

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) ABATE	Membro di designazione rappresentativa dei clienti

Relatore (MI) MODICA

Seduta del 17/03/2026

FATTO

La cliente riferisce di essere iscritta al sito F*, che utilizza per vendere itinerari di viaggio; in data 20.09.2025, un utente manifestava l'intenzione di ordinare un suo itinerario ma segnalava che il sito non accettava la richiesta in assenza di mail personale della venditrice; le giungeva quindi una mail dal sito F* nella quale si chiedeva di confermare i dettagli dell'ordine "schiacciando un tasto"; inseriva poi i dati della sua carta di credito emessa dall'intermediario. Veniva subito prelevata la somma di € 192,73 e poco dopo, con la pretesa finalità di "verificare la carta", le si chiedeva di versare la cifra di € 125,00. Chiede la restituzione degli importi fraudolentemente sottratti.

L'intermediario, controdeduce che la ricorrente ha fornito dati personali, dati delle carte e ha seguito le richieste dai truffatori, inclusa quella di inserire il codice 3D Secure e attivare una nuova carta; le operazioni risultano autorizzate dalla cliente, correttamente autenticate senza anomalie tecniche; la normativa sulle operazioni non autorizzate, D.lgs. 11/2010 non è applicabile perché l'utente ha compiuto personalmente le operazioni, anche se tratto in inganno; le procedure di sicurezza – notifiche push, autenticazione biometrica, corretta associazione del dispositivo – risultano rispettate; la cliente ha agito con grave negligenza, condividendo i dati delle carte, seguendo istruzioni sospette e ignorando segnali di rischio.

Chiede il rigetto del ricorso.

DIRITTO

La cliente disconosce due operazioni eseguite a valle di una truffa e chiede la restituzione dei relativi importi. Si tratta, in particolare, di due pagamenti on line disposti alle ore 13:29 e alle ore 15:37 del 20.09.2025 per complessivi € 317,73.

Sebbene l'intermediario affermi che le operazioni siano state integralmente poste in essere dalla cliente, dalla documentazione in atti non emerge alcuna dichiarazione confessoria esplicita in tal senso, sicché al operazioni contestate ricadono sotto il raggio d'azione del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).

Ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010, "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". L'assolvimento di tale onere è necessario ma non sufficiente, dovendo il prestatore ulteriormente provare, ai fini dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010: come chiarito dal Collegio di Coordinamento, "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" (decisione n. 22745/2019).

Il Collegio, richiamati gli artt. 97 e 98 della PDS2, l'articolo 10 bis del D. Lgs. 11/2010, le 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), richiama altresì l'art. 12 del d.lgs. 27.1.2010, n. 11, "Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento": "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". Il Collegio, ancora, ricorda che, in base all'art. 1, lett. qbis, l'"autenticazione forte del cliente" è definita come "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". L'autenticazione forte è richiesta nella fase di accesso al conto/enrollment dell'app/registrazione della carta sul wallet; nella fase di esecuzione delle singole operazioni; rispetto a qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Nel caso di specie, l'intermediario ha fornito prova di autenticazione con impiego di doppio fattore. Con riferimento al dispositivo utilizzato per l'autenticazione delle operazioni disconosciute, l'intermediario fornisce evidenza che si tratta del cellulare registrato dalla cliente fin dal 19/08/2024; pertanto, la registrazione è anteriore rispetto al primo contatto con il truffatore. Con riferimento a entrambe le operazioni, il pagamento risulta autenticato mediante inserimento dell'impronta digitale (elemento di inerenza) a seguito della ricezione di una notifica push sull'APP registrata sul dispositivo della cliente (elemento di possesso).

Del pari provata appare la colpa grave della cliente, vittima di una truffa banale cui avrebbe potuto sottrarsi con l'impiego di una media diligenza. Dalla documentazione versata in atti si evince infatti che

la cliente ha messo in vendita un itinerario di viaggio su marketplace dedicato e ha dato seguito alle richieste contenute in una mail civetta con la quale si richiedeva confermare i dettagli dell'ordine "schiacciando un tasto", lasciandosi poi guidare su whatsapp dal truffatore a inserire i dati della propria carta.

Alla luce delle specificità della vicenda, questo Collegio reputa che risulti provata non solo l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione nonché la sua regolarità formale, ma anche dimostrata la colpa grave di parte ricorrente (cfr. in proposito Collegio di Coordinamento, decisione n. 22745/2019), in quanto le modalità attuative delle operazioni disconosciute riflettono uno schema tipico e ormai noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, sms o altri strumenti, a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate. Nella vicenda in esame, inoltre, la truffa si è consumata su una piattaforma di vendita di servizi on line e dunque interamente fuori dai canali dell'intermediario.

Tenuto conto delle circostanze, la ricorrente deve essere considerata vittima di colpevole credulità, in quanto le modalità con le quali la truffa è stata realizzata rientrano tra quelle più diffuse e conosciute, che qualunque fruitore di servizi on line, dotato di normale avvedutezza e prudenza, deve essere in grado di riconoscere ed evitare, tanto più se, come nel caso di specie, si tratta di soggetto avvezzo ad operare su piattaforma e dunque appieno edotto circa le relative consuete modalità operative.

La riconosciuta colpa grave del cliente, pur a fronte di operazioni accompagnate da piena prova della Sca, non esclude naturalmente che il Collegio, tenuto conto delle peculiarità della fattispecie, possa individuare altri e diversi eventuali profili di responsabilità, per esempio sul versante del rispetto degli obblighi di protezione che gravano, per diritto comune, sul *bonus argentarius* anche *sub specie* di mancata gestione di eventi che segnalino la possibilità di frodi o anomalie; profili che, nella vicenda in esame, non ricorrono.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE