Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) MARIANELLO	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore FULVIO GIGLIOTTI

Seduta del 18/12/2025

FATTO

1. Con ricorso del 22.8.2025 – previo reclamo del 21.5.2025, riscontrato negativamente dall'intermediario in data 23.6.2025 – il ricorrente ha esposto di avere ricevuto, in data 24.5.2024, intorno alle 15,30, un sms proveniente dall'utenza associata al servizio clienti dell'intermediario convenuto, che lo avvertiva di un tentativo di accesso al suo conto corrente; preoccupato per un probabile attacco fraudolento al suo conto (in quanto non era stato lui a dare corso ad alcuna transazione), ma rassicurato dal fatto che l'utenza dalla quale provenivano gli *sms* era riconducibile a quella dell'intermediario, contattava l'utenza indicata e l'interlocutore, presentatosi quale operatore dell'intermediario, lo tranquillizzava, comunicandogli che sarebbe stato necessario, al fine di evitare di ricevere analoghi *sms*, aggiornare l'applicazione riconducibile all'intermediario convenuto.
Procedeva, quindi, dopo aver assunto l'ulteriore cautela di verificare il suo conto (che non mostrava operazioni sospette), all'adempimento indicato, constatando che in effetti l'applicazione mostrava un errore in linea con le affermazioni dell'interlocutore; all'esito dell'aggiornamento, "rientrato" sul suo conto, ne constatava lo svuotamento e – una volta realizzato di essere stato vittima di un raggiro informatico, attuato con una tecnica particolarmente aggressiva – disinstallava l'applicazione (ma tutti i messaggi che gli erano stati intanto inviati risultavano spariti; risultava, altresì, modificata l'utenza dalla

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

quale aveva ricevuto gli *sms*, con modifica del prefisso telefonico da 02 a 06).
All'esito delle necessarie verifiche con l'operatore dell'intermediario convenuto, constatava essere avvenuta una truffa in suo danno, per euro 14.845,68 (a causa di n. 5 bonifici dell'importo di euro 2.000,00 cadauno in favore di tale G. S.; e di un pagamento per euro 4.845,68).
Ha chiesto, quindi, il rimborso della somma fraudolentemente sottrattagli, il risarcimento del danno non patrimoniale asseritamente patito (quantificandolo in euro 2.500,00) e delle spese legali (quantificate in euro 1.000,00), oltre interessi.
2. Si è costituito l'intermediario, chiedendo il rigetto del ricorso.
In particolare, ha evidenziato parte resistente che:
- tutte le operazioni contestate (di cui n. 1 addebito su carta e n. 5 bonifici istantanei) sono state correttamente autenticate in *app* tramite il dispositivo mobile in esclusivo possesso del ricorrente ed unicamente associato al suo conto, in conformità con i requisiti previsti dalla c.d. "*Strong Customer Authentication*" o SCA;
- più in particolare, i cinque bonifici istantanei sono stati autorizzati dal device personale associato al conto del ricorrente in seguito a immissione del codice PIN di conferma dispositivo (fattore di conoscenza) e convalida della relativa notifica push di pagamento inviata all'interno dell'app installata sul suo dispositivo mobile personale, associata in via esclusiva al suo conto (fattore di possesso); e quanto all'addebito su carta di debito, risulta che questo pure sia stato autorizzato dal dispositivo mobile associato al conto del ricorrente, mediante l'applicazione della Strong Customer Authentication (SCA);
- parte resistente si è anche attivata per tentare il richiamo delle somme fraudolentemente sottratte al ricorrente, senza, però, ottenere risposta;
- il ricorrente ha posto in essere una condotta gravemente colposa, avendo provveduto ad eseguire pedissequamente le istruzioni impartitegli dall'ignoto interlocutore.
Ha inoltre escluso qualsiasi responsabilità per danni non patrimoniali, peraltro del tutto privi di riscontro probatorio; e per le spese di assistenza legale, sia in ragione dell'assenza di qualunque responsabilità che, in ogni caso, della non necessità di assistenza tecnica nella sede del procedimento avviato.
Ha quindi concluso per il rigetto integrale del ricorso.

DIRITTO

3. Ritiene il Collegio che la domanda del ricorrente sia parzialmente da accogliere, per le ragioni di seguito illustrate.
4. Le operazioni contestate sono state poste in essere 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; le fonti normative che, nel contesto considerato, regolano la c.d. "autenticazione forte" (in gergo, individuata dall'acronimo SCA: *strong customer authentication*) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10-*bis* del D. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'eba (*European Banking Authority*) e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare, parere del 21 giugno 2019).
5. Secondo le previsioni normative sopra richiamate, riferibili alla fattispecie, la responsabilità di un Prestatore dei servizi di pagamento (PSP) è esclusa quando, *avendo esso dato prova di utilizzare meccanismi di "autenticazione forte" dell'utente*, sia anche riuscito a dimostrare una condotta dolosa o

gravemente colposa dell'utente del servizio (con la precisazione che si intende per "autenticazione forte" 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).
Più in particolare, quando l'utente di servizi di pagamento neghi di aver 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 D. lgs. n. 11/2010.
Piuttosto, sarà onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente: in mancanza di ciò, egli sarà tenuto responsabile dei pregiudizi subiti dall'utente, in ragione del rischio d'impresa sopportato.
Ne consegue che l'intermediario non si libera dalla responsabilità provando la mera regolarità formale delle transazioni, dovendo lo stesso, ai sensi dell'art. 10 del D. lgs. n. 11/2010, documentare elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, anche in via presuntiva, della colpa grave (o del dolo) dell'utente (cfr. Collegio di Coordinamento ABF, n. 22745 del 10 ottobre 2019), fermo restando che in caso di mancanza di prova dell'avvenuto rispetto delle procedure di SCA richieste la responsabilità dell'intermediario andrà comunque dichiarata.
Qualora, poi, si trattasse di operazioni eseguite personalmente dal cliente, non potrebbe farsi applicazione della disciplina richiamata, e il PSP potrebbe rispondere solo in caso di apporto causale proprio, secondo il diritto comune.
6. Alla luce del quadro normativo sopra richiamato, e della connotazione fattuale della vicenda per la quale si procede, per come risultante dalle evidenze in atti, rileva il Collegio che le operazioni contestate devono ritenersi correttamente autenticate.
Invero, dalle evidenze informatiche prodotte da parte resistente è emerso che:
- i bonifici in contestazione (eseguiti in modalità "istantanea"; modalità che parte ricorrente asserisce non avere mai richiesto ma che, in realtà, risulta prevista dalle condizioni generali di contratto depositate dallo stesso ricorrente) sono stati autorizzati da *device* già associato al profilo del ricorrente (in particolare l'associazione del *device* risaliva al novembre 2023); e risulta utilizzato il codice PIN impostato dal cliente nel febbraio del 2020 e mai modificato.
Sono state altresì prodotte notifiche *push*/richieste di conferma all'utente, con indicazione dell'importo e del beneficiario (oltre alla precisazione che si trattava di bonifici istantanei);
- anche il pagamento con carta di credito – per il quale pure è stata prodotta la relativa notifica *push* – risulta eseguito con sistema di autenticazione a due fattori (SCA; modalità di autorizzazione: conferma tramite *password* su *device* certificato).
7. Per altro verso, è pacificamente emerso che parte ricorrente ha eseguito le istruzioni impartite dall'ignoto interlocutore, scaricando un programma che ha reso possibile le disposizioni fraudolente: il che, secondo un pacifico orientamento dei Collegi (da ult. cfr., ad es., Coll. ABF Napoli, n. 2208"5; Coll. ABF Roma, n. 1896/25; Coll. ABF Bologna, n. 7036/25) integra una condotta gravemente colposa del ricorrente.
Occorre anche considerare, tuttavia, che, nel caso di specie, i sistemi dell'intermediario – per come emerso in atti – hanno registrato (in manifesta discontinuità con l'operatività "storica" del ricorrente) n. 5 bonifici in uscita per l'importo di € 2.000,00 ciascuno, a distanza ravvicinatissima (alle ore 16:25, 16:27,

16:28, 16:29 e 16:30 del 24 maggio 2024 a favore di un unico beneficiario) e – alle ore 16:42 – un pagamento con carta di credito per oltre € 4.800,00 considerato – per l'importo - ad alto rischio dal sistema; né risulta pervenuto al cliente alcun *alert* relativo alle operazioni effettivamente eseguite, che (seppure con riguardo a un intervallo di tempo limitato, dalle ore 16,25 alle 16.42) avrebbe potuto richiamare la sua attenzione sulla natura truffaldina dell'attività in corso (ancorché, per vero, sembrerebbe che i truffatori abbiano acquisito il controllo da remoto del dispositivo del ricorrente, non risultando quindi chiaro se quest'ultimo avrebbe potuto prendere visione di eventuali sms *alert*).
Conseguentemente, neppure il comportamento di parte resistente appare esente da censure.
Invero, non si può trascurare che, nella specie, le operazioni truffaldine si sono concretizzate, tra l'altro, in cinque bonifici, tutti allo stesso beneficiario, tutti di significativo importo; e tutti posti in essere a distanza ravvicinatissima, a fronte di una operatività usuale *on line* del ricorrente affatto diversa.
In proposito, sebbene non sia normativamente previsto in capo agli intermediari uno specifico obbligo di monitoraggio preventivo delle transazioni (cfr. Q&A 4090/2018 dell'EBA, nonché, *ex multis*, la decisione del Collegio di Roma, n. 16114/21), è tuttavia opinione condivisa dai Collegi quella secondo la quale (oltre agli specifici indici di anomalia di cui al d.m. n. 112/2007, e anche al di fuori del più ristretto ambito (considera dal d.m. citato) delle frodi su carte di pagamento: e così, ad es., per operazioni di bonifico o ricariche on line) sia ben possibile valorizzare indici di frode ulteriori in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario), ove vi sia un'evidenza delle stesse.
Ciò è, appunto, esattamente quanto deve dirsi nel caso di specie, ove tutti gli elementi accennati (unicità del beneficiario (dei bonifici); distanza ravvicinatissima di tempo delle operazioni fraudolente (di tutte); importo consistente, anche e soprattutto dell'operazione con carta di credito; numero delle operazioni) ricorrono – in modo non contestato – nella vicenda considerata.
Appare allora evidente, alla luce delle considerazioni che precedono, che la stessa condotta di parte resistente risulta altrettanto censurabile, con la conseguenza di dover considerare assolutamente predicabile un concorso di colpa, in eguale misura (50%) di ambedue le parti; per cui l'intermediario dovrà farsi carico delle somme fraudolentemente sottratte al ricorrente nella misura della metà, e perciò per euro 7.423,00, oltre interessi dalla data del reclamo.
8. Non possono trovare accoglimento, invece, le domande relative al danno non patrimoniale asseritamente patito (quantificato in euro 2.500,00), solamente predicato da parte ricorrente, ma rimasto privo di qualsiasi riscontro; e alle spese legali (quantificate in euro 1.000,00, come da fattura allegata che, tuttavia, è nominativamente riferita a soggetto diverso dal ricorrente), non ricorrendo le condizioni sotto le quali, soltanto (cfr. Coll. Coordinamento ABF, n. 4580/2025), è possibile dare corso al riconoscimento di simili spese.
9. Ne consegue che l'intermediario convenuto dovrà farsi carico del 50% della somma indebitamente sottratta al ricorrente, risultando perciò tenuto a corrispondere a quest'ultimo la somma di euro 7.423,00, oltre interessi dalla data del reclamo.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente al risarcimento del danno per l'importo di € 7.423,00, oltre interessi legali dalla data del reclamo nei sensi di cui in motivazione.

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