

COLLEGIO DI TORINO

composto dai signori:

(TO) BARENGHI	Presidente
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) CARATTOZZOLO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) PUDDU	Membro di designazione rappresentativa dei clienti

Relatore GIUSEPPE SPENNACCHIO

Seduta del 27/04/2026

FATTO

La parte ricorrente ha affermato:

- di essere intestataria di n. 2 conti correnti, cointestati a ricorrente e aderente al ricorso, accesi presso l'intermediario resistente, in particolare:
 - o conto corrente n. *416 (cointestato);
 - o conto corrente n. *776 (intestato esclusivamente a lei);
- che, in data 30/10/2024, il padre riceveva una telefonata dal numero fisso *021 da un operatore del settore antifrode di un istituto di credito;
- che la conversazione si spostava sul numero personale della ricorrente, alla quale veniva comunicato che il suo conto corrente presso tale istituto di credito era stato compromesso per aver effettuato pagamenti su alcune piattaforme online;
- che il sedicente operatore, identificatosi come M. R., esercitando una manipolazione psicologica, le indicava di procedere con alcuni contro bonifici in modo da porre in sicurezza i suoi risparmi;
- che, durante la telefonata, il malfattore carpiva informazioni sull'esistenza di conti correnti presso la banca resistente e le comunicava che si sarebbe messo in contatto con l'intermediario al fine di verificare la presenza di movimenti anomali, per poi ricontattarla;

- che il pomeriggio del 30/10/2024, la ricorrente veniva contattata da tal M. V., qualificatosi come operatore della resistente, il quale le comunicava che, pur non essendovi stati movimenti anomali, era consigliabile mettere in sicurezza i fondi presenti sui propri conti correnti con trasferimenti tramite bonifici in una cassetta di sicurezza intestata ad un ufficiale giudiziario, tale S. L.;
- che procedeva, dunque, a effettuare n. 3 bonifici per un importo di € 13.298,00 dal conto a lei intestato;
- che il giorno seguente, 31/10/2024, veniva contattata dal numero *789 per porre in sicurezza i risparmi presenti nel conto cointestato con il padre;
- che, confusa e preoccupata da quanto stava accadendo, procedeva in tal senso;
- che riscontrando difficoltà nel compimento delle operazioni ed essendo sottoposta ad una forte manipolazione psicologica, si recava, come suggeritole dal malfattore, presso la cassa automatica della filiale per effettuare le operazioni;
- che non riuscendo comunque a completare l'operazione, il finto operatore la invitava a recarsi presso la cassa interna della banca;
- che si recava quindi all'interno della filiale ma, poiché vi erano molti clienti e aveva urgenza di tornare dal padre lasciato da solo a casa, non procedeva con le operazioni indicate dal truffatore e gli chiedeva di poter essere messa in contatto con la direzione;
- che la ricorrente veniva ricontattata dal sedicente R. M., che le comunicava di essere stato incaricato di realizzare il trasferimento del denaro presente sul conto nr. *416 su cassetta di sicurezza digitale, al fine di porre i suoi risparmi in sicurezza;
- che, seguendo le indicazioni dell'operatore, il quale continuava a sottolineare l'urgenza delle operazioni, procedeva per errore a trasferire il denaro sul proprio conto corrente n. *776 per poi effettuare n. 2 bonifici a un ufficiale giudiziario indicato dall'operatore;
- che, nel frattempo, allarmata dalla situazione, cercava di contattare più volte il proprio consulente per richiedere delucidazioni in merito alla complessa e preoccupante situazione che si era originata in relazione ai propri conti correnti;
- che, poiché il consulente non risultava in servizio, gli lasciava un messaggio in segreteria;
- che, compiute le operazioni indicate, il sedicente operatore le indicava di formattare il proprio telefono e che l'avrebbe contattata il lunedì successivo (04/11/2024) per confermare il buon esito delle operazioni;
- che, in data 04/11/2024 non riceveva alcuna telefonata, dunque contattava lei stessa l'operatore;
- che, insospettita dalla conversazione avuta con il finto operatore, minacciava di sporgere denuncia;
- che a quel punto il suo contatto veniva bloccato dall'interlocutore;
- che, in seguito, contattava il suo consulente spiegando la dinamica degli eventi e lui la informava che era stata probabilmente vittima di una truffa;
- che chiedeva urgentemente al proprio consulente di bloccare i bonifici effettuati, ma le rispondeva che ciò non era più possibile;
- che, sempre in data 04/11/2024, la ricorrente si recava presso le Autorità per sporgere querela, integrata poi in data 05/11/2024 e 08/11/2024;
- che provvedeva a segnalare alla banca quanto accaduto ricevendo, in data 22/11/2024, riscontro negativo circa la richiesta di rimborso;
- che, in data 12/11/2024, insieme al padre, procedeva a effettuare un reclamo alla banca sulla frode informatica avvenuta con diffida ad adempiere al rimborso di quanto era stato sottratto, oltre a risarcimento dei danni morali e materiali subiti e la richiesta

di comunicare le misure adottate per rafforzare la sicurezza dei sistemi e prevenire future situazioni analoghe, a tutela dei clienti;

- che poiché, in data 31/01/2025, l'intermediario ribadiva di non poter procedere con il rimborso del denaro richiesto e con la soddisfazione della richiesta di risarcimento, decideva di presentare ricorso all' Arbitro Bancario Finanziario;
- che i truffatori si sono avvalsi di avanzate tecniche di *spoofing* telefonico e manipolazione psicologica;
- che, fingendo di essere reali operatori degli istituti di credito di riferimento, utilizzando numeri telefonici apparentemente autentici e riconducibili alle reali utenze delle banche (come, per esempio, il numero *021), hanno ingenerato un falso clima di fiducia, una forte preoccupazione di perdere i propri risparmi e hanno fatto percepire la necessità di agire in modo rapido nel rispetto delle loro indicazioni per evitare conseguenze pregiudizievoli;
- che, nello specifico, i truffatori hanno messo in pratica il *caller-ID spoofing*, ossia far apparire la telefonata ricevuta dalla vittima come riferibile ad un'utenza sicura (nel caso in esame al settore antifrode di un istituto di credito di cui è cliente), riuscendo ad innescare nella vittima una certa fiducia;
- che tali elementi rendono comprensibile l'affidamento che ha posto sui propri interlocutori;
- che l'intermediario resistente è responsabile per non aver predisposto adeguate misure di sicurezza e tutela dei propri clienti, lasciando che effettuasse bonifici con cifre considerevoli e causali discutibili, senza bloccare le operazioni stesse e senza contattarla direttamente al fine di chiarire le ragioni per le quali venissero effettuate operazioni di quel tipo;
- che la banca ha lasciato che venissero effettuate tre operazioni con cifre considerevoli e causali discutibili;
- che si configura un preciso obbligo di diligenza della banca nei confronti del cliente e che l'intermediario deve rispondere in tutto o in parte del danno subito dal cliente quando questo sia stato indotto all'operazione sulla base di forme sofisticate di truffa, quale lo *spoofing*, e a causa dell'omissione di dovute condotte da parte della banca finalizzate a contrastare tali situazioni;
- che le operazioni in questione presentavano evidenti anomalie inerenti ad aspetti quali l'importo, la causale e il contesto;
- che non risulta che le siano stati forniti avvisi preventivi o adeguati circa i rischi di frodi come la pratica del *phishing* o lo *spoofing* e che quindi era privata degli strumenti essenziali per riconoscere e contrastare tali condotte;
- che dai fatti descritti emerge l'incapacità dell'istituto di credito di approntare idonee misure tecniche e organizzative e, conseguentemente, la vulnerabilità dei sistemi di sicurezza;
- che è stata tratta in inganno dalle modalità particolarmente insidiose della frode.

La parte ricorrente ha chiesto, pertanto, la restituzione della somma di €. 25.078,00= prelevata illegittimamente. In via subordinata, ha domandato il rimborso di una somma individuata dal Collegio, sulla base del riconoscimento di un concorso di colpa tra le parti.

L'intermediario nelle controdeduzioni ha precisato:

- che la ricorrente è contitolare con il padre del conto corrente n. *416 ed è unica titolare del conto corrente n.*776, ai quali è collegato il servizio "Rapporti a distanza tra Banca e Cliente", c.d. home banking;

- che le operazioni di bonifico sono state eseguite con addebito sul conto corrente n. *776, determinando ciò un difetto di legittimazione attiva in capo al cointestatario del conto n.*416;
- che i precedenti trasferimenti dal conto cointestato a quello della ricorrente hanno costituito meri giroconti tecnici su rapporti a lei intestati, finalizzati esclusivamente alla creazione della provvista necessaria per il compimento delle operazioni fraudolente;
- che vi sono numerosi elementi che evidenziano la colpa grave della ricorrente;
- che il primo contatto, da cui si è sviluppata poi la successiva frode, è stato effettuato da altro intermediario;
- che la ricorrente ha eseguito in modo acritico tutte le istruzioni fornite dall'operatore, a lei sconosciuto, disponendo "contro bonifici" dal conto corrente intrattenuto presso altra banca;
- che sarebbe stato sufficiente controllare il conto presso tale altro intermediario per scongiurare la frode;
- che la richiesta inerente all'eventuale titolarità di rapporti presso altri istituti di credito avrebbe dovuto allertare la ricorrente;
- che, ciononostante, la ricorrente non ha rilevato alcuna anomalia nel comportamento del malfattore;
- che la banca avverte la propria clientela di non prestare particolare attenzione al "Caller ID" che appare sul telefono;
- che il contatto ricevuto dall'operatore R. M. non configura spoofing, in quanto si tratta del numero della sede, non riconducibile ad alcuna struttura operativa;
- che, il frodatore ha contattato la ricorrente con un numero solo in apparenza riconducibile alla banca resistente, qualificandosi, tuttavia, come operatore del settore antifrode di un altro intermediario;
- che la ricorrente ha, quindi, interloquuto con un operatore mai sentito né conosciuto, dopo pochi minuti dal primo contatto con un altro intermediario, con il quale ha eseguito bonifici sotto dettatura;
- che le richieste del frodatore avrebbero dovuto far sorgere nella ricorrente diverse perplessità e quesiti, *in primis* sul perché spostare denaro in una cassetta digitale in assenza di movimenti sospetti e sul perché intestarla a un estraneo;
- che l'sms con cui le veniva comunicato il nuovo iban presentava una serie di anomalie, tanto che la ricorrente eseguiva i bonifici sull'iban indicato nel messaggio ma non indicando se stessa quale beneficiaria, posto che quella era la sua nuova coordinata bancaria, ma un soggetto terzo;
- che, quindi, era palese che il nuovo iban generato non fosse attribuibile alla ricorrente, bensì ad uno sconosciuto;
- che gli sms ricevuti erano affetti da vari elementi che la ricorrente avrebbe dovuto rilevare in quanto provenivano da un terzo intermediario, non riconducibile alla resistente, erano formulati in termini assolutamente generici ed erano caratterizzati da un tono visibilmente elementare e assolutamente non in linea con la normale operatività della banca e presentano contenuti fantasiosi;
- che la cliente tentava di contattare il suo consulente che, però, non era disponibile in quel momento;
- che proprio in tale eventualità è necessario contattare il servizio clienti, attivo 7 giorni su 7 e 24 ore al giorno;
- che, diversamente da quanto riferito, effettuava unicamente due tentativi di chiamata al proprio consulente, alle ore 15:41;

- che la ricorrente ha prestato fede all'assunto secondo cui un sedicente addetto antifrode di un terzo intermediario fosse stato incaricato da un ulteriore istituto di mettere 'in sicurezza' i propri risparmi, omettendo tuttavia di compiere qualsivoglia verifica sulla genuinità di tale anomala procedura;
- che, essendovi confessione in denuncia circa le modalità di "circuizione" della cliente, le modalità dispositive delle operazioni e il mancato controllo sulla contabilizzazione delle operazioni, la colpa è sufficientemente provata;
- che è bastata una narrazione piuttosto fantasiosa per indurre la ricorrente a disporre lei stessa incomprensibili bonifici per mettere in sicurezza i propri fondi, che invece erano semplici disposizioni di pagamento;
- che, poiché l'operazione è stata eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), essa deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2;
- che rientrano in tale fattispecie anche le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione;
- che la cliente deve restare vigile ed accorta nell'utilizzo degli strumenti di pagamento e delle relative credenziali di accesso e una sua negligenza la può esporre al rischio di frode, illecito che la banca non è in grado di prevedere e di evitare;
- che da tempo raccomanda la massima attenzione e cautela nell'utilizzo dei canali telematici, fornendo indicazioni dettagliate alla propria clientela, con varie modalità comunicative, sul comportamento da adottare per la sicurezza dei dati bancari;
- che, comunque, le operazioni sono state svolte in conformità alla sicurezza prescritta dalla normativa PSD2 e con un sistema di autenticazione "forte";
- che le operazioni sono state eseguite dallo stesso dispositivo in uso alla ricorrente e risultano correttamente autenticate, registrate e contabilizzate;
- che, a fronte delle operazioni eseguite e disposte dalla stessa ricorrente, ha inviato, al cellulare della cliente, le notifiche SMS, che le avrebbero consentito di attivarsi con tempestività per evitare ogni danno a suo carico;
- che la banca si è attivata per tentare il richiamo della somma oggetto di frode senza esito;
- che la banca non è tenuta a verificare preventivamente che l'operazione sia riconducibile alla effettiva volontà del cliente, ma a garantire ed assicurare che il processo di esecuzione dell'operazione sia svolto nel rispetto della Strong Customer Authentication;
- che non sussiste a carico della banca alcun obbligo di monitoraggio delle operazioni;
- che, per quanto concerne l'ulteriore richiesta di risarcimento danni, non è fornita di alcun elemento probatorio.

Tanto premesso, ha domandato il rigetto del ricorso.

DIRITTO

La parte ricorrente, in qualità di titolare del conto corrente n. *776 e di contitolare del conto corrente n. *416 intestato anche al padre, contesta gli addebiti in c/c operati dalla banca a seguito di tre bonifici eseguiti per un importo complessivo di €. 25.078,00=. Il Collegio rileva che, nel caso di specie, due delle tre anzidette disposizioni in uscita sono state precedute da operazioni di giroconto di pari importo, provenienti dal conto cointestato n. *416 e che, trattandosi di rapporti intrattenuti presso lo stesso intermediario ed intestati alla stessa ricorrente, per esse vi sarebbe l'esenzione, per

l'intermediario, dall'obbligo di applicare la SCA, non comportando comunque le medesime alcun pregiudizio economico per la stessa ricorrente.

Inoltre, secondo l'orientamento consolidato dell'Arbitro, la circostanza che il cointestatario del conto n. *416 abbia aderito al ricorso, benché le somme di cui alle operazioni disconosciute siano state sottratte dal rapporto n. *776, intestato alla sola ricorrente, pur sollevando dubbi sulla legittimazione attiva del soggetto aderente, non incide sull'ammissibilità del ricorso proposto dalla ricorrente.

Ciò premesso, il Collegio rileva in primo luogo che le operazioni oggetto del ricorso sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, entrato in vigore in data 13 gennaio 2018. A norma degli artt. 10 e 10-bis, d.lgs. n. 11/2010, *“è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento contestata è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure (...) o di altri inconvenienti”* (art. 10, comma 1), mentre l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'art. 7.

Pertanto il prestatore di servizi di pagamento rimborsa al pagatore l'importo dell'operazione medesima o riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, fatta salva la facoltà di dimostrare che, nell'ambito delle sue competenze, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti relativi al servizio di pagamento da questo prestato”. Ne consegue che qualora l'utente neghi di aver autorizzato un'operazione di pagamento già effettuata, l'onere di provare la genuinità della transazione ricade essenzialmente sul prestatore del servizio; e nel contempo quest'ultimo è obbligato a rifondere con sostanziale immediatezza il cliente in caso di operazione disconosciuta, tranne ove vi sia un motivato sospetto di frode e salva la possibilità per il prestatore di servizi di pagamento di dimostrare, anche in un momento successivo, che l'operazione di pagamento era stata autorizzata.

Il Collegio rileva innanzitutto come, dall'analisi della documentazione versata in atti, con riferimento alla dinamica della truffa oggetto di ricorso, non è contestata la circostanza che la ricorrente dichiarò chiaramente di aver dato seguito alle indicazioni ricevute telefonicamente da un sedicente operatore dell'intermediario, collaborando dunque con il truffatore per l'esecuzione dei bonifici di cui si discute. La circostanza che i bonifici siano stati eseguiti personalmente dalla ricorrente non è contestata.

Si evidenzia in merito che, secondo gli orientamenti condivisi dei Collegi, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2.

Applicato tale principio al caso in esame, il Collegio ritiene rilevante l'eccezione preliminare così sollevata dall'intermediario, decidendo quindi nel merito dell'eventuale responsabilità del medesimo sulla base dei principi comuni in materia di responsabilità. Infatti, in presenza di determinate circostanze, da valutarsi secondo il prudente apprezzamento del Collegio giudicante, è talora possibile riconoscere al ricorrente

l'accoglimento della propria richiesta di rimborso, avuto riguardo a particolari profili che possano aver connotato la condotta dell'intermediario.

Secondo gli orientamenti condivisi dei Collegi, si può rilevare una responsabilità concorrente del PSP sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode come, ad esempio, nei casi di mancata disponibilità del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore; o di mancata identificazione del tentativo di frode in corso, da parte del dipendente del PSP cui il pagatore si sia rivolto esponendo le richieste del frodatore; o ancora di mancato rilievo di indizi di frode, nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto ed il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere.

Nessuna di tali ipotesi sembra ricorrere nel caso di specie. Al riguardo l'intermediario sostiene che la cliente, non riuscendo a contattare il proprio consulente, avrebbe dovuto avvalersi del servizio di assistenza telefonica, garantito continuativamente, anziché attendere il contatto diretto con lo stesso consulente.

Per altro appaiono da considerare decisivi, in punto di valutazione della colpa grave della ricorrente, i rilievi dell'intermediario in merito alla condotta tenuta da quest'ultima. L'intermediario ha comunque indicato le modalità richieste per l'accesso ai servizi *on line* della banca. Ha chiarito, inoltre, che le operazioni sono state correttamente autenticate, registrate e contabilizzate, mediante l'utilizzo di validi elementi idonei a configurare un sistema di autenticazione forte.

Dalla documentazione in atti non è chiaro in che modo il truffatore sia riuscito a prendere contatto con la parte ricorrente. Dalla ricostruzione dei fatti, parrebbe come la cliente sia caduta vittima del noto fenomeno del c.d. *phishing* attraverso *vishing*, realizzato mediante iniziale ricezione di una telefonata truffaldina apparentemente proveniente da un'utenza telefonica riconducibile alla banca, nella quale un ignoto truffatore, che si qualificava come un operatore dell'intermediario resistente, induceva la cliente ad attivare apposita procedura atta a prevenire indebiti accessi alla propria area riservata dei servizi di *mobile banking* dell'intermediario.

Si evidenzia, per scrupolo di completezza, che in sede di ricorso la parte ricorrente ha contestato espressamente che la banca avrebbe dovuto avvedersi dell'anomala operatività posta in essere il giorno della frode e sospenderla cautelativamente a tutela del cliente. Circa il mancato monitoraggio delle operazioni sospette va rilevato che, secondo le posizioni condivise dei Collegi, è necessaria l'allegazione di circostanze specifiche idonee ad integrare una negligenza da parte dell'intermediario: circostanze che non sono rinvenibili nel caso in esame.

Non è comunque ipotizzabile un generale obbligo di monitoraggio *ex ante* in capo all'intermediario ed un connesso obbligo di bloccare l'operatività dello strumento di pagamento.

Né nel caso di specie sono ravvisabili indizi di frode che, secondo un orientamento arbitrale, sebbene il D.M. n. 112/2007 faccia riferimento alla prevenzione delle frodi sulle carte di pagamento, possono costituire un parametro di valutazione del comportamento del PSP, ove possibile, anche con riguardo ad operazioni eseguite con altri strumenti di pagamento (ad esempio, bonifici o ricariche *on line*), in ragione dell'unicità della *ratio* sottesa a tale normativa.

In definitiva, per tutte le considerazioni esposte il Collegio non ritiene che il ricorso possa trovare accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE