

COLLEGIO DI ROMA

composto dai signori:

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

Relatore DOMENICO NASO

Seduta del 04/12/2025

FATTO

Con ricorso introduttivo del presente giudizio preceduto da reclamo del 06/03/2025, parte ricorrente chiedeva all'Arbitro Bancario Finanziario il riconoscimento del diritto alla restituzione dell'importo di euro 44.997,00, corrispondente a tre operazioni di bonifico effettuate all'esito di frode perpetrata ai suoi danni tramite la tecnica del *vishing*.

Rappresentava il ricorrente di essere titolare di un conto corrente presso la Banca resistente e di un account su una piattaforma radicata presso un Intermediario estero e che, in data 19/02/2025, provvedeva a caricare sulla piattaforma copia del proprio permesso di soggiorno, in adempimento ad una richiesta di aggiornamento dei documenti.

In data 24/02/2025 il ricorrente veniva contattato da un'utenza fissa avente prefisso di Milano, da parte di un soggetto qualificatosi come operatore della piattaforma, il quale gli comunicava l'esito negativo del caricamento del permesso di soggiorno e che, conseguentemente, era necessario un aggiornamento della relativa app.

Il ricorrente veniva pertanto indotto a scaricare un'applicazione e, successivamente, eseguiva su indicazione del sedicente operatore, un bonifico di euro 20,00 dal conto radicato presso la convenuta al conto in essere sulla piattaforma, ai fini della presunta riattivazione dell'account.

L'operatore gli comunicava che, per problemi tecnici, l'operazione non era andata a buon fine e che sarebbe stato necessario riprovare nei giorni successivi, circostanza che si verificava in data 25/02/2025 e 26/02/2025.

Il giorno 27/02/2025 il ricorrente si avvedeva dell'esecuzione di tre bonifici, per complessivi euro 44.997,00, da lui autorizzati e trasferiti su un conto acceso fraudolentemente a suo nome presso diverso intermediario.

Il ricorrente presentava prontamente denuncia querela e si accorgeva, inoltre, che il cellulare era stato resettato da remoto, con cancellazione della cronologia di messaggi e chiamate; concludeva pertanto per il riconoscimento del suo diritto alla restituzione dell'importo complessivo di euro 44.997,00 fraudolentemente sottratto a seguito di truffa.

Nelle proprie controdeduzioni l'Intermediario resistente specificava che i bonifici venivano eseguiti personalmente dal ricorrente, previo accesso all'app installata sul dispositivo *mobile* (fattore di possesso) usualmente utilizzato dal ricorrente, mediante biometria (fattore di inerenza).

Secondo le risultanze documentali della resistente, il ricorrente utilizzava un sistema di identificazione "a due fattori", consistente nella autorizzazione delle operazioni di bonifico.

Rilevava la Banca resistente che il *vishing* del quale era rimasto vittima il ricorrente non poteva ascriversi ad un'ipotesi di *vishing* sofisticato, tenuto conto che il predetto veniva contattato per tre giorni consecutivi dai truffatori e procedeva a disporre ben tre bonifici istantanei, mediante riconoscimento biometrico, validando con l'impronta le operazioni, per dimostrare la propria identità.

L'esecuzione delle operazioni fraudolente, secondo quanto asserito dall'Intermediario, è stata determinata presumibilmente da un bonifico di euro 10,00 effettuato dal ricorrente in data 20.02.2025, ossia qualche giorno prima rispetto ai contatti telefonici indicati in denuncia, disposto in favore delle medesime coordinate bancarie verso cui sono stati eseguiti i successivi tre bonifici.

Tale operazione avrebbe, pertanto, sbloccato i limiti di importo previsti per i bonifici istantanei verso i nuovi beneficiari, non risultando invece all'Intermediario alcun bonifico di euro 20,00 nelle date di riferimento.

In sede di repliche il ricorrente aggiungeva che l'Intermediario estero coinvolto nella vicenda provvedeva al risarcimento per l'importo del 50% della perdita subita.

Deduceva che, mentre l'Intermediario estero aveva fallito nelle procedure di verifica consentendo l'apertura del conto truffaldino, la Banca resistente non bloccava i tre bonifici contestati.

In sede di controrepliche la resistente richiama le proprie conclusioni e precisava che, in caso di accoglimento del ricorso, la somma da restituire doveva essere ridotta ad euro 22.497,00, tenuto conto del rimborso da parte dell'Intermediario estero.

DIRITTO

Parte ricorrente chiede la restituzione della somma complessiva di euro 44.997,00, relativa all'esecuzione fraudolenta di tre bonifici istantanei disposti tra il 24 e il 26 febbraio dal conto corrente radicato presso la convenuta in favore di un rapporto apparentemente intestato a parte ricorrente e acceso presso un Intermediario estero.

Quest'ultimo, non convenuto in giudizio, ha rimborsato al ricorrente l'importo di euro 22.497,00, pari al 50% della perdita subita; pertanto, la domanda deve essere analizzata avuto riguardo al restante 50%.

Le operazioni contestate sono state effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (cosiddetta PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15/12/2017, entrato in vigore in data 13/01/2018, che modifica in più punti il d.lgs. n. 11 del 2010.

In particolare, ai fini della verifica del rispetto della Strong Customer Authentication (c.d. SCA), affinché l'Intermediario possa andare esente da responsabilità dovrà fornire prova, oltre che dell'insussistenza di malfunzionamenti, dell'adozione di un sistema di sicurezza adeguato e della corretta registrazione, autenticazione e contabilizzazione delle operazioni contestate.

Come sancito dal Collegio di Coordinamento con la decisione n. 22745/19: *<<...la previsione di cui all'art. 10, comma 2, del D.lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'Intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente>>.*

Secondo l'orientamento condiviso dai Collegi, quando l'operazione è eseguita per intero dal pagatore, deve considerarsi autorizzata e pertanto non soggetta al regime di responsabilità di cui alla PSD2.

Nella fattispecie per cui è causa, il ricorrente riferisce di aver caricato, in data 19.02.2025, sulla piattaforma radicata presso l'Intermediario estero copia del proprio permesso di soggiorno, ai fini dell'aggiornamento della documentazione.

In data 24.02.2025 il ricorrente veniva contattato telefonicamente da un sedicente operatore della piattaforma, per il tramite di un'utenza fissa con prefisso di Milano, che lo invitava ad un aggiornamento dell'applicazione, in considerazione dell'esito negativo della procedura di caricamento dei documenti.

Il ricorrente seguiva le indicazioni impartite e scaricava un'applicazione, utilizzando la propria impronta digitale per sbloccare e validare l'operazione di aggiornamento.

Nelle ipotesi di cd. *Vishing*, il Collegio è solito valutare la condotta del ricorrente alla stregua di *smishing* pacifico, ravvisando la colpa grave del ricorrente, nel caso di specie individuata nell'aver il predetto scaricato l'applicazione che avrebbe verosimilmente concesso il controllo da remoto del suo dispositivo.

Secondo l'orientamento dei Collegi, quando la frode viene attuata tramite installazione di app di terze parti – per il controllo da remoto del dispositivo – si ritiene sussista la colpa grave del ricorrente che <<[...] *su indicazione del frodatore, installi un'applicazione "la cui funzionalità risiede [...] nel permettere l'accesso ed il controllo di pc e smartphone da remoto", consentendo in tal modo al frodatore di agire indisturbato e disporre i pagamenti (cfr. Collegio di Roma, decisione n. 7806/2023)>> (Collegio di Roma, decisione n. 4317/2024; in senso conforme, Collegio di Milano, decisione n. 196/2003).*

L'Intermediario eccepisce, inoltre, che le operazioni sono state disposte dal *device* in possesso del cliente, con la digitazione delle sue credenziali ed autorizzazione mediante impronta digitale a seguito di ricezione di notifica *push*, circostanza peraltro non smentita dal ricorrente.

In presenza di un'operazione "autorizzata", non è in ogni caso esclusa la possibile responsabilità dell'Intermediario, che si ravvisa in misura concorrente nelle ipotesi di "operazioni sotto dettatura" laddove la frode ha avuto origine da un "*sms spoofed*" o da un "*vishing caller id*", elementi da ascrivere a difetti organizzativi della Banca.

Nel caso di specie, non risultano sms truffaldini provenienti dal canale ufficiale della Banca, avendo parte ricorrente specificato di aver ricevuto le telefonate esclusivamente da un operatore addetto della piattaforma e non della Banca resistente.

Tali elementi confermano il difetto di alcun apporto causale alla frode da parte della banca resistente, che esclude pertanto un concorso di colpa tra le parti: <<[...] *In base alle allegazioni di parte la transazione disconosciuta sembra sia stata posta in essere a seguito di frode informatica perpetrata con la tecnica del sito clone, tramite il quale non sono stati tuttavia veicolati messaggi truffaldini apparentemente provenienti dalla banca; infatti, nello specifico, il ricorrente pare aver inserito i dati della carta e le credenziali per il pagamento sul sito clone della piattaforma di compravendita, quindi al di fuori dei canali ufficiali della banca. Ciò posto, occorre valutare se la tecnica truffaldina utilizzata in*

danno dell'odierno ricorrente sia annoverabile tra quelle non sofisticate o viceversa tra quelle particolarmente insidiose: nel primo caso, alla stregua del phishing, sussisterebbe la colpa grave, che invece nel secondo caso sarebbe esclusa (cfr. Collegio di Coordinamento, decisione n. 3498 del 26 ottobre 2012). [...] >> (cfr. Collegi di Roma, decisione n. 6534/2024).

Sulle modalità di esecuzione delle operazioni fraudolente, l'Intermediario dimostra che le predette sono state tutte disposte previo accesso all'app installata sul *device* (elemento di possesso) del ricorrente prima dell'esecuzione dei pagamenti, mediante biometria (elemento di inerenza).

Una volta inserite le informazioni per eseguire l'operazione, ciascun bonifico è stato autorizzato mediante Mobile Code, con conferma attraverso biometria.

I dati relativi ai bonifici sono stati verosimilmente inseriti dai truffatori che avevano *medio tempore* ottenuto il controllo del dispositivo mediante l'applicazione scaricata dal ricorrente.

Dunque, dalla documentazione prodotta dall'Intermediario, risulta rispettato il sistema di identificazione a due fattori in fase di esecuzione dei tre bonifici, comprensivi del riconoscimento biometrico (elemento di inerenza) e della conferma dell'operazione mediante lo smartphone ove è stato attivato il Mobile Code (elemento di possesso).

A conferma della correttezza della condotta dell'Intermediario, si evidenzia che quest'ultimo ha inviato al ricorrente e-mail ed sms alert per ciascuna operazione di pagamento.

Alla luce dei suddetti principi, tenuto conto della estraneità della Banca resistente alla frode perpetrata, non può ravvisarsi alcuna colpa in capo all'Intermediario, essendo ravvisabile una esclusiva responsabilità in capo al ricorrente, per aver dato seguito con ingenuità alla truffa perpetrata.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE