Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) CESARE

Seduta del 10/03/2026

FATTO

Il ricorrente afferma di aver subito una frode per un bonifico istantaneo di € 1.800,00 eseguito in data 10 ottobre 2025. Espone di aver ricevuto, tramite la piattaforma di messaggistica, un contatto da parte di un soggetto che si qualificava come operatore dell'intermediario e che dimostrava di conoscere il suo codice cliente, i movimenti recenti del conto corrente e le procedure operative della banca, elementi che lo hanno indotto a ritenere che il contatto provenisse effettivamente dal personale dell'intermediario. Durante la conversazione gli è stato riferito che era stato rilevato un movimento sospetto da disconoscere e che avrebbe dovuto autorizzare tramite app bancaria un'operazione descritta come "disconoscimento di sicurezza". Afferma di aver seguito le istruzioni in buona fede, senza aver fornito le proprie credenziali né cliccato su link o messaggi esterni, e di aver scoperto solo successivamente che l'operazione autorizzata era in realtà un bonifico istantaneo a favore di terzi. Nello stesso giorno ha sporto denuncia presso la Polizia Postale e ha immediatamente contattato la banca per bloccare l'operatività del conto. Sostiene che, in presenza di tecniche di social engineering sofisticate poste in essere da truffatori in possesso di informazioni riservate riconducibili alla banca, non può configurarsi colpa grave a suo carico e che la sola prova dell'autenticazione forte non è sufficiente a ritenere l'operazione come autorizzata dal cliente. Il ricorrente domanda il rimborso di € 1.800,00, oltre interessi legali dal giorno dell'addebito al soddisfo.

Nelle controdeduzioni, l'intermediario afferma che l'operazione è stata disposta dal dispositivo in uso al ricorrente, registrato presso i propri sistemi informatici già in data 6 giugno 2025, e che l'accesso e la disposizione sono avvenuti nel pieno rispetto delle previsioni normative in materia di autenticazione forte. Osserva che lo schema descritto dal ricorrente, in cui il frodatore impartisce istruzioni telefoniche lasciando che sia il cliente stesso a disporre e autenticare l'operazione senza che il frodatore venga mai a conoscenza dei codici di accesso, configura un'ipotesi di social hacking, fenomeno dinanzi al quale i Collegi ABF hanno costantemente ritenuto l'operazione personalmente autorizzata dal cliente. Evidenzia che tale schema è ampiamente noto e che il ricorrente avrebbe potuto avvedersi della natura truffaldina del contatto, atteso che la chiamata proveniva da un numero di telefonia mobile non riconducibile ai canali ufficiali della banca. Riferisce di aver dato tempestivamente seguito alla richiesta di recall del bonifico in data 13 ottobre 2025, senza tuttavia ottenere riscontro dall'intermediario beneficiario. Chiede il rigetto del ricorso.

DIRITTO

La controversia riguarda il disconoscimento di un bonifico istantaneo di € 1.800,00 eseguito in data 10 ottobre 2025 dal ricorrente dalla propria app bancaria, a seguito di un contatto decettivo da parte di un soggetto che si spacciava per operatore dell'intermediario. È pacifico che l'operazione sia stata eseguita direttamente dal ricorrente, che ha personalmente disposto il pagamento seguendo le istruzioni del frodatore. Tale circostanza è confermata in termini confessori dalla denuncia presentata dallo stesso ricorrente alla Polizia Postale in data 10 ottobre 2025, dal modulo di disconoscimento dell'operazione e dalle repliche, nelle quali il ricorrente non disconosce di aver materialmente autorizzato il bonifico. I log informatici versati in atti dall'intermediario confermano altresì che la fase di accesso e la fase dispositiva sono state completate sull'app associata al dispositivo del ricorrente, installata dallo stesso in data 6 giugno 2025.

Secondo l'orientamento consolidato dei Collegi ABF, quando l'operazione di pagamento è eseguita per intero dal pagatore — sia nella fase dispositiva sia nella fase di autenticazione — essa deve

considerarsi autorizzata ai sensi dell'art. 5 del D.Lgs. n. 11/2010, con conseguente inapplicabilità del regime di responsabilità per le operazioni di pagamento non autorizzate previsto dalla direttiva 2015/2366/UE e dal D.Lgs. n. 11/2010. Rientrano in questa fattispecie le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione fraudolenta, come nel fenomeno del c.d. social hacking (Collegio di Milano, decisione n. 432/2023; Collegio di Roma, n. 8538/2021). Nella fattispecie in esame, il Collegio non procede pertanto alla verifica della corretta esecuzione e autenticazione dell'operazione contestata ai sensi degli artt. 10 ss. del decreto citato.

Il ricorrente eccepisce che l'operazione non potrebbe considerarsi autorizzata in quanto il suo consenso sarebbe stato viziato dal raggiro, e che la conoscenza da parte del frodatore di informazioni riservate sul conto sarebbe riconducibile a un accesso abusivo ai sistemi dell'intermediario, che avrebbe così concausato la frode. Le eccezioni non possono essere accolte. Quanto alla prima, come statuito dai Collegi territoriali, le operazioni effettuate dal cliente — seppure sulla base di un consenso viziato dal raggiro subito dal terzo — non possono configurarsi come non autorizzate, in quanto l'art. 5 del D.Lgs. n. 11/2010 qualifica come non autorizzata esclusivamente l'operazione effettuata in completa assenza del consenso del pagatore; nel caso di specie il consenso è stato prestato, ancorché viziato da errore indotto dal raggiro. Quanto alla seconda, l'allegazione di un accesso abusivo ai sistemi dell'intermediario è rimasta priva di qualsiasi supporto probatorio: il ricorrente non ha prodotto alcuna evidenza a sostegno di tale scenario, limitandosi a negare di aver cliccato su link malevoli o di aver comunicato propri codici personali.

Fermo che, in caso di operazioni compiute direttamente dal cliente, l'intermediario è esonerato dalla prova di autenticazione e non è configurabile una responsabilità oggettiva a suo carico, il Collegio può comunque rilevare una responsabilità concorrente del PSP secondo le norme di diritto comune, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode. Nel caso di specie, tuttavia, non ricorre alcuna delle ipotesi rilevanti: non risulta che il numero verde dell'intermediario fosse indisponibile al momento dei fatti, né che il ricorrente si sia rivolto a un dipendente della banca che non abbia identificato il tentativo di frode, né che vi fossero indici di anomalia tali da imporre il blocco della transazione. Alla luce delle considerazioni che precedono, il ricorso non può essere accolto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE