

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) SANTARELLI

Membro di designazione rappresentativa
degli intermediari

(MI) GILIBERTI

Membro di designazione rappresentativa dei
clienti

Relatore (MI) MODICA

Seduta del 29/01/2026

FATTO

La cliente riferisce di essere stata vittima di una truffa consumatasi su un falso sito di annunci; di avere ricevuto in data 21/04/2025 due richieste di OTP tramite SMS cui non dava seguito; di avere provveduto a bloccare la propria carta; di avere ricevuto in data 29/07/2025 una mail che le comunicava dell'avvenuto acquisto e-commerce confermato con uso di credenziali nel possesso della cliente.

Chiede la restituzione di 499,00 euro.

L'intermediario controdeduce che in data 21/04/2025 alle ore 14:01 è stata disposta l'operazione disconosciuta di acquisto e-commerce con carta di debito n.*1282 associata al c/c n. *1989; i codici OTP contenuti nei messaggi genuini ricevuti da parte della ricorrente effettivamente non risultano esser stati utilizzati; l'operazione contestata è stata correttamente contabilizzata, registrata e autenticata in quanto eseguita con il corretto inserimento delle credenziali; il ricorso è inammissibile per palese genericità della domanda, dovuta a carenza di rappresentazione dei fatti ed omissione di dati; sussiste la colpa grave della cliente in quanto non ha verificato la genuinità del suo interlocutore e non si è attenuta a quanto indicato nelle comunicazioni preventive contro le frodi.

Chiede che il ricorso sia dichiarato inammissibile o, in subordine, rigettato nel merito.

La cliente replica che non ha ricevuto alcuna richiesta da parte della banca di inserire il codice a 6 cifre per autorizzare un'operazione; che non sono state effettuate le procedure di verifica autorizzative il trasferimento di denaro.

L'intermediario controreplica che gli SMS genuini con l'intermediario, allegati agli atti e contenenti codici OTP non utilizzati, sono successivi alla prima operazione correttamente autorizzata e sono relativi a tentativi di truffa eseguiti alle ore 14:05 e 14:15 che non hanno determinato alcun addebito;

non si ravvisa alcuna anomalia dei sistemi informatici in sede di disposizione dell'operazione contestata.

DIRITTO

La cliente disconosce una operazione eseguita a valle di una truffa e chiede la restituzione del relativo importo. Si tratta, in particolare, di un'operazione e-commerce disposta con dati di pagamento già memorizzati dal commerciante effettuata alle ore 14:01 del 21/04/2025 per l'importo di 499,00 euro. Disattesa in via preliminare l'eccezione relativa alla genericità della domanda, che viceversa individua chiaramente sia il petitum sia la causa petendi, il Collegio richiama il 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 PSD2, 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, difetta la prova di autenticazione con impiego di doppio fattore. Dopo avere affermato che l'operazione è stata autorizzata tramite ricezione di notifica push su APP riepilogativa dell'operazione e conferma con inserimento del codice mPin creato dalla cliente in fase di attivazione dell'applicazione sul suo device, l'intermediario allega i log da cui risulta un'operazione autorizzata alle

ore 14:01 del 21/04/2025 di importo pari a 499,00 euro mediante “7- Push Notification – conferma della notifica tramite MPIN nella APP del Mobile Banking”. Dalla documentazione prodotta, tuttavia, non è dato verificare la riferibilità alla cliente del device cui è stata inviata tale notifica e dal quale è stata dunque disposta l’operazione. In mancanza di tale dato, che integra l’elemento del possesso, non può dirsi raggiunta piena prova della autenticazione, con conseguente integrale accoglimento del ricorso.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l’intermediario corrisponda alla parte ricorrente la somma di € 499,00.

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