COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) MODICA

Seduta del 09/09/2025

FATTO

La cliente riferisce di essere rimasta vittima di un raggiro nel 2022, ancora quando le frodi informatiche non erano particolarmente conosciute, avviatosi con la ricezione di un SMS apparentemente proveniente dalla banca. Afferma di non aver comunicato le proprie credenziali personali e ritiene che sussista una responsabilità della banca per l'accesso abusivo del truffatore al sistema bancario. Chiede il rimborso dell'importo sottrattole con l'operazione disconosciuta, pari a € 4.950,00.
L'intermediario controdeduce che l'operazione di bonifico è stata disposta e autorizzata con regolare utilizzo dei meccanismi di autorizzazione ed autenticazione forte (SCA) adottati e predisposti mediante l'utilizzo delle credenziali personalizzate della cliente; che non sono stati riscontrati malfunzionamenti ai propri sistemi informatici; che sussiste la colpa grave della cliente, la quale ha prestato una collaborazione attiva nell'esecuzione della truffa, cliccando sul link truffaldino contenuto in un SMS che presentava chiari indici di inattendibilità e seguendo pedissequamente le istruzioni del truffatore.
Inoltre, la ricorrente non ha allegato evidenza documentale circa le chiamate asseritamente ricevute e, in ogni caso, il numero fisso indicato nella denuncia non è in alcun modo riconducibile alla banca.
Chiede il rigetto del ricorso.

La cliente, nelle repliche, afferma che l'SMS civetta, non presentando evidenti criticità ed essendo incolonnato all'interno della chat ufficiale dell'intermediario, ha ingenerato un legittimo affidamento circa la genuinità dello stesso; che la vicenda truffaldina è stata caratterizzata da alcune attività sospette (es. cambio dispositivo) che avrebbero dovuto allertare l'istituto di credito. L'intermediario controreplica di aver adottato adeguati presidi di sicurezza a favore della clientela; di avere provato sia la corretta autenticazione, autorizzazione e contabilizzazione dell'operazione di bonifico contestata sia la colpa grave della cliente la quale ha seguito pedissequamente le istruzioni fornite dal truffatore, portando a compimento la truffa; che i sistemi della banca non hanno subito alcun malfunzionamento. Insiste per il rigetto.

DIRITTO

L'operazione contestata, un bonifico eseguito alle ore 12:44 del 20 dicembre 2022 per l'importo di € 4.950,00, ricade 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. q-*bis*, 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 afferma che l'operatività fraudolenta è stata preceduta dall'attivazione di una nuova licenza "smartotp" su un altro dispositivo associato all'utenza Internet Banking della ricorrente a seguito dell'inserimento Utenza + Password + OTP ricevuto via email + OTP ricevuto via SMS sul cellulare certificato dal cliente in fase di contrattualizzazione. Precisa, inoltre, che l'attivazione di una nuova APP/licenza smartOTP comporta l'impossibilità per il dispositivo precedente di accedere alla stessa, rendendola di fatto inattiva. Tuttavia, con riferimento all'avvenuta attivazione della licenza "smartotp" in data 20/12/2022 collegata all'utenza **233 sul device IOS_16.0.3, non vi è evidenza dell'inserimento di Utenza + Password (elemento di conoscenza), necessaria secondo la procedura descritta dall'intermediario e di cui si fa parola nella legenda esplicativa dei LOG.

Questo Collegio, sulla scorta del proprio univoco orientamento (cfr. decisione n. 2951/24), ritiene che la documentazione versata in atti dall'intermediario non consenta di ritenere raggiunta la prova in ordine alla adozione della SCA in fase propedeutica all'esecuzione dell'operazione disconosciuta.

Secondo l'unanime orientamento dei Collegi, in caso di difetto di piena prova anche solo con riguardo alle azioni antecedenti all'esecuzione dell'operazione contestata, il ricorso deve essere accolto integralmente, rimanendo assorbita ogni altra questione riguardante un eventuale profilo di colpa ascrivibile al cliente.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 4.950,00.

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

Firmato digitalmente da
ANDREA TINA