

## COLLEGIO DI BARI

composto dai signori:

|                |                                                           |
|----------------|-----------------------------------------------------------|
| (BA) TUCCI     | Presidente                                                |
| (BA) PORTA     | Membro designato dalla Banca d'Italia                     |
| (BA) BARTOLINI | Membro designato dalla Banca d'Italia                     |
| (BA) CIPRIANI  | Membro di designazione rappresentativa degli intermediari |
| (BA) BOTTALICO | Membro di designazione rappresentativa dei clienti        |

Relatore NICOLA CIPRIANI

Seduta del 13/04/2026

### FATTO

A. La ricorrente si rivolge all'Arbitro illustrando che l'8/11/2025, dopo aver pubblicato un annuncio su una piattaforma web per la vendita di un mobile al prezzo di € 340,00, è stata contattata da un potenziale acquirente. In particolare, la ricorrente precisa che un potenziale acquirente le ha inviato un link tramite WhatsApp allo scopo dichiarato di verificare se la sua carta di credito fosse abilitata alle operazioni di compravendita online; dopo aver cliccato sul link, la ricorrente ha inserito il numero della propria carta di debito, comprensivo di CVC. All'esito, la ricorrente ha ricevuto una notifica in App che la informava di una transazione di € 340,00, destinata a "Western Union Vienna" e ha conseguentemente provveduto a bloccare la carta. Successivamente, l'istante ha presentato formale denuncia e ha inoltrato il disconoscimento dell'operazione all'intermediario, precisando che dall'esame del relativo modulo si evince che aveva "di fatto disposto l'operazione che però rientra nei falsi acquisti". Con comunicazione del 03/12/2025, l'intermediario ha riscontrato il predetto disconoscimento, negando ogni sua responsabilità. Pertanto, la ricorrente chiede il rimborso della somma di € 340,00.

B. Costituitosi, l'intermediario rileva che la truffa si è consumata al di fuori del suo ambito di controllo e che l'esecuzione dell'operazione è da imputare alla stessa ricorrente, la quale ha agito senza "la cautela e l'accortezza necessarie", generando un danno che è "diretta conseguenza del suo incauto affidamento in una serie di richieste assolutamente anomale, pervenute da mittenti ignoti". Alla luce di quanto riportato nel modulo di disconoscimento, l'intermediario considera che il pagamento sia da qualificare come operazione autorizzata ex art. 5, commi 1 e 2 del D.Lgs. n. 11/2010 e di aver correttamente dato seguito all'ordine di pagamento disposto dalla ricorrente. In ogni caso, l'intermediario precisa che il sistema di autenticazione adottato prevede, per l'accesso ai servizi online,

l'inserimento simultaneo di password statiche (codice Titolare e PIN) e dinamiche (codice O-Key, generato dall'App mobile o via sms) e che, una volta collegati al servizio online, per autorizzare le operazioni dispositive è necessario inserire il predetto codice O-Key, a seguito della selezione della notifica ricevuta in App e della digitazione sul device del PIN oppure, se abilitati, dell'apposizione dell'impronta digitale o del riconoscimento facciale. Nel caso in esame, l'operazione disconosciuta dalla cliente è stata eseguita dopo essere stata "autenticata, correttamente registrata e contabilizzata" e non ha "subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione. Pertanto, l'intermediario conclude per il rigetto del ricorso.

## **DIRITTO**

1. La controversia concerne la richiesta di rimborso dell'importo relativo ad un'operazione di pagamento per l'ammontare complessivo di € 340,00.

2. Preliminarmente, il Collegio osserva che, dalla narrazione dei fatti e dalla documentazione in atti (cfr. in particolare il modulo di disconoscimento e la denuncia), emerge chiaramente che la ricorrente ha autorizzato personalmente l'operazione, pur se a seguito di asseriti raggiri perpetrati dal frodatore. In particolare, la ricorrente ha dichiarato di aver inserito i dati della propria carta di pagamento per adempiere alle richieste dei presunti acquirenti, sebbene nell'erroneo convincimento di verificare se la stessa fosse abilitata al compimento di tali operazioni.

Orbene, il Collegio rileva che – conformemente a quanto affermato per casi analoghi (cfr. Collegio di Bari, decisione n. 7864/2025; decisione n. 5871/2025; decisione n. 11080/2024; decisione n. 7894/2024; decisione n. 5815/2024) – la ricostruzione dei fatti e gli elementi riportati dalla stessa ricorrente conducono a ritenere inapplicabile la disciplina prevista dal d.lgs. n. 11/2010 per le ipotesi di utilizzi fraudolenti di strumenti di pagamento; infatti, è pacifico che l'operazione in esame sia stata conclusa personalmente dalla ricorrente, sia pure in virtù del raggiro subito.

3. Nel caso in esame, non appare nemmeno configurabile a carico del PSP una responsabilità concorrente sulla base delle evidenze disponibili e secondo le norme di diritto comune, il che potrebbe verificarsi in concreto, secondo le posizioni più recenti condivise dai Collegi, quando emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode come, ad esempio, nei casi di:

- a) mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;
- b) mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore;
- c) mancato rilievo di indizi di frode (di cui all'art. 8 del D.M. 30.04.2007, n. 112), nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere.

Il Collegio osserva che nessuna di queste ipotesi ricorre nel caso di specie.

Pertanto, alla luce delle valutazioni svolte, la domanda del ricorrente non può trovare accoglimento.

## **P.Q.M.**

**Il Collegio non accoglie il ricorso.**

IL PRESIDENTE