

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) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) SCARANO

Seduta del 28/04/2026

FATTO

La ricorrente, titolare di un conto corrente con annessa carta di debito presso l'intermediario, riferisce che tra il 30 aprile e il 2 maggio 2025 la carta veniva fraudolentemente utilizzata per eseguire sei ricariche su una piattaforma di scommesse online, per un importo complessivo di € 800,00. La ricorrente afferma di essersi accorta dell'ammancio il 01.05.2025, accedendo all'applicazione della banca, e di aver provveduto il giorno successivo, con l'aiuto di un familiare, a bloccare la carta di pagamento. In data 06.05.2025 sporgeva denuncia presso le Autorità competenti e presentava reclamo all'intermediario, che rispondeva negativamente. La ricorrente precisa di non aver mai ricevuto notifiche *push* né richieste di autorizzazione in tempo reale per le transazioni contestate, sostenendo che le stesse siano state eseguite in violazione dell'obbligo di autenticazione forte. Evidenzia di essere una persona anziana e scarsamente alfabetizzata digitalmente, che non controlla i messaggi che riceve a causa della diffusa circolazione di messaggi fraudolenti. Afferma che le transazioni presentavano evidenti caratteri di anomalia che l'intermediario ha ignorato e che la banca avrebbe dovuto adottare misure di protezione nei confronti dei soggetti più vulnerabili.

Conclude chiedendo il rimborso dell'importo di € 800,00, nonché la corresponsione degli interessi legali dal giorno dell'addebito al saldo effettivo, il rimborso delle spese di procedura versato pari ad € 20,00;

in via istruttoria, la produzione a carico dell'intermediario di *“tutti i log informatici di autenticazione e i report del sistema di fraud detection relativi alle sei operazioni contestate, al fine di verificare la validità del processo SCA e del monitoraggio delle anomalie”*.

Nelle controdeduzioni, l'intermediario afferma che i fatti alla base della contestazione sono descritti in modo generico, non fornendo elementi utili alla ricostruzione dell'accaduto e che non si ravvisano circostanze riconducibili a una frode. Sostiene che le operazioni siano state correttamente contabilizzate, registrate e autenticate, avendo la ricorrente ricevuto le notifiche *push* e avendo autorizzato ciascuna operazione con l'inserimento del PIN. Conclude affermando di essere privo di responsabilità in ordine alla perdita lamentata.

DIRITTO

Le operazioni contestate rientrano nell'ambito di applicazione del D.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13.01.2018) del D.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno.

Ai sensi dell'art. 10 del D.lgs. 11/2010, è onere dell'intermediario provare che le operazioni contestate siano state correttamente autenticate, registrate e contabilizzate e che non vi siano stati malfunzionamenti dei sistemi; solo successivamente spetta all'intermediario provare dolo o colpa grave dell'utente (Collegio di Coordinamento, decisione n. 22745/2019).

Con riferimento alla SCA, le fonti normative sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10-bis del D.lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato UE 2018/389 della Commissione Europea. Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente accede al suo conto di pagamento online, dispone un'operazione di pagamento elettronico ovvero effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Nel caso di specie, le operazioni contestate sono costituite da sei pagamenti effettuati mediante carta di debito su una piattaforma on-line per un importo complessivo di € 800,00, eseguiti rispettivamente il 30.04.2025 alle ore 12:53, 13:45 e 13:55; il 01.05.2025 alle ore 21:57 e il 02.05.2025 alle ore 00:00 e 01:10.

L'intermediario afferma che le operazioni sono state autenticate tramite notifica *push* inviata sul dispositivo mobile della ricorrente e autorizzate mediante inserimento del PIN. Dai log prodotti alle controdeduzioni risulta che per ciascuna operazione è stata inviata una notifica *push* (elemento di possesso) e che la conferma è avvenuta tramite inserimento dell'MPIN (elemento di conoscenza).

L'intermediario ha tuttavia omesso di fornire la documentazione idonea a dimostrare che la notifica *push* sia stata inviata al dispositivo nella disponibilità della ricorrente e che l'MPIN inserito in risposta provenga da quest'ultima, presupposto essenziale per dimostrare l'avvenuta autenticazione secondo i requisiti della PSD II e la riconducibilità delle operazioni alla ricorrente.

Secondo la giurisprudenza consolidata di questo Arbitro, la prova della Strong Customer Authentication richiede non solo la dimostrazione dell'utilizzo dei fattori di autenticazione, ma anche la verifica che il

dispositivo utilizzato sia effettivamente nella disponibilità e sotto il controllo del legittimo titolare. In mancanza della prova della riferibilità del *device* alla ricorrente, l'elemento del possesso non risulta dimostrato e la prova della corretta autenticazione forte non può dirsi raggiunta, con conseguente accoglimento integrale del ricorso. Come ribadito in caso analogo, infatti, *“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”* (Collegio di Milano, decisione n. 1067/2026).

Riguardo infine alla domanda accessoria di corresponsione degli interessi legali dal giorno dell’addebito al saldo effettivo, il Collegio dispone in base all’art. 11, D.lgs. 11/2010, secondo cui: *“il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l’operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell’accredito non sia successiva a quella dell’addebito dell’importo”*.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l’intermediario corrisponda alla parte ricorrente la somma di € 800,00 con buona valuta.

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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE