

## **COLLEGIO DI MILANO**

composto dai signori:

|                   |                                                           |
|-------------------|-----------------------------------------------------------|
| (MI) TINA         | Presidente                                                |
| (BA) BARTOLOMUCCI | 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 10/02/2026

## **FATTO**

Il cliente afferma che in data 23 settembre 2025 ha disposto un pagamento di 10 euro con il cellulare accedendo al sito dell'operatore telefonico per effettuare una ricarica telefonica presso il suo fornitore. Dopo l'operazione ha ricevuto una notifica di ricarica ma si è reso conto che l'addebito sul suo conto era di una somma diversa, pari a €575,39. Ritenendo di essere rimasto vittima di una truffa ha contattato immediatamente il numero verde dell'intermediario disconoscendo il pagamento e bloccando la carta. Ha sporto denuncia. La sua banca gli ha inizialmente riaccreditato la suddetta

somma per poi comunicargli in data 17 ottobre 2025 che dalle verifiche effettuate l'operazione era da ritenersi correttamente autorizzata dal cliente con le sue credenziali e che quindi l'importo inizialmente riaccreditato sarebbe stato nuovamente addebitato. Per tali ragioni il cliente domanda il rimborso della somma addebitata.

Nelle controdeduzioni, l'intermediario afferma di garantire un servizio internet banking con inserimento simultaneo di password statiche e dinamiche. Fornisce alla propria clientela ampia informativa in ordine alla prevenzione delle frodi informatiche nella sezione sicurezza del proprio sito. 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. In particolare risulta eseguita mediante autenticazione a due fattori appartenenti rispettivamente alle categorie della inerenza ossia il fattore biometrico TOUCH e del possesso ossia il codice generato dall'APP installata sul telefono del cliente. L'episodio fraudolento è imputabile esclusivamente alla negligenza del cliente la cui colpa grave emerge dalle seguenti circostanze. Il cliente non allega alcuna prova ai fatti che riporta. L'intermediario ha assolto al duplice onere probatorio posto a suo carico. Il cliente non ha assolto al proprio obbligo di custodia degli strumenti e dei codici di accesso per il servizio online. L'intermediario chiede quindi il rigetto del ricorso.

## **DIRITTO**

La controversia riguarda il disconoscimento di 1 operazione di pagamento eseguita in data 23 settembre 2025 per un importo di €575,39 a seguito di truffa ai danni del cliente. All'operatività contestata si applica il decreto legislativo 27 gennaio 2010 n. 11 come modificato dal decreto legislativo n. 218/17 di attuazione della direttiva 2015/2366/UE (PSD2).

L'articolo 10 del decreto legislativo n. 11/2010 prevede che il prestatore di servizi di pagamento deve provare che l'operazione è stata autenticata correttamente registrata e contabilizzata e che non ha subito malfunzionamenti. Successivamente deve dimostrare che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti dall'articolo 7 del decreto.

Nel caso di specie l'intermediario ha fornito prova dell'autenticazione dell'operazione contestata. In data 23 settembre 2025 alle ore 09:33 è stato effettuato un login dall'APP autorizzato mediante

fattore di possesso (validazione del token dell'app) e fattore biometrico (TOUCH). Successivamente alle ore 09:34 l'operazione è stata autenticata tramite un codice OTP dinamico generato tramite APP installata sul telefono (fattore di possesso) e generato previa validazione del fattore biometrico (fattore di inerenza). L'operazione risulta pertanto autenticata mediante ricorso a un elemento di inerenza (biometria) e a un elemento di possesso (OTP generato tramite APP) in conformità all'autenticazione forte richiesta dalla normativa PSD2.

Una volta provata l'autenticazione l'intermediario deve fornire la prova della colpa grave del cliente. Il cliente non fornisce dettagli in merito alle modalità con le quali è avvenuto l'utilizzo fraudolento. Nella denuncia e nel ricorso rappresenta solo di essersi accorto dell'utilizzo fraudolento consultando l'app della banca. Secondo l'orientamento condiviso tra i Collegi in aderenza al dato normativo è necessario e sufficiente ai fini dell'applicazione della PSD2 che il cliente neghi di aver autorizzato la transazione. Il Collegio può valutare la mancata allegazione dei fatti tra i vari elementi per formare il proprio convincimento circa la colpa grave del ricorrente solo una volta verificata la sussistenza della SCA.

Secondo l'orientamento consolidato dei Collegi, nelle operazioni fraudolente in cui l'intermediario ha provato l'autenticazione delle transazioni disconosciute con la Strong Customer Authentication e non risultano indizi di anomalie, le mancate allegazioni del cliente sulle circostanze di fatto della truffa rappresentano un elemento da cui il Collegio può trarre il proprio convincimento 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 debba determinare il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e pertanto se sia configurabile un legittimo affidamento dell'utente circa la genuinità del messaggio ricevuto.

Nel caso di specie il cliente non fornisce evidenze rispetto a quanto afferma in sede di ricorso in relazione alla dinamica della truffa e al presunto sito clone cui si sarebbe collegato. Non produce alcuna evidenza del messaggio decettivo o di altri elementi che possano dimostrare la natura particolarmente sofisticata della truffa in grado di escludere la colpa grave. A fronte di un sistema di autenticazione conforme ai requisiti dell'autenticazione forte come previsti dalla normativa vigente e in mancanza di elementi che consentano di affermare che l'operazione si sia svolta con modalità tali da escludere la colpa grave deve presumersi la colpa grave dell'utilizzatore dello strumento di pagamento e il ricorso va quindi rigettato.

**PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

IL PRESIDENTE