VoP) che in tempo reale verifica la corretta corrispondenza tra nome del beneficiario e le relative coordinate IBAN utilizzate nella disposizione di pagamento esponendo al cliente l'esito della verifica prima della conferma dell'operazione in aderenza alle previsioni del Regolamento UE 886/2024;
- Sono previsti controlli di primo, secondo e terzo livello in relazione al processo incassi e pagamenti
- La Banca è aderente indiretta alla rete interbancaria e allo swift per il tramite dei servizi messi a disposizione dalla Capogruppo e dall'outsourcer informatico, opportunamente disciplinati da uno specifico contratto di servizio.

Ufficio Back office

Emissione carte di credito, di carte prepagate e di carte di debito

- Sono state emanate e sono consultabili nella intranet aziendale disposizioni operative riferite alle fasi di emissione/sostituzione/blocco/estinzione/gestione operazioni fraudolente con riferimento alle carte di debito e di credito, nonché in merito alle modalità di accesso e di utilizzo delle piattaforme / circuiti di pagamento;
- Il sistema informativo con cui sono gestiti i servizi di monetica prevede blocchi a sistema.
- La Banca colloca carte di debito prodotte dalla Capogruppo Cassa Centrale secondo il catalogo prodotti tempo per tempo vigente ed associate all'ABI della Banca, la cui denominazione è presente sul dispositivo plastico.
- La Banca risulta estranea al processo di creazione del prodotto sia dal punto di vista informatico e dei presidi di sicurezza sia dal punto di vista commerciale.
- Per tutte le carte sono impostati limiti operativi per tipologia di operatività (prelievi, POS). Per l'operatività e-commerce è prevista la creazione di un apposito codice che deve essere inserito in fase autorizzazione della

transazione; le carte di nuova emissione sono abilitate ai circuiti esteri e sono dotate di funzionalità contact less.

- Presso ogni succursale è presente una giacenza di carte di debito, che vengono trasmesse direttamente dalla Capogruppo attraverso l'Ufficio Economato. Quest'ultimo inserisce i dati delle carte nel sistema gestionale della banca come valori in bianco. Ogni succursale, al ricevimento delle carte di propria spettanza, attraverso una scheda lavori, chiede che le carte stesse vengano caricate come valori in bianco della Succursale. L'ufficio Controlli permanenti, in fase di controlli ispettivi, verifica la corrispondenza della materialità delle carte con i valori in bianco che risultano contabilizzati.
- Il collocamento della carta avviene attraverso il sistema gestionale della banca. In fase di emissione quest'ultimo effettua dei controlli incrociati con la CAI bloccando l'emissione qualora riscontri dei match positivi.
- In sede di consegna, il cliente riceve due buste separate, una con la carta e l'altra con il PIN.
- Sono previsti controlli centralizzati antifrode in merito alle transazioni eseguite, che possono comportare il blocco dell'operatività.
- L'operatività a mezzo carte di debito rientra nel monitoraggio AML condotto attraverso l'applicativo di transaction monitoring.
- E' previsto un sistema di alert che avverte il cliente delle transazioni eseguite con la carta al fine di consentire il tempestivo blocco in presenza di frodi.
- Gli addebiti derivanti dall'utilizzo della carta di debito sono registrati nell'estratto conto che il cliente riceve a seconda della periodicità prescelta.
- La Banca colloca carte prepagate emesse dalla Capogruppo Cassa Centrale secondo il catalogo prodotti tempo per tempo vigente (carta ricarica, carte Evo e OOM+,...).
- La Banca risulta quindi estranea al processo di creazione del prodotto sia dal punto di vista informatico e dei presidi di sicurezza sia dal punto di vista della determinazione delle caratteristiche del prodotto. E' la società emittente a stabilire massimali e numero massimo di carte distribuibile a ciascun utente.
- Il processo di collocamento/vendita delle carte prepagate avviene attraverso il sistema gestionale della Banca che colloquia con la piattaforma Buon Consiglio, gestita dalla Capogruppo. In fase di emissione i dati della carta da collocare (numero, busta etc) e i dati del titolare

vengono inseriti in tale procedura Buonconsiglio ai fini dell'emissione ed attivazione.

- Presso ogni succursale è presente una giacenza di carte prepagate, che vengono trasmesse direttamente dalla Capogruppo attraverso l'Ufficio Economato. Quest'ultimo inserisce i dati delle carte nel sistema gestionale della banca come valori in bianco. Ogni succursale, al ricevimento delle carte di propria spettanza, attraverso una scheda lavori, chiede che le carte stesse vengano caricate come valori in bianco della Succursale. L'ufficio Controlli permanenti, in fase di controlli ispettivi, verifica la corrispondenza della materialità delle carte con i valori in bianco che risultano contabilizzati.
- I controlli antiriciclaggio in merito alla movimentazione sulle carte prepagate vengono svolti da apposite strutture della Capogruppo e dai settoristi AML attraverso la gestione delle evidenze generate dalla procedura Transaction monitoring.
- La Banca colloca carte di credito Nexi con brand CCB a saldo. La Succursale raccoglie la richiesta del Cliente di emissione carta, inserendola nel sistema gestionale della Banca. In questa fase l'operatore/responsabile di Succursale verifica i requisiti per procedere con la richiesta di emissione della Tessera, alla quale è sempre associato un fido.
- I plafond delle singole carte sono assoggettati al sistema delle Deleghe di potere;
- Una funzione batch giornaliera invia a Nexi un flusso informativo riferito alle richieste di emissione inserite nella giornata. Nexi, per il tramite della Capogruppo, invia quindi al Back Office della Banca le buste contenenti la carta di credito e le istruzioni per l'attivazione. Il PIN viene invece reperito direttamente dal cliente su sito Nexi. L'Ufficio Back Office trasmette a ciascuna succursale le carte di competenza.
- La Banca non svolge né può svolgere alcun ruolo in merito alla configurazione della carta di credito ed alle sue caratteristiche informatiche e di sicurezza.
- Per il corretto utilizzo delle carte sono previste da parte della società emittente le carte presidi di controllo nel continuo, in grado di evidenziare operatività anomala tali da consentire il blocco operativo della carta.
- È utilizzato un software specifico per le attività di Fraud Detection in ambito Internet Banking, gestito da Allitude in accordo con la struttura organizzativa che gestisce, per la Banca, le tematiche di Sicurezza.
- È presente un servizio di monitoraggio delle operazioni di pagamento e-

commerce effettuate con le carte prepagate e di debito. L'applicativo interno utilizzato per effettuare questo monitoraggio analizza le operazioni effettuate dagli utenti, attribuendo a tali operazioni uno score. Questo rating alimenta uno score delle attività complessivamente effettuate con una determinata carta prepagata. Al superamento di determinati limiti (limiti aggregati di spesa, transazioni singole di importi troppo elevati, eccessivo numero di transazioni effettuate in un determinato lasso temporale...), si presuppone il rischio anti-frode e pertanto viene posto un blocco sulla carta (che sarà successivamente sbloccabile dall'utente qualora il sospetto di

- I sistemi utilizzati per i pagamenti prevedono la segregazione delle utenze.
- Sono presenti Contratti di servizio con le società terze che supportano la Banca nella distribuzione dei servizi di pagamento elettronico rivolti alla clientela e nel corrente funzionamento operativo, in cui sono debitamente identificati ruoli operativi, presidi di sicurezza e rispettivi impegni atti a garantire lo svolgimento di un servizio conforme ai disposti normativi vigenti tempo per tempo.

Ufficio Back office

Ulteriori apparecchiature e dispositivi

- L'acquisto degli ATM/ATM evoluti è compreso nel servizio esternalizzato "Servizio ATM" di Allitude Spa cui la Banca ha aderito. Il servizio gestisce, oltre che l'approvvigionamento anche gli aspetti della sicurezza fisica e logica ed il monitoraggio proattivo avanzato dei sistemi. Sono consolidati in Allitude tutti i rapporti contrattuali con controparti esterne al Gruppo, il loro ingaggio in caso di problematiche ed il monitoraggio delle performance in conformità ad apposite nuove clausole contrattuali che regolano tempi di intervento, SLA e penali in caso di mancato rispetto.
- L'acquisto delle apparecchiature che consentono il ricircolo del contante è effettuato dalla Banca mediante l'utilizzo di contratti aventi previsioni conformi alle disposizioni di vigilanza; è in essere un programma di manutenzione volto ad assicurare, nel continuo, che i software installati siano conformi alle prescrizioni normative
- Il rilascio agli esercenti degli apparati POS è regolato da uno specifico contratto di servizio che responsabilizza l'esercente nella tenuta e custodia del dispositivo rispetto al possibile rischio di installazione di apparati capaci di clonare i dati delle carte della clientela.

Ufficio Tesoreria

Gestione Servizi di Investimento

Oltre ai presidi trasversali ed a quelli indicati con specifico riferimento al processo Antiriciclaggio, con particolare riferimento al sistema di transaction monitoring, risultano i seguenti presidi:

- In fase di apertura di un dossier titoli viene svolto il processo di adeguata verifica con acquisizione di informazioni e documenti sul cliente, titolare effettivo, esecutore, sull'origine dei fondi, su scopo e natura del rapporto;
- Sono previsti controlli di linea assegnati alle strutture organizzative della Banca relativamente alla gestione delle richieste di trasferimento titoli e/o disponibilità finanziarie, con acquisizione di specifica documentazione di supporto (es. atti notarili di donazione,...), secondo le disposizioni disciplinate da regolamenti ed ordini di servizio a supporto, tempo per tempo vigenti.
- Vengono disposti blocchi operativi apposti e gestiti dall'Ufficio Antiriciclaggio sui rapporti oggetto di sequestro/sequestro preventivo/confisca ed intestazione al FUG.
- La regolamentazione esterna ed interna sancisce il divieto di intestazione fittizia di rapporti o di accensione di rapporti in capo a soggetti che presentano opacità nella catena partecipativa (trust, fiduciarie etc).
- Per l'apertura o il mantenimento di rapporti in capo a determinate categorie di soggetti che presentano un elevato livello di rischio AML è previsto il processo di Adeguata verifica rafforzata, con coinvolgimento di Direzione e referente AML,
- Sono previsti controlli a distanza da parte della Capogruppo in merito a specifici KRI tempo per tempo definiti.

Ufficio Antiriciclaggio

Processo Antiriciclaggio - Valutazione e reporting operazioni sospette - gestione attività antiriciclaggio

- La funzione antiriciclaggio è externalizzata alla Capogruppo. Presso la banca è collocata la figura del referente AML che opera in stretto raccordo e sotto la supervisione della funzione externalizzata.
- Tanto le attività riferite al processo (adeguata verifica, segnalazione di operazioni sospette, tenuta AUI etc) quanto le attività di verifica e controllo sono svolte, oltre che dal referente interno, anche dalla funzione AML externalizzata, pertanto, eventuali condotte "fraudolente" poste in essere a livello locale sono comunque oggetto di ulteriore attività di controllo anche

da parte della Capogruppo. Il processo AML è inoltre assoggettato alle verifiche della Funzione Internal Auditing esternalizzata alla Capogruppo;

- Le transazioni riferite ai clienti che transitano nel sistema gestionale della banca vengono automaticamente registrate nell'Archivio Unico Informatico (AUI), eventuali interventi su quest'ultimo restano comunque tracciati, ragione per la quale il rischio di eventuali manipolazioni appare sostanzialmente remoto.;
- E' stata adottata uno specifico applicativo per il monitoraggio delle transazioni della clientela. Tale procedura, denominata "Transaction Monitoring", è dedicata al controllo sulla movimentazione della clientela e alla contestuale individuazione di operazioni suscettibili di sospetto di riciclaggio o di finanziamento del terrorismo. Eventuali anomalie nella gestione delle evidenze generate dalla procedura di transaction monitoring sono oggetto di controllo sia da parte del referente AML che da parte della funzione AML esternalizzata.;
- L'intero processo è regolamentato in modo dettagliato. Il personale della funzione e quello di rete beneficiano nel continuo di interventi formativi finalizzati a fornire competenze tecniche, cultura e consapevolezza nella gestione delle attività afferenti il processo AML;
- Il monitoraggio della clientela avviene anche attraverso il periodico aggiornamento dell'adeguata verifica, la cui frequenza è determinata dal profilo di rischio del cliente.
- Generalmente i provvedimenti di sequestro preventivo/sequestro/confisca sono notificati alla Banca su una casella di posta pec gestita e monitorata non dall'Ufficio Antiriciclaggio, ma dall'Ufficio Segreteria, pertanto eventuali attività tese ad agevolare il trasferimento fraudolento di fondi oggetto di tali provvedimenti potrebbe tradursi in ulteriori richieste da parte dell'autorità procedente che transiterebbero sempre su tale casella di posta comportando l'attivazione di processi di escalation anche nella forma di whistleblowing. L'intestazione dei rapporti al FUG viene gestito da un ulteriore ufficio.

Ufficio Economato

Processo di Acquisto di beni e servizi

Oltre ai presidi trasversali ed a quelli indicati con specifico riferimento al processo Antiriciclaggio, risultano i seguenti presidi:

- La tracciabilità delle attività correlate agli acquisti, l'archiviazione della documentazione e il rispetto di adeguati livelli autorizzativi è garantita

dall'utilizzo di Ivalua come applicativo di gestione del processo della spesa. Nell'applicativo vengono tracciate le diverse fasi del processo (inserimento richiesta di acquisto, validazione, presa in carico, contrattualizzazione, fatturazione, autorizzazione al pagamento).

- La Banca ha adottato e pubblicato nella intranet aziendale il set regolamentare emanato dalla Capogruppo costituito dal Regolamento di Gruppo per la gestione della spesa dalla Procedura di Gruppo per la gestione della spesa e dai Controlli di Gruppo relativi al processo.
- La procedura standard di scelta del fornitore è quella della Gara (con la partecipazione di almeno 3 fornitori), mentre il ricorso alla negoziazione diretta, comunque con il coinvolgimento di più fornitori, deve essere giustificato dalla sussistenza di specifiche esigenze. La procedura di gara è obbligatoria qualora la controparte sia un Soggetto Collegato ex Circ. Bankit 285/13 oppure un soggetto iscritto nel Registro ex art. 136 TUB.
- È presente un registro Fornitori di Gruppo. Il censimento è corredato dall'acquisizione di un completo set documentale (Durc, Dichiarazione per Presa visione, liste crime/terr per fornitori strategici, etc.). L'iscrizione nell'albo può avvenire soltanto all'esito di un processo di accreditamento volto a valutare i requisiti etici, di solidità economico – finanziaria, di sostenibilità e di professionalità del fornitore. È prevista la suddivisione della tipologia dei fornitori e relativa differenziazione dei controlli che vengono effettuati nei loro confronti sulla base del livello di rischio e della tipologia di fornitura.
- Per acquisti di importo superiore ad una soglia determinata a livello di Gruppo è previsto il coinvolgimento del Servizio Procurement della Capogruppo.
- È presente una matrice di spesa nella quale alle diverse voci sono associati i procuratori in coerenza con i limiti definiti dal documento Deleghe di Potere.
- Sono presenti, anche se non ancora incorporati nella procedura IVALUA, controlli volti a verificare il rispetto del budget con riferimento alle diverse categorie di spesa; ad ogni Ordine di acquisto è associato obbligatoriamente una categoria di spesa da addebitare che è a sua volta associata ad un conto contabile.
- Ogni acquisto prevede il coinvolgimento e l'autorizzazione di diverse figure secondo un criterio di segregazione.
- Il pagamento di una fattura presuppone necessariamente l'inserimento di un ordine in Ivalua ed il completamento delle varie fasi del processo.
- Sono previsti, vengono svolti e tracciati nell'apposita procedura informatica specifici controlli di primo livello in merito a: verifica di congruità ex post

delle spese classificate come "piccole"; verifica circa il corretto utilizzo degli attestati (particolare iter semplificato che deve essere mantenuto al di sotto dell'10% in controvalore degli acquisti); verifica di coerenza dei profili di "procuratore" all'interno di Ivalua con il documento "Deleghe di Potere"; verifica che negli acquisiti siano intervenuti almeno due soggetti distinti (richiedente e procuratore); Albo Fornitori: verifica documenti fornitori marginali e ordinari

- Per i dipendenti, la nota spese viene autorizzata dal Responsabile del dipendente che richiede il rimborso delle spese. La procedura informatica "Concur", interna a SAP, impone all'utente di caricare gli scontrini o i giustificativi di spesa che il Responsabile può quindi verificare in fase di autorizzazione.

Area Crediti

Processo di concessione del credito

Oltre ai presidi trasversali ed a quelli indicati con specifico riferimento al processo Antiriciclaggio, risultano i seguenti presidi:

- Il processo di concessione del credito è disciplinato in ogni fase dalla Regolamentazione di Gruppo, recepita dalla Banca, e dalle disposizioni attuative del processo. La regolamentazione adottate è pubblicata nella intranet aziendale ed è accessibile a tutto il personale;
- Ogni domanda di fido è tracciata nella procedura PEF, presente sull'applicativo SiBank, nel quale sono formalizzate le varie fasi del processo (domanda, istruttoria, pareri, delibera). Tale procedura è integrata con il sistema delle deleghe e calcola automaticamente l'organo deliberante. Le delibere c.d. "tecniche", relative a variazioni tecniche o che comunque comportano una bassa incidenza in termini di potenziale aggravio del rischio sono analiticamente disciplinate dal punto di vista regolamentare, e riservate a competenza deliberativa di specifici organi deliberanti.
- Nelle diverse unità informative nelle quali è articolata la PEF vengono tracciate e documentate le valutazioni poste a base dell'istruttoria e della concessione (finalità, destinazione dei fondi, origine di eventuali fondi propri).
- Nella pressoché generalità delle casistiche ogni pratica di fido prevede il coinvolgimento minimo di due soggetti (proponente e deliberante); per le pratiche per le quali è disposta l'istruttoria di secondo livello è previsto il coinvolgimento minimo di ulteriori due soggetti (addetto ufficio analisi e istruttoria e responsabile Ufficio Analisi Istruttoria) o di ulteriori soggetti

qualora la pratica non rientri nelle autonomie del Responsabile dell'Ufficio Analisi e Istruttoria.

- La procedura PEF recepisce anche i dati presenti nel sistema gestionale in merito al profilo di rischio AML e richiede un iter rafforzato con il coinvolgimento del referente AML in presenza di profili di rischio ALTO 100 (per pratiche di aumento fido o nuova concessione), con eventuale attribuzione della valutazione all'organo deliberante. In ogni pratica di fido è comunque presente un'unità informativa volta alla valutazione del rischio riciclaggio.
- La valutazione dei beni posti a garanzia è disciplinata dalla regolamentazione interna anche in ordine alle percentuali di scarto da applicare.
- Le perizie estimative riferite a beni immobili vengono affidate a periti terzi indipendenti iscritti in un apposito albo e convenzionati direttamente dalla Capogruppo.
- Il valore di beni mobili posti a garanzia può essere oggettivo (ad. esempio per i pegni di liquidità) oppure, in presenza di titoli, è determinato sulla base del valore nominale, il valore di mercato è soggetto a monitoraggio costante al fine di intercettare diminuzioni di valore e conseguenti necessità di integrazione della garanzia, in ulteriori casistiche (ad. es. pegni di merce) il valore è attribuito sulla base di perizie redatte da terzi estimatori indipendenti.
- L'erogazione del credito e la concessione di operatività sui rapporti sono di competenza della Segreteria Crediti, che non ha poteri deliberativi e che, in fase di erogazione, svolge ulteriori attività di verifica.
- La provenienza dei fondi del cliente è verificata nell'ambito del processo di adeguata verifica AML ed è altresì presidiato dal sistema di Transaction monitoring, integrato nel gestionale SiBank e che genera, con riferimento ad operatività potenzialmente anomala, specifiche evidenze da valutare anche nell'ottica di un'eventuale segnalazione di operazione sospetta.