

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) MIOLA	Membro di designazione rappresentativa degli intermediari
(NA) VERDICCHIO	Membro di designazione rappresentativa dei clienti

Relatore MASSIMO MIOLA

Seduta del 11/12/2025

FATTO

La ricorrente, titolare di una carta di credito n. ***0411 emessa dall'intermediario in *partnership* con altro intermediario non convenuto nel procedimento, chiede il rimborso di n. 4 operazioni eseguite con la carta e da lei non autorizzate. In particolare, rappresenta che la carta non è mai stata utilizzata in modo continuativo ma solo sporadicamente e sotto suo pieno controllo; che le operazioni non autorizzate sono state eseguite in data 28.05.2025 alle ore 20:11, 20:12, 20:13, 20:14 presso il medesimo esercizio e consistono di n. 3 transazioni da € 990,00 e una da € 500,00, per un totale di € 3.470,00; inoltre, afferma di aver ricevuto il 31.05.2025, n. 4 SMS che informavano delle transazioni dall'altro intermediario emittente la carta. Provvedeva, quindi, al blocco immediato della carta e al disconoscimento delle operazioni.

La ricorrente a tale proposito ipotizza una clonazione della carta, dato che afferma di non avere mai smarrito né ceduto la carta; di non avere mai comunicato PIN, OTP o credenziali a terzi; di non avere mai adottato comportamenti negligenti nella custodia dei dati.

Pertanto, insoddisfatta dell'interlocuzione avuta in fase di reclamo, presenta ricorso all'Arbitro per ottenere il rimborso della somma sottratta pari a € 3.470,00, oltre le spese legali.

L'intermediario, costituitosi, conferma i fatti alla base del ricorso ed afferma che le transazioni sono state autenticate con chip e PIN che richiedono la presenza fisica della carta; che sono stati inviati al cellulare della ricorrente gli SMS di conferma con prova fornita da società specializzata in messaggistica mobile; che i log informatici forniti dall'intermediario che gestisce il circuito di pagamento confermano la corretta autenticazione delle transazioni; che la ricorrente non ha denunciato il furto né lo

smarrimento della carta, affermando di esserne sempre rimasta nel possesso.

L'intermediario ritiene quindi che vi sia stata una violazione delle norme di sicurezza ed in particolare dell'obbligo di custodia della carta e del divieto di annotare il PIN sulla carta o su documenti conservati insieme. Infatti, per le operazioni effettuate con carta e PIN risulta impossibile un uso fraudolento senza conoscere il PIN, come confermato da analisi del Politecnico di Torino.

Pertanto, l'intermediario chiede il rigetto integrale del ricorso, in quanto infondato in fatto e in diritto, essendo le operazioni imputabili alla ricorrente.

Nelle repliche, la ricorrente ribadisce che la carta non è mai stata smarrita o sottratta ed è rimasta sempre in suo possesso; che il PIN non è stato mai condiviso o custodito in modo incauto; che la carta è stata pressoché inutilizzata prima delle operazioni contestate; che la sequenza di transazioni è stata ripetitiva, ravvicinata e di importo elevato presso lo stesso esercente, costituendo un tipico schema di frode. Ciononostante, l'intermediario non ha attivato i sistemi antifrode. Aggiunge che l'assenza di denuncia di furto dipenderebbe dal fatto che la carta non è mai stata rubata. Quanto alle spese legali, afferma che l'assistenza è stata necessaria per la complessità tecnica della fattispecie (log, protocolli ISO, normativa PSD2).

Pertanto, ribadisce la domanda del ricorso originario.

Nelle controrepliche, l'intermediario ribadisce che le operazioni contestate sono state effettuate con la materiale disponibilità della carta di credito n. ***0411 e con l'inserimento del codice PIN, noto esclusivamente al titolare. Tale circostanza non sarebbe mai stata contestata dalla ricorrente. Conclude chiedendo all'Arbitro di rigettare tutte le domande avanzate nel ricorso, poiché infondate.

Tanto premesso, si rileva quanto segue in

DIRITTO

La controversia attiene alla richiesta di rimborso di somme indebitamente sottratte a seguito di operazioni fraudolente compiute *on line*.

Il ricorso non merita di essere accolto.

Preliminarmente, giova rilevare che le operazioni contestate risultano essere state eseguite il 28/05/2025. Pertanto, esse rientrano nell'ambito di applicazione del d.lgs. 27 gennaio 2010, n. 11, di attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno (c.d. PSD), come modificato dal D.Lgs. 218/2017, di recepimento della direttiva 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018. In particolare, le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10-bis del d. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare, il parere dell'EBA del 21 giugno 2019).

Come costantemente rilevato da questo Arbitro, la novellata normativa ha rafforzato il regime di speciale protezione e di altrettanto speciale *favor probatorio* a beneficio degli utenti, introdotto dal d. lgs. n. 11/2010 ante modifica e ripetutamente evidenziato da numerose decisioni dell'ABF, anche del Collegio di Coordinamento (cfr. decisioni n. 991/2014; n. 5304/2014; n. 3498/2012; n. 21285/2021).

La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, comma 4, d. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011.

Ai fini che interessano la presente decisione, vengono in considerazione le seguenti principali disposizioni precettive del d. lgs. 11/2010: a) l'art.10, comma primo, stabilisce che, in caso di

disconoscimento di un'operazione di pagamento da parte dell'utente, è onere del prestatore di servizi di pagamento provare che la stessa operazione è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema; b) con riguardo a quest'ultimo profilo, l'art. 8 stabilisce una serie di obblighi gravanti sul prestatore dei servizi, volti a salvaguardare la sicurezza del sistema, primo fra tutti quello di assicurare l'inaccessibilità ai terzi delle credenziali di sicurezza personalizzate, fatti salvi gli obblighi posti in capo all'utente ex art. 7; tale ultima disposizione prevede che *“l'utilizzatore abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso [...] e che a tal fine adotta le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo”*; in particolare, l'art. 8, comma 2, dispone che *“i rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate sono a carico del prestatore di servizi di pagamento”*; c) in difetto della prova della corretta autenticazione, viene meno, per il prestatore dei servizi, la possibilità stessa di riferire le operazioni contestate al cliente; d) l'art. 10, comma secondo, precisa che, in ogni caso, l'apparente corretta autenticazione non è, di per sé, necessariamente sufficiente a dimostrare la riconducibilità dell'operazione all'utente che la disconosca, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'art. 7, essendo, invece, onere del prestatore dei servizi fornire la prova della frode, del dolo o della colpa grave dell'utente; e) l'art. 12, comma primo, pone a carico del prestatore di servizi di pagamento le perdite derivanti dall'utilizzo dello strumento smarrito, sottratto o utilizzato indebitamente, intervenuto dopo la comunicazione di smarrimento o furto prevista dall'art. 7, comma primo, lett. b); f) l'art. 12, terzo comma, nel prevedere la franchigia di € 50,00, entro la quale l'utente può essere tenuto a sopportare la perdita derivante dalle operazioni compiute prima della comunicazione testé menzionata, fa salva l'ipotesi che l'utente *«abbia agito in modo fraudolento o non abbia adempiuto ad uno o più di cui all'art. 7 con dolo o colpa grave»*, nel qual caso l'intera perdita resta a suo carico; g) l'art. 12, comma 2-bis stabilisce, inoltre, che *«salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente»*, come definita dall'art. 1, lett. q-bis, necessaria, ai sensi dell'art. 10-bis, quando l'utente accede al suo conto di pagamento *on-line*, dispone un'operazione di pagamento elettronico ovvero *«effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi»*; h) l'art. 7, comma primo, enuclea gli obblighi gravanti sull'utente abilitato all'utilizzo di uno strumento di pagamento: in particolare, questi è tenuto ad utilizzare detto strumento nel rispetto delle condizioni contrattuali che ne disciplinano l'emissione e l'uso, i cui termini devono essere obiettivi, non discriminatori e proporzionati (comma primo, lett. a); il secondo comma precisa, poi, che, *«ai fini di cui al comma 1, lettera a), l'utilizzatore, non appena riceve uno strumento di pagamento, adotta le misure idonee a proteggere le credenziali di sicurezza personalizzate»*.

Al riguardo, il Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce *“un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]*. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso

fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro). La ratio di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coord., decisione n. 3947/2014; in senso conforme: Coll. Coord., decisione n. 3498/2012; Coll. Coord., decisione n. 991/2014.; Coll. Coord., decisione n. 22745/19, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, ex art. 10, comma 2, d. lgs. n. 11/2010; Coll. Coord., decisione n. 21285/2021).

Con specifico riferimento al requisito di autenticazione forte (SCA), L'art. 10-bis, comma 1, del d.lgs. n.11/2010 dispone che, in conformità all'articolo 98 della PSD2 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, *"i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi"*. L'art. 1, lett. q), del d.lgs. n.11/2010 ("Definizioni") definisce per *"autenticazione: la procedura che consente al prestatore di servizi di pagamento di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, incluse le relative credenziali di sicurezza personalizzate fornite dal prestatore"*. La definizione di autenticazione forte (SCA) è fornita dalla successiva lettera q-bis), che riprende l'art. 4 del Regolamento 2018/389, specificando che per autenticazione forte del cliente si intende: *"un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente) che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione"*.

Ai sensi dell'art. 38 del Regolamento Delegato (UE) 2018/389 della Commissione Europea, tale requisito si applica a tutte le transazioni successive al 14/09/2019. Inoltre, nella *Opinion* del 21 giugno 2019 (EBA-Op-2019-06) l'EBA ha fornito chiarezza sugli elementi utili alla SCA, con un ulteriore livello di dettaglio, attraverso specifici esempi di soluzioni tecniche, per ciascuna categoria di elementi, *compliant* o meno con le disposizioni regolamentari.

Venendo al caso di specie, la ricorrente richiede il rimborso di 4 operazioni eseguite tramite la carta di credito n. ***411 in data 28.05.2025 alle ore 20:11, 20:12, 20:13, 20:14 presso l'esercizio "H24 *AN ***ARO", di cui 3 pagamenti da € 990,00 e uno da € 500,00 per un totale di € 3.470,00.

Preliminarmente, il Collegio rileva che risultano allegate al ricorso diverse denunce presentate all'Autorità di P.S. Precisamente, una prima, sporta il 31.05.2025, ove i ricorrenti riferiscono di un blocco per "uso scorretto" di precedenti carte nn. ***180 e ***223 poi sostituite con nuove carte nn. ***695 e ***325 rilasciate il 29.05.2025 e fanno riferimento a delle operazioni del 28.05.2025 disconosciute (4 pagamenti POS presso l'esercizio "H24 *AN ***ARO", di € 500 ciascuno per un totale di € 2.000,00) e del 29.05.2025 (ulteriori 19 pagamenti POS presso lo stesso esercizio, per € 9.487,00) per un totale di € 11.487,00 (23 operazioni) ipotizzando una clonazione delle carte. Una seconda, recante la data del 03.06.2025, avente ad oggetto ulteriori 8 operazioni fraudolente compiute il 28.05.2025, sempre presso il medesimo esercizio "H24 *AN ***ARO", per complessivi € 4.990,00. Infine, una terza denuncia sporta in data 09.06.2025, in cui ricorrente riferisce di aver ricevuto, il 31.05.2025 (in realtà il 28.05.2025), n. 4 SMS alert inviati dall'altro intermediario emittente la carta, che segnalavano acquisti con la carta di credito n. ***0411 ed in particolare 4 operazioni di cui 3 da € 990,00 e una da € 500,00 eseguite il 28.5.2025 (totale € 3.470,00) presso lo stesso esercizio "H24 *AN ***ARO" alle 20:11, 20:12, 20:13, 20:14. Solo tali operazioni costituiscono oggetto della domanda avanzata dalla ricorrente nel presente giudizio. Si aggiunge che in denuncia si fa riferimento anche ad

ulteriore ricarica di carta prepagata da € 2.000,00 tramite App (presumibilmente volta alla creazione di provvista), seguita da 4 pagamenti POS da € 500,00 ciascuno (viceversa non oggetto di domanda). Il Collegio evidenzia pertanto che dalle denunce allegate al ricorso risulta che la ricorrente è titolare di diverse tipologie di carte: 1) carta di credito n. ***411 utilizzata per eseguire le operazioni di cui è richiesto il rimborso nel ricorso in questione e citata nella denuncia integrativa del 09.06.2025 (carta di credito con opzione revolving); 2) carta prepagata n. ***580 utilizzata per la ricarica da € 2.000,00 tramite app, citata sempre nella stessa denuncia; 3) carte di debito collegate ad un conto corrente (le n. ***180 e n. ***223) e 2 nuove carte sostitutive rilasciate il 29.05.2025 (n. ***695 e n. ***325).

A fronte del disconoscimento dell'operazione di pagamento da parte del ricorrente, come già menzionato, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata, ai sensi dell'art. 10, commi 1 e 2, del d.lgs. 11/2010. Nel caso in esame, trova inoltre applicazione l'art. 10-bis, comma 1, del suddetto d.lgs. 11/2010, come modificato, il quale statuisce che i prestatori di servizi di pagamento applichino l'autenticazione forte del cliente qualora l'utente: *a) acceda al suo conto di pagamento online; b) disponga un'operazione di pagamento elettronico; c) effettui qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.* Il Collegio rileva preliminarmente sul punto che, ai sensi del Regolamento Delegato (UE) 2018/389 della Commissione Europea, il requisito di autenticazione forte (SCA) ricorre in presenza di due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza, purché indipendenti tra loro, nonché la presenza di un collegamento dinamico.

L'intermediario resistente produce in proposito apposita documentazione tecnica tesa a provare che l'autenticazione è intervenuta secondo le modalità della SCA. In particolare, l'intermediario riferisce che le operazioni di cui è chiesto il rimborso (n. 4 pagamenti POS) sono state autenticate tramite Microchip con digitazione del PIN, che richiede la presenza fisica della carta. Nella prospettiva della SCA, la carta integra l'elemento di possesso ed il PIN l'elemento di conoscenza. A riprova di tale sistema di autenticazione, l'intermediario ha prodotto log informatici, forniti dall'intermediario che gestisce il circuito di pagamento, che confermano la corretta autenticazione. In particolare, per tutte le operazioni è allegata una decodifica del capo "POS" (L1533C), da cui risulta l'utilizzo della tecnologia EMV (microchip) e PIN.

Le operazioni di pagamento contestate risultano pertanto essere state autenticate, correttamente registrate e contabilizzate dall'intermediario.

Giova rilevare, tuttavia, che, come sancito dal Collegio di Coordinamento con la decisione n. 22745/2019: *«La previsione di cui all'art. 10, comma 2, del d.lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente».* L'onere della prova della genuinità della transazione, ovvero della frode, dolo o colpa grave dell'utente ricade quindi sul prestatore del servizio e può ovviamente essere fornita pure per mezzo di presunzioni gravi, precise e concordanti, secondo quanto dispone l'art. 2729 c.c., di un comportamento fraudolento, doloso o gravemente colpevole dell'utente (*ex multis*, cfr. Collegio Napoli, decisione n. 1091/2018). La stessa Corte di Cassazione, a tale specifico riguardo, ritiene che sia ammissibile la prova indiziaria della sussistenza della colpa grave (cfr. Cass. n. 654/2010).

Venendo al caso in esame, l'intermediario sostiene che vi sia stata da parte della ricorrente una violazione delle norme di sicurezza ed in particolare dell'obbligo di custodia della carta e segretezza del PIN, dato che per le operazioni effettuate con microchip e PIN sarebbe impossibile un uso fraudolento senza conoscenza del PIN. La ricorrente, dal canto suo, afferma di non aver comunicato a terzi PIN, OTP o credenziali, né di avere smarrito o ceduto a terzi la carta, negando altresì che la stessa sia stata

oggetto di furto, ipotizzando l'intervenuta clonazione della stessa.

Il Collegio rileva sul punto che, alla luce della posizione espressa dal Collegio di Coordinamento, l'impiego della tecnologia a *microchip* rende l'ipotesi della clonazione, se non di impossibile evenienza, almeno altamente improbabile, facendo ritenere che l'esecuzione delle operazioni sconosciute debba essere ricondotta all'incauta custodia della carta e del PIN da parte dell'utente, salvo che quest'ultimo non fornisca la prova di circostanze tali da far ritenere plausibile l'ipotesi della clonazione (Collegio di Coordinamento, decisione n. 897/14; in termini, Collegio di Coordinamento, decisioni n. 991/14 e 3947/14).

Di recente, i Collegi territoriali hanno convenuto di confermare l'orientamento consolidatosi a seguito dei menzionati pronunciamenti del Collegio di Coordinamento, precisando che è da escludere la clonazione della carta di pagamento, con conseguente rigetto del ricorso, qualora l'intermediario abbia dimostrato che le operazioni sono state autenticate tramite *microchip* e con la corretta digitazione del PIN, nonché l'assenza di anomalie. Il Collegio rileva altresì che la ricorrente ha dedotto la intervenuta clonazione della propria carta di debito, ma non ha fornito alcuna prova in proposito. Ed infatti, non risulta sufficiente invocare, da parte del ricorrente, una pretesa clonazione dello strumento di pagamento, dovendo essa *“fornire la prova di circostanze tali da far ritenere quantomeno plausibile l'ipotesi della clonazione, per cui limitarsi a sostenere di non aver mai perso l'uso della carta paventando la clonazione non appare bastevole”*: Collegio di Napoli, decisioni n. 9478/2024; n. 252/2025; n. 6686/2025).

A questa stregua, laddove il ricorrente affermi di non aver eseguito personalmente l'operazione e di non avere ceduto a terzi e/o smarrito e/o subito il furto dello strumento di pagamento, l'orientamento consolidato dei Collegi è nel senso che *“è da escludersi la clonazione della carta di pagamento, con conseguente rigetto del ricorso, qualora: l'intermediario abbia dimostrato nonché l'assenza di anomalie; il ricorrente non abbia allegato alcun riferimento descrittivo e circostanziale idoneo a rendere verosimile l'asserita clonazione. Similmente a quanto condiviso a proposito degli utilizzi fraudolenti on line non circostanziati dall'utente, nella fattispecie in esame le mancate allegazioni del cliente rappresentano un elemento da cui il Collegio deve trarre il proprio convincimento circa la colpa grave del ricorrente medesimo”* (così Collegio di Milano, decisione n. 12728/2022; Collegio di Milano, decisione n. 1061/2023).

Le circostanze esposte, unitamente alla mancata allegazione da parte della ricorrente di dettagli su come le operazioni fraudolente denunciate siano in concreto avvenute, induce a ritenere che esse siano ascrivibili esclusivamente alla colpa grave della ricorrente stessa.

Con riferimento all'adozione da parte dell'intermediario di sistemi di *alert*, si fa rinvio a quanto affermato dal Collegio di Coordinamento nella decisione n. 24366/2019, secondo cui *“Fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto”*. Recentemente, il Collegio di Coordinamento ha altresì precisato che *“la mancata attivazione del servizio sms – alert costituisce in ogni caso una carenza organizzativa imputabile all'intermediario che, oltre a produrre l'effetto giustificativo solo a fronte della specifica dichiarazione liberatoria di rifiuto del cliente ad avvalersene (già affermata dal precedente “coordinamento”), non può non essere rilevata anche d'ufficio”* (cfr. decisione n. 8672/2024).

Nel caso di specie le parti concordano sulla ricezione degli SMS di conferma delle operazioni. Al riguardo, l'intermediario ha versato evidenza fornita da una società specializzata in messaggistica mobile, che i Collegi ritengono idonea a provare la ricezione del messaggio in caso di valorizzazione, come nel caso in esame, del campo *“Data di recapito al cliente”*. In ogni caso, è emerso che la mancata attivazione ovvero il mancato funzionamento del servizio di *sms-alert* (o servizio assimilabile) possono essere ritenuti irrilevanti laddove l'invio dell'SMS non avrebbe potuto, in concreto, impedire o contenere la perdita relativa alle operazioni non autorizzate dal titolare dello strumento di pagamento, ossia

nell'ipotesi in cui sia stata eseguita una sola operazione di pagamento fraudolenta ovvero quando le operazioni risultino effettuate a breve distanza di tempo l'una dall'altra. Nel caso di specie, le operazioni in questione sono state eseguite a un minuto di distanza le une dalle altre, quindi gli SMS *alert* non sarebbero stati comunque in grado di scongiurarne il compimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE