

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) GILIBERTI

Seduta del 18/12/2025

FATTO

Parte ricorrente, nel proprio ricorso afferma che:

- alle ore 00:30 del 12/05/2025 notava la presenza di alcune mail che la informavano di operazioni mai autorizzate a partire dalla data del 09/05/2025;
- non riusciva a mettersi in contatto con la banca in quanto il numero di emergenza, che così non può definirsi, è attivo solo nei giorni feriali, dalle 09:00 alle 18:00;
- richiedeva e veniva autorizzato un cambio di numero di cellulare;
- effettuava un giroconto di € 3.000,00;
- procedeva a bloccare la carta e a presentare denuncia presso le Autorità;
- la comunicazione con la banca era confusa, poiché sono state inviate comunicazioni di avvenuta apertura della pratica di rimborso in contrasto con quanto riferito dagli operatori, secondo cui sarebbe stato necessario ripresentare la richiesta;
- l'intermediario forniva dati e procedure scorrette;
- presentava modulo di rimborso all'intermediario in data 06/06/2025, re-inviato in data 17/06/2025 e diffida legale in data 16/07/2025;
- l'importo del rimborso richiesto all'intermediario è pari ad € 3.714,00;
- l'intermediario comunicava la propria volontà dopo oltre due mesi;
- l'intermediario, negando il rimborso non provava la colpa grave del cliente;

- l'autenticazione forte è solo apparente in quanto il truffatore può entrare in app solo con il pin e modificare i dati.

Pertanto, chiede il rimborso dell'importo di € 3.714,00 oltre alle somme oggetto delle operazioni eseguite tramite carta di credito per ulteriori € 1.930,00 ed il mancato realizzo degli interessi.

L'intermediario, nel contestare l'avversa pretesa, sostiene che:

- il disconoscimento delle operazioni con carte, richiamate nel ricorso, non è mai pervenuto alla banca, né tramite denuncia alle autorità competenti, né tramite l'apposito modulo di contestazione;
- la cliente, nella ricostruzione della vicenda, omette ogni riferimento a eventuali chiamate intercorse apparentemente con la banca;
- il 07/05/2025 è stata installata una nuova app su altro device, dal quale sono state poi autorizzate e autenticate le disposizioni di pagamento;
- tale installazione è potuta avvenire solo con la comunicazione delle credenziali da parte della ricorrente;
- le operazioni disconosciute sono state correttamente contabilizzate, registrate e autenticate;
- la truffa va inquadrata nella fattispecie del phishing;
- non sono state prodotte evidenze circa la possibile frode, ragion per cui non è possibile valutarne la sofisticatezza per l'esclusione della colpa grave;
- ha attuato campagne di sensibilizzazione contro le frodi e informato la propria clientela.

In sede di replica la ricorrente precisa che:

- l'intermediario non ha prodotto evidenze idonee a dimostrare le proprie affermazioni;
- dal 12/05/2025 al 15/07/2025 ha sollecitato il riscontro dell'intermediario alla richiesta di rimborso;
- l'intermediario non fornisce evidenza circa la violazione del dovere di custodia delle credenziali;
- non corrisponde al vero la mancanza di disconoscimento delle operazioni con carta oggetto di ricorso;
- ha custodito le proprie credenziali;
- dato che il pin è costituito da n. 3 cifre, un frodatore potrebbe individuarlo reiterando i tentativi in giorni diversi;
- il codice cliente non è sicuro in quanto riproducibile e non aggiornabile, mentre la data di nascita è un dato pubblico;
- l'intermediario non effettua alcuna comunicazione circa l'installazione di nuove app;
- le operazioni contestate, oltre ad aver azzerato il conto, non ne rispecchiano la normale operatività;
- i clienti non potevano utilizzare l'autorizzazione forte perché l'intermediario ha introdotto l'utilizzo dei dati biometrici il 10/06/2025;
- solo recentemente è stata introdotta la possibilità di conoscere i device sui quali è installata l'app;
- si trovava in vacanza con il marito e avendo in uso una sim locale non hanno mai avuto contatti con la banca di nessun tipo;

- disconosce il device dal quale sono state effettuate le operazioni;
- il codice otp non è stato utilizzato per ogni singola operazione;
- l'intermediario ha operato una ricostruzione irrazionale e semplicistica.

DIRITTO

In via preliminare si osserva che la parte ricorrente nel ricorso chiede il rimborso di 5 bonifici non autorizzati per complessivi € 3.714 e di alcune operazioni effettuate fraudolentemente con la carta di credito, per € 1.930.

Sul punto, l'intermediario eccepisce che la richiesta di rimborso delle operazioni con carta non può essere accolta in questa sede in quanto il disconoscimento delle stesse non gli è mai pervenuto, né tramite denuncia alle Autorità, né tramite apposito modulo di contestazione.

Alla luce della documentazione depositata in atti il Collegio osserva come effettivamente non siano stati rinvenuti elementi atti a confermare l'avvenuta previa contestazione all'intermediario delle operazioni effettuate con la carta del cliente.

In ragione di detta omissione, e nel rispetto del principio di corrispondenza tra reclamo e ricorso, le operazioni con carta non saranno oggetto di valutazione da parte del Collegio dovendosi ritenere tale parte della domanda inammissibile.

Alla data delle operazioni trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU, entrato in vigore il 13/01/2018.

Al netto della riferita parziale inammissibilità della domanda, il ricorso ha ad oggetto n. 5 bonifici contestati per un importo complessivo pari ad € 3.714,00 tutti eseguiti tra il giorno 9.5.2025 ed il giorno 12.5.2025.

Nella denuncia depositata in atti il ricorrente descrive i fatti nei medesimi termini del ricorso.

Si rileva che le operazioni oggetto di contestazione sono state precedute dall'installazione della app bancaria su un nuovo dispositivo, oltre che dall'accesso in app.

La truffa risulta essersi articolata in diverse giornate: in data 07/05/2025 allorché il truffatore enrollava la app sul proprio device e nelle date 09-10-12/05/2025 allorché veniva eseguite le operazioni contestate.

La cliente riferisce in merito ai soli accadimenti del 12/05/2025, quando nel controllare le e-mail si avvedeva a suo dire dell'esecuzione delle operazioni fraudolente.

A seguito delle controdeduzioni, la cliente disconosce il device indicato dall'intermediario sul quale è stata installata l'app senza, in ogni caso, circostanziare gli accadimenti del 07/05/2025.

Con riferimento alla *strong customer authentication* (cd. SCA) antecedenti all'esecuzione delle operazioni contestate, l'intermediario afferma che il cliente ha attivato la nuova APP in data 07/05/2025 su di uno smartphone Redmi.

Di tale attività viene fornita prova tramite specifica allegazione documentale da cui risulta che la fase di enrollment dell'app su nuovo dispositivo è stata autenticata tramite PIN (elemento di conoscenza) e invio sms OTP sul recapito telefonico registrato sull'anagrafica del Cliente (elemento di possesso).

Al pari viene documentato il corretto accesso tramite app eseguito tramite dispositivo su cui è stato effettuato l'enrollment, che secondo l'intermediario corrisponde a quello in uso al truffatore.

Le operazioni contestate sono state tutte eseguite tramite bonifico bancario e tutte oggetto del medesimo procedimento di autenticazione.

Sulla base delle evidenze prodotte dall'intermediario risulta che le operazioni sono state correttamente autenticata tramite: Smart code, quale elemento di conoscenza; mobile token app, quale elemento di possesso.

Dato atto della correttezza delle procedure di S.C.A., il Collegio riflette come la ricorrente non abbia riferito nulla in merito alle modalità con le quali è avvenuto l'utilizzo fraudolento. Nella denuncia e nel ricorso rappresenta solo di essersi accorta dell'utilizzo fraudolento ricevendo le e-mail di alert dall'intermediario.

Dunque, verificata nel caso di specie la sussistenza della SCA, secondo l'orientamento dei Collegi nelle contestazioni di utilizzi fraudolenti on line di strumenti di pagamento in cui:

- i) l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute;
- ii) il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA);
- iii) non risultano indici di anomalia delle operazioni e/o ulteriori elementi

le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, 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 (ovvero, per il *vishing*, del registro delle chiamate) debba determinare il rigetto del ricorso, in quanto non consente di verificare se il mittente/chiamante risulti riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la genuinità del messaggio o della telefonata ricevuti.

In ragione della descritta omissione e non ritenendo possibile cogliere elementi di anomalia nelle operazioni contestate in ragione del lasso di tempo in cui si sono compiute (n. 5 bonifici nell'arco di 3 giorni), la pretesa della ricorrente non può essere accolta.

PER QUESTI MOTIVI

Il Collegio dichiara il ricorso in parte inammissibile e in parte infondato.

IL PRESIDENTE