– PARTE SPECIALE R –

REATI DI FRODE E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

REATI IN MATERIA DI FRODE E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

1. I reati di delitti in materia di frode e falsificazione di strumenti di pagamento diversi dai contanti sono richiamati dall'articolo 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.

Trasferimento fraudolento di valori (Art. 512-bis c.p.)

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.

2. Le attività individuate come potenzialmente sensibili ai fini del d.lgs. 231/2001 con riferimento ai reati in materia di falsificazione strumenti di pagamento diversi dai contanti

L'analisi dei processi aziendali ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamata dall'articolo 25-octies.1 del d.lgs. 231/01.

Di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati in materia di falsificazione strumenti di pagamento diversi dai contanti:

1. Attivazione alla clientela di carte prepagate, bancomat, credito.
2. Attivazione o vendita di prodotti ai clienti per la gestione di pagamenti elettronici, quali: homebanking, POS, o attivazione di POS unattended (di proprietà della clientela).
3. Istruttoria pratiche di credito ad imprese, con riferimento alla valutazione della composizione societaria (riscontro soci e titolari effettivi), nell'ambito della gestione della Pratica Elettronica di Fido (PEF), al fine di riscontrare anomali/frequenti cambiamenti nei trasferimenti delle quote societarie, tali da indicare il sospetto della fittizia intestazione.
4. Utilizzo dei conti correnti dedicati "grandi opere", ovvero dei rapporti intestati alle curatele fallimentari, notai, COFIDI, agenti assicurativi – Servizi Bancari Tipici.

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 in materia di falsificazione strumenti di pagamento diversi dai contanti:

- Presenza di una normativa interna in cui sono riportati i controlli operativi applicati nella gestione delle attività di pagamento eseguite dalla clientela e in particolare:
  - controllo sulle operazioni di pagamento disposte dalla clientela con carte (debito/prepagate/credito);

- controllo e gestione blocchi operativi in presenza di operatività sospetta;
- controllo conti.

- Presenza di una normativa interna che riporta le modalità di accesso e di utilizzo delle piattaforme / circuiti di pagamento.

- Presenza di una normativa interna che disciplina gli step da seguire in fase di sviluppo di nuovi prodotti.

- La Banca non ha la possibilità di alterare i sistemi informatici in uso; pertanto, il reato potrebbe esclusivamente essere realizzato "in concorso" con la società Allitude o con altri fornitori di software.

- Presenza di software specifici a supporto delle attività c.d. di *fraud detection* con riferimento all'esecuzione delle transazioni operate con carte ovvero attraverso le funzionalità di pagamento dell'homebanking in uso alla clientela.

- Nell'ambito del servizio di gestione di conti correnti dedicati (grandi opere, notai, agenti assicurativi, curatele, COFIDI,…), esistenza di OdS specifici e di controlli finalizzati ad assicurare la corretta gestione delle somme e l'esecuzione delle disposizioni di pagamento in coerenza con quanto previsto dalla convenzione e/o disposto dal giudice fallimentare.

- Controlli di linea assegnati alle strutture organizzative della Banca relativamente alla gestione delle richieste di trasferimento titoli e/o disponibilità finanziarie (al di fuori da pratiche di successione,...) e acquisizione di specifica documentazione di supporto (es. atti notarili di donazione,...), secondo le disposizioni disciplinate da ordini di servizio a supporto, tempo per tempo vigenti.

- 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.