Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) MODICA

Seduta del 09/04/2026

FATTO

La cliente afferma che: in data 12/09/2025 effettuava un pagamento su un sito di e-commerce e subito dopo riceveva un sms che le forniva un numero di telefono da chiamare per confermare o disconoscere l'operazione eseguita; chiamava il numero indicato cui rispondeva un sedicente

operatore bancario di un intermediario terzo a conoscenza di tutti i suoi dati bancari; durante la telefonata riceveva tramite SMS dei codici da utilizzare finché la carta non veniva bloccata. Terminata la telefonata si rendeva conto che le erano stati addebitati due pagamenti indebiti da € 990,00 ciascuno.

Chiede la restituzione di € 1.980,00.
L'intermediario controdeduce che: le operazioni contestate sono state correttamente contabilizzate, registrate e autenticate; la ricorrente non ha allegato il messaggio civetta che, in ogni caso, in base alle sue affermazioni, non proveniva da un numero riconducibile alla banca, così come il numero di telefono che ha contattato telefonicamente; secondo l'orientamento costante dei Collegi ABF, la mancata allegazione del messaggio civetta o della chiamata di abboccamento determina il rigetto del ricorso perché non consente di verificare se il mittente era riconducibile all'intermediario e, pertanto, se l'affidamento era legittimo; sussiste la colpa grave della cliente che ha ammesso di aver comunicato al truffatore i codici OTP, segreti e personali, che ha ricevuto sul proprio telefono che hanno consentito al truffatore di portare a compimento le operazioni disconosciute.
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 operazioni e-commerce disposte alle ore 12:04 e 12:05 del 12 settembre 2025 per un importo complessivo di € 1.980,00.

Le operazioni 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 non ha fornito piena prova di SCA.

L'intermediario ricostruisce i singoli passaggi esecutivi delle operazioni fraudolente, fornendo una spiegazione dei processi di autenticazione adottati per l'accesso al servizio tramite sito web e l'autorizzazione delle operazioni. In particolare, l'intermediario chiarisce le procedure necessarie per l'installazione di 2 differenti app, l'App I* tramite cui vengono effettuate le operazioni, e l'App N*/I*N* che serve per la ricezione delle notifiche push contenenti i codici OTP e/o gli alert di esecuzione delle operazioni. Dalle spiegazioni fornite risulta che le operazioni contestate sono state precedute dall'installazione dell' App I* sul device del truffatore, ma non anche dell'App I*N*. Il codice necessario per l'attivazione dell'App I* è stato dunque trasmesso tramite push all'App I*N* installata sul device della ricorrente che lo ha comunicato ai truffatori, così come le notifiche push di conferma di esecuzione delle operazioni. Con particolare riguardo all'operatività internet della carta di pagamento utilizzata per la truffa, l'intermediario ha specificato che l'utente può disporre i pagamenti in modalità e-commerce utilizzando i dati riportati sulla carta (PAN, data scadenza e CVV), facendo accesso all'App I* e autorizzando la notifica dell'operazione che compare nell'App I* tramite fattore biometrico – se tale modalità è stata abilitata- o codice PIN. L'intermediario sostiene che le operazioni contestate sono state precedute dall'enrollment della App I** su un nuovo dispositivo mobile da parte dei truffatori.

In via generale, l'intermediario precisa che l'attivazione della App I**su un nuovo device avviene inserendo le credenziali statiche (userID e password - primo fattore) e il codice OTP inoltrato via SMS al numero di cellulare indicato in contratto oppure via notifica push su App I*N*, nel caso in cui tale applicazione sia stata attivata dal cliente medesimo (secondo fattore). L'utente riceve uno specifico alert che comunica l'attivazione dell'app su dispositivo mobile tramite SMS oppure notifica PUSH si App I*N* e tramite e-mail.

Nel caso di specie, l'intermediario afferma che alle ore 12:00 del 12/09/2025 è stata effettuata la registrazione dell'App I**su un nuovo dispositivo mobile tramite inserimento credenziali statiche (userID e password) e inserimento codice OTP inviato tramite notifica push all'App I*N* della cliente.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Tuttavia, sebbene i log allegati dovrebbero – a detta dell'intermediario - indicare il corretto inserimento sia del codice OTP sia delle credenziali statiche (password-primo fattore di conoscenza) il Collegio non rintraccia alcun riferimento alla password, dovendo pertanto reputare non provata la SCA per l'installazione dell'app sul device del truffatore.

In caso di difetto di piena prova sull'autenticazione anche solo delle fasi preliminari alle transazioni disconosciute, la domanda deve essere accolta integralmente, posto che la prova di autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.980,00.
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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE