

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore STEFANO DEPLANO

Seduta del 06/05/2026

FATTO

Parte ricorrente rappresenta che: i.) è titolare di un conto corrente presso la Banca resistente; ii.) in data 10 settembre 2025, alle ore 18:30, ha ricevuto un SMS che la informava di una disposizione di pagamento per 4.730,00 euro con l'invito a contattare il servizio antifrode; iii.) il messaggio appariva genuino; iv.) il sedicente operatore ha richiesto la sua collaborazione per ottenere l'accesso al PC da remoto; v.) ha dato corso a tale richiesta; vi.) il truffatore ha effettuato un bonifico dal sistema di *home banking*; vii.) è arrivata una notifica *push* alla quale ha fornito il proprio consenso; viii.) nonostante si trattasse di bonifico revocabile, l'operazione non è stata bloccata tempestivamente da parte dell'Intermediario; ix.) il giorno seguente è stato sollecitato il *recall*, non andato a buon fine.

Parte resistente riferisce che: i.) è stato tempestivamente tentato il *recall*; ii.) è pacifico che le operazioni siano avvenute dietro ricezione di un SMS, dal contenuto anomalo, da parte di un'utenza non riconducibile all'Intermediario e con la colpevole collaborazione della ricorrente; iii.) la Banca è stata contattata una volta trascorso l'orario di *cut-off*; iv.) l'operazione è stata eseguita personalmente e, quindi, non rientra nell'ambito applicativo della PSD2; v.) i *log* in atti confermano che l'accesso è avvenuto con inserimento del codice PIN e del fattore biometrico al ricevimento della notifica *push* in APP.

In sede di repliche si afferma che i bonifici SEPA sono sempre revocabili nelle 24 ore dall'esecuzione ma tale possibilità è stata negata alla ricorrente.

In sede di controrepliche si evidenzia che il tentato *recall* è stato tempestivo e che la ricorrente ha ricevuto un SMS *alert* ma ha omesso di attivarsi con prontezza.

Parte ricorrente chiede la restituzione della somma di 9.460,00 euro, pari all'importo di un'operazione di bonifico ordinario disconosciuta.

Parte resistente insiste per il rigetto del ricorso.

DIRITTO

1. – La controversia ha ad oggetto il disconoscimento di un'operazione di bonifico eseguita in data 10 settembre 2025, alle ore 19:03, per la somma di 9.460,00 euro.

2. – Sul piano cronologico, l'operazione contestata è stata effettuata sotto la vigenza del d.lgs. n. 11 del 2010, così come modificato dal d.lgs. n. 218 del 2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). La Banca convenuta, tuttavia, eccepisce che quella oggetto di scrutinio non sia un'operazione non autorizzata ai sensi dell'atto richiamato, essendo stata disposta per intero dalla parte attrice. Tale circostanza può considerarsi ammessa anche dalla parte ricorrente, come risulta dalle dichiarazioni contenute sia in denuncia che nel ricorso.

2.1. – Tanto comporta due ordini di conseguenze. Per un verso si deve escludere che al caso di specie possa essere applicata la disciplina sopra richiamata (si da escludere la responsabilità oggettiva del PSP), per altro verso occorre comunque scrutinare l'eventuale apporto causale dell'Intermediario alla frode, sulla base delle evidenze disponibili e secondo le norme di diritto comune. Si vuol dire che la natura (autorizzata) dell'operazione non esclude che la condotta dell'Intermediario possa essere scrutinata in base alle regole generali del diritto delle obbligazioni, sotto il profilo del corretto adempimento delle obbligazioni contrattuali, eventualmente integrate dalla regola che prescrive un dovere di comportamento secondo buona fede (cfr., ad esempio, Coll. Roma, dec. n. 361 del 2025 e Coll. Roma, dec. n. 2405 del 2025).

3. – Giova ad ogni modo evidenziare che l'Intermediario non si è sottratto all'onere di verificare la regolarità dell'operazione disconosciuta. La Banca, infatti, versa in atti i *log* da cui emerge che l'accesso all'APP è avvenuto da *browser* e autorizzato con notifica *push* (fattore di possesso) e inserimento del codice PIN (fattore di conoscenza). Dimostra inoltre che l'operazione dispositiva è stata validata alla ricezione della notifica *push* (fattore di possesso) mediante inserimento del codice PIN (fattore di conoscenza).

4. – Con riferimento alle circostanze di fatto alla base dell'odierno ricorso emerge che in data 10 settembre 2025 la ricorrente ha ricevuto un SMS da parte di un'utenza privata e non riconducibile all'Intermediario. Nel testo compariva il nome della Banca resistente e l'avviso di una disposizione di pagamento per 4.730,00 euro e l'indicazione di un numero da contattare.

4.1. – La ricorrente ha dato séguito all'indicazione; l'interlocutore si è presentato come un operatore della banca e ha riferito di movimenti sospetti sul conto corrente per i quali sarebbe stato necessario effettuare un bonifico al fine di arrestare l'operazione. Parte attrice ha ceduto al truffatore il controllo del PC da remoto sì che il malfattore ha potuto dare corso all'operazione disconosciuta. La ricorrente ha anche ricevuto sul proprio cellulare una notifica *push* volta all'autenticazione del pagamento mediante riconoscimento biometrico.

5. – Mette conto evidenziare, da ultimo, che il truffatore ha tenuto al telefono la ricorrente per circa due ore in modo da superare l'orario del *cut off* e scongiurare così la possibilità di revocare la disposizione. La Banca ha comunque tentato il *recall* (richiesto alle 20:23 del 10 settembre 2025) in data 11 settembre 2025 ma con esito negativo, per indisponibilità di fondi.

6. – Alla luce degli elementi di fatto così ricostruiti emerge che la truffa *de qua* è stata perpetrata mediante il fenomeno del c.d. *smishing*, tipo particolare di *phishing*, caratterizzato dalla ricezione del

messaggio ingannevole tramite SMS. Il *phishing* operato tramite SMS è ritenuto fenomeno diffusamente noto che qualunque utente dotato di normale avvedutezza e prudenza, come si ritiene siano quelli avvezzi all'uso dell'*home banking*, dovrebbe conoscere. Stessa conclusione vale per il connesso *vishing*, effettuato da un'utenza non riconducibile ai canali di comunicazione comunemente adoperati dall'Intermediario. Ne consegue che, sul piano causale, nessun addebito può essere mosso a quest'ultimo il quale si è anche tempestivamente attivato per effettuare il *recall*.

7. – Tanto premesso, il ricorso non è fondato e non può essere accolto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE