Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

## COLLEGIO DI MILANO

composto dai signori:

| | |
|---|---|
| (MI) TINA | Presidente |
| (MI) MODICA | Membro designato dalla Banca d'Italia |
| (MI) RIZZO | Membro designato dalla Banca d'Italia |
| (MI) SANTARELLI | Membro di designazione rappresentativa degli intermediari |
| (MI) SCARANO | Membro di designazione rappresentativa dei clienti |

Relatore (MI) SCARANO

Seduta del 17/02/2026

## FATTO

La parte ricorrente espone di aver ricevuto in data 23.07.2024 un messaggio riconducibile all'intermediario, con il quale veniva informato della predisposizione di un bonifico in uscita dal proprio conto corrente. Riceveva immediatamente anche una telefonata da un numero appartenente al

medesimo intermediario e, una volta disconosciuto il pagamento, il sedicente operatore gli comunicava la necessità di revocare il bonifico direttamente dall'app della banca. Il giorno dopo sporgeva denuncia alle Autorità competenti e, successivamente, presentava reclamo all'intermediario, che riscontrava negativamente.
Sostiene che la truffa subita era particolarmente insidiosa e difficile da riconoscere e che tale circostanza esclude il proprio dolo o colpa grave, mentre sussiste la responsabilità della banca che non ha adottato misure di sicurezza idonee a prevenire l'illecita captazione di dati e la sicurezza dell'*home banking*.
Conclude chiedendo la restituzione delle somme pari ad € 8.250,00.
Nelle controdeduzioni, l'intermediario eccepisce che il bonifico di € 5.000,00 sia stato disposto personalmente dal ricorrente tramite l'applicazione bancaria, con inserimento del PIN, e che l'operazione abbia seguito il regolare processo di autenticazione e registrazione. Ha precisato che il cliente è rimasto vittima di una tecnica di *spoofing* ormai nota, mediante la quale i messaggi fraudolenti ricevuti dalla vittima vanno a posizionarsi in coda a quelli genuini inviati da un mittente già conosciuto, come la propria banca. Ha rilevato che l'sms non conteneva riferimenti al conto del ricorrente e che, dalle evidenze prodotte, risulta che il messaggio fraudolento è stato ricevuto alle ore 18.43, ovvero un minuto dopo la ricezione della chiamata del sedicente operatore bancario. Ha aggiunto che solo la collaborazione del cliente, che ha rilasciato i dati di contatto, ha reso possibile la frode e che da tempo promuove campagne informative contro le truffe on-line.
Con le repliche, il ricorrente afferma che la sottrazione della somma di denaro non è ascrivibile alla propria condotta negligente, bensì all'inadeguatezza dei sistemi informatici della banca, e che non vi è prova dell'effettiva conoscenza dei messaggi *push* nel contesto temporale in cui la truffa si stava consumando. Precisa che secondo la giurisprudenza la sottrazione dei codici del correntista attraverso il *phishing* rientra nell'area del rischio di impresa e che l'intermediario ha l'obbligo di adottare degli accorgimenti adeguati per prevenire l'illecita captazione di dati attraverso il *phishing*. Sostiene che se la banca avesse agito diligentemente, si sarebbe accorta degli accessi anomali effettuati sul profilo dell'*home banking* della vittima e che lo svuotamento del conto corrente avrebbe dovuto mettere in allarme la banca che avrebbe dovuto, a sua volta, avvisarlo e permettergli di modificare le sue credenziali. In definitiva, la frode posta in essere dai truffatori che ha causato lo svuotamento del conto corrente è stata resa possibile dalla mancata vigilanza della banca e dall'inadeguatezza dei sistemi di sicurezza.
Con le controrepliche, l'intermediario ha ribadito, tra l'altro, che l'operazione è stata eseguita personalmente dal cliente tramite app della banca e inserimento del PIN e che non sussiste un dovere generale dell'intermediario di chiedere spiegazioni al cliente a fronte di operazioni non conformi alla sua consueta operatività, specie quando le operazioni sono poste in esser dal cliente stesso.

## DIRITTO

La controversia concerne un'unica operazione di bonifico dell'importo di € 5.000,00, eseguita in data 23.07.2024 alle ore 19:48, che il ricorrente ammette di aver personalmente disposto seguendo le istruzioni impartite dal frodatore, convinto di mettere così "al sicuro" il saldo del suo conto corrente.
Dalla denuncia versata in atti, lo stesso ricorrente riferisce che in data 23.07.2024 riceveva un messaggio dell'intermediario che lo informava che era stato effettuato un bonifico di € 3.250,00 dal suo conto e, subito dopo, riceveva una telefonata da un numero riconducibile al medesimo intermediario nel corso della quale un sedicente operatore confermava che "*avevano tentato di effettuare un bonifico da una posizione insolita con un nuovo dispositivo*". L'operatore gli comunicava che per bloccare

l'operazione sospetta, il cliente avrebbe dovuto accedere all'app della banca e bloccare l'operazione in uscita e che all'esito di questa operazione sarebbe stato richiamato. Effettuata l'operazione suggerita, dopo pochi minuti, il ricorrente riceveva un'altra telefonata dal finto operatore che gli comunicava che il suo conto corrente era oggetto di un "*attacco hacker*" e che per metterlo in sicurezza il cliente avrebbe dovuto effettuare un bonifico di € 5.000,00 all'iban da lui dettato. Eseguito il bonifico, il sedicente operatore confermava che l'operazione era andata a buon fine, promettendo di richiamarlo in serata. Il cliente non riceveva alcuna chiamata ulteriore e il giorno dopo si recava in banca scoprendo di esser stato truffato.

In sostanza, risulta che il ricorrente, pur raggirato dal terzo, ha inserito i dati del beneficiario e autorizzato l'operazione mediante i propri strumenti di autenticazione. Deve pertanto ritenersi pacifico che l'operazione sia stata materialmente eseguita dal titolare del conto sia nella fase dispositiva sia in quella autorizzativa.

Secondo l'orientamento condiviso dei Collegi ABF, quando l'operazione è eseguita per intero dal pagatore, l'operazione stessa deve considerarsi autorizzata; pertanto, non viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate di cui alla direttiva 2015/2366/EU ("PSD2") e al D. Lgs n. 11/2010, non essendosi in presenza di un utilizzo abusivo degli strumenti di pagamento in assenza di volontà dispositiva, ma di una disposizione che, sul piano tecnico-operativo, proviene dal titolare. Rientrano in questa fattispecie, in particolare, 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 tal senso si è espresso recentemente il Collegio di Milano con decisione n. 11531/2025 che ha precisato tra l'altro: "*Secondo l'interpretazione consolidata dei Collegi territoriali, la disposizione contenuta nell'art. 5 del D. lgs. 11/2010 in tema di consenso necessario del pagatore, letta congiuntamente ai successivi artt. 9 e 10, induce a ritenere 'autorizzata' l'operazione eseguita personalmente dal cliente ancorché il consenso sia corrotto dal dolo del frodatore: per quanto la volontà del cliente di effettuare tali operazioni sia stata viziata per effetto del raggiro subìto dal terzo ignoto, l'intermediario non poteva che considerare autorizzati i pagamenti effettuati personalmente dal titolare dello strumento di pagamento, non avendo alcuna possibilità di accorgersi della truffa perpetrata ai danni del cliente (Coll. Milano, dec. nn. 8007/2020; 19945/2021, 11546/2019; Coll. Roma, dec. n. 4658/2021)*" (v. inoltre Collegio di Milano, decisione n. 577/2026, nonché Collegio di Bari decisione n. 5815/2024).

Ne consegue l'inapplicabilità della disciplina speciale in materia di operazioni non autorizzate e l'esonero dell'intermediario dall'onere di provare l'autenticazione ai sensi dell'art. 10 del d.lgs. n. 11/2010.

Resta da verificare se, pur in presenza di operazione autorizzata, possa ravvisarsi una responsabilità dell'intermediario in relazione agli obblighi di buona fede e diligenza professionale nell'esecuzione del rapporto contrattuale e degli obblighi di protezione che gravano, per diritto comune, sul *bonus argentarius* (cfr. Collegio di Milano, decisione n. 11531/2025 cit.).

I Collegi hanno chiarito che, in simili fattispecie, una responsabilità concorrente del prestatore di servizi di pagamento può configurarsi solo ove emerga un apporto causale dell'intermediario alla frode, ad esempio per mancata disponibilità dei canali di assistenza, omessa rilevazione di macroscopici indici di anomalia o mancata gestione di un tentativo di frode portato a sua conoscenza.

Nel caso in esame non risultano elementi idonei a dimostrare tali circostanze. Non è stato documentato che il ricorrente abbia contattato l'intermediario prima dell'esecuzione del bonifico per verificarne la genuinità, né che vi siano stati blocchi cautelativi o segnalazioni interne ignorate. L'operazione contestata è unica, di importo corrispondente al limite giornaliero, come dichiarato dal cliente in sede di

denuncia, e non risultano in atti dati sulle movimentazioni storiche tali da consentire di qualificarla come macroscopicamente anomala rispetto al profilo operativo del ricorrente.
Quanto alla mancata attivazione o al mancato funzionamento di eventuali sistemi di *alert*, i Collegi hanno ritenuto irrilevante tale profilo nelle ipotesi di singola operazione, atteso che la ricezione dell'avviso non avrebbe comunque consentito, in concreto, di evitare il pregiudizio.
La condotta del ricorrente, quale emerge dalla denuncia, evidenzia invece che egli ha disposto il bonifico sotto dettatura telefonica, nella convinzione di mettere in sicurezza le somme, senza effettuare verifiche autonome circa l'identità dell'interlocutore, nonostante la notoria diffusione di simili tecniche fraudolente.
Alla luce di tali considerazioni, il Collegio ritiene che il ricorso debba essere respinto.

**PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

IL PRESIDENTE