

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) RUSSO	Membro designato dalla Banca d'Italia
(PA) SCANNELLA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore FEDERICO RUSSO

Seduta del 23/01/2026

FATTO

1. Parte Ricorrente è titolare di un conto presso l'Intermediario convenuto.

Riferisce di avere ricevuto, in data 20 maggio 2025, un messaggio dell'Intermediario che lo avvertiva dell'aumento del massimale per i bonifici *online*, e poco dopo, un ulteriore messaggio che lo avvisava di un bonifico da lei eseguito, dell'importo di € 19.450.

Riferisce, altresì, di avere ricevuto, poco dopo e segnatamente alle 11:19, una chiamata apparentemente proveniente dall'Intermediario, nel corso della quale un sedicente operatore le chiedeva se riconoscesse il pagamento. A fronte della domanda, Parte ricorrente rispondeva di non avere mai autorizzato il pagamento in questione. Veniva quindi rassicurata che l'app sarebbe stata bloccata (cosa, in effetti, avvenuta) e che sarebbero stati eseguiti *"tutti i controlli necessari per la restituzione"*.

2. Non avendo ricevuto alcun rimborso, Parte ricorrente, il 20 giugno 2025 alle ore 7.53, proponeva reclamo (poi reiterato il 3 luglio 2025), ribadendo che lo stesso Intermediario, con la chiamata del 20 maggio 2025, aveva riconosciuto e comunque era stato reso edotto del carattere fraudolento dell'operazione, e l'aveva rassicurata circa l'annullamento dell'operazione.

3. Insoddisfatta dell'interlocuzione avuta, Parte ricorrente proponeva ricorso dinanzi a questo Arbitro Bancario Finanziario, chiedendo la: *“Restituzione dell'importo indebitamente sottratto”*.

4. Si costituiva l'Intermediario, eccependo la propria diligenza, il rispetto della SCA e, per converso, la colpa grave di Parte ricorrente. Lamentava, inoltre, che Parte ricorrente avesse ommesso di precisare le circostanze della truffa. Dall'istantanea dello schermo prodotta da questa, infatti, risultava che, nella serata del 19 maggio 2025, ossia la sera prima della truffa, Parte ricorrente era stata contattata dai truffatori. In tale occasione, era stata evidentemente convinta, con raggiri, a fornire le credenziali ai truffatori, ed aumentare così il massimale per i bonifici. Precisava, pertanto, le seguenti conclusioni: *“In considerazione di tutte le argomentazioni esposte e dei documenti allegati, si chiede a Codesto Spettabile Arbitro Bancario Finanziario di respingere il ricorso, in quanto infondato in fatto e in diritto”*.

DIRITTO

I. In linea generale, le operazioni contestate sono state poste in essere 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 (c.d. PSD 2) ss.mm.ii., nonché – per quanto riguarda la *Strong Customer Authentication* (c.d. SCA) – anche delle 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 soprarichiamata normativa fissa una sostanziale inversione al principio dell'onere della prova fissato dall'art. 2697 c.c., chiaramente improntata al c.d. *principio di vicinanza o riferibilità della prova*, secondo cui l'onere della prova, in caso di disconoscimento di una operazione, deve essere attribuito dalla legge alla parte che a tale prova è più “vicina”, ossia al soggetto che ha predisposto la piattaforma poi utilizzata dal cliente. L'art. 10 del d.lgs. 11/2010 prevede, in particolare, che: *“1. Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti”* (il comma 1 bis detta poi una regola sostanzialmente analoga in caso di operazione disposta mediante prestatore di servizi di disposizione di ordine di pagamento). Al comma 2 la medesima norma aggiunge che: *“2. Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, 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'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente”*. Inoltre, l'art. 10-bis, comma 1, del medesimo D.Lgs. 27/1/2010 n. 11 - come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II) – statuisce che: *“Conformemente all'art 98 della Dir (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione Europea, i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente qualora l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico...”*. La nozione di *“autenticazione forte del cliente”* è definita dallo stesso art. 1 del d.lgs. 11/2010 lett. q-bis), secondo cui si definisce tale *“un'autenticazione basata sull'uso di due o più elementi, classificati nelle*

categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione [...]".

Un obbligo analogo di utilizzo di un sistema di autenticazione forte è, poi, previsto dal Reg. UE 389/2018, per tutte quelle operazioni che, a norma dell'art. 18, non possano essere considerate "a basso livello di rischio".

In conclusione, in deroga ai principi generali in materia di prova, è onere dell'Intermediario dimostrare la propria diligenza (e, nell'ambito di questa, l'utilizzo di un sistema di autenticazione forte) nonché la colpa grave dell'utente.

L'inversione dell'onere della prova anzidetta, tuttavia, non può tradursi in una *presunzione assoluta* a danno dell'Intermediario né in una sorta di responsabilità oggettiva di questo: egli deve, pertanto, potere dimostrare la colpa grave del cliente e, per converso, la correttezza del proprio operato: da un lato, provando di avere adempiuto alle proprie obbligazioni con la specifica diligenza prevista (*in primis*, come detto: l'utilizzo di un sistema di autenticazione forte), dall'altro, provando l'assenza di indici di anomalia, che avrebbero potuto indurre l'operatore avveduto a bloccare l'operazione, di modo che l'operazione contestata non avrebbe potuto essere eseguita senza la colpa grave del cliente.

Quanto alla prova della colpa grave, questa non può, ovviamente, essere ricavata dal semplice rispetto, da parte dell'Intermediario, delle procedure di sicurezza e dall'apparente assenza di anomalie. Tuttavia, detta prova può essere fornita anche in via presuntiva, purché si tratti di presunzioni gravi, precise e concordanti, consistenti in *"una serie di elementi di fatto particolarmente univoca e convergente, al punto che possa ragionevolmente ritenersi che l'utilizzo fraudolento sia effettivamente riconducibile sul piano causale alla condotta dell'utilizzatore"* (Collegio Coordinamento n. 6168/2013, Collegio Coordinamento n. 22745/2019; cfr. anche Collegio Bologna, 26 luglio 2022, n. 11167 e 14 luglio 2022, n. 10560, i quali hanno ritenuto che, in caso di furto della carta di debito, il PIN fosse custodito unitamente a questa, dalla circostanza che i prelievi andarono immediatamente a buon fine, senza alcun tentativo precedente fallito).

II. Nel caso di specie, come si è detto, posto che Parte ricorrente nega di avere eseguito personalmente le operazioni, si applica senz'altro la disciplina sopra richiamata. Occorre, pertanto: accertare, in via preliminare l'avvenuta prova della SCA; qualora tale prova non sia stata fornita dall'Intermediario, procedere all'accertamento dell'eventuale colpa grave del cliente; qualora tale prova sia stata fornita, procedere all'accertamento di un eventuale concorso di colpa dell'Intermediario.

La SCA risulta provata.

Dai *log* informatici prodotti dall'Intermediario, infatti – non disconosciuti, e dunque aventi valore di prova legale della corrispondenza delle registrazioni ai fatti rappresentati, giusta il disposto dell'art. 2712 c.c. – si evince che fu eseguito, il 19 maggio 2025, l'*enrollment* di due dispositivi, uno – presumibilmente – del cliente, e uno dei truffatori.

I fattori utilizzati furono: codice cliente, data di nascita e PIN (elemento di conoscenza: *"AUTH_METHOD... smartcode"*) e digitazione di un OTP ricevuto al dispositivo del cliente, come registrato all'interno dell'anagrafica della Banca (elemento di possesso. La corretta digitazione del PIN è attestata dallo *"status... SUCCESS"*). Quindi, con le medesime modalità, alle ore 19:03 fu disposto l'aumento dei massimali.

L'aumento dei massimali divenne operativo solamente alla mezzanotte. L'operazione dispositiva fu, invece, eseguita il 20 maggio 2025, alle ore 11:08:40. L'accesso all'homebanking avvenne col secondo dispositivo enrollato "S***57G" (quello dei truffatori), così come il bonifico. Anche in questo caso,

l'operazione fu autorizzata con lo Smartcode ("autorizzazione MPIN – inserimento SmartCode": elemento di conoscenza), tramite l'app installata nel dispositivo anzidetto (elemento di possesso).

Quindi, il dispositivo autentico del cliente fu bloccato, con invio dell'alert all'email del cliente.

In tutte le fasi della truffa, dunque, fu rispettato un sistema di autenticazione a doppio fattore, anche se – ma ciò è irrilevante, vista la correttezza della procedura di *enrollment* del dispositivo *civetta* – l'operazione dispositiva vera e propria fu eseguita da un dispositivo verosimilmente in mano ai truffatori.

III. Prima di procedere all'esame della colpa grave, occorre a questo punto ricostruire la probabile dinamica della truffa, dal momento che tanto la prospettazione di Parte ricorrente che dell'Intermediario risultano in parecchi punti lacunose e che, per converso, almeno fino alla data del ricorso Parte ricorrente non sembrava avere realmente compreso l'accaduto.

Tanto nel reclamo che nel ricorso, infatti, Parte ricorrente insiste nell'affermare che l'Intermediario avrebbe individuato sin da subito il carattere fraudolento dell'operazione, tant'è che, la mattina del 20 maggio 2025, lo avrebbe chiamato e si sarebbe adoperato per bloccarla. Parte ricorrente, dunque, afferma che la chiamata del 20 maggio 2025 provenisse effettivamente, per come appariva, dall'Intermediario.

Correlativamente, le risposte dell'Intermediario, tanto in sede di riscontro al reclamo che di controdeduzioni, sono alquanto anodine circa un punto essenziale ai fini della ricostruzione dei fatti oggetto di causa, ossia l'identità effettiva del soggetto che, alle 11 circa del 20 maggio, aveva contattato Parte ricorrente. Se è vero, infatti, che l'Intermediario nega, in modo abbastanza chiaro, di avere effettuato la precedente chiamata del 19 maggio, poco o nulla chiarisce circa la chiamata del 20, che è poi il punto cruciale della vicenda.

Sulla base della documentazione e di quanto affermato dalle parti, può allora considerarsi accertato che la truffa vera e propria iniziò il giorno precedente a quello ritenuto da Parte ricorrente. In particolare, come si evince dall'istantanea prodotta da Parte ricorrente, questa ricevette, in data 19 maggio 2025, alle ore 18:48, una chiamata apparentemente proveniente dalla Banca. La chiamata durò circa 20 minuti. Nel corso di questa chiamata (in realtà proveniente dai truffatori) il cliente cooperò in qualche modo – comunque non definito – involontariamente alla truffa. All'esito i truffatori riuscirono ad associare (*enrollment*) un dispositivo *civetta* al profilo del cliente e ad autorizzare un aumento del massimale per i bonifici. Con ogni probabilità, i truffatori informarono il cliente che l'avrebbero ricontattato la mattina successiva.

L'aumento del massimale si perfezionò, però, alle 23:00; all'esito il sistema inviò un'email, ragionevolmente ricevuta e letta dal cliente solo la mattina dopo. Oltre all'email, Parte ricorrente riferisce di avere ricevuto anche un messaggio che lo informava dell'avvenuta esecuzione del bonifico di € 19.450,00. Sebbene non vi sia una chiara evidenza di questo messaggio, è verosimile che si trattasse di un messaggio falso (*spoof*), sempre inviato dai truffatori, per preparare la truffa vera e propria (e.g., prospettando le attività successive come dirette a "revocare" il bonifico, e fornire così una giustificazione preventiva agli eventuali messaggi successivi ricevuti dalla Banca).

Poco dopo, Parte ricorrente ricevette una chiamata apparentemente proveniente dalla banca, che lo "avvisava" delle operazioni fraudolente e gli chiedeva di disconoscerle. Sebbene, come detto, l'Intermediario sul punto, tanto in fase di riscontro al reclamo che di controdeduzioni, abbia replicato in modo anodino e non abbia chiarito esplicitamente i fatti, può considerarsi accertato che anche questa telefonata provenisse, in realtà, dai truffatori, i quali avevano *spoofato*, come il giorno precedente, il numero dell'Intermediario. A questo punto, i truffatori, conquistata definitivamente la fiducia del cliente, lo convincevano a comunicare loro alcuni dei dati necessari per perfezionare la truffa, facendogli credere che si trattasse di elementi necessari per ottenere la restituzione del denaro, bloccando poi anche il dispositivo autentico del cliente. La telefonata iniziò alle 11:19, e durò 10 minuti e 16 secondi.

Questa è, in sintesi, la più probabile ricostruzione del fatto, fermo restando che lievi variazioni sono comunque irrilevanti al fine dell'accertamento della colpa grave del cliente. L'altro scenario è che il bonifico fosse stato eseguito in autonomia dai truffatori, il messaggio di alert fosse autentico, così come la chiamata del 20 maggio; tale scenario, però, appare poco verosimile (tenuto conto dell'*id quod plerumque accidit* in questo genere di truffe) e non spiegherebbe per quale motivo la banca non avesse, poi, proceduto all'annullamento o comunque al recall del bonifico (sicché, in assenza della prova di tali attività, o dell'effettiva impossibilità di eseguirle, andrebbe comunque affermata la responsabilità dell'Intermediario).

Quel che è certo, ad ogni modo, è che la truffa prese avvio, il 19 e/o il 20 maggio, da uno *spoofing*, ossia da una frode informatica (peraltro di assai facile realizzazione, e, purtroppo, senza possibilità di controllo da parte dell'Intermediario), caratterizzata dal fatto che i truffatori contattano la vittima da un numero apparentemente riconducibile all'Intermediario. Questo fa sì che le chiamate o i messaggi provenienti dai truffatori vengano erroneamente interpretate dal cellulare della vittima, e *incastrate* nelle conversazioni genuine tra l'Intermediario e il cliente.

IV. Tanto premesso, in linea generale, nei casi di c.d. *spoofing*, i più recenti orientamenti dei Collegi hanno escluso la sussistenza di una colpa grave del cliente, a meno che essa non risulti da elementi ulteriori, quali, meramente a titolo di esempio, la presenza di errori nel testo del messaggio *civetta*, o, più in generale, dalla condotta del cliente nel corso della truffa.

La qualificazione come *spoofing* (nelle sue varianti), come detto, presuppone che i truffatori abbiano adottato una più sofisticata (ancorché di assai facile realizzazione) tecnica fraudolenta, che implica il *camuffamento* dell'indirizzo del mittente (email, sms, chiamata vocale) con un indirizzo o numero effettivamente utilizzati dall'Intermediario *bersaglio* della truffa. Nello *spoofing*, in altri termini, il messaggio, l'email o la chiamata appaiono realmente provenire dal mittente; nel *meno insidioso phishing*, invece, i truffatori si limitano, al massimo, a modificare il campo del "*nome del mittente*", mentre l'indirizzo email (nel caso delle email), ovvero il numero dal quale provengono l'SMS o la telefonata non sono riconducibili all'Intermediario bersaglio della truffa. In tale seconda ipotesi va affermata la colpa grave del cliente, che viene invece oggi, come detto – dopo un contrasto protrattosi per diversi anni tra i Collegi – generalmente esclusa nei casi di *spoofing*, pur con le precisazioni sopra riportate.

V. È pur vero che, come detto, nei casi di *spoofing* non può normalmente rivenirsi alcuna responsabilità dell'Intermediario, il quale non può avere cognizione di quello che accade nel dispositivo del cliente, e al di fuori dal proprio sistema informatico.

Tuttavia, il testo normativo (art. 11 d.lgs. 11/2010 ss.mm.ii.) preclude al Collegio di dare rilevanza a tale circostanza. La norma, infatti, è univoca nell'affermare la responsabilità dell'Intermediario, salvo che non dimostri (oltre alla SCA, anche) la "colpa grave" del cliente.

Per tali motivi, non pare condivisibile la soluzione, talora affiorata nella giurisprudenza dei Collegi, di ripartire la colpa tra le parti, secondo le regole del concorso di colpa, ex art. 1227 c.c.

L'affermazione di un concorso di colpa, infatti, presupporrebbe comunque la preventiva affermazione della colpa grave del cliente (e, dunque, la sua esclusiva responsabilità ex d.lgs. 11/2010), temperata, però, da un concorso di colpa dell'Intermediario (correttamente sul piano concettuale, sul punto, ex *multis*, Collegio Bari, 2794/2025). Ove, di contro, non si accerti la colpa grave del cliente, la fattispecie del concorso appare inapplicabile, dal momento che la norma primaria, sul punto, esclude in radice la responsabilità del cliente (e non si può ragionevolmente prospettare, sul piano concettuale, un *concorso di colpa grave*, o una colpa grave parziale).

La questione ermeneutica, allora, ruota attorno a una domanda fondamentale, ossia entro che limiti nelle fattispecie di *spoofing*, e in particolare di *Caller ID spoofing*, possa affermarsi la colpa grave del cliente, ovvero una colpa semplice.

Vale, sul punto, la pena di evidenziare che nelle ipotesi di *Caller ID spoofing*, ossia quando la truffa sia perpetrata tramite una chiamata telefonica, e non tramite un SMS o un'email, l'accertamento in questione risulta particolarmente complesso e delicato. Mentre, infatti, nello *spoofing* perpetrato tramite SMS o email permane una traccia scritta, che consente di verificare, ad esempio, la presenza di eventuali errori grammaticali o nel nome dell'Intermediario, nelle ipotesi, appunto, di *Caller ID spoofing* il contenuto della telefonata (e, dunque, il carattere decettivo o meno delle domande e delle affermazioni dei truffatori) rimane nella sfera esclusiva del cliente, e non è verificabile dall'Intermediario, né dal Collegio.

Si pone, dunque, il problema di stabilire su chi gravi l'onere di provare il carattere decettivo o meno della telefonata *spoof*, e se questo, in particolare, possa considerarsi presunto.

Ritiene questo Collegio che la formulazione normativa fornisca un'indicazione univoca, impossibile da derogare. L'art. 10 del d.lgs. 11/2010, infatti, prevede come visto espressamente che: *“È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente”*. Di conseguenza, in mancanza di prova della colpa grave del cliente, la domanda di questi non potrà che essere accolta, non essendo stata raggiunta la prova liberatoria, posta a carico dell'Intermediario.

VI. È vero, sul punto, che, come evidenziato dall'Intermediario, le frodi informatiche sono sempre più oggetto dell'attenzione dei media che propongono spesso servizi dedicati. Tuttavia, a giudizio di questo Collegio, allo stato attuale ciò non implica, ancora, una *colpa grave* del cliente che si sia fidato di una chiamata apparentemente proveniente dalla banca, ma una semplice colpa lieve, tenuto conto della minore soglia di attenzione (ampiamente documentata dalla letteratura in materia), indotta dal fatto di leggere, nella chiamata in arrivo, il numero consueto della Banca.

Per fornire, di contro, prova della colpa grave del cliente, l'Intermediario dovrebbe dimostrare di essersi preventivamente attivato in modo efficace, e di avere informato effettivamente il cliente stesso, circa la possibilità di un *caller id spoofing*.

Di ciò, del resto, pare essersi parzialmente reso conto l'Intermediario, il quale ha documentato di avere inserito, nella pagina di *log in*, un *alert* circa le possibili frodi informatiche. Tale *alert*, tuttavia (allegato alle controdeduzioni), si limita a recitare: *“hai ricevuto una email che ti chiede di aggiornare i tuoi dati personali con link”*.

Sebbene la scelta appaia, in linea teorica, apprezzabile ed efficace, il messaggio effettivo non è, comunque sufficiente a far ritenere dimostrata la colpa grave del cliente.

Manca, infatti, in tale *alert*, da un lato – e con rilievo del tutto assorbente – l'avviso esplicito che l'email potrebbe apparentemente provenire dall'indirizzo effettivamente utilizzato dalla Banca; dall'altro l'ulteriore precisazione che, oltre all'email, i truffatori potrebbero utilizzare anche un SMS o una chiamata vocale, pure essi apparentemente provenienti dal numero genuino dell'Intermediario, e incastrarsi nelle precedenti conversazioni tra Banca e utente.

Insufficiente, al riguardo, appare la precisazione secondo cui *“[DENOMINAZIONE INTERMEDIARIO] non ti chiederà mai, contattandoti tramite email o telefono...”*. Anche tale stringa di testo, infatti, non chiarisce il punto essenziale, ossia che la chiamata o l'SMS potrebbero apparentemente provenire, come detto, dal numero genuino dell'Intermediario.

Irrilevante, altresì, il fatto che informazioni più precise e dettagliate siano contenute in altre pagine del sito dell'Intermediario, pure se accessibili tramite *link* cui rinvia lo stesso alert, (*“per maggiori*

informazioni consulta...): non vi è, infatti, prova che il cliente le abbia effettivamente consultate, o che debba consultarle prima di procedere ad autorizzare l'operazione.

In conclusione, la formulazione attuale dell'avviso, pur costituendo un avvio di buona pratica da seguire, è, ad oggi, idonea a integrare, al più, la colpa del cliente, ma non anche la colpa grave richiesta dalla legge, la quale presuppone, per definizione, una negligenza inescusabile.

Per integrare, di contro, la colpa grave del cliente, l'avviso dovrebbe essere corretto già nella sua intestazione (e.g., *"hai ricevuto una email, un SMS o una telefonata, anche apparentemente provenienti dalla Banca, che ti chiedono..."*).

VII. In ragione di quanto sopra, può ritenersi dimostrata la semplice colpa lieve del cliente, ma non anche la colpa grave. Ne consegue che la domanda, visto l'art. 10 del d.lgs. 11/2010, deve essere integralmente accolta.

VIII. Ogni altra domanda o eccezione rigettata.

PER QUESTI MOTIVI

In accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 19.450,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE