

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) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) FORMAGGIA

Seduta del 24/02/2026

FATTO

Il ricorrente, nella denuncia allegata al ricorso, descrive la vicenda (rimasta ne ricorso estremamente criptica) affermando che a fronte di una denuncia presentata in data 11/08/25, ha diritto a ricevere il rimborso integrale di somme disposte fraudolentemente da terzi, mediante 2 bonifici istantanei (per € 1.300,00) e un acquisto tramite carta di debito in modalità e-commerce (per € 6,99), per totali € 1.306,99; che la banca si è limitata sinora a restituire soltanto € 650, 00.

Chiede che gli siano restituiti tutti gli importi sottratti con frode, sia i bonifici che il prelievo dalla carta di debito, rispetto ad Euro 650,00 già rimborsati dalla Banca, e cioè Euro 656,90 + Euro 20 del ricorso.

L'Intermediario replica che in data 20 agosto 2025, controparte trasmetteva modulo di disconoscimento delle operazioni di bonifico eseguite, nonché dell'operazione eseguita con la carta di debito, cui la Banca dava riscontro nella medesima data informando l'istante di aver provveduto ad accreditare a suo favore una somma pari al 50% dell'importo frodato, come da accredito eseguito in data 21 agosto 2025: che, rispetto allo schema truffaldino asseritamente subito, il cliente si è limitato a dedurre di aver ricevuto, in data 9 agosto 2025, un contatto telefonico dalla banca, durante il quale veniva informato dell'esecuzione di due bonifici istantanei fraudolenti; che in presenza di tale fenomeno (di *vishing*) i Collegi ABF ravvisano la colpa grave dell'utente; che l'intermediaria adotta un sistema di autenticazione forte di accesso all'area riservata e di autorizzazione delle disposizioni di pagamento nel pieno rispetto delle previsioni normative; che il cliente aveva attivato il Servizio Token-app in data

9/08/2025 sullo smartphone presumibilmente in uso ai truffatori, solo un'ora prima della disposizione delle operazioni contestate; che è presumibile ritenere che il cliente abbia colposamente collaborato con il truffatore, rivelando il codice PIN e il codice OTP ricevuto tramite SMS, prodromici all'attivazione dell'app bancaria su un nuovo dispositivo; che sono stati inviati appositi alert di avvenuta esecuzione delle operazioni, tramite e-mail; che le modalità con cui si è realizzata la truffa sono note e il cliente aveva ricevuto nel tempo diverse informative contro i rischi delle truffe online; che il cliente si è attivato con colpevole ritardo nel disconoscimento delle operazioni, avendo chiamato il servizio di assistenza soltanto in data 11/08/25, ovvero due giorni dopo l'esecuzione dei pagamenti; che i bonifici istantanei sono irrevocabili per definizione, e il cliente era stato debitamente informato dell'introduzione di questo servizio, tramite comunicazione tracciata.

Conclude chiedendo di respingere il ricorso e la richiesta risarcitoria in quanto infondati.

Nelle repliche, il ricorrente insiste per l'accoglimento del ricorso ed eccepisce di possedere un dispositivo mobile diverso per modello da quello indicato nei log informatici della banca; di non aver mai rivelato a terzi codici segreti o condiviso fattori di autenticazione, non avendo ricevuto alcuna chiamata relativa al proprio conto corrente; che la truffa si è resa possibile in quanto terzi sono riusciti ad avere accesso ad una base dati dell'intermediario; di aver bloccato il conto appena trascorse 2 ore dall'esecuzione dei bonifici; di aver presentato denuncia soltanto l'11/08/25, in quanto si trattava del primo giorno utile dopo la truffa per effettuare tale incombenza.

L'intermediario nelle controrepliche ribadisce le proprie argomentazioni difensive sottolineando la colpa grave del cliente e insistendo per il rigetto del ricorso.

DIRITTO

Le operazioni in contestazione sono 3, tutte eseguite il 9/08/2025, per l'importo complessivo di € 1.306,99; consistono, in particolare, in 2 bonifici istantanei eseguiti alle ore 11:00 e 11:08 rispettivamente per € 1.000,00 ed € 300,00, e in una distanziata operazione di e-commerce con carta di debito eseguita alle 20:05 per € 6,96.

Lo stesso cliente, nel ricorso, riconosce espressamente che la banca ha effettuato in fase di riscontro al reclamo un parziale rimborso per una somma pari a € 650,00, ed agisce dinanzi all'Arbitro esclusivamente per il rimborso della somma residua pari a € 656,90; ed infatti la resistente versa in atti il riscontro a suo tempo fornito al cliente e la contabile attestante l'avvenuto accredito, avente data valuta 9/8/25 (giorno di verifica della truffa).

Nella allegata denuncia presentata in data 11/8/25, il cliente sostiene, attraverso una descrizione assai sintetica delle circostanze nelle quali si sarebbe verificata la truffa, di aver ricevuto una chiamata, apparentemente proveniente dalla propria banca, che lo informava di due operazioni di bonifico istantaneo disposte dal proprio conto per un importo totale di € 1.300,00 (operazioni corrispondenti per importo e beneficiario alle prime 2 operazioni disconosciute), a margine della quale provvedeva a far inserire un blocco dispositivo sul proprio conto corrente.

In sede di repliche, contraddicendo in parte tali dichiarazioni, il cliente afferma invece di non aver mai ricevuto una chiamata dalla propria banca in relazione al conto corrente, e che i truffatori sarebbero entrati in possesso delle sue credenziali e codici segreti in quanto sarebbero riusciti ad accedere in autonomia ad una base dati della banca, negando di aver mai collaborato con gli stessi per la condivisione di dati riservati; chiarisce inoltre di aver inserito il blocco dispositivo non appena trascorse 2 ore dall'esecuzione dei bonifici istantanei contestati.

Alla data delle operazioni descritte dal cliente e del bonifico oggetto della presente controversia 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 (PSD II), entrato in vigore il 13/01/2018. In particolare, Le fonti normative regolanti la materia sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato

UE 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019).

La prova di autenticazione delle operazioni, di cui l'intermediario è onerato, rappresenta, in aderenza al dato normativo, un *prius* logico rispetto ad ogni ulteriore accertamento, compreso quello sulla colpa grave del cliente.

Secondo il consolidato orientamento dei collegi, solo nel caso in cui risulti pacifico o dimostrato che le operazioni contestate siano state compiute direttamente e interamente dal cliente (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'intermediario è esonerato dalla prova di autenticazione. Diversamente, ove vi siano operazioni non compiute interamente dal cliente, occorre l'accertamento della sussistenza della SCA (*Strong Customer Authentication*), con riferimento alle singole operazioni e ad ogni fase attraverso cui si sono realizzate, sempre con onere della prova a carico dell'intermediario. Infatti, secondo l'orientamento consolidato dei collegi, l'autenticazione forte è richiesta quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza, inerenza, possesso. I due fattori devono essere reciprocamente indipendenti e appartenere a categorie diverse. In caso di difetto di piena prova sull'autenticazione, per ogni fase, delle transazioni disconosciute, la domanda deve essere accolta, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.

Resta il fatto che, comunque, non è configurabile una responsabilità oggettiva a carico dell'intermediario, sicché spetta al Collegio verificare se, in concreto, vi sia stata una responsabilità concorrente del PSP secondo le norme di diritto comune, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode (quali ad esempio, la mancanza o temporanea indisponibilità del numero verde del PSP, o il mancato rilievo di indizi di frode).

L'intermediario afferma che le operazioni in questione sono state autorizzate con doppio fattore di autenticazione, nel rispetto della normativa di cui al D.lgs. 11/2010, come emerge dalla documentazione prodotta. Fornisce LOG ed altre evidenze e, negli atti, si riporta al loro contenuto, dandone in sostanza una spiegazione coerente.

A questo proposito si rammentano i principi generali espressi dai collegi in merito alla valenza da attribuire alle informazioni presenti nei *log* prodotti dagli intermediari per provare l'autenticazione forte del cliente nelle operazioni di pagamento disconosciute (artt. 10, comma 1 e 10-*bis* del D.lgs. 11/2010), nei casi in cui dalla tracciatura informatica non risulti in modo esplicito uno dei fattori di autenticazione inseriti (conoscenza, possesso o inerenza). Tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte, i collegi ritengono che, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP (Prestatore dei Servizi di Pagamento) nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione.

I collegi ritengono inoltre che eventuali dichiarazioni confessorie del cliente possano assumere valore di prova legale ai sensi dell'art. 2730 c.c..

Dalle evidenze e relativi Log esplicativi risulta, con riferimento alle operazioni antecedenti all'esecuzione delle operazioni oggetto del ricorso, che esse sono state disposte a seguito dell'attivazione dell'app su uno smartphone in uso ai truffatori, avvenuto in data 9/8/25 alle ore 10:06, e dunque il giorno di verifica della truffa, soltanto un'ora prima della disposizione del primo bonifico istantaneo.

In particolare, risulta che il cliente ha attivato la nuova app ING in data 9.8.2025 su uno Smartphone dal quale vengono inviate tutte le PUSH.

Che il processo di *enrollment* sia stato eseguito su un dispositivo diverso da quello in uso al cliente, risulta confermato dal cliente stesso, il quale invero, in sede di repliche, ha specificato di possedere uno smartphone del tipo “*Iphone 8*” e non “*Iphone 13*” come risultante dai log informatici versati in atti dall’intermediario.

L’intermediario afferma e documenta che l’attivazione dell’app sul dispositivo è avvenuta tramite la corretta verifica dei seguenti passaggi: inserimento del codice cliente e data di nascita ed inserimento di 3 cifre del PIN (fattore di conoscenza); scelta ad opera del cliente della password statica (“*smartcode*”) che da quel momento in avanti sarebbe stata utilizzata per il completamento delle disposizioni di pagamento impartite tramite app; digitazione del codice OTP a seguito della ricezione di un sms sul numero di telefono registrato del cliente (fattore di possesso).

Il numero indicato nei Log informatici corrisponde a quello che il cliente ha dichiarato come proprio in sede di denuncia. Dai log prodotti si ricava dunque che il processo di *enrollment* è stato autorizzato a seguito dell’inserimento del PIN, quale fattore di conoscenza, e dell’inserimento del codice OTP ricevuto tramite SMS, quale fattore di possesso.

Documenta che la disposizione dei due bonifici istantanei, delle ore 11:00 e delle ore 11:03, è stato preceduto da un accesso dal web al profilo del cliente, completatosi alle ore 10:59, tramite un processo che ha richiesto –oltre al solito inserimento della data di nascita e del codice cliente- l’inserimento di due fattori di autenticazione, in particolare il codice PIN quale fattore di conoscenza, e il riconoscimento facciale – *FaceID*, quale fattore di inerenza.

Quanto alle operazioni contestate, si osserva, con riguardo ai 2 bonifici istantanei, che essi risultano autenticati tramite fattore di conoscenza, rappresentato dall’autorizzazione dell’operazione digitando sullo smartphone lo *smartcode*, una *password* statica, precedentemente impostata in fase di *enrollment*, e fattore di possesso, rappresentato dall’aver inserito lo *smartcode* e finalizzato il pagamento sul *device* abilitato, e che dopo avere inserito i dati del bonifico, veniva inviata notifica *push* sul dispositivo del cliente.

Anche quanto alla terza operazione di pagamento e-commerce, eseguita con carta di debito su canale online, risulta sussistente corretta autorizzazione tramite *PUSH* ricevuta sul dispositivo previamente abilitato dai truffatori, quale elemento di possesso, e validazione del riconoscimento facciale *faceID*, quale elemento di inerenza. Si osserva in proposito che, in relazione alle cd. “*push based*” *authentication* i *smartcode* cui l’utente autorizza la transazione tramite l’utilizzo di un Pin o di un impronta digitale a seguito della ricezione di notifica *push* sul proprio *device*, l’EBA, con la [Q&A n. 4984/2019](#), ha chiarito che la notifica *push* può essere utilizzata alla stregua di un elemento di possesso a condizione che “*i prestatori di servizi di pagamento adottano misure volte ad attenuare il rischio che gli elementi dell'autenticazione forte del cliente classificati come possesso siano utilizzati da soggetti non autorizzati*”.

Per tutto quanto rilevato dalle evidenze documentali in atti, risulta comprovata la sussistenza della SCA.

Resta da valutare la condotta delle parti per appurare se quella dell’intermediario abbia eventualmente contribuito causalmente alla verifica della frode.

Il cliente assume di aver ricevuto una chiamata apparentemente inoltrata dalla propria banca, che lo informava di due presunti bonifici in uscita; si contraddice poi però nelle repliche, dove assume di non aver mai ricevuto alcun contatto telefonico e che la truffa avrebbe preso le mosse unicamente dall’accesso dei truffatori alle basi dati dell’intermediario. Tali contraddittorie versioni, che lasciano oltremodo generica la descrizione della fattispecie truffaldina lamentata, non trovano alcuna integrazione documentale, non avendo il cliente prodotto il registro delle chiamate.

In analoghe situazioni i collegi territoriali si sono orientati nel senso che le mancate o imprecise allegazioni del cliente sulle circostanze di fatto della frode sono elementi che, valutati nel complesso delle specificità del caso concreto, possono condurre al convincimento sulla sussistenza della colpa

grave del cliente. In più, hanno ritenuto che porti al rigetto del ricorso la mancata produzione del registro delle chiamate, non consentendo tale lacuna 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.

A fronte di tale condotta colposa del cliente, quella dell'intermediario non appare connotata da elementi di responsabilità indicativi di un concorso colposo. Si sottolinea, in proposito, che mancano contestazioni sia sul blocco del pagamento, che il cliente assume risalire a due ore dal perfezionamento delle transazioni fraudolente senza fornire alcun dettaglio relativo alle circostanze in cui sarebbe avvenuto, sia sul superamento del plafond di spesa, che peraltro dalla documentazione contrattuale allegata dall'intermediario non risulta superato. E si sottolinea, a proposito delle notifiche di avvenuta esecuzione delle operazioni fraudolente, che l'intermediario ha documentato l'invio tramite e-mail degli *alert* a margine delle operazioni eseguite con riferimento soltanto ai 2 bonifici istantanei, ossia i primi due pagamenti; con riferimento alla terza operazione, ha invece espressamente dichiarato di non aver inviato alcuna notifica *alert*. Ma, mentre le prime due operazioni sono avvenute in un arco temporale ristretto, (dalle ore 11:00 alle ore 11:08), la terza operazione è stata realizzata dopo circa 9 ore dalla disposizione del secondo pagamento (alle ore 20:05). Quest'ultima deve quindi ritenersi a sé stante, cosa che rende irrilevante il mancato *alert*. Infatti, secondo l'orientamento dei Collegi, la mancata attivazione ovvero il mancato funzionamento del servizio di sms-*alert* (o di servizio assimilabile) è irrilevante nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta (ovvero di più transazioni così ravvicinate da potersi considerare come una unica).

Per tutto quanto rilevato il ricorso va respinto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE