

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) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) SANTARELLI

Seduta del 09/04/2026

FATTO

Parte ricorrente riferisce che in data 17.09.2025 alle ore 19:18 riceveva sulla propria utenza telefonica un messaggio SMS che sembrava riconducibile all'intermediario (in quanto proveniente dallo stesso mittente con cui normalmente vengono inviati i codici di sicurezza per le transazioni *online*) con il quale veniva avvisato di un'operazione in uscita da € 2.885,90 e pertanto invitato a contattare un certo numero di telefono. Contestualmente comparivano dalla APP dell'intermediario le notifiche afferenti tale operazione e successivamente iniziavano a comparire sul telefono un numero ingestibile di analoghe notifiche, tutte reiterate, rendendo nei fatti impossibile negare l'operazione. Pertanto, chiamava il numero indicato dall'SMS, al quale rispondeva un operatore che si qualificava 'assistente della banca'. Durante tale telefonata (i) una delle operazioni menzionate nelle varie notifiche veniva accettata e pertanto veniva effettuato un primo bonifico di € 2.885,90 a favore di una persona sconosciuta; (ii) si aggiungeva anche un'ulteriore richiesta per ulteriori € 2.000,00; (iii) il sedicente operatore gli riferiva che era vittima di un tentativo di frode in diretta e che sarebbe arrivata a breve una telefonata da parte delle Autorità Antifrode. A questo punto parte ricorrente riceveva alle ore 19:29 una telefonata alla quale rispondeva e interloquiva con un soggetto che si identificava come un Maresciallo dei Carabinieri, da cui era indotto a lasciarsi guidare per risolvere il tentativo di frode in corso e, così, seguendo le indicazioni del truffatore, effettuava dei giroconti dal suo conto presso l'intermediario resistente finalizzate ad un ipotetico storno. Nel frattempo, si aggiungevano altre richieste di pagamento provenienti dalla app T* (una per € 613,36, un'altra per € 2.137,98 e una

terza per € 2.102,93), che venivano eseguite senza alcuna sua autorizzazione. Il tutto per complessivi € 9.740,17. Presentata denuncia e reclamo all'intermediario, senza esito positivo, in questa sede parte ricorrente chiede che l'intermediario convenuto venga condannata al pagamento dell'intero importo oggetto di truffa.

L'intermediario chiede il rigetto del ricorso sulla base delle seguenti prospettazioni ed argomentazioni: (a) le operazioni sono state correttamente contabilizzate, registrate e autenticate con il corretto inserimento delle credenziali; (b) parte ricorrente ha agito con colpa grave in violazione delle disposizioni di legge e contrattuali, eseguendo le azioni che di volta in volta gli venivano indicate dal frodatore; (c) è infatti pacifico che le richieste avanzate dal frodatore erano a tal punto palesemente irragionevoli, che la stessa parte ricorrente, utilizzando una minima diligenza, ben avrebbe dovuto - fin da subito - provvedere autonomamente al tempestivo blocco del proprio strumento di pagamento e a contattare la Banca attraverso i canali di comunicazione ufficiali; (d) nessuna valenza probatoria può essere attribuita agli SMS prodotti che non recano la data in cui la supposta frode si sarebbe verificata e che presentano evidenti indici di anomalia; (e) parte ricorrente è evidentemente caduto vittima di un episodio di *phishing*, sebbene la Banca avesse debitamente attivato una campagna informativa antifrode a beneficio della propria clientela, attraverso la quale anche parte ricorrente è stata messa al corrente dei possibili rischi del *phishing* e delle sue potenziali declinazioni, quali appunto il caso di specie; (f) nulla può essere eccepito in merito ai presidi di sicurezza adottati dalla Banca, che stati superati dal comportamento gravemente colposo imputabile al Ricorrente, il quale ha personalmente disposto nonché autorizzato le operazioni di pagamento in parola.

Parte ricorrente ha replicato per evidenziare quanto segue: (i) pur avendo inizialmente negato l'autorizzazione, è stato però raggiunto da un flusso reiterato ed incontrollato di notifiche, ritenendo che l'App della banca permette a terzi di inviare a flusso continuo un numero ingestibile di notifiche push; (ii) tale invio massiccio ha generato un vero e proprio blocco funzionale dello smartphone, rendendo di fatto impossibile per l'utente non solo gestire il proprio conto, ma lo stesso utilizzo del device; (iii) compito della Banca non è solo quello di verificare la SCA, ma anche quello di monitorare operazioni che presentano anomalie evidenti; monitoraggio che, in questo caso, è stato del tutto assente; (iv) sarebbe stato possibile e doveroso che la banca, attraverso l'App, sospendesse temporaneamente l'operatività: il fatto che un tale sistema non sia stato implementato dimostra che il sistema di sicurezza della banca non è aggiornato; (v) quanto ai pagamenti avvenuti a mezzo T*, non si comprende come possa la Banca non aver percepito l'anomalia di operazioni avvenute attraverso una piattaforma social network. In conclusione, parte ricorrente contesta l'idoneità del sistema di autenticazione forte adottato dalla Banca e l'addebito di colpa grave.

Anche l'intermediario ha replicato riportandosi alle conclusioni in atti e osservando ancora quanto segue: (a) le operazioni disconosciute sono conformi al disposto dell'art. 10 del D.Lgs. n. 11/2010; (b) la Banca ha fornito specifici elementi di fatto idonei a dimostrare la condotta gravemente colposa di parte ricorrente, la quale si pone quale causa esclusiva e determinante dell'evento dannoso lamentato; (c) la ricezione delle richieste di pagamento e delle correlate notifiche push di autorizzazione costituisce evidenza del corretto e regolare funzionamento dei

sistemi di sicurezza adottati dalla Banca, atteso che tali notifiche rappresentano il presidio attraverso cui il cliente viene informato dell'operazione e chiamato a prestare, ovvero negare, un consenso espresso e ai fini della sua esecuzione; (d) dunque, le operazioni risultano regolarmente autenticate, correttamente registrate e contabilizzate, senza che siano emersi elementi indicativi di anomalie operative o interferenze esterne nei sistemi della Banca.

DIRITTO

I principi che si applicano alla materia delle operazioni fraudolente sono note e presuppongono che l'intermediario provi l'autenticazione forte (SCA) nelle varie fasi anche prodromiche alla loro esecuzione e quindi sia in relazione al momento in cui il cliente accede al suo conto di pagamento online sia quanto dispone un'operazione di pagamento elettronico così come in relazione a qualsiasi azione, tramite un canale a distanza, che possa comportare un rischio di frode nei pagamenti o altri abusi. Sempre secondo i principi reiteratamente applicati grava sull'intermediario fornire la prova della eventuale colpa grave del cliente.

Partendo dalla SCA, materia del contendere sono 5 operazioni - 3 operazioni con carta di debito e di 2 pagamenti online "*MoneyB**" – effettuate il 17.09.2025 dalle 19:24 alle 19:48 per importo complessivo di € 9.740,17.

Con riferimento alla fase prodromica necessaria per autorizzare le operazioni di pagamento *online*, l'intermediario ha prodotto i *log* e la relativa legenda, da cui risulta che le transazioni disconosciute sono state eseguite all'interno di n. 3 sessioni *in-app* avviate in data 17 settembre 2025 rispettivamente alle ore 17:19 UTC (19:19 ora locale), alle ore 17:32 UTC (19:32 ora locale) e alle ore 17:47 UTC (19:47 ora locale), secondo le modalità di autenticazione multifattoriale (SCA). Ha inoltre prodotto documentazione attestante che, alla data della frode, il dispositivo attraverso cui è stato compiuto l'accesso e tramite cui sono state in seguito predisposte nonché autorizzate le operazioni di pagamento era associato univocamente al conto del ricorrente e che tale associazione risale al 25 giugno 2021. Dall'esame di quanto prodotto l'accesso in App risulta autorizzato mediante riconoscimento biometrico (cfr. dicitura "*LOGIN_WITH_REFRESH_TOKEN*" e relativa descrizione in legenda) – elemento di inerenza – e utilizzo del device certificato (cfr. dicitura "*MFA_OSC*" e relativa descrizione in legenda nonché colonna "*device_token*" corrispondente a quello di parte ricorrente) che rappresenta un elemento di possesso. Dunque, il Collegio ritiene, in linea con i propri precedenti raggiunta la prova dell'autenticazione forte relativamente alla fase del login (cfr. decisione n. 6148/2024; decisione n. 1325/2025; da ultimo, decisione n. 9189/2025).

Venendo alle 3 operazioni oggetto del contendere, dalla documentazione prodotta e relativa legenda risulta che le stesse sono state effettuate in modalità 3DS, con codice di *dynamic linking* associato alla transazione generato al momento della disposizione del pagamento (vedi dicitura "*Authorization Code*"), tramite conferma della notifica *push* (contenente la schermata riepilogativa del pagamento) ricevuta sul dispositivo in uso a parte ricorrente (elemento di possesso) a seguito di accesso in APP e, quanto all'elemento di inerenza, con riutilizzo del relativo fattore inserito in fase di accesso all'app (cfr. opinion EBA Q&A 2018_4141 che ha

chiarito come la normativa consenta di riutilizzare uno dei fattori di autenticazione inseriti per l'accesso al conto per disporre un'operazione di pagamento *online* nell'ambito della medesima sessione, purché l'associazione di entrambi fattori produca il *dynamic linking*, come è accaduto nella specie). Dunque, la prova della SCA per le tre operazioni in esame è stata raggiunta (cfr. per risultanze analoghe la già citata decisione del Collegio Milano n. 9189/2025 e, prima la decisione n. 5401/2025).

Quanto ai pagamenti MoneyB*, l'intermediario spiega che la funzione MoneyB*** è un sistema di trasferimento istantaneo di denaro tra i propri utenti, che funziona come segue: il cliente che voglia effettuare un pagamento deve selezionare un contatto dalla sua lista utenti, inserire l'importo del pagamento e una causale e immettere il PIN di conferma da lui stesso creato al momento della prima associazione del *device* personale (fattore di conoscenza). A questo punto, al cliente viene presentata una schermata riepilogativa del pagamento in cui viene richiesto di confermare o annullare l'operazione MoneyB*** tramite una notifica *push* dal dispositivo associato (fattore di possesso). Con riferimento al caso di specie, la documentazione prodotta comprova l'applicazione del sistema multifattoriale di autenticazione forte con immissione del codice PIN di conferma di esclusiva conoscenza del Ricorrente (fattore di conoscenza) e impostato da quest'ultimo in data 22 aprile 2021 e le notifiche *push* autorizzative relative ai MoneyB* in questione (fattore di conoscenza).

I fatti che hanno portato alla truffa in esame – per passare alla condotta delle parti e ai profili rilevanti ai fini della colpa grave - sono descritti nella denuncia presentata in data 17.09.2025, in cui si trova una narrazione sostanzialmente coincidente con quella del ricorso e cioè (i) la ricezione di un SMS da un mittente che pareva essere l'intermediario convenuto, SMS con cui parte ricorrente veniva invitato a chiamare un certo numero telefonico; (ii) la contestuale ricezione di una notifica dall'app dell'intermediario che chiedeva di approvare o rifiutare l'operazione oggetto del citato SMS; (iii) la telefonata effettuata da parte ricorrente al numero indicato nello stesso SMS e quindi il contatto con un soggetto che si presentava come un operatore dell'intermediario; (iv) l'interruzione di tale telefonata e la ricezione poco dopo di un'ulteriore chiamata da un diverso numero da parte di un altro soggetto che si qualificava come Maresciallo dei Carabinieri; (v) l'esecuzione reiterata, nonostante i dubbi delle direttive impartite da tale sedicente Maresciallo che portavano all'esecuzione delle transazioni oggetto del contendere.

Parte ricorrente ha prodotto evidenza dell'SMS civetta, che inserito in una *chat* che riporta la denominazione dell'intermediario, ma che non reca il giorno di ricezione, indica una presunta "operazione in uscita" e invita a chiamare il numero 02**, che non risulta essere un numero dell'intermediario. Tale messaggio è seguito da altro SMS fraudolento, secondo cui ogni successiva operazione sarebbe stata uno storno o una simulazione, con invito a seguire le istruzioni dell'operatore. L'esame di tale secondo messaggio suggerisce un *modus procedendi* poco verosimile, invitando a eseguire operazioni 'simulate' ("saranno solamente simulazioni") con l'asserito obiettivo dello storno. Non vi è agli atti lo *screenshot* della telefonata effettuata da parte ricorrente al numero indicato nel primo SMS, ma la sua effettuazione è ammessa e come già detto il numero non corrisponde a un contatto dell'intermediario convenuto. L'insieme di tali

circostanze induce il Collegio a ritenere sussistente la colpa grave di parte ricorrente, tenuto altresì conto che, benché la fattispecie possa essere qualificata come *spoofing*, tuttavia il tenore letterale dei messaggi non poteva creare alcun affidamento sulla loro genuinità (ciò anche a prescindere dal fatto che la facilità con cui si possa utilizzare l'escamotage dello *spoofing* sia ormai nota) e che ormai gli organi di stampa riportano frequentemente di truffe effettuate da falsi appartenenti alle forze dell'ordine.

Infine, vanno esaminati gli aspetti che attengono ad una eventuale responsabilità concorrente dell'intermediario. Parte ricorrente ha contestato 5 operazioni, eseguite in un arco temporale di 24 minuti (tra le 19:24 e le 19:48) di cui tre effettuate con carta di pagamento in favore di una medesima e nota piattaforma *online* di social network (T*). Agli atti non vi è evidenza dell'attivazione di un servizio di sms-alert, ma solo le notifiche *push* per l'autorizzazione delle singole operazioni.

Tuttavia, quel che rileva nella specie sotto il profilo qui in esame è che l'intermediario ha documentato di aver predisposto e attuato uno specifico strumento di prevenzione delle frodi. In particolare, afferma di aver implementato un avviso di sicurezza in-app relativo a potenziali frodi con cui l'App quando rileva che l'utente, al momento dell'apertura dell'applicazione, sta ricevendo o effettuando una chiamata, richiama l'attenzione del cliente sul potenziale rischio di frodi telefoniche chiedendo di verificare l'identità del chiamante e di scegliere tra due pulsanti: uno atto a confermare che la telefonata è genuina ("*No, it's safe*") ed uno finalizzato a segnalare la truffa in corso ("*Yes, get help*"). L'invio di tali alert a parte ricorrente è comprovato dai log prodotti che li tracciano e che evidenziano per 5 volte la dicitura "*vishing cancel*".

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE