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 07/03/2025

FATTO

1. La presente controversia ha ad oggetto sei operazioni, eseguite tra il 24 e il 26 luglio 2024, per complessivi € 96.050,00. Si tratta, in particolare, delle seguenti operazioni, tutte disconosciute dal Ricorrente:

n.	data/ora	descrizione operazione	importi
1	24/07/2024 12:22	bonifico	30.000,00 €
2	25/07/2024 15:06	bonifico	19.000,00 €
3	26/07/2024 12:31	bonifico istantaneo	14.900,00 €
4	26/07/2024 12:53	bonifico istantaneo	14.850,00 €
5	26/07/2024 13:38	bonifico istantaneo	14.950,00 €
6	26/07/2024 15:14	bonifico istantaneo	2.350,00 €
			96.050,00 €

In particolare, il Ricorrente (in avanti, *brevius*, anche: "Parte ricorrente"), il 31 luglio 2024, alle ore 15:09, proponeva denuncia orale presso una stazione dei Carabinieri, esponendo di essere stato contattato, lo stesso giorno, dall'Intermediario (presso il quale intratteneva un conto), che lo invitava a recarsi presso la filiale. Giunto in filiale, aveva appreso che il proprio conto era stato bloccato per sospetta frode, dal momento che risultavano le sei operazioni di bonifico istantaneo sopra descritte, tutte effettuate tra il 24 e il 26 luglio, per complessivi € 96.050,00. A domanda dell'Ufficiale verbalizzante, rispondeva: *"A.D.R. non ho mai dato le credenziale di accesso al mio conto a nessuno, compreso i miei familiari: A.D.R. non ho mai smarrito documenti a me intestati; A.D.R. non ho mai pubblicato su social networks dati sensibili ricollegabili al mio conto corrente; A.D.R. non ho mai ricevuto mail di phishing o quant'altro; A.D.R. non ho ricevuto sul mio telefono comunicazioni in ordine a tali operazioni fraudolente, premesso che invece normalmente ogni operazione mi viene comunicata mediante mail; A.D.R. allego alla presente copia della lista movimenti che indicano le operazioni fraudolente".*

Il Ricorrente dichiara, a questo punto, di avere ricostruito meglio, nei giorni successivi, la vicenda. Il 13 settembre 2024, pertanto, inoltrava formale reclamo all'Intermediario, aggiungendo che, il 1° giugno 2024 (ossia, cinquantatré giorni prima delle operazioni contestate) era stato contattato telefonicamente da un sedicente operatore dell'Intermediario, il quale gli aveva chiesto di effettuare talune operazioni per "*implementare le dotazioni di sicurezza associate al rapporto".* Riferisce di avere chiuso la telefonata e di avere contattato il numero verde dell'Intermediario (800xxx4) "*per richiedere conferma delle legittimità delle operazioni richieste, che fu ribadita dall'operatore".* Il Ricorrente, quindi, afferma di "*aver effettuato le operazioni richieste dal proprio notebook a seguito di un successivo appuntamento telefonato concordato per il 4 giugno 2024, nel corso del quale peraltro non ha mai comunicato la propria password".* Chiedeva, pertanto, il rimborso delle somme.

L'Intermediario riscontrava il reclamo con lettera datata 25 settembre 2024, nella quale affermava la legittimità delle operazioni e, per converso, la colpa grave del cliente. Escludeva, peraltro, "*precisamente*" di avere mai rassicurato il Ricorrente circa la "*conferma delle legittimità delle operazioni richieste*".

Dopo pochi giorni, e precisamente il 30 settembre 2024, l'Intermediario scriveva nuovamente al Ricorrente, affermando che nessuna chiamata, proveniente dal numero registrato del cliente, era mai stata effettuata al numero verde dello stesso Intermediario, nel periodo compreso tra il 1° gennaio 2024 e il 27 settembre 2024.

2. Insoddisfatta dell'interlocuzione avuta in sede di reclamo, Parte Ricorrente adiva questo Arbitro Bancario Finanziario ribadendo la ricostruzione dei fatti prospettata nel reclamo, e chiedendo: *"Per i motivi sopra esposti si ribadisce la richiesta di restituzione di quanto ingiustamente sottratto (…), ossia dell'importo di euro 96.050,00".* Aggiungeva inoltre che tutte le operazioni in questione risultavano effettuate da un dispositivo abusivamente associato al proprio conto.

3. Si costituiva l'Intermediario, evidenziando alcune asserite incongruenze nella prospettazione di Parte ricorrente ed eccependo, comunque, che sia l'associazione del dispositivo (avvenuta il 4 giugno 2024) che le operazioni disconosciute (eseguite tra il 24 e il 26 luglio 2024) erano state eseguite nel rispetto delle norme previste, con diligenza dell'Intermediario medesimo e, per converso, con colpa grave dello stesso Ricorrente. Il dispositivo "abusivo", peraltro, sembrava coincidere con quello indicato nel ricorso come autentico dal cliente. Ribadiva, ancora, l'inesistenza delle asserite chiamate al numero verde dell'Intermediario e aggiungeva, infine, di essersi attivato immediatamente per tentare il recupero delle somme, "*purtroppo con esito negativo".* Chiedeva, pertanto: *"Per i motivi tutti sopra esposti, alla luce delle considerazioni da noi svolte e della*

documentazione prodottavi, vi chiediamo di voler rigettare il ricorso per l'assoluta assenza di responsabilità in capo alla Banca e che nulla venga riconosciuto, pertanto, al ricorrente in termini di rimborso e/o risarcimento".

4. I Ricorrenti depositavano repliche, ribadendo la ricostruzione sopra indicata delle tre telefonate al numero verde e delle rassicurazioni ricevute dall'Intermediario, e indicando, come prova, i tabulati telefonici prodotti in un uno al ricorso. Quanto all'apparente incongruenza circa il nome dei dispositivi, osservava che – per caso o *pour cause* – i nomi indicati dei due dispositivi erano idonei a ingenerare confusione. Tuttavia, il dispositivo *autentico* del ricorrente era quello indicato con la denominazione "*i(…)",* mentre quello abusivamente associato e utilizzato dai truffatori era denominato "*8(…)".* Ciò, del resto, si evinceva dal differente sistema operativo utilizzato (indicato anche nei *log* informatici prodotti dall'Intermediario). Negava, sotto altro profilo, di avere mai fornito le proprie credenziali ai truffatori, come pure di avere mai ricevuto qualsivoglia messaggio che lo avvisasse dell'avvenuto *enrollment* del secondo dispositivo "8(…)". Evidenziava, infine, il carattere sospetto delle operazioni, che avevano svuotato il conto del Ricorrente. Insisteva, pertanto, nell'accoglimento del ricorso.

5. L'Intermediario depositava controrepliche, ribadendo che dai propri registri telefonici non risultava alcuna chiamata al numero verde, proveniente dal Ricorrente. Incorporava, a tal fine, nelle controrepliche un tabulato, consistente nell'interrogazione a una *query* al proprio *database,* il quale evidenziava che, nel periodo compreso tra il 1° aprile 2024 e 30 settembre 2024, nessuna telefonata risultava essere stata effettuata dal Ricorrente. Si riportava, per tutto quant'altro, alle controdeduzioni e insisteva per il rigetto del ricorso.

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 il 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 fosse stata fornita dall'Intermediario, procedere all'accertamento dell'eventuale colpa grave del cliente; all'esito, qualora fosse dimostrata la predetta colpa grave, procedere all'accertamento di un eventuale concorso di colpa dell'Intermediario.

III. Sotto il primo profilo, la SCA risulta provata, sia con riferimento all'operazione di *enrollment* del dispositivo "8(…)", che con riguardo alle singole operazioni dispositive, da questo dispositivo eseguite.

III.1. L'Intermediario ha, infatti, prodotto i *log* informatici delle operazioni. Siffatti documenti vanno inquadrati tra le riproduzioni informatiche, compiutamente disciplinate dall'art. 2712 c.c. Ai sensi di tale disposizione, le riproduzioni con mezzi (anche) informatici fanno piena prova dei fatti e delle cose rappresentate, qualora la controparte non ne disconosca la conformità ai fatti o alle cose medesime (cfr., *ex plurimis*, Collegio Palermo, 30 luglio 2024, n. 9039).

Circa le modalità del disconoscimento, questo deve essere *"chiaro, circostanziato ed esplicito, dovendosi concretizzare nell'allegazione di elementi attestanti la non corrispondenza tra realtà fattuale e realtà riprodotta"* (Cass. 13/05/2021, n. 12794; conf., *ex plurimis:* Corte appello sez. lav. - Firenze, 11/11/2021, n. 600; Corte appello sez. lav. - Catanzaro, 05/01/2023, n. 2; Corte appello sez. IX - Napoli, 17/01/2023, n. 183).

Nel caso di specie, le riproduzioni non sono state disconosciute in modo specifico dal Ricorrente, sicché fanno piena prova dei fatti e delle cose rappresentate, giusta il combinato disposto dell'art. 2712 c.c. e dell'art. 2719 c.c. È, del pari, irrilevante che i *log* siano stati prodotti in "pdf", dal momento che ciò non incide sulla loro natura di riproduzione (*rectius*: di copia della riproduzione), soggetta al combinato disposto degli artt. 2712 e 2719 citati.

Del resto, non sarebbe ragionevole né conforme a diritto pretendere la produzione dei *log* in codice sorgente, in codice binario o in linguaggio macchine: qualunque documento informatico è, infatti, una sequenza di bit che, per essere resa leggibile all'essere umano, deve necessariamente essere convertita, attraverso *l'output* della macchina, in una stringa di testo che abbia un significato comprensibile. La produzione dei codici sorgente, in linea teorica, potrebbe essere necessaria se, in un procedimento davanti al giudice ordinario (ma non in ABF, v. *infra*), fosse mossa una specifica contestazione di tipo informatico, *e.g.*: concernente il vero e proprio flusso di dati, in ipotesi erroneamente interpretato dal *software* che genera *l'output*. Ma fuori da tale ipotesi, un qualunque documento informatico, come un documento di testo redatto al computer (ma lo stesso vale per una *chat* di un comune sistema di Instant Messaging, per un file audio, per un file contenente un'immagine, *etc.*), può sicuramente essere prodotto, appunto, in un formato immediatamente leggibile all'essere umano (file di testo, foglio elettronico, ecc.) senza che, per tale motivo, possa essere considerato una prova inadeguata sul piano tecnico e giuridico.

In conclusione, ritiene questo Collegio che i *log* informatici (accompagnati da idonea legenda), resi sotto forma di foglio di calcolo o, come nel caso di specie, in pdf, siano ad ogni effetto una riproduzione con mezzi informatici, dal momento che descrivono una sequenza di eventi, registrati dalla macchina, e rappresentati, attraverso un codice alfanumerico, in un linguaggio comprensibile dall'utente e dalle parti nel procedimento.

Vale la pena aggiungere che, anche qualora le riproduzioni in parola fossero state correttamente disconosciute, esse avrebbero potuto comunque essere valutate dal Collegio. Invero, il "*disconoscimento*" previsto dall'art. 2712 c.c. si limita a degradare la riproduzione al rango di *prova semplice,* consentendone comunque la verifica con ogni mezzo, ivi comprese le presunzioni (Cass. 29/04/2022, n. 13519). Ciò vale, a maggior ragione, nel procedimento in ABF, "*la cui istruttoria è circoscritta a quanto in forma documentale versato in atti dalle parti del giudizio a norma del vigente regolamento"* (*ex plurimis,* v. Collegio Napoli, n. 4821 del 22 marzo 2022; Collegio Milano, n. 5041 del 24 marzo 2022; Collegio Roma, n. 17582/2017; v. anche Collegio Napoli, 9144/2019; Collegio Bologna, n. 1308/202). Risulterebbe, pertanto, incompatibile con il procedimento dinanzi

all'Arbitro Bancario Finanziario la *verifica* di una riproduzione disconosciuta, attraverso consulenza tecnica o prove testimoniali, dal momento che tali mezzi istruttori non possono trovare ingresso nel relativo procedimento.
A giudizio del Collegio, in conclusione, i *log* informatici prodotti dall'Intermediario, se non disconosciuti in modo *"chiaro, circostanziato e specifico"*, fanno piena prova dei fatti rappresentati. Se correttamente disconosciuti, invece, sono comunque utilizzabili nel procedimento in ABF come *prova semplice,* salva ovviamente la possibilità per la controparte di fornire la prova contraria (cfr., *ex plurimis,* Collegio Palermo, 30 luglio 2024, n. 9039; Collegio Palermo 3343/2024 e 3437/2024; la prova contraria, peraltro, è nel caso di specie assente).
III.2. Tanto premesso, i *log* informatici attestano che *l'enrollment* del dispositivo "8(…)" avvenne con la seguente modalità (all. 1 e all. 2 alle controdeduzioni). In data 4/06/2024 alle ore 14.33 fu eseguito il *login* dal nuovo dispositivo mobile. L'accesso fu autorizzato mediante inserimento all'interno dell'App ufficiale di *Codice Utente, Data importante* e *Pin Dispositivo.* Il combinato utilizzo dei tre fattori integra sicuramente un fattore di conoscenza.
Quindi, alle ore 14:34, fu eseguito il vero e proprio *enrollment*, ossia l'associazione del nuovo dispositivo *"8(…)" all'homebanking* del Ricorrente. Tale operazione fu autorizzata con tramite *SecureCall*, ossia da una chiamata effettuata dal numero certificato dell'Intermediario a quello del Ricorrente (peraltro coincidente con quello indicato nella produzione dello stesso Ricorrente). All'esito della chiamata, il cliente digitava il proprio PIN (v. all.1 controdeduzioni, pag. 1, colonna 2: "*operation description… enrollment OK"; "tipo sca… SecureCall"; "inserimento_Codice_Pin…SI").*
III.3. Circa l'idoneità del sistema *SecureCall* va premesso che, in campo di truffe informatiche, nessun sistema di sicurezza può considerarsi definitivamente affidabile e che un sistema, oggi pacificamente considerato *compliant* dai Collegi, potrebbe dopo pochi mesi rivelarsi vulnerabile a un particolare tipo di attacco. In linea generale, il sistema *SecureCall*, in tutte e due le varianti utilizzate (chiamata da cliente a *SecureCall*, ovvero da *SecureCall* a cliente), andrebbe utilizzato con molta cautela da parte degli Intermediari, e solo all'esito effettive verifiche di sicurezza, dal momento che parrebbe, sul piano tecnico, vulnerabile a tecniche di *spoofing* (su cui, diffusamente, *infra,* a proposito della colpa grave). In particolare, in linea teorica, truffatori potrebbero *spoofare* il numero del cliente per chiamare il *SecureCall* e autorizzare un'operazione abusiva (situazione già riscontrata dai Collegi: cfr. Collegio Torino, 24 aprile 2024, n. 4920); ma potrebbero anche, salvo che l'Intermediario fornisca prova contraria, *spoofare* il numero *SecureCall* per chiamare il cliente al suo numero autentico e farsi comunicare in modo fraudolento il PIN).
III.4. Nel caso di specie, tuttavia, non risulta che tali evenienze si siano verificate. Non è, infatti, contestato che la chiamata *SecureCall* del 4 giugno 2024 provenisse davvero dall'Intermediario (anzi, come visto, la circostanza è provata ai sensi dell'art. 2712 c.c.); pertanto, con specifico riferimento al caso concreto, comprensivo di tutti i suoi elementi di fatto, il sistema deve essere considerato *compliant* con riferimento al fattore del possesso. La digitazione del PIN da parte del cliente, avvenuta sia all'esito della telefonata *SecureCall* che, soprattutto, nella immediatamente precedente fase di accesso, (circostanza che, secondo i Collegi, rende cumulabili i fattori utilizzati), realizza, invece, un valido fattore di conoscenza. In conclusione, l'operazione di *enrollment* può considerarsi autorizzata da due fattori indipendenti di possesso (chiamata da *SecureCall* a cliente) e conoscenza (username e PIN digitati in fase di accesso, oltre alla nuova digitazione del PIN all'esito della chiamata *SecureCall*: in senso conforme, v. Collegio Torino, 13101/2024; Collegio Bologna, 12329/2024; Collegio Milano, n. 333/2025).

Va peraltro sin d'ora avvertito, ma sul punto si tornerà sotto il profilo della colpa grave, che l'operazione fu seguita da un SMS di conferma dell'avvenuta operazione, inviato al cellulare autentico del cliente *"i(…)"* alle 14:34:09.

III.5. A questo punto, chiunque avesse effettuato *l'enrollment* del dispositivo *"8(…)"* non ne approfittò immediatamente per aggredire il conto del Ricorrente ma rimase inattivo per cinquanta giorni. Le successive operazioni dal dispositivo *"8(…)"* oramai certificato, infatti, furono eseguite tra il 24 e il 26 luglio 2024.

Anche con riguardo ad esse, l'Intermediario ha prodotto *log* informatici non disconosciuti e dunque idonei a fare piena prova ai sensi dell'art. 2712 c.c. Dai predetti tabulati risulta, per ognuna delle operazioni, un *login* via app dal cellulare *"8(…)"* (ormai *enrolled* dal 4 giugno 2024) e la successiva autorizzazione tramite digitazione del PIN, digitato in app. L'allegato alle controdeduzioni "*trace antifrode(…).pdf*", infatti, riporta alla terza, quarta e quinta colonna, rispettivamente, l'avvenuto *login* da dispositivo certificato, la descrizione del tipo di operazione (per ognuna: "*authentication login OK"* e, nella riga immediatamente successiva, *"PIN a video su Mobile"),* nonché, alla sesta colonna, l'avvenuto inserimento del PIN *("inserimento_Codice_Pin*" = "*SI*"). I dati, accompagnati da idonea legenda esplicativa, sono ulteriormente supportati dall'all.1 alle controdeduzioni che descrive nel dettaglio le operazioni.

In conclusione, le operazioni dispositive furono tutte autorizzate da un fattore di possesso (*login* tramite app nel dispositivo precedentemente associato al cliente) e da un elemento di conoscenza (successiva digitazione del PIN), indipendenti tra loro. La prova della SCA deve, pertanto, ritenersi raggiunta.

IV. Si passa, a questo punto, all'esame della colpa grave del cliente.

IV.1. 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), però, 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 effettivamente utilizzato dall'Intermediario *bersaglio* della truffa. Nello *spoofing*, in altri termini, il messaggio o la telefonata appaiono realmente provenire dal mittente; mentre nel meno insidioso *phishing,* i truffatori si limitano, al massimo, a modificare il campo del "*nome del mittente",* mentre l'indirizzo email (nel caso delle email) o il numero di telefono da cui parte la chiamata o l'SMS 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.

IV.2. Nel caso di specie, l'Intermediario, nelle controdeduzioni, riconduce la vicenda a un possibile caso di *spoofing.* Tuttavia, al di là del fatto che lo *spoofing* viene avanzato come mera ipotesi ("*presumibilmente"),* l'Intermediario stesso non manca di evidenziare la mancata prova dell'apparente provenienza della presunta telefonata truffaldina da parte della stessa Banca. Ha dunque contestato la ricostruzione in fatto.

La presenza o meno della contestazione da parte dell'Intermediario è, in ogni caso, irrilevante. Invero, anche nel processo civile, ove è espressamente sancita la regola di cui all'art. 115 c.p.c. *("Salvi i casi previsti dalla legge, il giudice deve porre a fondamento della decisione (…) i fatti non specificatamente contestati dalla parte costituita"*), il richiamato onere di contestazione specifica riguarda esclusivamente i fatti noti alla controparte e non anche i fatti ad essa ignoti (Cass. 25 gennaio 2022, n. 2223: *"il deducente è comunque*

tenuto a provare il fatto genericamente dedotto e/o non rientrante nella sfera di conoscibilità della controparte anche in assenza di contestazione specifica o generica o di non contestazione da parte di quest'ultima, mentre è tenuto a provare il fatto specificamente dedotto e/o rientrante nella sfera di conoscibilità della controparte soltanto se specificamente contestato"; conf. Cass. 2476/2013). La stessa regola deve ritenersi applicabile, nei medesimi limiti, al procedimento in ABF: non esiste un onere per la parte di contestare specificamente fatti, non rientranti nella propria sfera di conoscibilità, affermati dalla controparte.

Tanto premesso, nella dinamica dello *spoofing,* (come anche del *phishing)*, i fatti relativi alla prima fase della truffa, proprio perché verificatisi in un momento anteriore all'accesso del cliente alla piattaforma dell'Intermediario (che non sa nulla di quanto sta accadendo in quel momento al cliente), non sono normalmente da questi conosciuti né conoscibili senza la collaborazione del cliente. Conseguentemente, essi non devono essere specificamente contestati, per come sopra chiarito. Correlativamente, secondo l'orientamento dei Collegi, indipendentemente dall'avvenuta contestazione, l'utente che affermi di essere stato vittima di un caso di *spoofing* – fattispecie potenzialmente idonea, come detto, ad escludere sua colpa grave – ha l'onere di fornire evidenza della telefonata, *e.g.,* producendo lo *screenshot* del dispositivo (o dell' SMS o copia dell'email); e ciò al fine di consentire all'Intermediario e al Collegio di verificare l'effettiva idoneità del messaggio o della chiamata ad indurre in errore l'utente medio (numero di telefono o indirizzo email effettivamente riconducibile all'intermediario, presenza di errori di ortografia nell'eventuale messaggio, ecc.). In mancanza di tale produzione, la truffa non può essere considerata *spoofing,* ma semplice *phishing;* sicché va affermata la colpa grave dell'utente (Collegio Palermo, 24607/2021; Collegio Palermo, 22903/2021; Collegio Milano, 12195/2022). Va, al riguardo, ulteriormente evidenziato che le lacune assertive e probatorie afferenti alla fase iniziale della truffa (ricezione della telefonata, dell'SMS o dell'email *civetta,* indirizzo del link truffaldino) sono particolarmente lesive del diritto alla difesa dell'Intermediario, considerato che il combinato disposto degli artt. 7 comma 2 e 10 comma 2 del d.lgs. 11/2010 pone su questo l'onere di provare la colpa grave dell'utente nella violazione dell'obbligo di adottare *"tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate".* Per potere esercitare il proprio diritto alla difesa, dunque, l'Intermediario deve essere posto nella condizione di conoscere il dettaglio della prima fase della truffa.

Nel caso di specie, la presunta telefonata *spoof* non è dimostrata. Infatti, il Ricorrente, anche se dimostra di avere chiesto al gestore telefonico i tabulati relativi al traffico in entrata e che questo fu rifiutato dallo stesso, non produce neanche uno *screenshot* che dimostri l'esistenza della presunta telefonata del 1° giugno 2024, né, a maggior ragione, la provenienza della chiamata da un numero apparentemente riferibile all'Intermediario.

Sono, al riguardo, inconducenti i tabulati telefonici prodotti dal Ricorrente (all. 6, 7 e 8 al Ricorso). È vero, infatti, che essi non sono stati disconosciuti dall'Intermediario, sicché fanno piena prova ai sensi dell'art. 2712 c.c. dell'esistenza delle tre telefonate al numero verde dello stesso Intermediario. Ed è altresì vero che il medesimo valore di prova privilegiata non riveste, di contro, il tabulato addotto come controprova dall'Intermediario. Il documento in questione, infatti, è stato prodotto solamente in sede di controrepliche: in una fase in cui, non esistendo in rito un termine per ulteriori contro-controrepliche da parte del Ricorrente, non può sussistere un neppure un onere di disconoscimento *ex* art. 2712 c.c. da parte di questo.

Se è vero, però, che i tabulati prodotti dal Ricorrente provano l'esistenza di tre telefonate da questi effettuate al numero verde (1/06/2024, 08.36.08, durata 68 secondi; 1/06/2024, 09.27.46, durata 139 secondi; 1/06/2024 12.48.34, durata 846 secondi: dunque, circa 14

minuti), essi non formano alcuna prova in ordine al contenuto delle stesse conversazioni, né, a ben vedere, in ordine alla stessa attinenza delle tre telefonate con la truffa, per come descritta nel Ricorso. Per converso, del resto, l'Intermediario, già in sede di primo riscontro al reclamo oltre che in sede di controdeduzioni, ha negato *"recisamente"* di avere garantito la legittimità della procedura; circostanza, peraltro, assai verosimile, considerata l'enorme diffusione delle truffe *online*, assai frequentemente eseguite con tecniche di *spoofing-phishing.*

Analogamente, l'Intermediario ha documentato (all. 3, 4 e 5 controdeduzioni) di avere avviato una campagna antifrode, ove si avvertono i clienti dei possibili rischi legati alle fattispecie di *phishing-spoofing.*

IV.3. L'insieme delle superiori circostanze impedisce a questo Collegio di ritenere accertato il fatto come prospettato nel ricorso. Nel procedimento in ABF, infatti, l'istruttoria "*è circoscritta a quanto in forma documentale versato in atti dalle parti del giudizio a norma del vigente regolamento"* (*ex plurimis,* v. Collegio Napoli, n. 4821 del 22 marzo 2022; Collegio Milano, n. 5041 del 24 marzo 2022; Collegio Roma, n. 17582/2017; v. anche Collegio Napoli, 9144/2019). Ne consegue che, qualora un determinato fatto primario o secondario risulti contestato dalle parti e non possa essere ricavato, neanche per presunzioni, dalle prove documentali in atti, il Collegio deve necessariamente ritenerlo non provato. L'accertamento del fatto *de quo,* infatti, dovrebbe essere condotto attraverso l'assunzione di una prova testimoniale; mezzo istruttorio che potrà, ovviamente, essere richiesto dal Ricorrente davanti al giudice ordinario, ma che non può, per sua stessa natura, trovare ingresso nel procedimento dinanzi all'Arbitro Bancario Finanziario.

IV.4. Si aggiunga, infine, che l'Intermediario ha documentato, come anticipato, l'invio in data 4 giugno 2024 (e la contestuale consegna al gestore telefonico del Ricorrente) di un SMS c.d. "parlante" al dispositivo "*i(…)"* (autentico), all'esito della procedura di *enrollment* del dispositivo *civetta "8(…)".* Il testo del messaggio, incorporato nelle controdeduzioni (pag. 2), è: *"** ATTENZIONE** HAI AUTORIZZATO UN NUOVO DISPOSITIVO AD OPERARE SUI TUOI SERVIZI APP E HOME BANKING, L'IDENTIFICATIVO DEL DISPOSITIVO E': i(…)".* Anche tale riproduzione non è stata disconosciuta dal Ricorrente, e pertanto forma piena prova dei fatti rappresentati.

È, sul punto, irrilevante che il Ricorrente, nelle repliche, abbia negato di avere ricevuto il messaggio *"in considerazione della probabile intromissione dei truffatori nei sistemi di comunicazione della banca".* Invero, la contestazione del fatto registrato da una riproduzione *ex* art. 2712 c.c. non soddisfa i requisiti del disconoscimento imposto dalla stessa norma (*ex plurimis*, Cass. 23 aprile 2018, n.9977). Deve, dunque, ritenersi provato che il messaggio fu inviato dall'Intermediario al gestore telefonico del Ricorrente.

La dimostrazione, poi, dell'avvenuta consegna al gestore, sebbene non provi pienamente anche l'effettiva consegna del messaggio dal gestore al cliente, è senz'altro un elemento sufficiente a fondare un ragionamento di tipo presuntivo. Naturalmente, non di presunzione assoluta si tratta, ma di una presunzione semplice; il cliente, però, che, a fronte della prova dell'invio e della consegna al gestore telefonico del destinatario di un SMS, affermi di non averlo ricevuto, ha l'onere di fornire elementi idonei, ancorché pure essi in solo via presuntiva, a far dubitare del contrario (*e.g.*: istantanea del dispositivo, dal quale si evincano gli SMS ricevuti in quella data, *etc.*). In caso contrario, deve ritenersi che il messaggio, consegnato al gestore telefonico, sia stato anche consegnato al cliente.

Nel caso di specie, tale *contro-presunzione* non è stata fornita dal Ricorrente, il quale si è, come visto, limitato ad avanzare la possibilità che il messaggio sia stato intercettato dai truffatori, che avrebbero manomesso i sistemi informatici dell'Intermediario. Tale ricostruzione, però, oltre a non essere supportata da alcun tipo di evidenza (*screenshot* degli SMS ricevuti, *etc.*), non è neanche supportata da una coerente allegazione in punto

di fatto (indizi tipici del c.d. *sim swap,* quali il dedotto malfunzionamento del cellulare del cliente, ecc.). L'SMS parlante, dunque, deve presumersi ricevuto dal Ricorrente, difettando ogni elemento idoneo a ritenere il contrario.

IV.5. Non va infine trascurato che, nel caso di specie, il lasso di tempo intercorso tra l'*enrollment* del dispositivo "8(…)" e le prime operazioni dispositive fu di cinquanta giorni. Si tratta di uno iato temporale, come detto, fortunosamente lungo, dal momento che i truffatori, secondo *l'id quod plerumque accidit,* una volta assunto il controllo dell'*home banking* del cliente, cercano di svuotare immediatamente il suo conto, ad evitare che la truffa possa essere scoperta e interrotta (si noti, al riguardo, che l'estratto conto prodotto dal Ricorrente - all. 3 ricorso – evidenzia, alla data del 30 giugno 2024, un saldo attivo di € 96.498,83). Il lasso di tempo, come detto, fu talmente esteso che il cliente, operando un minimo di diligenza (*e.g.,* semplicemente guardando gli SMS ricevuti, o accedendo alla propria app e visualizzando i dispositivi associati) avrebbe potuto scoprire la prima fase della truffa e inibirne la prosecuzione, nella sua fase propriamente lesiva (bonifici).

V. La presenza della colpa grave del Ricorrente, tuttavia, non esclude la possibilità di una colpa concorrente o esclusiva dell'Intermediario almeno per alcune delle operazioni disconosciute.

In particolare, il Collegio ritiene nella fattispecie dirimente la mancata allegazione e prova, da parte dell'Intermediario, del funzionamento di un servizio di *alert* associato alle operazioni dispositive, ovvero del rifiuto del cliente ad avvalersene.

Sul punto, il Collegio di Coordinamento, con la decisione n. 24366/19, ha affermato che *"[f]ra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene"; (ii) gli effetti della mancata adozione del servizio di sms-alert devono comunque essere valutati alla stregua delle circostanze di fatto del singolo ricorso".*

L'Intermediario, in merito, afferma (peraltro solo in sede di controrepliche) che: *"Quanto al servizio di SMS Alert, la banca offriva a tutta la propria clientela la possibilità di attivare tale servizio; ma era onere dei clienti attivarlo tramite il servizio di banca a distanza, scegliendo la soglia d'importo che attivava il messaggio".* Tale condotta non soddisfa i requisiti minimi di diligenza fissati dal Collegio di Coordinamento, secondo cui – come detto – il servizio deve essere attivato di *default*, salvo rifiuto esplicito del cliente ad avvalersene.

Nel caso di specie, a giudizio di questo Collegio, il corretto funzionamento del sistema di *alert* - peraltro utilizzato, come visto, per il precedente *enrollment* del dispositivo "8(…)" - avrebbe potuto impedire l'esecuzione almeno delle operazioni successive alla prima.

Dalla descrizione dei fatti, invero, risulta che il primo bonifico truffaldino fu eseguito il 24 luglio 2024, alle ore 12:22, mentre il secondo fu eseguito il successivo 25 luglio 2024, alle ore 15:06.

Per la prima operazione, invece, il mancato invio dell'SMS alert è irrilevante. Invero, sebbene in linea di principio il bonifico possa essere revocato dal cliente e, dunque, l'invio di un SMS alert potrebbe impedire anche la prima operazione (Collegio Palermo, 5 giugno 2023, n. 5628), ciò non è accaduto nel caso di specie. Invero, dai *log* prodotti dall'Intermediario (all. 1 controdeduzioni, come detto non disconosciuto) risulta che il primo bonifico aveva data di esecuzione "24/7/2024": ossia una data pari a quella dell'inserimento. Sul punto, l'art. 17 del d.lgs. 11/2010 sancisce la generale irrevocabilità di un ordine di pagamento con addebito diretto (quale è il bonifico) *"oltre la fine della giornata operativa precedente il giorno concordato per l'addebito dei fondi"* (comma 3); regola confermata dall'art. 12 del contratto (all.2 del Ricorrente, sezione III, relativa ai servizi di pagamento). Oltre tale data non si potrà più "revocare" unilateralmente il pagamento, ma

solo chiedere il "recall", procedura che, salvo differenti pattuizioni contrattuali, richiede necessariamente il consenso del beneficiario alla restituzione. L'eventuale invio dell'*SMS alert,* pertanto, non avrebbe potuto impedire l'esecuzione del primo bonifico del 24 luglio 2024, mentre avrebbe potuto impedire l'esecuzione dei successivi.

VI. Va poi evidenziato il carattere *sospetto* dell'intera sequenza truffaldina, che comportò il pressoché totale azzeramento del conto nell'arco di tre giorni, attraverso cinque bonifici dalle causali spesso improbabili, molte delle quali indirizzate verso il medesimo beneficiario, persona fisica (ad eccezione della seconda operazione, di € 19.000,00 e che ha causale "*lavori di ristrutturazione casa vacanza*", tutte le altre sono dirette al medesimo beneficiario e indicano, con leggere differenze, la causale: "*estinzione mutuo*"). Come correttamente dedotto dal Ricorrente, la pluralità di bonifici di rilevante importo a distanza temporale ravvicinata, rappresenta una movimentazione assolutamente anomala rispetto alla normale operatività del conto corrente, assai modesta (cfr. all. 3 ricorso, contenente la movimentazione del conto tra il 1/07/2024 e il 31/7/2024).

Sul punto, il DM 30 aprile 2007, n. 112, *Regolamento di attuazione della legge 17 agosto 2005, n. 166, recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento"* all'art. 8, individua il "Rischio di frode" quando viene raggiunto uno dei parametri ivi indicati.

Sebbene il DM 112/2007 non abbia un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate, esso costituisce comunque espressione di un generale obbligo di monitoraggio delle operazioni, da valorizzare per valutare la condotta dell'intermediario. Tanto più che la logica ispiratrice dell'intera disciplina in materia di pagamenti elettronici è proprio di garantire il cliente, onerando l'Intermediario di adottare particolari cautele e accorgimenti tecnici per prevenire frodi.

Da ciò discende che, secondo gli orientamenti condivisi dai Collegi, il carattere sospetto di una sequenza di operazioni può essere ravvisato anche al di fuori dei limiti di cui al citato DM, ossia: per operazioni diverse da quelle eseguite su *carte,* nonché in ipotesi diverse da quelle indicate nel DM.

Nel caso di specie gli elementi sopra indicati avrebbero dovuto indurre l'Intermediario ad adottare cautele ulteriori; *e.g.:* chiedere un'ulteriore verifica al primo numero registrato o all'indirizzo email originariamente associato al cliente. Il mancato assolvimento a tali obblighi di cautela, se non comporta una responsabilità esclusiva dell'Intermediario, nel caso concreto determina un pur limitato concorso di colpa di questo.

Conformemente, inoltre, alle più recenti determinazioni di questo Collegio, in caso di cumulo tra mancato invio di SMS e indici di frode, il Ricorrente ha diritto a un rimborso pari alla somma integrale di tutte le operazioni eseguite a distanza di oltre 5 minuti dalla prima, e di un'ulteriore somma, quantificabile in misura pari al 20% delle restanti, prime operazioni (Collegio Palermo, 4148 e 4200 del 4 aprile 2024).

In conclusione, va accertato il diritto della Ricorrente al rimborso come da seguente tabella:

n.	data/ora	descrizione operazione	importi	oltre 5 min	operazioni fraudolente	totale rimborsare
1	24/07/2024 12:22	bonifico	30.000,00 €		6.000,00 €	6.000,00 €
2	25/07/2024 15:06	bonifico	19.000,00 €	19.000,00 €		19.000,00 €
3	26/07/2024 12:31	bonifico istantaneo	14.900,00 €	14.900,00 €		14.900,00 €
4	26/07/2024 12:53	bonifico istantaneo	14.850,00 €	14.850,00 €		14.850,00 €

5	26/07/2024 13:38	bonifico istantaneo	14.950,00 €	14.950,00 €		14.950,00 €
6	26/07/2024 15:14	bonifico istantaneo	2.350,00 €	2.350,00 €		2.350,00 €
			96.050,00 €	66.050,00 €	*6.000,00 €*	***72.050,00 €***

Per un totale, così, di € 72.050,00
VII. Ogni altra domanda ed eccezione assorbita.

PER QUESTI MOTIVI

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 72.050,00.
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

Firmato digitalmente da
MARIA ROSARIA MAUGERI