

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) RIZZO

Seduta del 09/04/2026

FATTO

Il cliente afferma di essere stato derubato per un acquisto mai effettuato.

Nella denuncia, in particolare, il cliente afferma che, in data 05/11/2025, ignoti malfattori hanno clonato la sua carta n. 516*****25 ed effettuato una transazione dal valore di € 307,45.

Il ricorrente domanda, quindi, la restituzione della somma sottrattagli.

Nelle controdeduzioni, l'intermediario convenuto, riportato il fatto, afferma quanto segue:

- il cliente è titolare della carta di debito n.516*****25 abilitata al servizio internet banking;

- il cliente, nel modulo di disconoscimento, afferma di avere ricevuto delle strane e-mail riferite all'importo del disconoscimento, lasciando dedurre che l'operazione è stata effettuata dallo stesso in seguito a un raggio;
- sulla base dei LOG risulta che l'operazione oggetto di controversia è stata disposta e validamente autorizzata tramite SCA con la carta del cliente attraverso il dispositivo usualmente utilizzato dallo stesso, e deve quindi qualificarsi come autorizzata ai fini del D.lgs. 11/2010;
- la banca ha anche inviato al cliente una notifica PUSH per l'autorizzazione che descriveva compiutamente la natura dell'operazione e il suo ammontare effettivo;
- il cliente non ha mai denunciato né lo smarrimento, né il furto della carta di pagamento e del suo cellulare tramite cui è stata effettuata l'operazione disconosciuta;
- il cliente non indica quali siano i fatti che rendano plausibile una responsabilità dell'intermediario, né aggiunge alcuna allegazione al ricorso per chiarire la ricostruzione della vicenda, circostanza che avvalorava la sua colpa grave.

L'intermediario convenuto domanda, quindi, il rigetto del ricorso in quanto infondato in fatto e in diritto.

DIRITTO

Oggetto della presente controversia è una operazione di pagamento in e-commerce, per un importo di € 307,45, posta in essere il 05/11/2025 alle ore 11:34. Alla data dell'operazione trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.

È agli atti la denuncia del cliente presentata in data 08/11/2025 alle 11:16.

Quanto all'autenticazione forte, corretta registrazione e contabilizzazione dell'operazione contestata, dall'esame dei log informatici prodotti agli atti dall'intermediario convenuto risulta che la stessa è stata, correttamente, autenticata tramite i fattori del POSSESSO del dispositivo identificato come bdc*****52; e della CONOSCENZA del codice PIN inserito in risposta alla PUSH (MSG INPUT – AuthType:PIN).

Analizzando la condotta delle parti e i profili rilevanti per la valutazione di sussistenza della colpa, osserva il Collegio come il ricorrente non abbia riferito nulla in merito alle modalità con le quali è avvenuto l'utilizzo fraudolento, limitandosi a reiterare il disconoscimento dell'operazione, affermando che la propria carta di pagamento sarebbe stata clonata.

Tanto premesso, si rammenta come, secondo l'orientamento dei Collegi ABF, nelle contestazioni di utilizzi fraudolenti on line di strumenti di pagamento in cui: i) l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute; ii) il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA); iii) non risultano indizi di anomalia delle operazioni e/o ulteriori elementi; le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del cliente medesimo. Più in particolare, i Collegi sono unanimi nel ritenere che la mancata allegazione, da parte del cliente, del messaggio civetta (ovvero, per il vishing, del registro delle chiamate) debba determinare il rigetto del ricorso, in quanto non consente di

verificare se il mittente/chiamante risulti riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la genuinità del messaggio o della telefonata ricevuti.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE