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 21 gennaio 2026, afferma che:

- in data 27/11/2025 riceveva una telefonata da un numero di telefono riconducibile all'intermediario e una voce registrata gli comunicava che era stato rilevato un tentativo di utilizzo del suo conto corrente e lo invitava a premere il tasto "1" per disconoscere l'operazione;
- premeva il tasto "1" e veniva richiamato da un altro numero riconducibile all'intermediario;
- il sedicente operatore bancario lo invitava ad accedere all'app della banca ove gli inviava una notifica per annullare l'operazione che confermava;
- detta notifica non conteneva alcun dettaglio relativo all'operazione, ma solo la richiesta di confermare l'operazione e la possibilità di scegliere tra sì e no;
- il sedicente operatore gli intimava poi di non accedere al suo conto corrente per le successive 24 ore e gli fissava un appuntamento per il giorno successivo per completare le operazioni;
- successivamente riceveva un SMS di annullamento delle operazioni e si insospettiva;
- contattava dunque il numero verde della banca e apprendeva di essere stato truffato;
- sporgeva dunque denuncia alle Autorità competenti e presentava reclamo all'intermediario che rispondeva negativamente;

- sussiste la responsabilità della banca che: *i)* non ha garantito la sicurezza dei suoi sistemi di comunicazione; *ii)* non ha inviato gli SMS alert relativi alle operazioni eseguite; *iii)* non ha bloccato le operazioni anomale.

Chiede, pertanto, il rimborso della somma sottrattagli pari a € 1.600,00 e il "riconoscimento di eventuali danni subiti – la valutazione delle carenze nei sistemi di sicurezza dell'intermediario".

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

- le operazioni contestate sono state correttamente autorizzate, contabilizzate e registrate;
- il ricorrente non ha fornito spiegazioni chiare né documentazione idonea a ricostruire l'esecuzione della truffa;
- l'orientamento dei Collegi ABF è concorde nel ritenere non accoglibile un ricorso laddove si rilevi la mancata allegazione dei messaggi civetta;
- controparte ha prodotto un unico messaggio apparentemente proveniente da un software per l'invio di SMS massivi, certamente non riconducibile alla banca e non ha allegato il registro chiamate del proprio telefono;
- in ogni caso il fenomeno della manipolazione dei numeri dei mittenti di chiamate e di messaggi tramite programmi di spoofing è da tempo noto e afferisce ai sistemi di comunicazione digitale che sono sotto la sorveglianza, competenza e responsabilità degli operatori del servizio telefonico e non degli intermediari;
- ha inviato al cliente le e-mail di avviso "Inoltro richiesta Bonifico", effettuate in concomitanza all'esecuzione delle operazioni e ha provveduto a bloccare in via precauzionale l'utenza a seguito della chiamata al servizio di assistenza clienti;
- come ripetutamente affermato dalla giurisprudenza ordinaria, non esiste alcun obbligo normativo di monitoraggio ex ante delle operazioni sospette.

Chiede, pertanto, il rigetto del ricorso.

DIRITTO

La controversia ha ad oggetto il disconoscimento di n. 2 operazioni di bonifico istantaneo per un importo complessivo di € 1.600,00, eseguite il 27/11/2025 alle ore 15:11 (€ 1.450,00) e 15:13 (€ 150,00).

È in atti la denuncia del cliente presentata lo stesso giorno.

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.
Con riferimento al caso di specie, i singoli passaggi di autenticazione sono illustrati nella relazione tecnica allegata alle controdeduzioni dell'intermediario.
In via generale tale relazione tecnica spiega che sul conto corrente intestato al cliente è attivo lo schema di autenticazione "S55" che prevede la SCA per l'accesso alla piattaforma di home banking e le disposizioni di pagamento.
In particolare, l'elaborato tecnico indica per le operazioni di login la password come primo fattore di autenticazione e come secondo fattore un "Token monouso One Time Password, OPT", che individua in "PIN, notifica push, QRCODE o riconoscimento tramite biometria".
Le operazioni dispositive, invece, avverrebbero tramite firma dell'operazione tramite un "Token monouso One Time Password, OPT", che individua in "PIN, notifica push, QRCODE o riconoscimento tramite biometria".
In sostanza la relazione tecnica riconduce al Token monouso One Time Password (OTP) fattori considerati elementi di conoscenza (PIN), possesso (push) e inerenza (biometria), senza tuttavia specificare quale sia la modalità in concreto adottata dall'utente.
Dai log allegati, d'altra parte, non si ricava la prova del doppio fattore di autenticazione con riferimento a ciascuna delle fasi delle operazioni contestate.
In particolare, per quanto riguarda l'autenticazione relativa alla fase di accesso al conto corrente, che secondo l'intermediario dovrebbe essere stato autorizzato con l'inserimento della password la firma OTP consistente in una notifica push ricevuta sul device del cliente, le evidenze prodotte appaiano poco chiare.
Infatti dai LOG emerge quanto segue:

- il giorno 27/11/2025 alle ore 14:59 risulta effettuato un login dal canale=dekstop e dal codice cliente n. **542;
- Il codice id risulta riferibile al cliente, ma non vi sono riferimenti univoci al device utilizzato;
- l'esito dell'autenticazione è valorizzato con esito ok;
- risulta l'applicazione della SCA tramite schema di autenticazione S55 (allegato 5, colonna Q), che stando alla legenda esplicativa fornita dall'intermediario sta ad indicare l'inserimento della password e dell'OTP;
- nel log hubautenticazione-06045K2542 (allegato 5 controdeduzioni) risultano alcuni campi valorizzati con PASSWORD (1° fattore di autenticazione) e alcuni campi valorizzati con la dicitura OTP_SIGNATURE_PAYLOD (2° fattore di autenticazione);
- per i campi valorizzati con password, la colonna W- autenticazione terminata riporta l'esito false, mentre per i campi valorizzati con OTP_SIGNATURE_PAYLOD la cella W24 è valorizzata con true.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Secondo l'intermediario la dicitura OTP_SIGNATURE_PAYLOD indica una One Time Password nella forma di notifica push, QRCODE o riconoscimento tramite biometria e l'accesso al conto corrente, nel caso di specie sarebbe stato autorizzato con notifica push.
Nel file di log si riscontra la presenza di un login successivo delle ore 15:05 (precedente quindi alle operazioni dispositive delle ore 15:11 e 15:13) eseguito da un dispositivo mobile in Trentino e quindi, verosimilmente dal cliente ma l'intermediario nulla dice in merito a tale accesso. Non è dunque possibile stabilire se tale accesso sia stato prodromico/necessario solo per autorizzare le operazioni dispositive, come del resto parrebbe dalle dichiarazioni rilasciate dal cliente in sede di denuncia.
Sul punto si osserva che, invece, la relazione tecnica indica OTP_SIGNATURE_PAYLOD come secondo fattore sia per l'accesso al conto che per le operazioni dispositive. Se l'accesso al conto dal dispositivo mobile fosse necessario per l' OTP_SIGNATURE_PAYLOD, i LOG ne avrebbero dovuti indicare 2 (uno per l'acceso e uno per le operazioni di bonifico), invece ve ne è uno solo.
Questo Collegio, in linea con l'orientamento consolidato dell'Arbitro, ritiene che in caso di difetto di piena prova sull'autenticazione delle transazioni disconosciute il ricorso deve essere accolto integralmente, posto che la mancanza anche parziale 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.
Solo *ad abundantiam* si osserva che la prova della SCA non è raggiunta neppure con riferimento all'esecuzione dei bonifici contestati, per i quali l'intermediario non ha specificato come il cliente avrebbe autorizzato le notifiche push, né ha indicato il riutilizzo della password utilizzata come elemento di conoscenza per l'accesso al conto. In proposito si rammenta che il più recente orientamento del Collegio di Milano esclude la valutazione di riutilizzabilità del fattore del login in assenza di espresse dichiarazioni dell'intermediario (in questo senso, cfr. Collegio di Milano, decisione n. 9784/25). Inoltre, non vi sono riferimenti univoci al device.
Tutto quanto esposto deve concludersi per l'accoglimento della domanda di rimborso, mentre non può reputarsi fondata la richiesta di danni per la sua totale vaghezza (i danni vengono dallo stesso ricorrente descritti come "eventuali", dunque non vi è neppure certezza del loro verificarsi).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.600,00.
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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE