

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BARENGHI	Membro designato dalla Banca d'Italia
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) D'ANGELO	Membro di designazione rappresentativa dei clienti

Relatore GIAN LUCA GRECO

Seduta del 09/03/2026

FATTO

Il ricorrente chiede la restituzione della somma di € 5.474,00, corrispondente all'importo di operazioni di pagamento asseritamente fraudolente.

La parte ricorrente ha affermato:

- che, in data 25/08/2025, ha subito una grave frode bancaria sul suo conto iban n. LT77***4987;
- che, dopo alcune notifiche di pagamenti annullati, è stata contattata dal numero ufficiale clienti dell'intermediario +370***608 e che il sedicente operatore A.G., tramite *SMS spoofing*, lo ha indotto a convalidare pagamenti, disporre bonifici di sicurezza, bloccare e sostituire la carta n. 4138***6173;

- che, dopo un'ora e trenta minuti, comprendeva l'inganno, interrotto la chiamata e bloccato tutte le carte;
- che la frode perpetrata - per un totale di € 5.474,00 - è avvenuta a causa della vulnerabilità dei sistemi di comunicazione dell'intermediario;
- che ha segnalato la vicenda alla Polizia Postale e presentato reclamo formale all'intermediario, tuttavia quest'ultimo ha risposto negativamente, sostenendo che il ricorrente aveva autorizzato le operazioni contestate;
- che l'intermediario non ha garantito la sicurezza dei suoi canali e, pertanto, ha violato il dovere di tutela dei depositi;
- che le autorizzazioni sono state estorte tramite raggiro a seguito di *spoofing*;
- che ha riscontrato online alcuni casi analoghi e che, in particolare, ricorre un precedente ABF simile - a favore di una sua familiare - conclusosi con il rimborso alla parte ricorrente.

L'intermediario, nelle controdeduzioni, ha rappresentato:

- che le operazioni oggetto di contestazione sono due pagamenti e sette operazioni di prelievo;
- che, in particolare, il pagamento di € 470,00 in favore di B.I. effettuato con carta n. ***3221 è stato autorizzato dal ricorrente, non potendo trovare applicazione la disciplina prevista dalla PSD2;
- che l'autenticazione dell'operazione di € 470,00 comprende una notifica *push* inviata dall'app sul dispositivo registrato dal cliente, nonché contestuale accesso al conto mediante app realizzato con riconoscimento biometrico dell'impronta digitale;
- che, in seguito alla predetta operazione, è stata inviata sul dispositivo registrato dal ricorrente una notifica *push* riportante l'ammontare speso;
- che il pagamento in favore di B.I. è stato altresì eseguito in ossequio ai Termini e alle Condizioni Personali di Contratto;
- che, con riferimento ai n. 7 prelievi per un totale di € 3.464,00 e al pagamento di € 1.540,00 in favore di G. effettuati con carta n. ***6173, il ricorrente ha permesso ai truffatori di accedere al proprio conto e di collegare liberamente lo strumento di pagamento;
- che la carta n. ***6173 era già in possesso dei truffatori, i quali la avevano precedentemente acquisita mediante i distributori automatici di carte e poi attivata con la collaborazione dell'utente;
- che il ricorrente ha rispettivamente fatto accesso al conto mediante riconoscimento biometrico dell'impronta digitale, attivato la carta, associato la carta al suo codice id, visualizzato sull'app e comunicato il codice PIN della carta ai truffatori;
- che il pagamento di € 1.540,00i e i prelievi contestati sono stati regolarmente eseguiti con il dispositivo del cliente tramite l'uso fisico del chip della carta e del suo codice PIN;
- che tali circostanze risultano altresì confermate dalle dichiarazioni rese dal ricorrente in sede di denuncia;
- che, nonostante non gravi sull'intermediario un obbligo di monitoraggio ex ante delle operazioni sospette, durante l'esecuzione di operazioni di pagamento tentate, ha inviato degli *alert* di prevenzione frode al ricorrente, che tuttavia ha sbloccato manualmente i pagamenti;

- che le circostanze fattuali dimostrano una condotta connotata da gravissima negligenza da parte del ricorrente, il quale ha dato seguito alle richieste anomale del suo interlocutore, nonostante l'irragionevole finalità della telefonata (attivazione di protocolli antifrode);
- che la frode rientra nella tipica ipotesi nota come *impersonation scam*, che il ricorrente avrebbe potuto evitare usando l'ordinaria diligenza, dato che si tratta di truffa nota e di cui parlano anche i mezzi di informazione pubblica;
- che, inoltre, il fenomeno delle truffe online è oggetto di un'apposita pagina sul suo sito web della banca facilmente accessibile a chiunque;
- che la condotta del ricorrente non poteva essere prevista né evitata, pur avendo l'intermediario adottato tutte le idonee misure di sicurezza esigibili nell'adempimento della prestazione dovuta;
- che la telefonata proveniente da un'utenza con prefisso lituano apparentemente riconducibile all'intermediario non costituisce indice sintomatico della sua responsabilità.

Nel replicare alle controdeduzioni, la parte ricorrente ha precisato:

- che l'intera vicenda truffaldina deriva da una falla organizzativa della banca, in quanto il numero ufficiale dell'assistenza dell'intermediario è stato oggetto di *spoofing*, consentendo così ai sedicenti operatori della banca di carpire la sua fiducia;
- che la diffusione delle frodi impone all'intermediario più elevati doveri di diligenza professionale, non essendo corretto allocare sull'utente il c.d. "rischio tecnologico";
- che, appena compreso il raggio, ha provveduto a bloccare le carte e a sporgere denuncia;
- che poiché il sistema di sicurezza è stato compromesso a monte dall'impersonificazione del canale di assistenza, l'intermediario avrebbe dovuto blindare il canale di comunicazione;
- che l'assenza o l'inefficacia dei presidi organizzativi integra inadempimento degli obblighi di sicurezza e dei doveri di correttezza/buona fede;
- che, a supporto delle sue argomentazioni, ricorrono la normativa e precedenti giurisprudenziali.

L'intermediario, nelle controrepliche, richiamando quanto già indicato nelle controdeduzioni e insistendo per l'accoglimento delle proprie conclusioni, specifica altresì:

- che non sussiste alcuna falla nei sistemi di sicurezza dell'intermediario in quanto le transazioni tentate sono state poste in essere autonomamente dai truffatori, i quali riescono a carpire da differenti siti online i dati che gli utenti inseriscono e a eseguire le transazioni stesse;
- che, poiché l'importo delle transazioni civetta è inferiore a € 30,00 e dunque non è previsto l'obbligo di autenticazione forte del cliente in quanto operazioni di modesta entità, la presenza di tali operazioni non può in alcun modo essere interpretata come segnale di vulnerabilità o malfunzionamento del sistema di sicurezza;
- che, considerato che non sussiste a proprio carico alcun obbligo di monitoraggio con conseguente blocco preventivo di operazioni potenzialmente anomale, nessuna carenza organizzativa può essere imputata all'intermediario anche in ragione della corretta predisposizione e tempestiva attivazione dei sistemi *alert*.

Ciò posto, la parte ricorrente domanda il rimborso della somma di € 5.474,00.
In sede di repliche, parte ricorrente domanda in via subordinata il riconoscimento della franchigia di legge e ogni ulteriore misura di equità ritenuta congrua.
L'intermediario resistente chiede il rigetto del ricorso, con accertamento della corretta autenticazione delle operazioni contestate.
In via subordinata, chiede di accertare e dichiarare la colpa grave del ricorrente nell'aver effettuato e consentito l'esecuzione delle operazioni con conseguente esclusione della responsabilità in capo all'intermediario.

DIRITTO

La controversia ha ad oggetto n. 9 operazioni per un totale di € 5.474,00 eseguite con due diverse carte di pagamento tra le ore 15:11 e le ore 16:43 del 25/08/2025.

In particolare,

- n. 1 pagamento online di € 470,00 in favore di B.I. eseguito alle ore 15:11 del 25/08/2025 con carta n. ***3221 associata al conto n. LT77***4987;
- n. 7 prelievi eseguiti presso Santa Maria L tra le ore 16:03 e le ore 16:09 del 25/08/2025 con carta n. ***6173 associata al conto n. LT77***4987, di cui: n. 1 prelievo di € 506,00 (comprensivo di € 6,00 a titolo di commissione), n. 5 prelievi di € 510,00 ciascuno (comprensivi di € 10,00 a titolo di commissione per ogni prelevamento) e n. 1 prelievo di € 408,00 (comprensivo di € 8 a titolo di commissione);
- n. 1 pagamento di € 1.540,00 in favore di G. sito in Torre del Greco (NA) eseguito alle ore 16:43 del 25/08/2025 con carta n. ***6173 associata al conto n. LT77***4987.

Circa i fatti, la parte ricorrente ha riferito nella denuncia che, per quanto sia stata vittima di un raggiri da parti di terzi (in particolare, con la tecnica del *Caller ID spoofing* ed *SMS spoofing*), ha personalmente disposto le operazioni oggetto del presente ricorso, sia mediante bonifici che mediante la creazione di una carta virtuale.

In considerazione del fatto che il ricorrente ha ammesso di aver personalmente dato il consenso all'esecuzione delle operazioni, per quanto sotto la pressione truffaldina, il Collegio ritiene che non dovrebbe qui porsi la questione circa la prova dell'autenticazione delle operazioni contestate (che peraltro, dalle evidenze documentali versate in atti, risulterebbe comunque effettuata in modo conforme a quanto normativamente richiesto in relazione all'autenticazione forte del cliente). In altre parole, l'esistenza del consenso del pagatore al compimento di operazioni on line poi disconosciute esclude che possa venire in rilievo quanto disposto dal d.lgs. 11/2010 con riguardo alle conseguenze sul piano giuridico del difetto di autorizzazione, per cui il Collegio non può che rigettare la richiesta di rimborso delle predette operazioni.

Alla medesima conclusione il Collegio giungerebbe anche considerando i prelievi in controversia come non interamente eseguiti dalla parte ricorrente, alla luce della condotta gravemente colposa dalla stessa tenuta nella custodia delle credenziali.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE