

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) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) RIZZO

Seduta del 24/02/2026

FATTO

La cliente afferma quanto segue:

- in data 28/09/2025, con lo scopo di effettuare una ricarica telefonica presso il suo fornitore, ha disposto un pagamento di € 20,00 con il proprio cellulare accedendo a quello che sembrava essere il sito del proprio operatore telefonico;
- durante la procedura, la cliente notava una difformità rispetto a operazioni di ricarica fatte in passato, essendo il pagamento questa volta richiesto tramite inserimento dei dati della carta;
- la cliente proseguiva comunque nel procedimento, inserendo i propri dati e confermando l'operazione sul sito dell'operatore telefonico e sull'APP di banca.
- dopo l'operazione in questione, la cliente si rendeva conto di ulteriori anomalie, in quanto la schermata visualizzata risultava diversa da quella abitualmente utilizzata per le ricariche telefoniche e i dati inseriti apparivano come modificati o sovrascritti in modo non coerente;
- subito dopo la conferma, la cliente riceveva un messaggio dalla banca nel quale veniva indicata l'esecuzione di un'operazione di pagamento dell'importo di € 390,33 in favore del soggetto a lei sconosciuto I*****g;
- la cliente ha immediatamente bloccato la carta, sporto denuncia e disconosciuto il pagamento;
- la sua banca ha respinto la richiesta di rimborso affermando che l'operazione è stata da lei correttamente autorizzata;
- la cliente non soddisfatta della soluzione a cui è giunta la banca si riferisce all'Arbitro Bancario e Finanziario.

La ricorrente domanda, quindi, il rimborso integrale dell'importo di € 390,00, oltre gli interessi e le spese della presente procedura.

Nelle controdeduzioni, l'intermediario convenuto afferma quanto segue:

- l'operazione di pagamento in contestazione risulta approvata correttamente tramite un sistema di autenticazione forte e senza alcun malfunzionamento o compromissione dei sistemi, nel rispetto dei requisiti SCA;
- sussiste la colpa grave della cliente in quanto: la cliente è stata messa nelle condizioni di conoscere l'importo e il beneficiario dell'operazione che stava autorizzando: al momento dell'effettuazione del pagamento è stata, infatti, trasmessa al suo telefono una notifica "PUSH PARLANTE" per la validazione dell'operazione, questa indicava chiaramente ammontare del pagamento e beneficiario; la cliente ha, però, ignorato la notifica in questione; la cliente ammette di aver rilevato delle anomalie nelle richieste fatte dal sito in fase di pagamento, cionondimeno ha inserito i dati e autorizzato l'operazione; l'operazione disconosciuta è avvenuta tramite il telefono utilizzato in precedenza dalla ricorrente in altre sessioni di pagamento.
- la banca fornisce alla propria clientela ampia informativa in ordine alla prevenzione delle frodi.

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

DIRITTO

Oggetto della presente controversia è un'operazione disconosciuta, per l'importo di € 390,33, posta in essere il 28/09/2025. 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.

La ricorrente produce agli atti evidenza della presentazione della denuncia il 28 settembre 2025.

Quanto all'autenticazione forte, corretta registrazione e contabilizzazione delle operazioni contestate, dall'esame dei log informatici prodotti agli atti dall'intermediario convenuto risulta che l'autenticazione è avvenuta tramite l'applicazione di mobile token del PSP sullo smartphone, sbloccata con codice PIN, che genera un codice che ha il valore dei due fattori della SCA congiunti ("conoscenza" del PIN e "possesso" dello smartphone). Rileva, inoltre, il Collegio che la ricorrente stessa riferisce, in sede di denuncia, di avere inserito i dati richiesti nell'app della banca.

Analizzando la condotta delle parti e i profili rilevanti per la valutazione di sussistenza della colpa, questo Collegio deve, anzitutto, rilevare come la ricorrente non produca documentazione relativa al sito clone dell'operatore telefonico. Cionondimeno, già dalla ricostruzione della ricorrente precedentemente esposta può escludersi che la truffa abbia assunto i caratteri dello spoofing, trattandosi, invece, di una variante di phishing.

L'orientamento dei Collegi ABF evidenzia, ormai da tempo, che simili tipologie di truffa si svolgono secondo uno schema tipico e noto, consistente nell'indurre il titolare dello strumento, tramite e-mail a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o, più genericamente, l'opportunità di verificare o implementare caratteristiche di sicurezza. La diffusione del fenomeno è tale che in questi casi la condotta del cliente, secondo l'orientamento dei Collegi, è generalmente connotata da colpa grave, in quanto l'impiego di una media diligenza sarebbe sufficiente a impedire la frode.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE