– PARTE SPECIALE U –

REATI FRODE E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

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, comma 2 c.p.

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.

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 dei processi aziendali ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-*octies* del D. Lgs. 231/2001.

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:

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;

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 dei pagamenti nell'ambito del processo di gestione tesoreria Enti Pubblici
    b. 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;
    c. 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;
    d. 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;
    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).

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:

- La Banca ha adottato normativa interna in cui sono riportati i controlli operativi applicati nella gestione delle attività e in particolare:
  - controllo operazioni carte;
  - controllo e gestione blocco / sblocco per violazione delle regole;
  - controllo conti.
- La Banca ha adottato normativa interna che riporta le modalità di accesso e di utilizzo delle piattaforme / circuiti di pagamento.
- La Banca ha recepito il "Regolamento sulla Trasparenza delle Operazioni e dei Servizi Finanziari".
- La Banca ha recepito il "Regolamento di Gruppo in materia di nuovi prodotti" che definisce gli step da seguire in fase di sviluppo di un nuovo prodotto.
- La Banca adotta normativa interna relativamente ai processi di liquidità.
- La Banca adotta normativa interna relativamente alla gestione delle attività di tesoreria.
- La Banca adotta normativa interna relativamente all'attività di tesoreria Enti.
- La Banca adotta normativa interna per la gestione delle attività di pagamenti Estero.
- Il sistema informativo con cui sono gestiti i servizi di monetica prevedono blocchi a sistema.
- 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 e-commerce 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 frode risultasse infondato).

- I sistemi utilizzati per i pagamenti prevedono la segregazione delle utenze.
- Il portale informatico utilizzato per la gestione delle operazioni di Tesoreria permette il controllo e la verifica delle contabilizzazioni e dei movimenti di tesoreria.
- L'infrastruttura tecnologica utilizzata per l'erogazione del servizio di Tesoreria Enti è strutturata in osservanza delle regole definite dal TUEL. L'operatore non ha la possibilità di forzare operazioni non conformi poiché l'infrastruttura prevede blocchi a sistema.
- Relativamente al servizio di tramitazione nel regolamento dei sistemi di pagamento (Target2, EBA, SEPA), adozione di un sistema informativo che sia 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.
- La procedura di tesoreria, nell'arco della giornata contabile, identifica secondo cicli prestabiliti le operazioni destinate agli enti gestiti, prende in carico i bonifici ricevuti dalla rete interbancaria e accredita i rispettivi rapporti dei beneficiari.
- Sono presenti presidi procedurali (verifica dell'esistenza del rapporto del beneficiario, dell'esistenza dell'esercizio aperto e di altri elementi formali) affiancati da controlli di linea in carico agli operatori.
- L'erogazione delle pensioni segue le procedure della Banca previste per la gestione delle attività di Tesoreria.
- Controlli di linea assegnati alle strutture organizzative della Banca relativamente alla gestione dei pagamenti (e dei relativi regolamenti) eseguiti con corrispondenti estere.
- Controlli finalizzati a verificare la corrispondenza del cliente e dei soggetti collegati al cliente con legami anagrafici di delega, rappresentanza e titolarità effettiva - rispetto ai nominativi presenti nelle liste sensibili ai fini antiriciclaggio e di contrasto al finanziamento del terrorismo.
- Aggiornamento dell'elenco dei nominativi contenuti nelle liste oggetto di monitoraggio con frequenza giornaliera attraverso lo scarico dai database dell'info-provider esterno.

- Il soggetto che inserisce gli ordini di pagamento non può autorizzarli, in quanto tale attività deve essere svolta da un secondo soggetto avente potere autorizzativo (principio di segregazione).
- Previsione di un processo di verifica e di autorizzazione sul pagamento richiesto per gli ordini di importo superiore a determinate soglie.
- Blocco automatico della richiesta di pagamento, sul sistema informativo aziendale utilizzato per la gestione delle richieste di pagamento, laddove il beneficiario del pagamento sia un soggetto diverso dalla controparte (il sistema, infatti, consente la creazione di richieste di pagamento esclusivamente mediante l'aggancio ad un rapporto esistente, a sua volta collegato a una controparte presente in anagrafica o a un dipendente effettivamente presente in anagrafica, per il pagamento degli stipendi).
- I livelli autorizzativi previsti per il benestare al pagamento corrispondono ai poteri definiti dal sistema di deleghe e delle procure, alle strutture responsabili nonché alla governance in materia di poteri di rappresentanza necessari per agire in nome e per conto della Banca.
- L'acquisto degli ATM è effettuato dalla Banca. Una volta effettuato l'acquisto, gli ATM vengono presi in carico da Allitude che effettua le installazioni e programmazioni di tipo tecnico e informatico.
- Sono presenti contratti di esternalizzazione opportunamente formalizzati con la Società Allitude e con Capogruppo che rispettano le linee guida EBA in materia di outsourcing.
- Sono presenti ulteriori contratti di servizio con Capogruppo per quelle attività afferenti a servizi di pagamento erogate dalla stessa.

Le modalità operative per la gestione dei processi in cui emerge il rischio di commissione di reati di frode e falsificazione di strumenti di pagamento diversi dai contanti sono disciplinate nella normativa interna, sviluppata ed aggiornata a cura delle strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo. In particolare, si fa riferimento al Regolamento Generale Aziendale che descrive i principali compiti di ciascuna unità organizzativa, al Codice Etico e alla regolamentazione tempo per tempo vigente in materia di:

- ripartizione delle deleghe per la gestione delle risorse finanziarie;
- gestione degli strumenti di pagamento elettronici;
- gestione dei sistemi di pagamento;
- gestione del servizio di tesoreria per conto di enti pubblici;
- modalità operative per la gestione dei pagamenti;

- modalità operative per la gestione dei processi di liquidità;
- Trasparenza;
- Approvazione nuovi prodotti.

Inoltre:

- Per il corretto utilizzo delle carte sono previste da parte della società emittente le carte (ad es. Nexi, Visa, Mastercard, …) presidi di controllo nel continuo, in grado di evidenziare operatività anomala tali da consentire il blocco operativo della carta.
- Presenza di controlli antiriciclaggio (ad es. EPA per prelievo ricorrente all'ATM ovvero oltre certe soglie di importo con carta prepagata...) attivabili dalla funzione centralizzata AML con successivi approfondimenti in locale tramite il referente AML.
- Presenza di controlli antiriciclaggio e antifrode sul transato effettuato sul canale POS che, prevedono successivi approfondimenti in locale tramite il referente AML.
- Controlli di linea giornalieri sulle disposizioni di pagamento gestite per conto della clientela
- Presenza di specifici controlli sulle disposizioni di pagamento da e verso i gestori wallet, in grado di evidenziare un elenco di clienti che hanno intrattenuto rapporti con società che gestiscono piattaforme di trading e/o società di scambio di beni digitali.
- Presenza di controlli di secondo livello presso il servizio incassi e pagamenti di CCB e verifiche periodiche che presuppongono anche verifiche rafforzate in caso di utilizzo anomalo.
- 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.
- Presenza di condizioni contrattuali con la clientela che, anche tramite la gestione reclami, garantiscono la stessa da eventuali addebiti/accrediti di operazioni non riconosciute.
- 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.
- Procedure poste all'individuazione e segnalazione delle operazioni ritenute potenzialmente sospette effettuata anche tramite una specifica procedura informatica, in grado di evidenziare operazioni anomale (EPA – Evidenze P Antiriciclaggio). Per le carte prepagate presenza di controlli volti ad evidenziare

situazioni di anomalia (es. prelievo contante agli ATM non coerenti con il profilo del titolare della carta). Per le disposizioni da e verso i gestori wallet, il controllo mira ad evidenziare i clienti che hanno intrattenuto rapporti con società che gestiscono piattaforme di trading e/o società di scambio di beni digitali, intestatari di IBAN esteri come indicati in una istruzione operativa.

- Il responsabile di ciascun punto operativo è tenuto, alla fine di ogni giornata lavorativa, ad effettuare accertamenti sulle operazioni svolte (verifiche rafforzate), allo scopo di individuare casi di potenziali operazioni sospette.
- Presenza e valutazione di un sistema di alert operativi ricevuti dalle società terze che gestiscono rispettivamente il portafoglio carte di pagamento (credito/debito/prepagate) e servizi di pagamento elettronico distribuiti dalla Banca alla clientela.
- L'eventuale rilascio di carte di credito/debito/prepagate a favore dei soggetti apicali della Banca (ove non espressamente vietato) prevede un sistema di controllo sistematico e continuo in merito alla coerenza delle transazioni effettuate rispetto alle finalità della delibera di delega assunta.
- 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.
- Presenza di un sistema di sicurezza informatico e applicativo sui servizi di pagamento elettronico offerti alla clientela in grado di garantire un'operatività coerente con la volontà dei titolari dei rapporti, in grado di prevenire condotte di natura fraudolenta poste in essere da soggetti terzi.