Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) VITERBO	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO GIACOMO VITERBO

Seduta del 17/12/2025

FATTO

Il ricorrente riferisce di essere titolare del conto corrente n. ***694, aperto presso l'intermediario resistente, e che il 20 agosto 2024, alle 10:33, ha ricevuto sul proprio *smartphone* un SMS, apparentemente proveniente da quest'ultimo, con l'avviso dell'autorizzazione di un'operazione di pagamento e l'invito a chiamare un numero di telefono per disconoscerla. Precisa che tale messaggio si è inserito in coda a precedenti messaggi genuini dell'intermediario e che, facendo affidamento sulla genuinità della comunicazione, ha così contattato il numero indicato. Riporta che alla chiamata ha risposto un soggetto che: - si è qualificato come operatore dell'intermediario; - gli ha confermato che era in corso un tentativo di truffa in suo danno; - lo ha poco dopo contattato da un numero in uso all'intermediario; - gli ha prospettato la necessità di dover bloccare il conto e gli ha preannunciato "*la revoca e lo storno dei movimenti in uscita*". Precisa che durante la conversazione ha ricevuto ulteriori messaggi con l'invito ad eseguire "operazioni inverse" per bloccare i tentativi di addebito e dei messaggi con dei "*codici di blocco*". Evidenzia che non ha comunicato all'interlocutore alcun codice personale e che "*poteva verificare la conferma delle operazioni di storno delle varie somme bonificate in favore dell'IBAN: ***3317 come anticipato telefonicamente*". Soggiunge che il giorno seguente si è rivolto alla propria filiale e ha appreso di essere rimasto vittima di una truffa e che l'IBAN destinatario dei bonifici autorizzati risulta riferibile ad un conto intrattenuto da un altro soggetto sempre presso l'intermediario resistente. Tanto premesso, ritiene l'intermediario responsabile dell'accaduto per non aver adottato adeguate misure di sicurezza idonee a proteggere le transazioni e i dati e un sistema di autenticazione forte. Esclude poi la configurabilità di una propria negligenza grave, giacché le tecniche di realizzazione della truffa l'hanno resa particolarmente sofisticata e insidiosa. Soggiunge che la

circostanza che le n. 4 operazioni siano state eseguite nel giro di 45 minuti avrebbe dovuto essere considerata anomala e avrebbe dovuto attivare un blocco cautelativo.
Chiede, pertanto, il rimborso dell'importo di € 9.890,00 fraudolentemente sottratto e le "*spese di lite*".
Costituitosi, l'intermediario evidenzia che il ricorrente non ha allegato copia dei messaggi asseritamente ricevuti, ma soltanto una trascrizione che, in ogni caso, mostra che il numero contattato dal cliente non è riconducibile ai propri recapiti. Rileva, inoltre, che nei messaggi asseritamente ricevuti non è stato fatto alcun riferimento al numero di carta o di conto, né al nominativo del titolare del rapporto. Precisa, poi, che i *log* prodotti dimostrano che i bonifici contestati sono stati eseguiti dall'APP mobile del cliente e autorizzati con PIN. Osserva, altresì, che dalle dichiarazioni rese può dedursi che il cliente ha eseguito i bonifici in conformità alle istruzioni ricevute dal sedicente operatore bancario, con conseguente inapplicabilità della disciplina speciale in materia di operazioni non autorizzate. Eccepisce, infine, la non rimborsabilità delle spese legali.
Chiede, pertanto, di rigettare il ricorso.
In sede di repliche, il ricorrente ribadisce che il messaggio ricevuto risultava provenire dal contatto solitamente utilizzato dall'intermediario. Rileva che la documentazione informatica prodotta da quest'ultimo non mostra i fattori di sicurezza utilizzati per l'autorizzazione e che non è stato fornito alcun riferimento esplicativo. Fa, poi, presente che non è stato attivato alcun sistema di *alert* e che l'intermediario ha ignorato le circostanze anomale delle operazioni, non attivandosi per prevenire il danno. Evidenzia, infine, che l'operatività contestata era in palese contrasto con quella usuale. Insiste, quindi, per l'accoglimento del ricorso.
Nelle controrepliche, l'intermediario ribadisce che il ricorrente non ha provato l'inserimento dei messaggi nel consueto canale dove riceveva le comunicazioni genuine. Quanto alla SCA, precisa che il log "*Res_INV03764680 – PaymentDetails*" mostra l'accesso all'*home banking* dall'APP del cliente e l'esecuzione dei bonifici attraverso l'inserimento del PIN. In ultimo, osserva che, dalla narrazione del cliente, emergono plurimi segnali che avrebbero dovuto farlo sospettare di stare subendo una truffa e che, comunque, quest'ultimo non si è preoccupato di verificare prontamente la disponibilità presente sul suo conto e di conseguenza non ha nemmeno chiesto il *recall* dei bonifici, i quali erano ordinari e, quindi, annullabili fino alle ore 20:00 dello stesso giorno. Insiste per le conclusioni rassegnate in sede di controdeduzioni.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di quattro operazioni di bonifico ordinario (rispettivamente, per i seguenti importi: € 2.870,00; € 2.100,00; € 2.800,00; € 2.120,00), eseguite il 20 agosto 2024 tra le 10:57 e le 11:02 per un importo totale di € 9.890,00, successivamente contestate.
In via preliminare, il Collegio ritiene infondata l'eccezione opposta dall'intermediario per cui le operazioni contestate sarebbero state disposte e autorizzate personalmente e volontariamente dal ricorrente, seppure a seguito di raggiri, dal che conseguirebbe l'inapplicabilità della disciplina speciale in materia di operazioni non autorizzate di cui agli art. 10 ss. del d.lgs. n. 11/2010. Al riguardo, si osserva che il ricorrente, in sede di denuncia, non ha dichiarato espressamente di aver disposto e autorizzato le operazioni in discorso, ma si è limitato genericamente a riferire di avere interloquito con il falso operatore e seguito una "procedura" durata circa due ore. Orbene, il Collegio richiama il consolidato orientamento dell'Arbitro secondo il quale, da un lato, l'operazione deve considerarsi autorizzata, e non è quindi soggetta al regime di responsabilità previsto dalla PSD2, se eseguita per intero dal pagatore con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione, il che non risulta essersi verificato nel caso di specie; e, dall'altro, si è stabilito che, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la

normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP.

Nel merito, il Collegio rileva che le operazioni contestate sono state eseguite 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), entrato in vigore il 13 gennaio 2018. Inoltre, le operazioni contestate sono state eseguite successivamente all'entrata in vigore delle disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del Regolamento Delegato (UE) della Commissione, del 27 novembre 2017, n. 2018/389, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (cfr. anche il disposto dell'art. 5, d. lgs. n. 11/2010, come novellato).

La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, comma 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento della Banca d'Italia del 5 luglio 2011.

In particolare, ai sensi dell'art. 10, d.lgs. n. 11/2010, "qualora l'utilizzatore 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 2 del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere 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'utilizzatore 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" (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è, altresì, precisato che "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".

Ai sensi del successivo art. 12, comma 2 bis, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Per "autenticazione forte" si intende "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" (art. 1, lett. q-bis, d.lgs. 11/2010). Deve, inoltre, ritenersi che gli elementi selezionati devono essere reciprocamente indipendenti, sì che la violazione di un elemento non deve compromettere gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione.

Si deve, altresì, rilevare che l'art. 10-bis, comma 1, d.lgs. 11/2010, stabilisce che "i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

Al riguardo, il Collegio di Coordinamento ha in più occasioni precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia). La *ratio* di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coordinamento, decisioni n. 3947/2014 e, da ultimo, n. 22745/2019, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, *ex* art. 10, comma 2, d.lgs. n. 11/2010).
Tratteggiato il quadro normativo di riferimento, occorre premettere che, nel caso di specie, l'intermediario resistente afferma che le operazioni contestate sono state autorizzate in APP dal dispositivo registrato solitamente utilizzato dal cliente (elemento di possesso) con l'inserimento del PIN (elemento di conoscenza). Tuttavia, il Collegio rileva che l'intermediario ha prodotto i log relativi alle suddette operazioni senza fornire allegazioni specifiche circa l'individuazione delle stringhe attestanti l'inserimento dei fattori, né una legenda esplicativa. Inoltre, dalle evidenze prodotte non risulta chiaro quale codice o valore attesti univocamente l'utilizzo del dispositivo registrato del cliente; non risultano neanche prodotte evidenze relative all'*enrollment* del *device* utilizzato o ad operatività pregressa non contestata che mostrino, eventualmente, l'utilizzo di un *device* identificato con lo stesso codice univoco. Sul punto, non constano neppure dichiarazioni confessorie del cliente in ordine all'eventuale digitazione del PIN tramite la propria APP per l'autorizzazione delle operazioni, o comunque in merito ad un eventuale utilizzo della stessa durante l'espletamento della frode.
Stante l'incertezza in merito all'APP concretamente utilizzata per l'esecuzione delle operazioni disconosciute, si deve confermare l'orientamento di questo Collegio (cfr. decisioni n. 2918/2025; n. 3749/23 e n. 787/23) che, in tali casi, non ha considerato assolto l'onere probatorio relativo all'autenticazione. Orbene, secondo l'orientamento consolidato dell'Arbitro, la mancanza della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta, infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente. Ne consegue il riconoscimento del diritto del ricorrente al rimborso degli importi oggetto delle quattro operazioni di bonifico contestate.
Non può, invece, trovare accoglimento la richiesta di refusione delle "*spese di lite*", in quanto priva di quantificazione e di evidenze a supporto.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 9.890,00.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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