Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) DELL'ANNA MISURALE

Seduta del 09/06/2026

FATTO

Il cliente, con ricorso del 4 dicembre 2025, afferma che:

- in data 23.07.2024 riceveva una chiamata dal numero ufficiale dell'intermediario A;
- l'interlocutore si presentava come operatore dell'ufficio antifrode dell'intermediario A, dimostrando di conoscere i suoi dati personali e bancari. Riferiva quindi che risultavano eseguiti tentativi di bonifici sul conto, chiedendo la sua collaborazione per la "messa in sicurezza" del rapporto;
- chiedeva il collegamento da remoto del PC del cliente, che acconsentiva;
- gli veniva quindi richiesto di fare accesso al conto, senza richiedere la comunicazione delle credenziali;
- la durata complessiva della vicenda è stata di sette ore e 15 minuti il giorno 23 luglio e di quattro ore circa il giorno successivo;
- in questo arco temporale, il cliente vedeva al monitor ciò che il sedicente operatore stava eseguendo;
- nelle prime ore questi tentava di eseguire sette bonifici, che venivano bloccati dalla banca;
- riusciva, quindi, a richiedere un prestito di € 33.400,00, comunque bloccato;

- riusciva tuttavia con successo a effettuare tre giroconti da conto deposito a conto corrente presso l'intermediario A e tre bonifici in uscita verso la carta del cliente riferibile all'intermediario B, per un totale di € 88.000,00;
- dalla carta riferibile all'intermediario B venivano quindi eseguite n. 12 operazioni tra bonifici istantanei, ordinari, pagamenti diretti e acquisto criptovalute;
- si disconoscono tutti i movimenti sul conto e sulla carta in quelle giornate;
- la somma sottratta è pari, nel complesso, a € 39.697,68.

Chiede, pertanto, il rimborso della detta somma.

L'intermediario A, con le proprie controdeduzioni, afferma quanto segue:

- le operazioni eseguite sul conto corrente, con fuoriuscita di € 88.000,00, sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali;
- seppur il frodatore abbia utilizzato tecniche di *social engineering* ed efficacia persuasiva tale da indurre il cliente a ritenere (erroneamente) che la conversazione si stesse svolgendo con un reale operatore della banca, il cliente stesso, dando pienamente credito alla telefonata, ha, di fatto, consentito la consumazione della fattispecie di truffa ai propri danni, con ciò violando il dovere di tenere un comportamento idoneo a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento (art. 7, comma 2, D. Lgs. n. 11/2010);
- il ricorrente riferisce che uno dei numeri da cui è stato contattato coincideva con quello dell'odierna resistente (configurando ID caller spoofing), mentre l'ulteriore no (configurando semplice vishing);
- il cliente ha ricevuto notifiche push da parte dell'intermediario, le quali descrivevano esattamente le operazioni;
- il cliente ha cooperato con il frodatore consentendo il controllo da remoto del proprio dispositivo e disponendo giroconti e bonifici, pur se in parte inseriti dal truffatore, dal proprio dispositivo, con la convinzione che sarebbero poi stati stornati;
- la banca ha posto in essere campagne di sensibilizzazione della clientela proprio al fine di fornire ai clienti strumenti per poter riconoscere la frode;
- infine, si evidenzia che l'intermediario ha esperito il tentativo di *recall* delle disposizioni, con esito negativo.

Conclude, pertanto, chiedendo il rigetto del ricorso.

L'intermediario B, con le proprie controdeduzioni, afferma quanto segue:

- preliminarmente, osserva che il ricorrente ha ricevuto dalla resistente il rimborso di n. 3 operazioni di pagamento inserite in contestazione, per complessivi € 37,00;
- la resistente ha inoltre rimborsato l'importo di € 198,68 in relazione all'operazione di acquisto criptovalute;
- quanto alle operazioni di pagamento rimanenti, tutte queste operazioni sono state correttamente contabilizzate, registrate e autenticate con il corretto inserimento delle credenziali;
- tra i profili riconducibili alla colpa grave del ricorrente, occorre anzitutto evidenziare l'assoluta genericità della ricostruzione dei fatti fornita. La narrazione risulta priva di elementi concreti circa le modalità con cui soggetti terzi avrebbero potuto accedere al conto, mancando qualsiasi dettaglio utile a circoscrivere la dinamica degli accadimenti;

- quanto al contatto telefonico, lo stesso è avvenuto da parte di un operatore dell'intermediario A, quindi non riferibile alla resistente;
- si ritiene dunque che, con colpa grave, il ricorrente abbia assecondato le richieste ricevute da un soggetto sconosciuto dal quale era stato contattato da un numero riferibile ad un altro intermediario, circostanza che induce a ritenere che sia vittima di colpevole credulità nell'ambito di uno schema di truffa da tempo ormai noto;
- il ricorrente, pur riferendo di aver nutrito un persistente sentore di incertezza circa la vicenda sin dalle prime fasi della conversazione telefonica, della durata di ben 7 ore e 15 minuti, non ha tuttavia adottato alcuna misura di autotutela idonea a prevenire l'evento dannoso;
- il ricorrente non ha preso contatto con il Servizio Clienti per la verifica della circostanza pur avendo più volte indicato che la questione gli è parsa dubbia.

Chiede, pertanto, in via principale il rigetto del ricorso, in estremo subordine limitare l'accoglimento della domanda riconoscendo una responsabilità dell'intermediario soltanto concorrente da ripartirsi con gli altri intermediari intervenuti.

In sede di repliche, il cliente, richiamati i propri scritti, rileva nei confronti dell'intermediario A che quest'ultimo attribuisce erroneamente al cliente una richiesta di restituzione dell'importo di € 88.000,00; in realtà, l'importo della domanda è pari a € 39.697,86, pari alla somma effettivamente sottratta e non recuperata. L'importo di € 88.000,00 costituisce solo il totale delle movimentazioni intercorse tra il conto presso l'intermediario A e la carta dell'intermediario B, intestata al medesimo cliente.

Nei confronti dell'intermediario B, il cliente replica che la carta era solita essere utilizzata per operazioni di importo modesto, mentre nel corso della frode sono stati registrati importanti accrediti sulla carta seguiti da altrettanto rilevanti operazioni dispositive in uscita.

L'intermediario A, in sede di controreplica, sottolinea che le operazioni di bonifico in uscita risultano eseguite il 23 luglio 2024; il giorno successivo (24 luglio) la banca ha provveduto a bloccare la posizione del cliente a seguito della segnalazione di frode, nel corso di una chiamata intercorsa con il cliente stesso che quindi ne era perfettamente edotto; quanto alla richiesta di prestito avvenuta nel corso della frode, si precisa che la stessa non si è perfezionata e che nessuna somma è stata accreditata al cliente a tale titolo.

L'intermediario B, in sede di controrepliche, rileva che il ricorrente non ha fornito, neanche in questa occasione, le prove concrete a dimostrazione del fatto che le operazioni sono state realmente realizzate senza il suo consenso, limitandosi a disconoscere le operazioni, rendendo impossibile ricostruire in maniera univoca le modalità di realizzazione degli eventi;

ribadisce che tutte le operazioni di pagamento in discussione sono state autorizzate: (i) tramite il dispositivo mobile in uso al ricorrente e associato all'account del ricorrente due giorni prima della vicenda in discussione, ovvero in data 21 luglio 2024; (ii) tramite il parametro biometrico in uso sul dispositivo mobile associato. Insiste, quindi, per l'accoglimento delle conclusioni già rassegnate.

DIRITTO

La controversia ha ad oggetto il disconoscimento di un certo numero di operazioni; di cinque tra queste si chiede il rimborso.

Proprio al fine di delimitare il perimetro della controversia e delle domande del ricorrente si osserva quanto segue.
L'operatività contestata si è articolata, dapprima, in movimenti di bonifico per complessivi € 88.000,00 dal conto corrente del cliente acceso presso l'intermediario A (d'ora in avanti primo intermediario), in favore della carta di titolarità del cliente emessa dall'intermediario B (d'ora in avanti secondo intermediario).
Successivamente, dalla predetta carta sono stati eseguiti pagamenti verso terzi, solo in parte recuperati o rimborsati; con il presente ricorso, il cliente chiede la restituzione delle somme non ancora recuperate, che quantifica in € 39.697,86.
In sede di repliche, il cliente chiarisce espressamente che le operazioni in uscita dal conto del primo intermediario non formano oggetto di domanda restitutoria:
Pertanto, nel prosieguo l'esame sarà unicamente concentrato sulle operazioni in uscita effettuate tramite la carta di titolarità del cliente, emessa dal secondo intermediario e non rimborsate. Dovrà infatti anche tenersi conto che il secondo intermediario ha documentato il rimborso delle tre operazioni di minor importo (€ 15,00, 2,00 e 20,00), per un totale di € 37,00, già riaccreditati al cliente come da evidenze prodotte in atti.
Quanto all'operazione di acquisto criptovalute per € 3.000,00, il secondo intermediario documenta che la stessa risulta integralmente rimborsata, a fronte del riaccredito di € 2.801,32 derivante dalla vendita delle criptovalute acquistate, con l'ausilio dell'esercente e del rimborso del residuo, pari a € 198,68, direttamente da parte del secondo intermediario.
Venendo allora alle operazioni disconosciute e non ancora rimborsate, queste, come anticipato, sono cinque, dell'importo complessivo di € 39.450,00 (inferiore al *petitum* di € 39.697,68, che non tiene conto dei rimborsi documentati). Le operazioni sono state eseguite tra il 23.07.2024 e il 24.07.2024
È in atti la denuncia del cliente presentata il 25 luglio 2024 ed integrata il 27 successivo.
Ebbene, le fonti normative applicabili alla fattispecie in esame sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10-*bis* del D. Lgs. n. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA 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 (v. in particolare il parere dell'EBA del 21 giugno 2019). Nello specifico è richiesta l'autenticazione forte (SCA) quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.
Al riguardo, giova precisare che l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione 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; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del

dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.
'operatività oggetto del presente ricorso, costituita da operazioni verso terzi eseguite a mezzo della carta di pagamento del cliente emessa dal secondo intermediario, è stata preceduta da diverse operazioni eseguite sul conto corrente acceso presso il primo intermediario e precisamente: operazioni di giroconto dal conto deposito del cliente, in favore del conto corrente, per un totale di € 90.000,00; successive operazioni di bonifico eseguite in favore della carta del secondo intermediario, per un totale di € 88.000,00, oltre alla richiesta telematica di un prestito che però, pacificamente, non ha avuto esito positivo e si è quindi conclusa senza alcuna erogazione.
Si torna a sottolineare che il cliente non ha incluso dette operazioni nell'odierno *petitum* e anzi in sede di repliche, come già rilevato, ha espressamente escluso di voler esercitare qualsivoglia pretesa restitutoria rispetto ai bonifici che hanno comportato la fuoriuscita di € 88.000,00 dal conto tenuto presso il primo intermediario, precisando che la richiesta di rimborso si riferisce unicamente alle operazioni verso terzi eseguite tramite la carta del secondo intermediario, che hanno comportato una perdita economica.
Pertanto, come anticipato, le operazioni eseguite tramite il conto acceso presso il primo intermediario risultano del tutto estranee al *petitum* del presente procedimento per espressa dichiarazione del cliente.
Fermo tale decisivo rilievo, per mera completezza si osserva, in ogni caso, che le operazioni di giroconto debbono ritenersi meramente costitutive della provvista come sottolineato dal Collegio di Coordinamento (cfr. decisione n. 8671/2024) e che i bonifici eseguiti verso la carta emessa da secondo intermediario, pur essendo rivolti a beneficio di rapporto incardinato presso diverso intermediario, non hanno comunque comportato alcuna perdita economica per il cliente, essendo transitati sulla carta allo stesso intestata.
In ragione di ciò, secondo il consolidato orientamento del Collegio di Milano, è circostanza decisiva che in (tutte) le operazioni c.d. "di provvista" (ancorché a valere su rapporto acceso presso altro intermediario) rileva in modo assorbente la mancanza di un effettivo pregiudizio economico per il cliente. Di conseguenza, in ipotesi simili viene attribuito rilievo esclusivo alle sole operazioni finali che comportano l'effettiva uscita dei fondi verso i truffatori (*ex multis*, Collegio di Milano, decisione n. 9290/2025 e decisione n. 3641/2026).
Tutto ciò considerato, l'accertamento della SCA dovrà riguardare soltanto le operazioni a favore di terzi eseguite tramite carta emessa dal secondo intermediario, che costituiscono l'unico oggetto della domanda restitutoria del cliente.
Ebbene, con riferimento alle azioni antecedenti all'esecuzione delle operazioni contestate, in particolare l'accesso al conto e l'associazione del *device* si osserva quanto segue.
Il secondo intermediario rileva che tutte le operazioni di pagamento contestate sono state autorizzate con parametro biometrico per il tramite del dispositivo mobile associato all'account del ricorrente in data 21 luglio 2024 (*i.e.*, due giorni prima della frode). In particolare, emerge che in tale data sia stato eseguito un accesso del ricorrente in "strong log in" da tale dispositivo mobile e che questo sia stato associato come unico dispositivo per eseguire e autorizzare operazioni di pagamento.
In virtù delle evidenze ricavabili dai LOG e dalle relative indicazioni esplicative, risulta quindi che l'utente ha fatto accesso al conto mediante password (elemento di conoscenza) e OTP sms (elemento

di possesso), con conferma di associazione del *device* nella medesima sessione mediante ulteriore OTP sms (in presenza di analoghi log è stata reputata conforme a SCA la procedura di autenticazione dal Collegio di Milano, con decisione n. 816/2026).
Fermo quanto sopra evidenziato, si osserva che, secondo le dichiarazioni rese dello stesso cliente nei propri scritti difensivi, risulta pacifico che l'operazione di associazione del device in esame sia stata eseguita in maniera genuina dallo stesso cliente, che non denuncia alcun accesso abusivo in questa fase.
Come noto, secondo l'orientamento dei Collegi, eventuali dichiarazioni confessorie del cliente possano assumere valore di prova legale ai sensi dell'art. 2730 c.c., ai fini della prova della corretta autenticazione, che può quindi dirsi pacifica quantomeno rispetto alla descritta fase preliminare.
Quanto agli accessi prodromici all'esecuzione dei bonifici, il secondo intermediario osserva che gli accessi prodromici all'esecuzione dei bonifici del 23 e del 24 luglio 2024 sono avvenuti mediante l'utilizzo del *device* associato (fattore di possesso) con validazione biometrica.
Produce al riguardo evidenza dalla quale si ricava che i Login sono stati effettuati dal device associato tramite inserimento del parametro biometrico (function loginBiometric); l'esito dell'accesso è valorizzato con OK (in presenza di evidenze analoghe, il Collegio di Milano ha ritenuto provata la SCA in sede di login con decisione n. 11352/2025).
Con riferimento alle operazioni contestate il secondo intermediario afferma che l'operazione è stata autenticata tramite device utilizzato dal ricorrente e fattore biometrico.
Al riguardo, produce evidenze dalle quali si ricava che le operazioni risultano autorizzate mediante il *device* associato dal cliente; la validazione tramite fattore biometrico ("*additionalInfo_authType": "bioToken*" che, secondo la legenda fornita, significa che la transazione è stata autenticata mediante l'inserimento del parametro biometrico).
Le operazioni risultano quindi autorizzate con ricorso a un fattore di possesso e a un fattore di inerenza (in presenza di evidenze analoghe, il Collegio di Milano, decisione n. 11352/2025 ha reputato provata la SCA).
Può quindi passarsi all'esame della condotta delle parti e in particolare dei profili rilevanti per la valutazione di sussistenza della colpa grave a carico del ricorrente.
Il cliente afferma che la truffa avrebbe avuto origine da una chiamata proveniente da un numero, apparentemente riconducibile ad utenza ufficiale del primo intermediario; solo in seguito sarebbe pervenuta una ulteriore telefonata da altro numero, non riferibile a detto intermediario.
Produce evidenza del registro chiamate, da cui risultano, il giorno 23.07.2024, chiamate provenienti dal citato numero riferibile al primo intermediario, oltre alla chiamata proveniente da numero non riferibile.
La presenza di chiamate in apparenza riferibili all'intermediario è, come noto, riconducibile al c.d. ID *caller spoofing*, forma di frode ritenuta maggiormente insidiosa rispetto all'ordinario *vishing*. Tuttavia, nel caso di specie, si osserva che la situazione di apparenza riguarda unicamente il primo intermediario, sul cui conto le operazioni, meramente costitutive della provvista, non formano oggetto di domanda restitutoria nel presente procedimento; nessuna apparente riferibilità è invece ascrivibile al secondo intermediario, presso cui sono state eseguite le transazioni contestate.
Il ricorrente ha altresì prodotto evidenza di sms/e-mail relativi alla conferma di contatto con il presunto operatore antifrode e alla "mancata esecuzione" di talune operazioni di bonifico; anche tali

comunicazioni sono apparentemente riferibili al primo intermediario, mentre il secondo intermediario risulta del tutto estraneo.
Peraltro, non può trascurarsi che il cliente ha dichiarato, sia nella denuncia sia nel ricorso, di aver concesso al proprio interlocutore (sedicente operatore antifrode della banca) il controllo da remoto del proprio computer, durante tutto il contatto telefonico durato oltre sette ore; sicché parrebbe verosimile ritenere che i frodatori abbiamo operato a distanza, ad es. inserendo le disposizioni di pagamento poi confermate dall'utente.
Al riguardo si rappresenta che, consentendo l'accesso al PC da remoto, si consente al truffatore l'accesso al conto, con possibilità di inserire le operazioni fraudolente anche senza la necessità di richiedere al cliente informazioni aggiuntive.
Secondo l'orientamento del Collegio di Milano (da ultimo, decisione n. 1011/2026), la circostanza di consentire il controllo remoto di un PC o di un *device* costituisce violazione degli obblighi di custodia e segretezza delle credenziali (cfr. anche Collegio di Milano, decisioni n. 3309/2025; n. 11631/2024).
Non solo: il cliente dichiara di aver visualizzato sullo schermo lo svolgimento di attività (protrattesi per diverso tempo); tuttavia, non si è avveduto di quanto stava in realtà accadendo e della reale operatività realizzata, e non ha contattato gli intermediari, pur affermando di aver nutrito dubbi e perplessità in merito.
Per tutto quanto esposto deve reputarsi configurarsi a carico del ricorrente la colpa grave.
Quanto alla condotta degli intermediari convenuti, entrambi hanno rappresentato e documentato di aver esperito, a seguito della comunicazione della truffa, tentativi di *recall* delle disposizioni.
Quanto alle notifiche di avvenuta esecuzione delle operazioni fraudolente si osserva quanto segue.
Invero le operazioni rientranti nella domanda del cliente e non rimborsate risultano eseguite nelle seguenti date e orari:

- 23.07.2024 ore 15:26;
- 23.07.2024 ore 15:30;
- 23.07.2024 ore 15:32;
- 23.07.2024 ore 16:37;
- 24.07.2024 ore 10:51.

Se quindi le prime tre operazioni a valere sul rapporto acceso presso il secondo intermediario sono state eseguite nell'arco di pochi minuti, la quarta è stata eseguita dopo un'ora e la quinta addirittura il giorno successivo.
Non vi è evidenza dell'attivazione di un servizio di alert che avrebbe potuto consentire al cliente di evitare le ultime due operazioni.
Ebbene, i Collegi sono unanimi nel ritenere che la mancata attivazione del servizio di sms-alert (o altro assimilabile, come notifica tramite app dell'intermediario oppure e-mail, con una valutazione di equivalenza da condurre caso per caso) costituisce in genere un profilo di responsabilità dell'intermediario, salvo l'esplicito rifiuto dell'utente di avvalersene.
La mancata attivazione ovvero il mancato funzionamento del servizio di sms-alert (o di servizio assimilabile) è irrilevante solo nelle ipotesi di più transazioni a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, in quanto la ricezione dell'alert non potrebbe limitare, in questo caso, il pregiudizio dell'utente.
Sotto questo profilo sussiste, dunque, una responsabilità dell'intermediario.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Ulteriore elemento che deve far propendere per una responsabilità concorrente dell'intermediario risiede nella circostanza che la carta tramite la quale sono stati eseguiti i pagamenti oggetto del presente ricorso è abitualmente utilizzata solo per pagamenti di modesta entità ed esigenze ordinarie, mentre nel corso della frode si sono registrati importanti accrediti cui sono seguite le operazioni dispositive oggetto di contestazione, per poco meno di € 40.000,00. A dimostrazione di ciò vi sono gli estratti del conto accesso presso il secondo intermediario prodotti dal ricorrente dal cui esame si rinvengono in effetti, nel periodo interessato, per lo più piccoli pagamenti, operazioni nell'ordine delle decine o centinaia di euro, senza evidenza di disposizioni di importo comparabile a quelle eseguite in occasione della frode perpetrata ai danni del cliente.
La somma che l'intermediario dovrà restituire al cliente a titolo di responsabilità concorrente può essere commisurata all'importo totale delle due ultime operazioni disconosciute, pari a € 10.400,00.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso nei confronti del primo intermediario; accoglie parzialmente il ricorso nei confronti del secondo intermediario e dispone che lo stesso corrisponda alla parte ricorrente la somma di € 10.400,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario soccombente corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE