

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MEZZACAPO	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore COSIMO DAMIANO FABIO MASTROROSA

Seduta del 30/04/2026

FATTO

Parte ricorrente ha adito questo Arbitro al fine di chiedere la condanna dell'intermediario al pagamento della somma di euro 9.960,00

In particolare ha dedotto di aver ricevuto un SMS e una telefonata apparentemente provenienti dalla banca, con segnalazione di anomalie e bonifici dall'estero. In stato di forte stress, veniva indotta a disporre ricariche, pagamenti e tre bonifici.

A fronte di un rimborso parziale, agisce per la restituzione delle somme e per il risarcimento dei danni, anche non patrimoniali.

Dall'atto introduttivo e dalla denuncia emerge la seguente ricostruzione in fatto.

Dalla denuncia versata in atti, emerge che il giorno 11/12/2024 alle ore 12,51 la ricorrente riceveva un messaggio dal servizio clienti della banca, con il quale veniva informata che sarebbe stata contattata da un operatore, in quanto si erano verificate alcune anomalie sulla sua carta.

Dopo pochi minuti riceveva una telefonata proveniente dal numero riconducibile alla suddetta banca, con cui un sedicente operatore allertava la ricorrente per alcuni bonifici effettuati poco prima dall'estero. Constatata la veridicità delle affermazioni, la ricorrente, in preda al panico e allo stress, veniva dapprima indotta ad effettuare tre ricariche di euro 1.000,00, 1.000,00 e 9.500,00 da un conto tenuto presso la banca beta a favore della carta prepagata emessa dall'odierna resistente;

Successivamente, veniva indotta a recarsi presso un punto vendita di un esercente con un taxi chiamato dal truffatore.

Una volta giunta a destinazione, parte ricorrente effettuava alcuni pagamenti, nell'erroneo presupposto di mettere in sicurezza i suoi risparmi, anche a seguito di una chiamata asseritamente proveniente dai Carabinieri.

A seguito del rimborso parziale, parte ricorrente agisce per "il rimborso delle somme prelevate illecitamente dal c/c [e] il risarcimento dei danni patiti anche di natura non patrimoniale".

Conclude il ricorso si chiedendo la restituzione della somma di euro 9.960,00, pari ai tre bonifici non autorizzati.

Nelle controdeduzioni l'intermediario afferma quanto segue.

In via preliminare eccepisce l'inammissibilità del ricorso per la genericità e per la scarsa chiarezza della richiesta: la ricorrente, infatti, nella parte "oggetto della controversia" fornisce una descrizione del tutto generica dei fatti, menzionando alcune operazioni senza indicarne né l'ammontare né il rapporto sul quale sarebbero state effettuate.

Inoltre, non distingue le richieste formulate nei confronti della banca Beta da quelle formulate nei confronti dell'intermediario odierno resistente, il quale, con riferimento alle operazioni effettuate a valere sulla carta rilasciata dalla banca Beta, pertanto, eccepisce la carenza di legittimazione passiva. Alla luce di quanto sopra, la resistente limita le sue osservazioni:

1. al bonifico istantaneo di euro 155,00, di cui la Cliente è stata prontamente informata dalla Società a mezzo e-mail delle ore 13:07;
2. al bonifico istantaneo di euro 1.800,00, di cui la Cliente è stata prontamente informata dalla Società a mezzo e-mail delle ore 13:24;
3. al pagamento e-commerce di euro 195,00;
4. al bonifico ordinario di euro 8.000,00, di cui la Cliente è stata prontamente informata dalla Società a mezzo e-mail delle ore 13:50.

Con riferimento a dette transazioni, autorizzate dalla stessa ricorrente, la banca evidenzia che alle ore 13:02:47, sono stati inseriti username e password corrette (credenziali che solo la Ricorrente poteva e doveva conoscere) per accedere alla sua area personale.

La piattaforma rilevava però che l'accesso era stato eseguito da un dispositivo non certificato in precedenza. Pertanto, veniva inviato alle ore 13:02:48, via sms al numero certificato della cliente, l'OTP necessario a proseguire il processo di certificazione 6 del "nuovo" dispositivo.

Il messaggio ricevuto sul numero della ricorrente avvisava chiaramente che il codice serviva per certificare un nuovo dispositivo, con la precisa indicazione (i) a fare attenzione alle truffe e (ii) a non comunicare il codice a terze persone.

Nonostante tutti gli avvertimenti, la Cliente ha utilizzato il codice. Peraltro, la resistente assume anche di aver prontamente informato la ricorrente, a mezzo e-mail delle ore 13:03, della conclusione con esito positivo della certificazione del nuovo dispositivo.

In punto di colpa grave, sottolinea l'inverosimiglianza della dinamica della frode che avrebbe dovuto allertare la ricorrente, la quale, peraltro, ha ignorato tutti gli sms e le email alert inviatele.

Con riguardo alle tre operazioni di bonifico, la banca ha avviato le opportune procedure di richiamo (c.d. recall), che, tuttavia, non hanno sortito effetto.

La recall concernente la transazione di euro 155,00 è al momento sospesa, a fronte del mancato riscontro dell'intermediario del beneficiario, mentre le procedure di richiamo relative alle transazioni di euro 1.800,00 e di euro 8.000,00 sono state rifiutate dagli intermediari dei beneficiari, rispettivamente in data 14 gennaio e 15 gennaio 2025.

In ultimo, quanto alla domanda di risarcimento del danno non patrimoniale, ne deduce l'infondatezza per mancato riscontro probatorio

Parte ricorrente replica quanto segue:

- per quanto riguarda le operazioni eseguite mediante la carta rilasciata dall'intermediario resistente la ricorrente chiede la ripetizione di tutti i trasferimenti effettuati contro la sua volontà il giorno 11/12/24 e precisamente € 157,00+€1.802,00+8.001,00 = € 9.960,00 (somma indicata negli allegati al ricorso);
 - a pag. 6 punto 4.10 ultima riga "Termini e condizioni carta" allegati da controparte risulta espressamente che "nel caso in cui si venisse a conoscenza di sospette o effettive frodi o minacce alla sicurezza relative alla Carta ****, il cliente verrà contattato telefonicamente o via e-mail e la carta potrebbe essere preventivamente bloccata dall'emittente." Da ciò deriva che alla ricorrente non può essere attribuita alcuna colpa nemmeno di semplice leggerezza per aver risposto all'interlocutore truffaldino e che l'intermediario avrebbe dovuto bloccare fin da subito la Carta dopo le prime operazioni eseguite all'estero dal nuovo dispositivo;
 - l'11.12.2024, venivano autorizzate operazioni di euro 195,00, euro 4,99, euro 3,99, euro 3,99, euro 7,99, ed euro 4,99, per l'importo di € 220,95 (poi rimborsato dall'intermediario);
 - la circostanza che il presunto truffatore fosse a conoscenza delle transazioni dalla stessa asseritamente non effettuate, ha «consentito ai malviventi di conquistare con facilità la fiducia della ricorrente la quale, [...] si è vista costretta a dar credito alle incalzanti richieste telefoniche che provenivano proprio dal numero fisso e dal cellulare dell'operatore per non perdere tutti i risparmi di una vita, così come era già avvenuto per i prelievi illeciti già effettuati dall'estero di cui aveva avuto riscontro»;
 - convinta di parlare con un operatore della banca e rassicurata anche dalla telefonata dei Carabinieri, ha dovuto soggiacere alla volontà e alle indicazioni del truffatore comunicando la password. Le successive operazioni non sono state effettuate dalla ricorrente bensì dal truffatore/i quali, con un dispositivo non autenticato erano a conoscenza oltre che del numero telefonico della vittima anche dell'importo di tutti i fondi depositati;
 - nega di aver riferito il codice OTP, non pervenuto in quanto «il telefono della ricorrente era stato clonato»;
 - le operazioni sono del tutto prive del consenso;
 - la banca, a fronte delle richieste dei bonifici istantanei effettuati nello spazio di pochi minuti avrebbe dovuto imporre un blocco automatico o, quantomeno, chiedere una conferma telefonica;
 - le procedure di richiamo effettuate sono state effettuate solo il 13 gennaio 2025 e cioè dopo oltre un mese dagli avvenuti bonifici fraudolenti malgrado la comunicazione della truffa fosse avvenuta la mattina del giorno successivo (12.12.24). Tale inerzia, costituendo colpa grave della resistente, ha compromesso la possibilità di recall per recuperare il denaro sottratto e di una tempestiva identificazione dei malviventi;
 - ha subito anche danni di natura non patrimoniale, come risulta dall'allegato di cui si riserva di chiedere il risarcimento al giudice competente.
- Nelle controrepliche la banca deduce quanto segue.
- È solo con le repliche che la Cliente chiarisce quali sono le transazioni di cui pretende il rimborso, ossia i tre bonifici di euro 155,00 (oltre a euro 2 di commissioni), euro 1.800,00 (oltre a euro 2 di commissioni) ed euro 8.000,00 (oltre a euro 1 di commissioni).
Ne deriva, peraltro, che la pretesa di rimborso del pagamento e-commerce di euro 195,00 è da ritenersi espressamente rinunciata.
 - Le cinque operazioni on line predisposte prima dei bonifici (e restituite) non sono bonifici eseguiti «dal dispositivo alieno» (cfr. repliche p. 2 e 5), bensì, pagamenti disposti su sito internet e autorizzati mediante l'inserimento sul sito del PAN e del CVV della carta prepagata,
Non vi sono state, quindi, falle nei sistemi di sicurezza adottati dalla Società, ma la ricorrente ha fornito al presunto truffatore le predette credenziali di sicurezza. Come si è già detto nelle controdeduzioni, a seguito del disconoscimento da parte della Cliente di detti pagamenti, la banca ha provveduto ad

avviare la procedura di chargeback, e il circuito VISA ha riconosciuto alla stessa il rimborso delle somme.

- controparte non fornisce la prova di aver subito la clonazione della sim, né denuncia l'accaduto.

DIRITTO

Come espressamente chiarito nelle repliche, parte ricorrente disconosce tre bonifici on line disposti l'11.12.2024, dell'importo di euro 157,00, di euro 1.802,00 e di euro 8.001,00, per un totale di euro 9.960,00.

L'intermediario ha infatti restituito di altre cinque operazioni, riscontrando negativamente la richiesta di rimborso della sesta transazione di euro 195,00.

Tale pagamento non viene però ricompreso nella richiesta specificata nelle repliche, limitata ai soli tre bonifici.

La suddetta precisazione consentirebbe di ritenere superate le eccezioni di genericità della domanda e di difetto di legittimazione passiva, giacché la ricorrente ha delimitato la domanda alle sole operazioni compiute a valere sulla carta dell'odierna resistente.

I bonifici disconosciuti sono stati disposti da un device nuovo certificato.

La certificazione del nuovo dispositivo si è perfezionata a seguito dell'inserimento a sistema di username e password della Ricorrente (fattore di conoscenza) e del codice OTP trasmesso, a mezzo sms, sul numero di cellulare della stessa (fattore di possesso).

Le nuove raccomandazioni formulate dall'EBA nella recentissima Opinion pubblicata nell'aprile 2024 (i) suggeriscono, in occasione della registrazione di un nuovo device, di prevedere uno spazio temporale idoneo prima che il nuovo device sia effettivamente operativo e utilizzabile per eseguire disposizioni;

(ii) sottolineano la necessità di misure di sicurezza aggiuntive, tra cui l'obbligo di integrare il monitoraggio delle transazioni eseguito dal PSP dell'ordinante con lo screening delle operazioni di pagamento ricevute da parte del PSP del beneficiario, finalizzato a individuare schemi di frode sospetti basati, tra l'altro, sull'importo, l'origine, la frequenza di tali operazioni rispetto al profilo del titolare del conto, nonché sull'eventuale deviazione del nome del beneficiario nelle operazioni contro il nome del beneficiario stesso detenuto dal PSP del beneficiario.

Le tre transazioni sono state eseguite per il tramite del nuovo device certificato (fattore di possesso) e previo inserimento della password della Cliente (fattore di conoscenza).

Con riguardo alla modalità della truffa, dalla denuncia versata in atti, emerge che il giorno 11/12/2024 alle ore 12,51 la ricorrente riceveva un messaggio da un numero identificabile come servizio clienti della banca con il quale veniva informata che sarebbe stata contattata da un operatore, essendosi verificate alcune anomalie sulla sua carta.

Quanto all'sms truffaldino, si osserva che:

- 1) il mittente sembra riconducibile alla banca;
- 2) il testo contiene un errore grammaticale ("un anomalia") e il registro linguistico muta tra un messaggio e l'altro;
- 3) risulta seguito da un messaggio genuino della banca, come riscontrabile dai log prodotti

Su questo punto si richiama il Collegio di Roma, decisione n. 6197/24).” Nei casi di spoofing l'Arbitro, per consolidato orientamento, cui il Collegio ritiene nel caso di specie di dare continuità, non ritiene sussistere la colpa grave del cliente, proprio in ragione della peculiare sofisticatezza della frode, a meno che non si riscontrino indici di inattendibilità del messaggio esca, che avrebbero dovuto generare un innalzamento della soglia di attenzione rispetto alla credibilità del contatto, quali ad esempio errori grammaticali o sintattici, accertando in tal caso un concorso di colpa”

Con riferimento alla modalità della truffa, parte ricorrente dichiara di aver ricevuto una telefonata proveniente dal numero riconducibile al suddetto intermediario, con cui un sedicente operatore allertava la ricorrente per alcuni bonifici effettuati poco prima dall'estero.

Quanto alla chiamata truffaldina, si evidenzia che anche il numero riportato in denuncia corrisponde a un'utenza riferibile alla banca odierna resistente, ma non viene prodotta la lista chiamate.

Nella riunione del 18 febbraio 2026, il Collegio ha deliberato di chiedere alla parte ricorrente la produzione di copia delle schermate relative al registro chiamate del giorno della truffa.

In riscontro, parte ricorrente ha prodotto delle schermate, in cui accanto al contatto truffaldino (denominato "Sospetto Spam"), compare un punto esclamativo e un segnale di alert.

Produce altresì una schermata riportante un'utenza privata.

Occorre valutare se la fattispecie sia riconducibile al vishing callerId spoofing - una frode insidiosa al pari dello sms spoofing – oppure rappresenti un semplice vishing.

Valutando gli indici di anomalia, parte ricorrente deduce che l'intermediario avrebbe dovuto intercettare l'anomalia della movimentazione, a motivo del suo profilo storico e della sua invalidità.

Tuttavia stanti le predominanti anomalie nell'exkursus storico operativo come sopra già evidenziate, unitamente alla mancata produzione documentale come richiesta, inducono questo Collegio a decidere come da seguente dispositivo:

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE