

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO MAIMERI

Seduta del 06/02/2026

FATTO

Con ricorso del 28.7.2025, parte attrice afferma che, in data 24.1.2025, alle ore 16:02, riceveva sulla sua utenza telefonica una chiamata dal numero +3902*****361, riconducibile al servizio clienti dell'intermediario, nella quale il sedicente operatore bancario gli chiedeva la conferma dell'avvenuto ricevimento, nei giorni precedenti, di un *sms* relativo ad un bonifico di € 1.418,60 da lui realmente eseguito in data 7.1.2025, così inducendolo a credere che effettivamente fosse un gestore della sua banca; il sedicente operatore lo informava, poi, sulla necessità di procedere, secondo le nuove normative bancarie, ad una conversione dal suo attuale IBAN tedesco "DE" ad un nuovo IBAN italiano "IT", concludendo che a breve lo avrebbe richiamato per attivare la relativa procedura; alle ore 16:40 dello stesso giorno veniva nuovamente contattato dal presunto operatore che lo guidava nella predisposizione del bonifico bancario verso quello che definiva come il suo nuovo iban, dettandone la causale; rassicurato dal fatto che l'interlocutore avesse il suo numero di cellulare, conoscesse il suo numero di conto corrente e fosse in possesso di un nuovo IBAN che corrispondeva alla stessa banca, il ricorrente realizzava l'operazione di bonifico ordinario *online* richiesta, per l'importo di € 32.305,29, inserendo il proprio nome e cognome; durante lo svolgimento della suddetta operazione, alle ore 16.46 il ricorrente riceveva sul proprio cellulare un primo messaggio *sms* con il quale gli veniva confermato che era stato eliminato il suo iban e di seguire le istruzioni dell'operatore per le nuove coordinate bancarie e poi un successivo messaggio nel quale si confermava che era stato eseguito il giroconto. Il ricorrente, visionando la ricevuta dell'ordine di bonifico, si accorgeva che nel campo della causale compariva la dizione "cambio iban" e nel campo del beneficiario il suo nome era stato sostituito da quello, a lui sconosciuto, di un altro soggetto. In merito a tali anomale difformità, il ricorrente chiedeva immediatamente chiarimenti all'operatore (con il quale era sempre rimasto in contatto telefonico durante l'operazione), dal quale veniva rassicurato che si trattava solo di un conto temporaneo di

transizione. A quel punto il ricorrente, sospettando di essere vittima di una truffa, procedeva dalla sua *app* all'immediata revoca del bonifico ordinario alla quale, però, la banca non dava esecuzione. Il ricorrente inviava quindi una *mail* al supporto della banca, comunicando di voler bloccare il bonifico in uscita. La sua domanda di disconoscimento/revoca del bonifico ordinario, sebbene attivata pochi minuti dopo l'operazione, non veniva accolta dalla banca. A completamento della fattispecie, il legale di parte ricorrente, in data 30.4.2025, inviava al beneficiario del bonifico intimazione di restituzione della somma di € 32.305,59 indebitamente accreditata sul suo conto corrente; tale richiesta, però, veniva riscontrata negativamente in data 23.5.2025 dall'avvocato di tale beneficiario del bonifico, sostenendo che il suo cliente era «stato a propria volta vittima di un raggiro analogo a quello in cui è caduto il ricorrente in questione», a causa del quale, oltre all'accredito ingiustificato dell'importo sottratto al ricorrente di € 32.305,59, erano state attivate varie movimentazioni in uscita dal suo conto corrente. Appare, pertanto, evidente che l'attacco dei frodatori ha coinvolto a catena più soggetti, dalle ore 13.00 del giorno 23.1.2025 alle ore 7.43 del 25.1.2025, ed ha visto dalle ore 16.52 alle ore 17.37 del 24.1.2025 il transito della somma di € 32.305,59 del ricorrente su più conti correnti, con operazioni anomale ed il conto del nuovo beneficiario del bonifico disposto da parte ricorrente addirittura bloccato dai frodatori, senza che i sistemi di *alert* dalla banca rilevassero nulla per ben due giorni. Per tutto quanto esposto il ricorrente chiede di condannare l'intermediario a rimborsare e/o restituire al ricorrente la somma di € 32.305,29 oggetto del bonifico del 24.1.2025.

In sede di controdeduzioni, l'intermediario, dopo aver ricapitolato i fatti essenziali della vicenda per cui è causa, deduce che, come ammesso dallo stesso ricorrente in sede di denuncia, l'operazione contestata è stata predisposta nonché autorizzata dal ricorrente tramite l'*app* della banca installata sul dispositivo mobile personale in suo esclusivo possesso ed unicamente associato al suo conto, in conformità con i requisiti previsti dalla *Strong Customer Authentication (SCA)*. La predetta transazione è stata predisposta all'interno di una sessione *in-app* per l'accesso al conto, avviato dal ricorrente in data 24.1.2025 alle ore 15:41 UTC (16:41 ora locale) tramite SCA, ovvero mediante (i) l'inserimento dell'*ID* biometrico (fattore di inerenza); (ii) l'utilizzo dell'*app* installata sul dispositivo mobile personale del Ricorrente, associato in via esclusiva al suo conto (fattore di possesso); (iii) tale operazione è stata infine autorizzata alle ore 15:52 UTC (16:52 ora locale) del 24.1.2025 in seguito alla convalida della *push* riepilogativa di pagamento, tramite l'immissione del codice PIN di conferma dispositivo, precedentemente creato dal ricorrente e di sua esclusiva conoscenza (fattore di conoscenza); il ricorrente ha dunque agito con colpa grave, in violazione delle disposizioni di legge e contrattuali, seguendo le istruzioni del frodatore e predisponendo nonché autorizzando la transazione successivamente disconosciuta, nonostante: a) fosse stato informato sui rischi del *phishing* attraverso la campagna anti-frode predisposta dalla banca; (b) l'*sms* fraudolento contenesse evidenti indici di anomalia, che avrebbero dovuto allertare lo stesso ricorrente. Nulla può essere eccepito in merito ai presidi di sicurezza adottati dalla banca, i quali sono stati superati dal comportamento gravemente colposo imputabile al ricorrente, il quale ha personalmente disposto nonché autorizzato l'operazione di pagamento in parola mediante l'applicazione della SCA. L'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e non sono stati riscontrati malfunzionamenti né intrusioni nei sistemi informatici della banca. Al contrario, l'operazione di pagamento risulta essere stata autorizzata tramite lo stesso dispositivo mobile in uso da parte del ricorrente fin dal giorno 31.3.2023. La schermata riepilogativa dell'operazione di bonifico contestata, equivalente al sistema di *sms alert*, è stata debitamente inviata al dispositivo personale del ricorrente associato al conto e l'operazione è stata quindi autorizzata secondo il regolare flusso di autenticazione multifattoriale. Inoltre, trattandosi di una singola operazione, l'attivazione di ulteriori sistemi di *alert ex post* è comunque irrilevante ai fini dell'accertamento di una - invero inesistente - presunta responsabilità della banca.

La banca ritiene che il ricorso proposto da parte ricorrente sia da considerarsi infondato per i seguenti motivi: (i) corretta autenticazione, registrazione e contabilizzazione dell'operazione di pagamento controversa. (ii) comportamento gravemente colposo imputabile al ricorrente: quest'ultimo ha infatti assecondato in tutto e per tutto le richieste del frodatore, fino anche a predisporre ed autorizzare l'operazione di pagamento contestata all'interno della *app* della banca associata al suo conto corrente, assicurando così il perfezionamento della frode stessa. In riferimento al generale fenomeno del *phishing* e alle sue possibili declinazioni, da tempo l'intermediario ha intrapreso una capillare serie di campagne informative finalizzate a rendere edotta la propria clientela in merito. Tra le altre cose, la banca mette a disposizione sul proprio sito *internet* ufficiali importanti informazioni relative alle misure di tutela che il cliente è tenuto ad adottare nell'utilizzo degli strumenti di pagamento, nonché alle modalità per comunicare prontamente alla banca l'uso non autorizzato dei medesimi. L'*sms* fraudolento ricevuto dal ricorrente il 7.1.2025 (giorni prima della frode), presentava i seguenti indici di anomalia: -) non risultava inserito in alcuna catena di messaggi genuini inviati dalla banca; -) presentava evidenti errori ortografici e sintattici (uso improprio delle maiuscole, spazi mancanti tra le parole); -) riportava, all'inizio del testo, una sequenza casuale di numeri e lettere priva di qualsiasi significato logico; -) il tono del messaggio è visibilmente elementare e non conforme allo stile comunicativo della banca, che non utilizza mai toni allarmanti né richiede interventi immediati da parte dei propri clienti. Tale *sms* civetta conteneva l'invito a contattare un numero telefonico, in nessun modo riferibile al Servizio Clienti della banca, qualora il ricorrente non avesse autorizzato un bonifico dell'importo di € 1.418,60. Peraltro, il numero telefonico indicato in tale messaggio era diverso da quello utilizzato dal frodatore nella successiva chiamata del 24.1.2025. A fronte della evidente inattendibilità del messaggio e considerato che – come già evidenziato – il ricorrente non aveva disposto alcun bonifico di tale importo nella data di ricezione dell'*sms* civetta (7.1.2025), egli avrebbe dovuto sin da subito verificarne la veridicità, contattando direttamente il Servizio Clienti della banca attraverso i canali ufficiali di assistenza. Al contrario, il ricorrente ometteva qualsivoglia verifica, pur trattandosi di un *sms* che prospettava un bonifico non autorizzato e di importo significativo. Se il ricorrente si fosse tempestivamente attivato, segnalando l'*sms* civetta del 7.1.2025, sarebbe stato prontamente posto nelle condizioni di mettere in sicurezza il proprio conto e, conseguentemente, avrebbe potuto riconoscere la natura truffaldina della successiva chiamata del 24.1.2025, impedendo così il perfezionarsi della frode. L'evento fraudolento avrebbe potuto essere agevolmente scongiurato mediante l'esercizio di un seppur minimo livello di diligenza da parte del ricorrente, già a partire dalla data del 7.1 e in tutti i casi durante la chiamata fraudolenta del 24.1.2025, rilevando l'anomalia della comunicazione ricevuta. La chiamata cosiddetta "civetta" proveniva, infatti, da un'utenza telefonica istituzionalmente preposta alla sola ricezione di chiamate in ingresso (c.d. *inbound*), destinata esclusivamente alla gestione delle richieste di blocco degli strumenti di pagamento da parte della clientela. Tutti i presidi di sicurezza posti in essere dalla banca non hanno subito malfunzionamenti ma sono stati superati dallo stesso ricorrente, che si è attenuto alle irragionevoli istruzioni impartite dal frodatore nel corso della conversazione telefonica, prestando il suo consenso all'esecuzione della transazione in disputa. L'operazione, pur formalmente ordinaria, è stata eseguita come trasferimento immediato in quanto disposta a favore di una correntista sempre della stessa banca, divenendo quindi irrevocabile al momento della ricezione (16:52 ora locale del giorno venerdì 24.1.2025). Il ricorrente ha segnalato l'operazione mezz'ora dopo la sua autorizzazione, quando le somme erano già state distratte dal conto della beneficiaria, per questo la banca non ha potuto recuperare la somma sottratta. Stante quanto sopra, al ricorrente va quindi attribuita una colpa grave per l'uso improprio del proprio strumento di pagamento, circostanza che comporta l'insussistenza dei presupposti previsti dalla normativa per un rimborso delle somme *de quo* a suo favore. Tutto ciò considerato e premesso si chiede il rigetto del ricorso in quanto infondato in fatto e in diritto.

In sede di repliche, parte ricorrente, oltre a ribadire quanto già indicato nel ricorso, osserva ulteriormente che un profilo di particolare gravità emerge dal fatto che il truffatore era in possesso non solo dei dati identificativi del ricorrente (nome e codice fiscale), ma altresì dell'esatto saldo del conto corrente intestato al medesimo. Una simile circostanza non può ragionevolmente essere ascritta ad una frode generica, ma rivela, con ogni probabilità, la sussistenza di una violazione nei sistemi di sicurezza e protezione dei dati dell'intermediario, che avrebbe dovuto garantire la riservatezza e l'integrità di tali informazioni. L'acquisizione da parte di terzi non autorizzati di dati bancari così specifici evidenzia una disfunzione organizzativa e/o una lacuna nei presidi di sicurezza posti a tutela della clientela. Non può non evidenziarsi la grave anomalia operativa verificatasi nel caso di specie: al momento della disposizione del bonifico: l'ordine riportava come intestatario lo stesso nome del ricorrente, mentre il conto beneficiario risultava intestato a soggetto terzo, estraneo alla relazione contrattuale. L'intermediario, nell'esecuzione di un pagamento verso un beneficiario interno al proprio circuito, avrebbe potuto e dovuto rilevare l'incongruenza tra il nome indicato nell'ordine e l'effettivo intestatario del conto destinatario e, conseguentemente, attivare un meccanismo di *alert* o di blocco automatico dell'operazione. La banca, nel caso concreto, non ha fornito alcuna evidenza di aver implementato sistemi idonei a segnalare tale evidente incongruenza né di aver adottato procedure per interrompere o sottoporre a verifica preventiva operazioni di pagamento che presentino elementi sospetti di frode. La banca avrebbe dovuto accorgersi che il bonifico avente come causale "cambio Iban" ed effettuato come giroconto non sarebbe mai potuto essere diretto a soggetti terzi! Gli stessi documenti allegati dalla banca attestano che il bonifico avente come causale "cambio Iban" è stato disposto come giroconto tant'è che non conteneva neppure l'indicazione del nome del destinatario, che è infatti apparsa solo in seguito con la "conferma". La banca afferma che il pagamento sia stato eseguito "istantaneamente", ma al contempo la conferma del bonifico già depositata e la *chat* di assistenza qualificano l'operazione come bonifico ordinario, soggetto dunque alla disciplina ordinaria dei trasferimenti SEPA e, come tale, revocabile entro 48 ore. Eppure, nonostante il ricorrente abbia dato l'allarme con la richiesta di revoca del bonifico neppure mezz'ora dopo l'esecuzione, la banca non ha revocato il bonifico e anzi, ha dichiarato che i soldi erano già stati trasferiti. La responsabilità della banca si aggrava ulteriormente in considerazione della totale assenza di sistemi di allerta preventiva: (i) nessun *alert* è stato inviato in ragione dell'importo elevato dell'operazione; (ii) nessun *alert* per la discrepanza tra l'intestatario indicato (lo stesso ricorrente) e quello reale (terzo estraneo); (iii) nessun alert per la causale palesemente inconsueta ("cambio Iban"), che avrebbe dovuto attivare controlli rafforzati. Tali omissioni evidenziano un comportamento gravemente negligente dell'intermediario, incompatibile con gli standard di diligenza professionale imposti dalla normativa vigente e dalla giurisprudenza consolidata. Si configura una responsabilità piena e diretta dell'intermediario per l'omesso blocco dell'operazione fraudolenta. La telefonata fraudolenta proveniva da un numero telefonico riconducibile al servizio clienti della banca, elemento che, in sé considerato, è idoneo a ingenerare un legittimo affidamento in capo al cliente circa l'autenticità della comunicazione ricevuta.

In sede di controrepliche, la banca sostanzialmente ripropone le eccezioni già formulate con le controdeduzioni.

In relazione alle rispettive argomentazioni, parte ricorrente chiede all'Arbitro il rimborso della somma distratta, pari a € 32.305,29. Dal canto suo, l'intermediario chiede al Collegio «il rigetto *in toto* del ricorso in quanto infondato in fatto e in diritto per le ragioni di cui in narrativa».

DIRITTO

La controversia concerne il rimborso di € 32.305,29, sottratti a seguito di un bonifico disposto il 24.1.2025 e poi disconosciuto da parte ricorrente. L'operazione è stata autorizzata per intero dal ricorrente e, pertanto, è sottratta alla disciplina prevista dal d.lgs. n. 11/2010.

Parte ricorrente afferma di aver ricevuto sulla sua utenza telefonica una chiamata dal numero +3902*****361, riconducibile al servizio clienti dell'intermediario, nella quale il sedicente operatore bancario gli chiedeva la conferma dell'avvenuto ricevimento, nei giorni precedenti, di un *sms* relativo ad un bonifico di € 1.418,60 da lui realmente eseguito in data 7.1.2025, così inducendolo a credere che effettivamente fosse un operatore della sua banca. Il sedicente operatore lo informava, poi, sulla necessità di procedere, secondo le nuove normative bancarie, ad una conversione dal suo attuale IBAN tedesco "DE" ad un nuovo IBAN italiano "IT", concludendo che a breve lo avrebbe richiamato per attivare la relativa procedura. Il ricorrente veniva nuovamente contattato dal presunto operatore che lo guidava nella predisposizione del bonifico bancario verso quello che definiva come il suo nuovo iban, sempre presso lo stesso intermediario. Il ricorrente procedeva quindi a disporre il bonifico € 32.305,29 inserendo il proprio nome e cognome e indicando come causale quanto dettato dal truffatore. Durante lo svolgimento della suddetta operazione, il ricorrente riceveva sul proprio cellulare un primo messaggio *sms* con il quale gli veniva confermato che era stato eliminato il suo IBAN e di seguire le istruzioni dell'operatore per le nuove coordinate bancarie; riceveva poi un successivo messaggio nel quale si confermava che era stato eseguito il giroconto. Solo successivamente il ricorrente, visionando la ricevuta dell'ordine di bonifico, si accorgeva che nel campo della causale compariva la dizione "cambio IBAN" e nel campo del beneficiario il suo nome era stato sostituito da quello, a lui sconosciuto, di un altro soggetto.

Parte ricorrente ammette di aver disposto in prima persona le operazioni, come si desume dalla denuncia.

Il ricorrente ha allegato lo *screenshot* dei messaggi truffaldini. Nel primo messaggio esca, inviato al ricorrente giorni prima della truffa, il mittente corrisponde al nome dell'intermediario resistente; non vi è prova di tale primo messaggio esca risalga ai giorni precedenti alla truffa e faccia riferimento ad un bonifico di € 1.418,60 eseguito realmente dal ricorrente in data 7.11.2025. Giorni dopo tale messaggio, il 24.1.2026, il ricorrente è stato contattato telefonicamente da un'utenza riconducibile alla banca. L'operatore bancario, durante la chiamata, chiedeva al ricorrente la conferma dell'avvenuto ricevimento di tale *sms* risalente al 7.1.2026. Ciò può aver contribuito a generare un affidamento del ricorrente nel fatto che si stesse interfacciando effettivamente con un operatore della sua banca.

L'intermediario eccepisce che l'*sms* fraudolento in questione, ricevuto dal ricorrente il 7.1.2025 (giorni prima della frode), presenta i seguenti indici di anomalia:

- non risulta inserito in alcuna catena di messaggi genuini inviati dalla banca;
- presenta evidenti errori ortografici e sintattici (uso improprio delle maiuscole, spazi mancanti tra le parole);
- riporta, all'inizio del testo, una sequenza casuale di numeri e lettere priva di qualsiasi significato logico;
- il tono del messaggio è visibilmente elementare e non conforme allo stile comunicativo della banca, che non utilizza mai toni allarmanti né richiede interventi immediati da parte dei propri clienti.

L'intermediario eccepisce inoltre che il numero telefonico indicato in tale messaggio è diverso da quello utilizzato dal frodatore nella successiva chiamata del 24.1.2025. Dopo aver disposto l'operazione di bonifico sotto la guida dell'operatore, il ricorrente riceveva un primo messaggio *sms* con il quale gli veniva confermato che era stato eliminato il suo IBAN e di seguire le istruzioni dell'operatore per le nuove coordinate bancarie e poi un successivo messaggio nel quale si confermava che era stato eseguito il giroconto. Il numero corrisponde alla linea telefonica della banca abilitata a bloccare le carte. Sul sito dell'intermediario si precisa che il numero è abilitato soltanto a bloccare le carte. L'intermediario precisa che la chiamata cosiddetta "civetta" proveniva da un'utenza telefonica istituzionalmente

preposta alla sola ricezione di chiamate in ingresso, destinata esclusivamente alla gestione delle richieste di blocco degli strumenti di pagamento da parte della clientela.

Ciò posto, la banca eccepisce che quella in esame non è un'operazione non autorizzata, essendo stata disposta per intero dalla parte ricorrente. La circostanza può considerarsi ammessa dalla parte ricorrente, come risulta dalle sue dichiarazioni contenute sia in denuncia che nel ricorso. Secondo l'orientamento condiviso tra i Collegi, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2. Rientrano in questa fattispecie le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni "sotto dettatura"). In questi casi, dunque, non è configurabile una responsabilità oggettiva del PSP. Il Collegio potrà comunque rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode. Tenuto conto di quanto precede, il Collegio non ha proceduto alle verifiche richieste dalla normativa speciale di cui al d.lgs. 27.1.2010, n. 11, per come modificato dal d.lgs. 15.12.2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento (specialmente la verifica della c.d. *strong customer authentication*).

Ciò posto, occorre verificare se possa in concreto configurarsi un apporto causale dell'intermediario alla frode, così come richiesto dall'orientamento consolidato dei Collegi ABF. Invero, la natura autorizzata dell'operazione non esclude che la condotta dell'intermediario possa essere scrutinata in base alle regole generali del diritto delle obbligazioni, sotto il profilo del corretto adempimento delle obbligazioni contrattuali, eventualmente integrate dal principio di buona fede. In questa prospettiva, si rappresenta che in alcune recenti decisioni il Collegio di Roma, pronunciandosi su operazioni sotto dettatura, ha riconosciuto una responsabilità concorrente dell'intermediario quando la frode è riconducibile all'ipotesi dello *spoofing* e si rinvenivano elementi di sofisticazione della frode. Tale approccio muove dalla considerazione per cui la messaggistica via *sms* è da considerarsi un difetto organizzativo del prestatore di servizi, atteso che trattasi di modalità facilmente aggirabile dai malfattori attraverso la tecnica dell'*sms spoofed*. In base a tali premesse, il Collegio ha determinato in via equitativa ex art. 1226 c.c. la quota di responsabilità da addebitare all'intermediario.

Seguendo questa linea anche nel caso di specie (dove la circostanza che la frode sia partita da un numero telefonico riferibile all'intermediario e quindi in grado di assicurare il ricorrente), il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda la somma di € 12.000,00, equitativamente determinata.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 12.000,00, determinata in via equitativa.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE