

## COLLEGIO DI MILANO

composto dai signori:

|                         |                                                           |
|-------------------------|-----------------------------------------------------------|
| (MI) TINA               | Presidente                                                |
| (MI) MODICA             | Membro designato dalla Banca d'Italia                     |
| (MI) DELL'ANNA MISURALE | Membro designato dalla Banca d'Italia                     |
| (MI) SANTARELLI         | Membro di designazione rappresentativa degli intermediari |
| (MI) AFFERNI            | Membro di designazione rappresentativa dei clienti        |

Relatore (MI) AFFERNI

Seduta del 19/05/2026

## FATTO

La ricorrente, titolare di un conto corrente presso l'intermediario convenuto, espone di aver ricevuto in data 13.01.2026 una notifica tramite l'app della banca relativa a un addebito di € 25,94. Mentre tentava di bloccare la propria carta di debito, veniva contattata telefonicamente da un sedicente operatore dell'intermediario. L'interlocutore, dopo averle chiesto conferma della sua identità, la informava di un'operazione fraudolenta in corso e la indirizzava a un collega per bloccare i pagamenti e la carta. Successivamente, le veniva comunicato che avrebbe ricevuto una notifica all'interno dell'app, sulla quale avrebbe dovuto cliccare "acconsenti" per ottenere il rimborso dell'importo di € 25,94. La cliente, eseguita l'operazione e ricevuto l'accredito, si convinceva della genuinità del contatto. L'interlocutore la informava quindi che terzi malintenzionati stavano tentando di effettuare ulteriori pagamenti e che, prima di procedere al blocco definitivo della carta, le sarebbero state inviate altre notifiche per bloccare e stornare tali operazioni fraudolente. La ricorrente, come da lei stessa dichiarato nella denuncia presentata in data 14.01.2026, ammette di aver notato la dicitura "autorizza il pagamento" sulle notifiche ricevute, ma di aver proceduto ugualmente dopo aver chiesto spiegazioni al finto operatore, il quale la rassicurava sulla necessità di tale azione per bloccare le transazioni. A seguito di ciò, venivano addebitate sul suo conto tre operazioni per un importo complessivo di € 758,75, di cui chiede il rimborso.

L'intermediario resiste al ricorso, sostenendo che le operazioni contestate sono state autorizzate dalla cliente tramite il suo dispositivo abituale e con l'inserimento delle corrette credenziali di sicurezza, in conformità con il sistema di autenticazione forte (SCA). Afferma, pertanto, che le operazioni debbano

considerarsi autorizzate ai sensi del D.Lgs. n. 11/2010. In subordine, eccepisce la colpa grave della cliente, la quale avrebbe dato seguito a un raggiro facilmente riconoscibile, autorizzando attivamente le operazioni nonostante le chiare indicazioni contrarie fornite dall'app. A sostegno delle proprie difese, l'intermediario ha prodotto i log informatici relativi alle operazioni, corredati da legenda esplicativa, attestanti l'avvenuta autenticazione tramite notifica PUSH inviata al dispositivo della cliente (elemento di possesso) e la successiva validazione tramite inserimento del PIN personale (elemento di conoscenza).

La ricorrente non ha replicato.

## DIRITTO

La questione sottoposta all'esame di questo Collegio attiene alla responsabilità dell'intermediario per operazioni di pagamento disconosciute dall'utente, eseguite nel contesto di una frode informatica nota come "vishing".

La disciplina di riferimento è contenuta nel Decreto Legislativo 27 gennaio 2010, n. 11, come modificato dal D.Lgs. n. 218/2017, di attuazione della Direttiva (UE) 2015/2366 (PSD2). Tale normativa pone a carico del prestatore di servizi di pagamento (PSP) un preciso regime probatorio. Ai sensi dell'art. 10 del citato decreto, qualora l'utente neghi di aver autorizzato un'operazione, è onere del PSP dimostrare che l'operazione sia stata "autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti".

La responsabilità del PSP può essere esclusa, tuttavia, qualora l'intermediario fornisca anche la prova che l'utente abbia agito in modo fraudolento o non abbia adempiuto ai propri obblighi "con dolo o colpa grave".

Il Collegio deve quindi procedere a una duplice verifica: in primo luogo, se l'intermediario abbia assolto all'onere di provare la corretta autenticazione delle operazioni; in secondo luogo, se sussistano elementi sufficienti a configurare la colpa grave della ricorrente.

Il D.Lgs. n. 11/2010 impone al PSP di applicare un'autenticazione forte del cliente (Strong Customer Authentication - SCA) quando l'utente dispone un'operazione di pagamento elettronico. La SCA richiede l'uso di almeno due elementi tra loro indipendenti, appartenenti alle categorie della conoscenza (qualcosa che solo l'utente sa, es. PIN), del possesso (qualcosa che solo l'utente possiede, es. smartphone) e dell'inerenza (qualcosa che l'utente è, es. impronta digitale).

Nel caso di specie, l'intermediario ha prodotto i log informatici delle transazioni contestate. Da tale documentazione, e dalla relativa legenda, emerge che le operazioni sono state autorizzate mediante una procedura che ha previsto: (a) l'invio di una notifica PUSH sull'app installata sul dispositivo mobile registrato e in uso alla cliente (elemento di possesso); e (b) la validazione di tale notifica tramite l'inserimento del codice PIN personale della cliente (elemento di conoscenza).

Tale procedura risulta conforme ai requisiti della SCA previsti dalla normativa. L'intermediario ha pertanto assolto all'onere probatorio su di esso gravante ai sensi dell'art. 10, comma 1, del D.Lgs. n. 11/2010, dimostrando che le operazioni sono state regolarmente autenticate.

Accertata la regolarità formale delle operazioni, occorre valutare la condotta della cliente al fine di verificare la sussistenza della colpa grave, idonea a escludere la responsabilità dell'intermediario.

Nel caso in esame, diversi elementi depongono per la configurabilità di una condotta gravemente colposa da parte della ricorrente. In primo luogo, la stessa ha dato seguito a istruzioni ricevute da un contatto telefonico proveniente da un numero di cellulare e non da un numero verde ufficiale dell'istituto, elemento che avrebbe dovuto indurre a un primo sospetto. La diligenza minima impone di non fornire dati o autorizzare operazioni sulla base di contatti telefonici inattesi, ma di interrompere la comunicazione e contattare autonomamente la banca tramite i canali ufficiali.

L'elemento decisivo, tuttavia, emerge dalla stessa ammissione della ricorrente, contenuta nella denuncia sporta alle autorità. Ella ha dichiarato di aver visualizzato sulle notifiche push la dicitura "autorizza il pagamento" e, nonostante il dubbio manifestato all'interlocutore, di aver proceduto ugualmente, prestando fede alle rassicurazioni del truffatore secondo cui tale azione era necessaria per "bloccare" i pagamenti. Tale comportamento integra una palese violazione degli obblighi di diligenza e custodia delle proprie credenziali. L'aver ignorato un avvertimento chiaro, inequivocabile e proveniente da un canale ufficiale (l'app della banca), per seguire le istruzioni di un soggetto sconosciuto contattato telefonicamente, costituisce una condotta che travalica la semplice negligenza per assurgere al livello di colpa grave.

In conclusione, l'intermediario ha fornito la prova sia della corretta autenticazione delle operazioni sia della colpa grave della ricorrente. Quest'ultima, con il suo comportamento, ha di fatto neutralizzato i presidi di sicurezza, rendendo possibile la frode. Pertanto, ai sensi dell'art. 12 del D.Lgs. n. 11/2010, la perdita derivante dalle operazioni non autorizzate deve rimanere a suo carico.

#### **PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

IL PRESIDENTE