

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) PERON

Seduta del 31/03/2026

FATTO

Parte ricorrente rappresenta al Collegio che, in data 10/10/2025, è stata contattata da un soggetto interessato a un prodotto messo in vendita sulla piattaforma S*. La presunta acquirente l'ha indotta, tramite l'invio di un QR code, ad accedere a una pagina web contraffatta del portale, dove la parte ricorrente ha seguito le istruzioni della frodatrice che richiedevano di confermare l'identità eseguendo il "blocco" di alcune somme. Tratta in inganno, ha autorizzato il pagamento di € 499,00 avvedendosi dell'addebito reale solo successivamente; resasi conto della frode, ha quindi provveduto a bloccare la carta contattando il servizio dell'intermediario.

Per queste ragioni parte ricorrente chiede il rimborso della somma.

L'intermediario, controdeduce precisando che parte ricorrente è titolare della carta di debito n. 44** abilitata all'internet banking e rileva l'assenza di aggiornamenti su indagini o azioni legali contro i truffatori. Secondo l'intermediario, la frode non è riferibile alla propria sfera di competenza, poiché l'esecuzione del pagamento è imputabile esclusivamente alla parte ricorrente, che ha impartito un ordine non revocabile regolarmente autenticato tramite SCA. Viene eccepita la colpa grave della parte ricorrente per aver dato seguito a richieste anomale di soggetti ignoti, conducendo la trattativa al di fuori della piattaforma ufficiale e ignorandone i consigli di prudenza. Inoltre, la parte ricorrente ha trascurato

il testo della notifica PUSH, che indicava chiaramente un'autorizzazione di pagamento di € 499,00 e non un "blocco" della somma. L'intermediario ribadisce infine di adempiere correttamente agli obblighi informativi sulla sicurezza e prevenzione delle truffe tramite il proprio sito istituzionale.

Per questi motivi l'intermediario chiede il rigetto del ricorso.

Le parti non hanno depositato repliche

DIRITTO

La fattispecie in oggetto concerne la richiesta di rimborso di parte ricorrente del complessivo importo di € 499,00, sottratto in data 10/10/2025 alle ore 20:45, tramite un'operazione d'acquisto online.

Dalle dichiarazioni rese dalla parte ricorrente nella denuncia, risulta che la stessa, nell'ambito della trattativa avviata su un sito online, ha scansionato un QR code esterno alla piattaforma di vendita. Tale azione ha indirizzato parte ricorrente verso un sito esterno dove un supporto virtuale ha richiesto l'inserimento dei dati della carta per completare l'acquisto di un prodotto dal valore di € 40,00. Parte ricorrente ha quindi inserito volontariamente i propri dati bancari e, seguendo le indicazioni del supporto virtuale, ha utilizzato l'app dell'intermediario per approvare un asserito blocco temporaneo di € 499,00 finalizzato all'autenticazione della carta.

L'operazione contestata è disciplinata dal D.lgs. 27/01/2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e del relativo Provvedimento attuativo della Banca d'Italia del 05.07.2011. Come è noto, i principi fissati da tale impianto normativo, in materia di strong customer authentication (SCA), fissano due passaggi ineludibili che attengono al piano degli oneri probatori:

a) è l'intermediario a dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, avendo presente che l'autenticazione forte (SCA) è richiesta sia nella fase di accesso al conto / enrollment dell'applicazione / registrazione della carta sul wallet, sia nella fase di esecuzione delle singole operazioni; inoltre la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza, inerenza, possesso. Tali elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse;

b) è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento. In quest'ambito dunque, costante giurisprudenza arbitrale, ritiene che l'eventuale negligenza del cliente possa solo venire in rilievo solo allorquando l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di alert.

Peraltro secondo l'orientamento dei Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP. Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D.lgs. 11/2010.

Con riguardo alla prova del sistema di autenticazione forte dell'intermediario, il Collegio constata che dai log prodotti risulta che i fattori di autenticazione per l'esecuzione dell'operazione sono: (i) verifica del possesso del dispositivo registrato mediante validazione di una credenziale dinamica (OTP) generata dall'app a seguito di notifica push (fattore possesso); (ii) codice PIN inserito per validare la PUSH (fattore conoscenza). L'operazione è quindi stata autorizzata con inserimento del codice PIN di sola conoscenza della cliente per validare la notifica PUSH inviata nel dispositivo registrato, integrando la SCA con i due fattori di autenticazione necessari. La PUSH in questione, come da evidenze, riportava chiaramente le informazioni relative alla natura, somma e beneficiario dell'operazione.

Il Collegio osserva inoltre che la stessa parte ricorrente ammette in sede di ricorso di aver autorizzato l'operazione ritenendo si trattasse di una operazione di "blocco" della cifra ai fini della corretta conferma della propria identità, necessaria alla conclusione dell'operazione di vendita online.

Il Collegio, ritenuta provata la SCA, procede a verificare se parte ricorrente abbia agito con colpa grave e se vi sia stato un concorso di colpa da parte dell'intermediario.

Dalla ricostruzione dei fatti fornita da parte ricorrente questa, in data 10/10/2025, è stata contattata nella chat della piattaforma S* da una sedicente acquirente che le ha inoltrato lo screenshot di una finta comunicazione d'acquisto. Tale messaggio fraudolento, non riferibile all'intermediario, conteneva istruzioni per "accettare la vendita" e "confermare il pagamento" tramite la scansione di un QR code. Il Collegio constata che dalle evidenze in atti risulta che nonostante la presenza di evidenti errori grammaticali ("midello", "smariphone") e una sintassi innaturale, parte ricorrente ha scansionato il codice raggiungendo un sito esterno. In questo sito, una chatbot ha richiesto l'inserimento dei dati della carta e l'autorizzazione di una notifica PUSH sull'app dell'intermediario, assicurando falsamente la parte ricorrente che l'importo di € 499,00 fosse solo un codice di verifica senza addebito reale. Dall'analisi delle evidenze emerge che la comunicazione è avvenuta su canali esterni all'intermediario e che l'interfaccia della chatbot non imitava correttamente quella originale di S*, mancando persino del logo ufficiale. Si rileva infine che la piattaforma di vendita dispone di una sezione specifica che avverte di non uscire mai dall'applicazione tramite link esterni per completare le transazioni.

Alla luce di tali evidenze probatorie il Collegio ritiene che la condotta di parte ricorrente sia connotata da colpa grave e che non vi siano forme di responsabilità concorrente in capo all'intermediario, il quale ha anche inviato una notifica alert al dispositivo in uso alla parte che l'informava dell'esecuzione dell'operazione di pagamento del 10/10/2025, specificando natura della somma, ammontare e beneficiario.

Per questi motivi il Collegio, ritenuta provata la SCA da parte dell'intermediario e ritenuta la sussistenza di una colpa grave in capo alla parte ricorrente, ritiene che il ricorso non possa trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE