

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 09/12/2025, riceveva un SMS contenente un link per aggiornare l'indirizzo di spedizione e sbloccare la consegna di un presunto pacco. Trovandosi effettivamente in attesa di una spedizione, la parte ricorrente ha dato credito alla comunicazione

cliccando sul link e inserendo i propri dati personali e bancari. Successivamente ha riscontrato un addebito non autorizzato di € 573,00 motivo per cui, compreso di essere vittima di una truffa, ha contattato l'intermediario per procedere al blocco della carta.

Per questi motivi parte ricorrente chiede il rimborso delle somme addebitate e del contributo versato all'ABF.

L'intermediario nelle sue controdeduzioni afferma che la parte ricorrente è titolare della carta di debito n. 53**, utilizzata per l'operazione oggetto di controversia. L'intermediario ribadisce di fornire un'ampia informativa sulle procedure di sicurezza e sulle tecniche per prevenire le truffe, precisando che il pagamento disconosciuto è stato regolarmente autenticato tramite SCA, registrato e contabilizzato in assenza di anomalie tecniche.

Viene eccepita la colpa grave della parte ricorrente sulla base di diversi elementi: la stessa ha ammesso in sede di denuncia di aver comunicato i propri dati personali e bancari dopo aver cliccato su un link sospetto, un'operatività che non è in alcun modo riconducibile all'intermediario. Secondo l'orientamento consolidato dei Collegi, l'inserimento di dati sensibili al di fuori dei circuiti operativi ufficiali configura una "colpevole credulità", data la nota diffusione di tali modalità fraudolente. L'intermediario ritiene pertanto di aver assolto il proprio onere probatorio dimostrando l'efficacia della SCA e l'inadempimento della parte ricorrente agli obblighi di custodia degli strumenti e dei codici di accesso.

Per questi motivi l'intermediario chiede: in via principale, dichiarare inaccoglibile, in quanto immotivata ed infondata, la richiesta restitutoria, oggetto del presente ricorso; in subordine, nella denegata ipotesi che il Collegio, nonostante i richiamati orientamenti già espressi su analoga fattispecie, ritenga di poter ravvisare profili di responsabilità nell'accaduto definire la ripartizione fra le parti del danno in esame, in misura proporzionale alle rispettive effettive responsabilità, ai sensi dell'art. 1227, 1 e 2 comma c.c.

Richiamando i propri scritti, parte ricorrente replica all'intermediario precisando che, sebbene non neghi l'avvenuta conferma tecnica dell'operazione, tale circostanza non equivale a una volontà consapevole di disporre il pagamento. Parte ricorrente sostiene la sussistenza di un vizio del consenso dovuto a una falsa rappresentazione della realtà: il messaggio fraudolento, simulando una comunicazione relativa alla spedizione di un pacco e privo di riferimenti bancari, l'ha indotta a ritenere di aggiornare i dati di consegna e non di autorizzare una transazione. Viene inoltre evidenziato come la truffa costituisca un caso di ingegneria sociale strutturata, tale da trarre in inganno anche un utente mediamente diligente. Secondo parte ricorrente, l'intermediario confonderebbe l'autenticazione tecnica con la consapevolezza sostanziale dell'operazione; pertanto, la prova della colpa grave non può considerarsi assolta dal semplice richiamo alle modalità di autenticazione, le quali confermano l'identità dell'autore del clic ma non il contenuto che lo stesso credeva di approvare.

L'intermediario, richiamando le precedenti difese, controreplica sostenendo che la responsabilità esclusiva della parte ricorrente sia confermata dalle sue stesse repliche, nelle quali ammette di aver confermato personalmente l'operazione. Viene contestata come infondata la distinzione tra autorizzazione tecnica e sostanziale sollevata dalla controparte. L'intermediario rileva inoltre che l'SMS "civetta", prodotto solo in sede di replica, presenta evidenti errori grammaticali ed era stato segnalato automaticamente dall'operatore telefonico come potenziale spam ("forse indesiderato"), elementi che avrebbero dovuto indurre la parte ricorrente alla massima cautela.

DIRITTO

La fattispecie in oggetto concerne la richiesta di rimborso di parte ricorrente del complessivo importo di € 585,11, sottratto a seguito di un'operazione online eseguita in data 09/12/2025 alle ore 8:36.

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.

Passando ad esaminare il sistema di autenticazione forte dell'intermediario, il Collegio constata che base delle evidenze risulta che l'operazione è stata autenticata tramite autenticazione della PUSH ricevuta nel dispositivo generalmente usato dalla cliente per accedere all'Internet banking (elemento possesso). Validazione che avviene con utilizzo dell'impronta digitale per confermare la notifica di pagamento ricevuta (elemento inerenza). L'operazione di pagamento è quindi stata autorizzata, dopo che parte ricorrente ha inserito le credenziali della propria carta di pagamento sul sito fraudolento, con una notifica PUSH arrivata sul suo dispositivo e dalla stessa validata con impronta digitale. Si noti che parte ricorrente afferma in sede di denuncia di aver inserito i dati della propria carta ed aggiunge in sede di repliche di avere effettivamente confermato l'operazione (*"non nego l'avvenuta conferma tecnica dell'operazione"*).

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.

In proposito il Collegio constata che dalla ricostruzione della vicenda, basata sulla denuncia e sulle repliche della parte ricorrente, il caso appare riconducibile a una fattispecie di *smishing*: parte ricorrente ha ricevuto un SMS da un mittente estraneo all'intermediario, che l'ha indotta ad accedere a un sito fraudolento per modificare i dati di spedizione di un pacco. In tale contesto, ha inserito i propri dati bancari e confermato l'operazione, nell'erronea convinzione di stare gestendo una spedizione e non di stare disponendo un pagamento.

Passando all'analisi dell'SMS civetta ricevuto, il Collegio constata che il messaggio non proviene da un numero riferibile all'intermediario e viene automaticamente segnalato dal dispositivo della cliente come "forse indesiderato" e "spam". Inoltre, tale SMS errori ortografici grossolani e il link a cui si chiede di accedere non è riferibile all'intermediario.

Per quanto sopra esposto il Collegio ritiene che la condotta di parte ricorrente sia connotata da colpa grave e che non vi siano evidenze di una responsabilità concorrente dell'intermediario, ragion per cui il ricorso non può trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE