

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) PERLINGIERI	Membro di designazione rappresentativa dei clienti

Relatore GIOVANNI PERLINGIERI

Seduta del 31/03/2026

FATTO

Con il ricorso del 17 ottobre 2025, si riferisce che

- in data 30 giugno 2025, la società istante effettuava richiesta di *upgrade* per un volo tramite il sito ufficiale della Compagnia aerea e, non ricevendo risposta, seguiva le indicazioni della sezione 'Connettiti a noi' del sito *web*, accedendo alla pagina *Facebook* ufficiale della Compagnia;
- attraverso il sistema di messaggistica, sedicenti operatori della Compagnia richiedevano i dati della carta con il pretesto di verificare l'identità del cliente per procedere con l'*upgrade*, effettuando ripetute transazioni con importi diversi, qualificate come 'transazioni di prova' dal medesimo operatore;
- il giorno successivo, i criminali continuavano a richiedere ulteriori transazioni, chiedendo di trasferire la conversazione su WhatsApp, e la ricorrente acconsentiva, fiduciosa che la messaggistica traesse origine dal sito ufficiale della Compagnia aerea,
- venivano eseguite operazioni di pagamento per complessivi € 1.128,97.

La ricorrente lamenta che la resistente non avrebbe dimostrato l'uso di una corretta autenticazione forte e che i sistemi antifrode erano insufficienti dato che, nonostante le operazioni coinvolgessero controparti in Paesi ad alto rischio, come l'Uganda, la resistente non avrebbe bloccato operazioni ripetitive e anomale, né applicato meccanismi di *transaction monitoring* conformi alle EBA *Guidelines*. Pertanto chiede il rimborso di € 1.128,97, oltre interessi legali.

Con controdeduzioni dell'1 dicembre 2025, si costituisce la banca convenuta, per precisare che:

- è questione di cinque operazioni di *e-commerce* eseguite il 30 giugno e l'1 luglio 2025 tramite carta emessa da altro intermediario, tutte autenticate con riconoscimento biometrico. Il blocco della carta

avveniva oltre un mese dopo, il 4 agosto 2025;

- le operazioni sono da considerarsi autorizzate personalmente dalla ricorrente, incorsa in colpa grave;
- la frode avveniva tramite canali *social* 'apparentemente ufficiali', nonostante i noti rischi;
- la ricorrente avrebbe comunicato dati completi della carta via *WhatsApp*, violando l'obbligo di diligente custodia dei dati dello strumento di pagamento;
- le operazioni sono state autenticate con SCA pienamente conforme;
- non sono emersi indici di anomalia;
- la ricorrente effettuava personalmente le operazioni sebbene con 'consenso viziato' ma comunque espresso tramite i propri dispositivi e credenziali e attendeva oltre un mese prima di bloccare la carta e denunciare; inoltre, la ricorrente non utilizzava strumenti di protezione aggiuntivi come quelli di *spending control* che consentono, in particolare, di personalizzare la spendibilità della carta in relazione alla zona geografica (Italia, Europa e altri continenti), al canale di utilizzo (POS fisico, prelievo ATM e e-commerce) e alla categoria merceologica degli esercenti.

La banca conclude che le operazioni devono considerarsi autorizzate e il ricorso deve essere integralmente respinto.

La ricorrente replica con memorie dell'8 gennaio 2026 affermando di aver agito attraverso canali istituzionali della Compagnia aerea, che risultavano regolarmente collegati dal sito della compagnia. Pertanto, il raggirio si sarebbe basato su *social engineering* sofisticato, reso credibile dal contesto. Inoltre, sarebbero mancati *alert* o blocchi automatici da parte della resistente, essendo le operazioni ravvicinate, verso operatori di *money transfer* internazionali, tipicamente considerate ad alto rischio, nonché di importo significativo. Non risulterebbero utilizzati dalla resistente algoritmi di *machine learning*, *alert* personalizzati, controlli proattivi in tempo reale, né erano mai stati attivati né consigliati strumenti come *spending control*, limiti geografici, limiti merceologici.

DIRITTO

La controversia ha a oggetto la richiesta di accertamento della illegittimità della condotta della banca con riferimento ad alcune operazioni contestate. Si tratta di cinque pagamenti *online* dell'importo complessivo di € 1.128,97, eseguiti tra le 16:59 del 30 giugno e le 20:39 dell'1 luglio 2025 tramite carta aziendale emessa da altro intermediario e gestita dalla resistente. In particolare, si tratta di cinque *money transfert* verso l'estero effettuati tramite *app* o sito *web* di aziende straniere specializzate in rimesse *online*.

Come da denuncia sporta il 28 agosto 2025 e allegata al ricorso, la ricorrente dichiara che il 30 giugno 2025 richiedeva l'*upgrade* di un volo tramite il sito ufficiale di una Compagnia aerea. Non ricevendo assistenza, accedeva tramite il *link* 'Connettiti a noi' alla pagina *Facebook* ufficiale della Compagnia, da cui veniva reindirizzata a *Messenger* e poi a *WhatsApp*. Soggetti ignoti, spacciandosi per operatori della Compagnia, si facevano comunicare i dati della carta ed eseguivano le cinque operazioni contestate. Nel ricorso, la società conferma che i sedicenti operatori richiedevano i dati della carta con il pretesto di verificare l'identità della cliente, effettuando ripetute transazioni.

Dalla documentazione in atti e dalle dichiarazioni rilasciate da parte ricorrente nella ricostruzione dei fatti, risulta, insomma, che la stessa effettuava personalmente le transazioni. È noto che, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla direttiva PSD2.

Al riguardo, i Collegi hanno esaminato l'eventualità che il pagatore partecipi alla fase dispositiva e/o autorizzativa dell'operazione fraudolenta, per valutare se: i) a fronte di un apporto del pagatore solamente parziale (ad esempio quando autorizza l'operazione precedentemente inserita dal frodatore), l'operazione possa reputarsi comunque autorizzata; ii) sia configurabile una responsabilità

concorrente del psp, in relazione alle circostanze concrete, anche quando l'operazione sia stata eseguita per intero (personalmente) dal pagatore.

La resistente rende prova, tuttavia, che le operazioni venivano autenticate tramite sistema a due fattori che prevede il riconoscimento biometrico (impronta digitale o face ID-elemento di inerenza) con invio notifiche su *app* della resistente su dispositivo associato e certificato (elemento di possesso). Produce evidenza della certificazione del dispositivo e dell'abilitazione del riconoscimento biometrico avvenute quasi un anno prima dei fatti (il 2 settembre 2024) con *password* statica e sms otp.

Su tale consistenza probatoria, però, occorre rilevare che il dispositivo certificato è identificato come *iPhone* senza altri dettagli; e che gli sms otp relativi alla certificazione del dispositivo risultano inviati a numero di telefono che non corrisponde a quello indicato dalla rappresentante della ricorrente nella denuncia agli atti.

Non sono allegati, poi, i *log* relativi all'accesso all'*home banking*, ma sono presenti quelli relativi alle singole operazioni, dai quali risulta che tutte le operazioni venivano autorizzate, che per tre pagamenti i dati statici della carta erano previamente registrati sul sito del *merchant* e che per gli altri due risulta la digitazione del codice di sicurezza cvv posto sul retro della carta la carta.

Dai *log* risulta invece l'autenticazione 3DS 2.2.0 (Esito "Y-titolare autenticato"), protocollo necessario per applicare la SCA, e utilizzo di fattore biometrico ("OOB *Biometrics*"). Sono presenti i *log* delle notifiche *push* parlanti inviate e ricevute su dispositivo *iPhone*, con testo della notifica che dettaglia l'importo delle spese da autorizzare e a favore di quale esercente e richiesta di autorizzazione tramite App della resistente.

La ricorrente lamenta che sarebbero mancati blocchi automatici da parte della resistente, essendo le operazioni ravvicinate, verso operatori di *money transfer* internazionali, tipicamente considerate ad alto rischio, nonché di importo significativo.

Nella fattispecie in esame, in effetti, delle cinque operazioni, eseguite con la stessa carta, tre erano eseguite entro ventiquattro ore, ma soltanto due verso lo stesso 'punto vendita', mentre l'art. 8, d.m. n. 112 del 2007 individua indici di anomalia nel caso di tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle ventiquattro ore, siano effettuate presso un medesimo punto vendita.

Non emergono indici di frode ulteriori in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente, atteso che non ve n'è evidenza.

Decisivo ai fini della soluzione della controversia è il fatto che manca l'evidenza di sms o notifiche *alert* da parte della resistente, essendo le operazioni ravvicinate.

La mancata prova dell'attivazione del servizio di sms *alert* da parte dell'intermediario rappresenta una violazione degli obblighi posti a suo carico, rappresentante una grave carenza organizzativa, dato il difetto di una misura importate ai fini della garanzia della sicurezza del servizio (Collegio di Coordinamento, decisione n. 24366 del 2019). Costituisce orientamento consolidato dei Collegi territoriali che l'attivazione del servizio di sms *alert* costituisca un onere gravante direttamente sull'intermediario, a prescindere dal fatto che il cliente ne abbia o meno richiesto l'attivazione. Più precisamente, si ritiene che «la mancata attivazione del servizio di "sms-alert" costituisce [...] una carenza organizzativa imputabile all'intermediario resistente il quale, data la natura di misura di sicurezza del sistema di sms alert, non dovrebbe limitarsi a proporlo al cliente ma dovrebbe adottarlo in modo generalizzato (Coll. Roma, dec. 7976/2016. Conformi sul punto, fra le tante, Coll. Roma dec. n. 15447/2018; Coll. Palermo dec. n. 13205/2017 [...])» (Collegio di Coordinamento, decisione n. 243 del 2019).

Nel caso, mentre tra la prima e la seconda operazione intercorrevano solo sei minuti, la terza operazione veniva eseguita tre ore dopo la seconda. Pertanto, un sistema di *alert* avrebbe potuto contribuire all'esecuzione delle operazioni dalla terza in poi, per complessivi € 614,98.

Per altro verso, dalla denuncia emerge che la ricorrente entrava nel sito *web* di una Compagnia aerea e, accedendo alla pagina *Facebook* 'ufficiale' della Compagnia, comunicava imprudentemente a soggetti ignoti, spacciandosi per operatori della Compagnia, i dati della carta al fine della verifica della

sua identità. La conversazione, poi, si trasferiva, su consenso della ricorrente, sulla messaggistica privata (*WhatsApp* e *Messenger*). Inoltre il blocco della carta avveniva oltre un mese dopo, il 4 agosto 2025. Tale condotta si connota per colpa grave.

In definitiva, si accerta la responsabilità concorrente ex art. 1227 c.c. delle parti della presente controversia e il diritto della ricorrente alla restituzione delle somme corrispondenti ai pagamenti che sarebbe stato possibile evitare in presenza di sms *alert*.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente alla restituzione dell'importo di € 615,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE