Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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 SIMONE MEZZACAPO

Seduta del 30/04/2026

FATTO

1) Con ricorso del 9.08.2025 il ricorrente allega, mediante rinvio a quanto esposto nel pertinente verbale di denuncia orale alla P.G. del 13.07.2025 e relativa integrazione del giorno successivo, di essere titolare di un conto corrente radicato presso la banca resistente, e di una carta di debito emessa dalla stessa, e di essere stato vittima, in data 9.07.2025, di una frode telematica nell'ambito della quale ignoti sarebbero riusciti a disporre due operazioni di bonifico non autorizzate con addebito su tale conto, per un importo complessivo di Euro 4.292,00.

In particolare, il ricorrente allega, come appunto esposto nella suddetta denuncia alla P.G., di aver risposto ad una telefonata ricevuta in data 09.07.2025 sul proprio cellulare e proveniente dall'utenza n. ***7, asseritamente corrispondente al numero clienti della resistente, interloquendo così con un sedicente operatore della resistente e dando anche seguito all'invito dello stesso di scaricare e installare sul proprio *smartphone* una non meglio identificata applicazione, denominata "Questionario", necessaria a compilare un questionario per i clienti.

Oltre ad aver riscontrato nei giorni successivi l'impossibilità di accedere all'APP di *home banking*, il ricorrente rappresenta che in data 12.7.2025 sarebbe stato contattato dalla resistente avvedendosi così dell'effettuazione con addebito sul suddetto conto corrente a sé intestato di due bonifici online non autorizzati di Euro 1.300,00 e di Euro 2.992,00, disposti in data 09.07.2025, per un valore complessivo quindi di Euro 4.292,00.

Ciò posto, il ricorrente conclude chiedendo il risarcimento del danno nella misura della perdita subita in conseguenza della truffa allegata, corrispondente al suddetto importo complessivo di Euro 4.292,00 delle due operazioni di pagamento dallo stesso disconosciute.

2) Con proprie controdeduzioni, la banca resistente ha confermato che il ricorrente è titolare del conto corrente n. ***3 presso la stessa radicato, a cui è collegato dal 14.4.2022 il servizio "*Rapporti a*

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

distanza tra Banca e Cliente", c.d. *home banking*, che consente ai clienti di effettuare le operazioni di *inquiry* e dispositive su tutti i conti correnti personali a loro riferibili utilizzando il telefono cellulare o Internet, e sul quale sono stati addebitati i due bonifici disconosciuti dal ricorrente eseguiti in data 09.07.2025.

Al riguardo, la resistente eccepisce che le allegazioni del ricorrente evidenzierebbero che lo stesso sarebbe stato circuito da ignoti frodatori che avrebbero ottenuto i codici di accesso riservati del ricorrente avendoli quest'ultimo inseriti in una pagina "esca" per poi ottenere il download di un'app sconosciuta e l'esecuzione di istruzioni e comandi ricevuti. In particolare, secondo la resistente, le dichiarazioni di natura confessoria ex art. 2735 c.c. riportate in denuncia confermerebbero che il ricorrente abbia risposto ad una telefonata ricevuta in data 9 luglio 2025 da un numero telefonico ***7 tuttavia non riconducibile alla resistente, e abbia assecondato le istruzioni ricevute al telefono da uno sconosciuto sedicente operatore della resistente, cliccando quindi su un *link* sconosciuto ricevuto via messaggio, scaricando e installando così anche un'APP "malevola" denominata "Questionario ***", di cui non è stata però depositata evidenza, rendendo così possibile l'accesso al suo dispositivo da soggetti terzi, ed accorgendosi infine della truffa subita solo il giorno 12 luglio 2025.

Obietta inoltre la resistente l'assenza di allegazioni da parte del ricorrente di qualsivoglia dettaglio utile alla comprensione e qualificazione della frode come tale, in quanto il ricorrente non avrebbe infatti depositato agli atti del ricorso alcuna evidenza del download dell'App esterna scaricata, del registro chiamate in entrata, del link dell'App malevola e così via. Ciò comporterebbe dunque secondo la resistente il necessario rigetto del ricorso a motivo dell'assorbente circostanza dell'omesso adempimento dell'onere della prova ex art. 2697 c.c. posto a carico del ricorrente medesimo dei fatti costitutivi l'asserita frode.

In ogni caso la resistente eccepisce inoltre che l'accesso al suddetto servizio di home banking e la disposizione delle operazioni in questione avviene previa applicazione di una procedura di autenticazione forte (SCA) conforme ai requisiti di cui alla PSD2. Riferisce in particolare la resistente che l'accesso all'home banking via APP richiede l'inserimento di credenziali di sicurezza statiche e di un codice OTP dinamico generato da Mobile Token integrato nell'APP; per la disposizione delle operazioni di pagamento è necessario inserire nuovamente il PIN statico e un ulteriore codice OTP, anch'esso generato da Mobile Token integrato nell'APP. Specifica al riguardo la resistente che anche l'attivazione del Mobile Token avviene previa SCA, essendo al fine necessaria la digitazione delle credenziali di sicurezza statiche e di un codice OTP inviato al cliente. Al riguardo, nel caso di specie non risulterebbe essere stato attivato alcun ulteriore Mobile Token, confermando così secondo la resistente che la disposizione/autorizzazione delle operazioni in questione sarebbe stata effettuata dallo smartphone del ricorrente.

Alla luce di tali evidenze, la resistente eccepisce che in presenza di un sistema valutabile come sicuro, come quello dalla stessa adottato e in assenza di anomalie di sistema, si deve presumere che ci sia stata una negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento.

Al fine di escludere la propria responsabilità, la resistente conferma che dalle verifiche effettuate non sarebbe emerso alcun malfunzionamento o compromissione dei propri sistemi, che le operazioni rilevanti risultano correttamente autenticate, registrate e contabilizzate (così come previsto dall'art. 10 del D. Lgs. n. 11/2010), con le credenziali di sicurezza del ricorrente, come dimostrato nelle evidenze dei LOG prodotti in copia.

Quanto alla condotta tenuta dal ricorrente, la resistente eccepisce che quest'ultimo sarebbe incorso in colpa grave rilevante anche *ex* art. 7, punto 2, del D. Lgs. n. 11/2010 e successive modifiche, evidenziando in particolare che dalle dichiarazioni di natura confessoria rilasciate dal ricorrente stesso si evincerebbe che quest'ultimo sarebbe caduto vittima di una frode perpetrata mediante le, ormai note, tecniche di *phishing* e *vishing* che si realizzano mediante l'invio di un SMS che invita a cliccare su di

un link che dà accesso ad una pagina dove la *vittima* inserisce le proprie credenziali di accesso. In questo modo verrebbero quindi carpite le credenziali stesse - come asseritamente accaduto nel caso in esame - mediante accesso da APP "esterna" e/o l'utente verrebbe guidato all'inserimento di operazioni dispositive o a cedere le credenziali personali ai terzi frodatori.

Con riguardo all'azione di *recall* pure avviata in seguito al disconoscimento delle operazioni da parte del ricorrente, la resistente afferma di aver prontamente avviato, una volta ricevuta conferma del disconoscimento, la relativa procedura di richiamo dei fondi nei confronti della banca corrispondente, senza tuttavia esito positivo.

Conclude pertanto la resistente chiedendo il rigetto del ricorso, ritenendo di aver attuato tutte le misure di sicurezza e prevenzione idonee al fine di tutelare il cliente dal rischio frode, rese tuttavia inefficaci dalla condotta gravemente colposa tenuta dal ricorrente.

3) Nella propria riunione del 13.02.2026, il Collegio nell'esaminare il ricorso ha deliberato di richiedere alla parte ricorrente la produzione di copia delle schermate relative al registro chiamate del giorno dell'allegata truffa, al fine di riscontrare documentalmente l'allegata riconducibilità alla resistente dell'utenza telefonica da cui il ricorrente afferma di essere stato contattato il 9.07.2025.

In riscontro a tale richiesta istruttoria, il ricorrente non ha tuttavia prodotto la lista delle chiamate in entrata e/o in uscita, ma versato piuttosto in atti: *i)* lo *screenshot* di un SMS recante la segnalazione di una chiamata persa dal numero ***7; *ii)* lo *screenshot* di un messaggio, presumibilmente non genuino, ricevuto il giorno precedente la truffa, recante l'invito a compilare un questionario di verifica tramite un *link* ivi contenuto, al fine di evitare asserite limitazioni nell'operatività del conto. Di tale ultimo messaggio, apparentemente proveniente dall'intermediario resistente - come si evince dall'indicazione del mittente e dal fatto di essere inserito nel *thread* di altri SMS effettivamente ricevuti dalla resistente - il ricorrente ha fatto menzione anche nella denuncia alla P.G., precisando tuttavia di non avervi dato seguito (ciò benché sia stato prodotto in copia anche un ulteriore messaggio recante la dicitura "la verifica della sua identità è stata completata con successo, verrà data conferma nelle prossime 24 h"). Ad ogni buon conto, vale rilevare che secondo quanto allegato dal ricorrente la truffa in questione avrebbe preso avvio con la sopra riferita telefonata.

DIRITTO

1) La controversia oggetto del presente ricorso riguarda il disconoscimento, e la conseguente richiesta di rimborso, di due operazioni di bonifico online disposte entrambe in data 09.07.2025, la prima di Euro 2.992,00 e l'altra di Euro 1.300,00, per un importo complessivo di Euro 4.292,00, a favore dello stesso beneficiario e addebito sul conto corrente del ricorrente radicato presso la banca resistente.

2) Al riguardo, il Collegio ha presente innanzitutto che, in punto di diritto, le operazioni di pagamento contestate sono state effettuate sotto la vigenza del D.lgs. 11/2010, così come modificato dal D.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2), e del Regolamento UE n. 2018/389 in materia di autenticazione forte del cliente (SCA) e di standard aperti di comunicazione comuni e sicuri, applicabili alle operazioni della specie effettuate successivamente alla data del 14.09.2019.

3) Ciò posto, il Collegio rileva che la resistente ha rappresentato, e dettagliatamente documentato con idonei elementi istruttori, che la disposizione delle operazioni in esame ha richiesto il preventivo accesso all'area riservata della resistente e la conferma di ciascuna operazione mediante digitazione in ogni fase del codice PIN statico del ricorrente e di un OTP dinamico generato da Mobile Token, sicché il Collegio ritiene che, seppure nei limiti della sommaria istruttoria esperibile dinanzi a questo Arbitro, possa ritenersi adempiuto da parte della resistente medesima l'onere probatorio sulla stessa gravante ai sensi dell'art. 10, co. 1, del D.lgs. 11/2010 in merito all'avvenuta autenticazione delle operazioni disconosciute, alla loro corretta registrazione e contabilizzazione, nonché al mancato

verificarsi di malfunzionamenti delle procedure necessarie per la loro esecuzione o di altri inconvenienti, considerato specificamente che tale modalità di autenticazione a doppio fattore delle operazioni in questione, basata sulla combinazione di un elemento di conoscenza e di un elemento di possesso, è da ritenere conforme ai requisiti della SCA ai sensi del suddetto Regolamento UE n. 2018/389 (in tal senso cfr. ABF, Collegio di Roma, decisione n. 6197/2024).

4) Per contro, il Collegio ritiene che sussistano nella vicenda in esame rilevanti elementi di colpa grave addebitabili al solo ricorrente per l'avvenuta disposizione ed esecuzione delle operazioni di pagamento dallo stesso poi disconosciute, elementi questi non elisi né affievoliti, nel loro contributo causale rispetto al verificarsi dei fatti controversi, da eventuali altri elementi di colpa in ipotesi imputabili alla resistente. Rileva infatti a tal fine anche che i documenti prodotti dal ricorrente in riscontro alla richiesta d'integrazione istruttoria formulata da questo Collegio non sono tali da dimostrare l'avvenuto utilizzo nella vicenda in esame di una tecnica di truffa altamente decettiva quale l'ID *spoofing* dell'utenza telefonica di provenienza della riferita telefonata del 9.07.2025, da cui avrebbe poi preso avvio l'allegata truffa.

5) Il Collegio rileva specificamente al riguardo che, benché il ricorrente abbia allegato di aver ricevuto in data 09.07.2025 una telefonata dal numero ***7 che avrebbe presentato sul display del proprio *device* un identificativo riferibile alla banca resistente, e di essersi per ciò convinto a seguire le istruzioni ricevute dall'interlocutore sedicente dipendente della banca stessa, tra le quali quella di scaricare e installare sul proprio *device* un'applicazione denominata "Questionario ***", tuttavia il ricorrente stesso non ha però poi versato in atti copia della lista chiamate del proprio dispositivo, benché appositamente sollecitato in tal senso con apposita ordinanza istruttoria adottata nella seduta di questo Collegio del 13.02.2026. Pertanto non è possibile in questa sede riscontrare i dati di tale telefonata asseritamente ricevuta e l'eventuale effettiva corrispondenza dell'ID chiamante, quand'anche fraudolentemente manipolato mediante *spoofing*, ad un'utenza riconducibile alla banca resistente per ingenerare così nel ricorrente la falsa percezione di interloquire con un operatore dell'intermediario, secondo lo schema fraudolento, ritenuto particolarmente insidioso, del *Vishing* combinato con l'*ID spoofing* del chiamante.

6) Ciò impedisce quindi al Collegio di poter valutare con sufficiente certezza l'effettivo grado di maggiore sofisticatezza e insidiosità della truffa allegata dal ricorrente, ovvero di stabilire se il denunciato raggiro fosse tale da non poter essere incolpevolmente percepito da un utente mediamente diligente o se fossero riscontrabili concorrenti elementi di colpa eventualmente addebitabili alla resistente per le lacune organizzative e di sicurezza nella prestazione dei propri servizi all'utenza ascrivibili all'effetto dell'ID *spoofing* dei propri contatti (sul punto cfr. ABF, Collegio di Roma, decisione n. 4310/2025).

7) Ai fini della relativa valutazione, l'orientamento di questo Arbitro in materia è infatti nel senso di chiedere che il ricorrente produca evidenza delle chiamate fraudolente asseritamente ricevute, onde consentire appunto la verifica della corrispondenza tra il numero o l'ID di tali telefonate e quelli riconducibili alla resistente (in tal senso cfr. ABF, Collegio di Roma, decisione n. 8749/2024; Collegio di Milano, decisione n. 22105/2021). Nel caso in esame invece il ricorrente non ha fornito tale riscontro probatorio, lo stesso infatti ha prodotto, come detto, unicamente copia dello *screenshot* di un SMS di una chiamata persa, dal quale non è possibile quindi ricavare con certezza gli elementi necessari a comprovare l'effettivo ricorrere di una fattispecie di *caller ID spoofing* della telefonata da cui avrebbe invece preso avvio la denunciata truffa.

8) In aggiunta a ciò, il Collegio ritiene che un ulteriore elemento di colpa grave addebitabile al ricorrente sia costituito dal fatto che quest'ultimo ha installato sul proprio *device*, su indicazione del sedicente operatore della resistente, una non meglio identificata applicazione denominata "Questionario ***", non riconducibile all'intermediario resistente, compromettendo così la sicurezza del *device* stesso e avendo consentito verosimilmente a terzi di accedere e controllare da remoto il proprio

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

device e/o capire i dati e le relative credenziali di *home banking* necessarie a disporre poi le operazioni disconosciute (in tal senso cfr. ABF, Collegio di Roma, decisioni n. 6359/2025, n. 4317/2024 e n. 7806/2023).

9) In considerazione di tutto quanto sopra, il Collegio ritiene quindi che la domanda formulata dal ricorrente non possa essere accolta, in quanto la resistente ha innanzitutto fornito idonea prova dell'applicazione di una valida procedura di SCA sia per l'accesso all'APP di *home banking* del ricorrente sia per la disposizione delle operazioni di pagamento disconosciute. Inoltre, da un lato, non è stata provata l'esistenza di specifiche criticità organizzative e/o nelle procedure di sicurezza del servizio di pagamento offerto dalla resistente, e nel caso alla stessa addebitabili, non essendo stata fornita in particolare dal ricorrente idonea evidenza documentale dell'allegato utilizzo nel caso in esame di pratiche di *caller ID spoofing* della chiamata asseritamente ricevuta da cui avrebbe preso avvio la denunciata truffa, e dall'altro risultano invece gravi negligenze imputabili esclusivamente al ricorrente stesso, in assenza delle quali la truffa allegata verosimilmente non si sarebbe consumata. Non sussistono pertanto nel caso in esame i presupposti per valutare l'esistenza di un eventuale concorso di colpa tra le parti.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE