

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) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) MODICA

Seduta del 18/12/2025

FATTO

La cliente pubblicava un annuncio di vendita di una poltrona su un famoso sito di annunci e veniva contattata da un acquirente che chiedeva di procedere al pagamento mediante App della banca. Accettava tale proposta malgrado la procedura le fosse ignota e in data 15/05/2025 attuava procedure in App dietro indicazioni del presunto acquirente: riceveva la foto di un QR code generato da uno sportello ATM a Marghera (VE); inquadrava tale codice con il suo telefono mentre era in una zona vicino a Como (CO); veniva disposto da uno sportello ATM a Marghera un prelievo "smart" di € 1.000,00 dal c/c della cliente.

Chiede la restituzione di € 1.000,00.

L'intermediario controdeduce che la ricorrente ha eseguito l'accesso, ha inserito il numero di adesione, la password dell'app e il numero telefonico; l'operazione è stata correttamente contabilizzata, registrata e autorizzata, senza malfunzionamenti o intrusioni nei propri sistemi informatici; la cliente ha negligenemente violato l'art.13, comma 2, del contratto consentendo l'accesso al truffatore ai suoi dati sensibili.

Chiede il rigetto del ricorso.

Con le repliche la cliente insiste nella domanda, confermando quanto già rappresentato nel ricorso, precisando che ha concorso incolpevolmente quale vittima del reato di truffa, ex art.640 c.p.

DIRITTO

La cliente disconosce una operazione eseguita a valle di una truffa e chiede la restituzione del relativo importo. L'operazione contestata, un prelievo "smart" della somma di € 1000,00 presso sportello ATM effettuato alle ore 17:03:29 del 15 maggio 2025, 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 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, è stata fornita prova di autenticazione con impiego di doppio fattore.

L'intermediario ha chiarito preliminarmente che la procedura richiede che il cliente acceda all'App; che selezioni la voce "preleva adesso"; che inquadrando con lo smartphone abilitato il QR code rappresentato nell'apparecchiatura automatica prescelta. Sulla base delle evidenze prodotte con riferimento alla fase di accesso all'home banking delle ore 16:58:57 del 15/05/2025, risulta un "accesso mobile banking con

fingerprint” mediante utilizzo dell’APP su device (fattore di possesso) e inserimento fingerprint (fattore di inerenza). Dai log sicurezza risulta inoltre che la fase di prenotazione del prelievo smart (“attivazione fingerprint bancomatpay”) sia avvenuta contestualmente alla fase di login (ore 16:58:57), mediante utilizzo dell’APP su device (fattore di possesso) e inserimento fingerprint (fattore di inerenza), diverso, ancorché contestuale, rispetto a quello usato in fase di login. Effettuata la prenotazione del prelievo, la somma “prenotata” è stata erogata alle ore 17:03:29. L’esame dei log e le dichiarazioni delle parti inducono a ritenere che la cliente si trovasse già in ambiente conforme a SCA, cioè in App (“controllo-token” alle ore 16:59:50, elemento di possesso) a seguito di inserimento del fingerprint (elemento di inerenza), e che abbia provveduto a scansionare con app aperta sul suo smartphone il QR code inviato su diverso device. Il Collegio reputa compliant alla SCA la modalità autorizzativa sopra descritta (Collegio di Roma, decisione n. 3032/2023 e n.4169/25).

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. La cliente afferma di aver ricevuto due chiamate – di cui non fornisce alcuna evidenza – provenienti da numeri comunque non riconducibili all’intermediario. Ha inoltre accettato di concludere l’affare fuori dalla piattaforma su cui era stato pubblicato l’annuncio e sulla quale sarebbe stato opportuno rimanere anche in fase di esecuzione del pagamento del prezzo convenuto. Infine, ha accettato di ricevere la somma concordata mediante una procedura a lei ignota e mai sperimentata in precedenza. Tenuto conto delle circostanze del caso concreto, la ricorrente deve essere considerata vittima di colpevole credulità, in quanto le modalità con le quali la truffa è stata realizzata rientrano tra quelle che qualunque fruitore di servizi on line, dotato di normale avvedutezza e prudenza, deve essere in grado di riconoscere ed evitare (cfr. Collegio di Coordinamento n. 3498 del 26/10/2012).

La riconosciuta colpa grave della cliente, pur a fronte di operazioni accompagnate da piena prova della Sca, non esclude naturalmente che il Collegio, tenuto conto delle peculiarità del caso, 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