

## COLLEGIO DI MILANO

composto dai signori:

|                 |                                                           |
|-----------------|-----------------------------------------------------------|
| (MI) TINA       | Presidente                                                |
| (MI) MODICA     | Membro designato dalla Banca d'Italia                     |
| (MI) BALDINELLI | Membro designato dalla Banca d'Italia                     |
| (MI) CAPIZZI    | Membro di designazione rappresentativa degli intermediari |
| (MI) CESARE     | Membro di designazione rappresentativa dei clienti        |

Relatore (MI) CESARE

Seduta del 26/05/2026

## FATTO

La ricorrente afferma che, collegandosi sul sito s\*\*\*\*.it per inserire un oggetto da vendere, veniva contattata da un operatore che via chat le chiedeva di inserire i dati della carta di credito e del bancomat per effettuare prelievi di € 340,00 su ciascuna carta che le sarebbero stati restituiti a conferma dell'iscrizione al sito. Trascorsa circa mezz'ora, le somme non venivano restituite e la ricorrente comprendeva di essere stata truffata. Ha sporto denuncia ai Carabinieri e presentato procedura di disconoscimento; la banca ha comunicato l'esito negativo della pratica. Chiede il risarcimento dell'intero importo.

Nelle controdeduzioni l'intermediario afferma che in data 15.01.2026 la ricorrente ha eseguito 2 pagamenti online di € 340,00 ciascuno, rispettivamente alle ore 10:46 con carta di debito e alle ore 11:03 con carta di credito, per un importo complessivo di € 680,00, che il 21.01.2026 la cliente ha denunciato l'accaduto e disconosciuto. Sostiene che le operazioni siano autorizzate ai sensi dell'art. 5 del D.Lgs. n. 11/2010, avendo la cliente personalmente autorizzato i pagamenti; che entrambe le operazioni sono state autenticate mediante OTP dinamico generato tramite fattore biometrico sul device abitualmente utilizzato dalla cliente; che la push notification era parlante, recando tipologia, importo e beneficiario; che la motivazione fornita dal sedicente operatore era anomala e priva di credibilità. Precisa che la carta di debito è stata bloccata per motivi di sicurezza alle ore 11:02 del 15.01.2026, dopo la prima operazione, e che per la seconda è stato inviato un SMS alert al numero di cellulare contrattualizzato dalla cliente. Chiede il rigetto del ricorso.

## DIRITTO

La controversia riguarda il disconoscimento di 2 operazioni di pagamento online del 15.01.2026, di € 340,00 ciascuna, eseguite con carta di debito alle ore 10:46 e con carta di credito alle ore 11:03, per

un importo complessivo di € 680,00, nell'ambito di una truffa riconducibile alla tecnica del website spoofing.

In via preliminare, il modulo di disconoscimento compilato dalla ricorrente sulla modulistica dell'intermediario è equiparabile al reclamo preventivo ai fini della procedibilità del ricorso (Collegio di Milano, decisione n. 2614/2023; decisione n. 15485/2022).

Quanto alla qualificazione delle operazioni, la ricorrente ha dichiarato nel modulo di disconoscimento di non aver disposto le operazioni pur avendo le carte sempre in proprio possesso, indicando al contempo nel ricorso di aver fornito i dati delle carte e di aver autorizzato i prelievi su istruzione dell'operatore via chat. Il contributo della cliente in fase autorizzativa è pertanto parziale. Secondo l'orientamento consolidato dei Collegi, quando il concorso causale dell'utente è parziale, la transazione non deve intendersi autorizzata ai sensi dell'art. 5 del D.Lgs. n. 11/2010, restando ferma la necessità che il consenso sia prestato nella forma convenuta tra le parti (Collegio di Milano, decisione n. 4601/2024). Il Collegio procede pertanto all'esame della prova di autenticazione ai sensi degli artt. 10 e 10-bis del D.Lgs. n. 11/2010.

L'intermediario ha documentato che entrambe le operazioni sono state autenticate mediante la combinazione di fattore biometrico (inerenza, "authType": "TOUCH") e OTP dinamico generato tramite l'applicazione installata sul device identificato dal codice univoco CF\*\*\*\*\*E12AE42, corrispondente allo smartphone con sistema operativo iOS abitualmente utilizzato dalla cliente. I log prodotti consentono di verificare i singoli passaggi dell'autenticazione per ciascuna operazione. Il Collegio ritiene pertanto raggiunta la prova della SCA.

Accertata la SCA, il Collegio valuta la colpa grave della ricorrente ai sensi dell'art. 10 del D.Lgs. n. 11/2010 (Coll. Coord. n. 22745/2019). La push notification era parlante, recando tipologia, importo e beneficiario; per la seconda operazione è stato inviato un SMS alert al numero contrattualizzato, con l'indicazione dell'importo di € 340,00, della carta e del beneficiario. La storia narrata dal sedicente operatore era priva di credibilità. La fattispecie rientra nello schema tipico e noto del website spoofing, rispetto al quale l'impiego di ordinaria diligenza avrebbe consentito di riconoscere la truffa. Il Collegio ravvisa pertanto la colpa grave della ricorrente, da ravvisare anche nella circostanza che i fatti riportati dalla ricorrente non appaiono sufficientemente dettagliati da poter desumere aliunde altri elementi di colpa.

Alla luce delle considerazioni che precedono, il Collegio non accoglie il ricorso.

### **PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

**IL PRESIDENTE**