

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) AFFERNI

Membro di designazione rappresentativa
dei clienti

Relatore (MI) MODICA

Seduta del 24/03/2026

FATTO

Il cliente dichiara di avere pubblicato un annuncio per la vendita della propria automobile; di essere stato contattato, in data 17/11/2025, da un sedicente acquirente che avrebbe proceduto al pagamento tramite una “procedura di bonifico cardless” presso uno sportello ATM inviando un QR

code, da inquadrare tramite l'App della banca per ricevere il pagamento. Procedeva ad inquadrare il QR e ad autorizzare l'operazione tramite App seguendo le indicazioni ricevute; si avvedeva quindi di essere stato vittima di una truffa in quanto l'operazione era stata eseguita a favore di terzi e risultava ancora da contabilizzare. Procedeva a recarsi in filiale e a presentare denuncia presso le Autorità; presentava reclamo all'intermediario in data 18/11/2025, che veniva riscontrato negativamente.

Chiede la restituzione di € 1.500 oltre interessi legali.

L'intermediario controdeduce che il ricorso è infondato in quanto il cliente ha autorizzato l'operazione, inquadrando il QR code ricevuto e selezionando l'importo di addebito; l'operazione è stata correttamente contabilizzata, registrata e autenticata in quanto posta in essere tramite del proprio dispositivo certificato; non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici; il cliente era stato informato della possibilità di fruire del servizio Cardless. Afferma sussistere la colpa grave del cliente che ha riposto fiducia nei confronti del sedicente acquirente seguendo le indicazioni durante la telefonata, piuttosto che fornire i propri dati per ricevere l'accredito; le linee guida della piattaforma utilizzata per la vendita, indicano espressamente quali canali di pagamento utilizzare per ricevere il compenso.

Chiede il rigetto del ricorso o, in subordine, il riconoscimento di un concorso di colpa.

Il cliente replica che: l'autenticazione a doppio fattore non prova che egli fosse a conoscenza dell'operazione; ha seguito le indicazioni del truffatore sotto costrizione psicologica in un lasso temporale talmente breve da impedirgli di leggere attentamente la schermata del telefono; non sussiste colpa grave in quanto non ha rivelato le proprie credenziali e non ha utilizzato canali non ufficiali di pagamento; le linee guida della piattaforma utilizzata per la vendita non rilevano al fine di dimostrare la colpa grave. Insiste nella domanda.

L'intermediario controreplica che il lasso temporale indicato dal cliente è abbastanza lungo per poterlo rendere consapevole delle operazioni svolte; la banca non invita i clienti ad autorizzare le operazioni in stato di urgenza o concitazione; le linee guida della piattaforma rilevano in quanto chi accetta di vendere per suo tramite si suppone abbia accettato parimenti le condizioni di vendita ed i potenziali rischi connessi.

DIRITTO

Il cliente disconosce un prelievo smart eseguito a valle di una truffa alle ore 14:56 del 17/11/2025 e chiede la restituzione del relativo importo (€ 1.500,00).

L'operazione contestata 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. 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 ha fornito prova di autenticazione con impiego di doppio fattore. Sulla base delle evidenze prodotte con riferimento alla fase di accesso all'Home Banking delle ore 14:55.51 del 17/11/2025, infatti, risulta l'utilizzo dell'APP su device (fattore di possesso); l'inserimento FACE_ID (fattore di inerenza). In merito alla riconducibilità al cliente dei dispositivi utilizzati per l'autorizzazione dell'operazione, l'intermediario afferma che il dispositivo utilizzato per autorizzare l'operazione è il device modello Ip*** Xs; che l'enrollment dell'App su tale dispositivo in uso al cliente sia stato effettuata in data 21/12/2022. Il secondo dispositivo, che a detta del cliente sarebbe quello su cui avrebbe ricevuto il QR code da inquadrare, è identificato dall'intermediario con il modello "Ip*** 7 Plus", il cui enrollment sarebbe stato effettuato in data 30/04/2021. Dai log prodotti risulta che: per il dispositivo Ip*** 7 Plus è stata effettuata l'enrollment in data 30/04/2021; per il dispositivo Ip*** Xs è stata effettuata l'enrollment in data 21/12/2022; l'operazione fraudolenta è stata autorizzata con il dispositivo Iphone Xs; entrambi i dispositivi sono associati all'Userd ID 21556545. Quanto all'esecuzione dell'operazione, risulta che il cliente ha autorizzato l'operazione di prelievo nella medesima sessione Id in cui ha effettuato la login; l'operazione è stata eseguita alle ore 14:56.35; al fine dell'autenticazione dell'operazione fraudolenta, sono stati utilizzati possesso del dispositivo certificato dotato di token app e riconoscimento biometrico (fattore di inerenza) tramite Face_ID; entrambi i fattori di autenticazione riportano la dicitura "Status Ok", che indica il loro inserimento con successo; non si rilevano anomalie.

Pertanto, dall'esame dei log e delle dichiarazioni delle parti, risulta che il cliente si sia trovato in ambiente già conforme a SCA, cioè in App alle ore 14: 55.51 (elemento di possesso) a seguito di inserimento del FACE_ID (elemento di inerenza), e che abbia provveduto a scansionare con il suo smartphone il QR code inviato su un diverso device.

Del pari provata appare la colpa grave del cliente, vittima di una truffa banale cui avrebbe potuto sottrarsi con l'impiego di una media diligenza. Risulta decisiva in questo senso la circostanza che le trattative si siano svolte al di fuori dei canali messi a disposizioni della piattaforma e che il cliente abbia concluso la vendita fuori dall'ambiente protetto; inoltre, non vi è evidenza della chiamata da cui è originata la truffa: è comunque non contestato che si trattasse di utenza non riferibile all'intermediario.

Tenuto conto delle circostanze del caso concreto, il ricorrente deve essere considerato vittima di colpevole credulità, in quanto le modalità con le quali la truffa è stata realizzata rientrano tra quelle più diffuse e conosciute, 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 del cliente, pur a fronte di operazioni accompagnate da piena prova della Sca, non esclude naturalmente che il Collegio, tenuto conto delle peculiarità della fattispecie, 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. Sebbene il cliente affermi che la funzione "prelievo cardless" fosse a lui sconosciuta, l'intermediario documenta l'invio di una proposta di modifica unilaterale del contratto e inerente l'introduzione di tale servizio.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE