

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 GIUSEPPE SPENNACCHIO

Seduta del 10/12/2025

FATTO

La parte ricorrente chiede la restituzione della somma di €. 9.800,00= corrispondente all'importo di un'operazione di pagamento fraudolenta. Ha proposto reclamo in data 8 giugno 2025 nei confronti dell'intermediario, che vi ha dato riscontro negativo.

Afferma che in data 28 maggio 2025, intorno alle ore 17:33, rimaneva vittima di un vero e proprio attacco di *spoofing*, da parte di sedicenti operatori antifrode. Infatti veniva contattato da un numero riconducibile al contatto ufficiale di altro intermediario, e veniva informato di probabili connessioni anomale sul conto presso tale intermediario. Poiché la chiamata era confusionaria, per convincerlo lo richiama da un numero apparentemente riconducibile alla Polizia Postale. Tuttavia, poiché ancora non era convinto, i truffatori lo contattavano nuovamente da un numero della resistente, inducendolo così a cadere nella truffa ed a seguire le indicazioni del sedicente operatore.

Alle ore 19:03 del medesimo giorno riceveva una seconda telefonata dal sedicente operatore che lo avvisava di non operare sul conto fino alle ore 11:30 del 29 maggio 2025. Dopo quest'ultimo contatto, ipotizzando di essere stato vittima di una truffa, chiamava il *call center* della resistente, segnalando l'accaduto e diffidando l'istituto di pagamento dall'eseguire eventuali operazioni di pagamento disposte.

Tuttavia, nonostante si fosse tempestivamente attivato, si avvedeva che alle ore 17:50 gli era stata sottratta la somma di €. 9.800,00=. Date le modalità della truffa e la sofisticatezza della stessa, non può essergli attribuita alcuna colpa grave.

L'istituto di credito deve adottare la diligenza dell'accorto banchiere. La resistente è responsabile per il mancato storno dell'operazione di bonifico nonostante l'immediata segnalazione da lui effettuata.

Inoltre, il bonifico è stato disposto in contrasto con quanto compare in evidenza sul sito della banca circa il limite massimo di importo di €. 1.000,00= per ogni operazione.

L'intermediario ha l'obbligo di adottare degli accorgimenti adeguati a prevenire l'illecita captazione di dati attraverso il *vishing*, onde evitare accessi non autorizzati.

Sussiste, pertanto, la responsabilità contrattuale ed extracontrattuale ai sensi dell'art. 2050 c.c.

L'intermediario, nelle controdeduzioni, rappresenta:

- che dalla descrizione di quanto occorso è possibile evincere come il ricorrente sia titolare di un conto corrente presso la resistente, aperto in data 11 novembre 2022 e successivamente modificato con proposta di modifica unilaterale del contratto, inviata in data 15 maggio 2023;
- che l'operazione disconosciuta dal ricorrente è stata correttamente autorizzata mediante l'utilizzo delle credenziali statiche e dinamiche in possesso dello stesso cliente con autenticazione forte a due fattori, senza aver subito le conseguenze di alcun malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti;
- che parte ricorrente non ha fornito prova alcuna della truffa subita, non allegando in atti prova della chiamata asseritamente ricevuta;
- che, inoltre, il ricorrente ha fornito al falso operatore le proprie credenziali, condividendo i codici OTP a seguito di *vishing* ed incorrendo, dunque, in colpa grave;
- che, grazie alla proattività della banca, i clienti hanno a disposizione il servizio di *sms alert*;
- di aver predisposto un'ulteriore misura di protezione per assicurare ai propri clienti di avere sempre la certezza di essere realmente in contatto con la banca, tramite l'invio di una notifica in app, nella sezione "I miei messaggi";
- che una volta posti a conoscenza dalla banca della sussistenza di tali tipologie di truffe, mediante campagne informative, i clienti sono in grado di evitarle, mentre l'istituto di credito non può evitare o bloccare telefonate truffaldine della specie.

L'intermediario resistente chiede di rigettare il ricorso del ricorrente per infondatezza del medesimo.

DIRITTO

La controversia è regolata pienamente dalla disciplina in materia di servizi di pagamento, in particolare dalle norme relative all'autenticazione di operazioni di pagamento disposte *on line*, nonché all'onere della prova di autenticazione di tali operazioni in capo all'intermediario ed alla responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento (artt. 10, 10-bis e 12, d.lgs. 27 gennaio 2010, n. 11 modificato a seguito dell'entrata in vigore del d.lgs. 15 dicembre 2017, n. 218, di recepimento della Dir. UE 2366/2015 relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al Reg. UE n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta, e Regolamento Delegato UE n. 389 del 27 novembre 2017). Si rammenta

che, secondo la posizione consolidata dell'ABF, la disciplina sopra citata prevede un regime probatorio di favore per l'utente di strumenti e servizi di pagamento.

In particolare, l'art. 10, d.lgs. n. 11/2010, prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento, una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare, innanzitutto, l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la loro esecuzione o di altri inconvenienti. Secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo, l'antecedente logico rispetto alla prova della colpa grave dell'utente.

In secondo luogo, il PSP è tenuto a dimostrare il comportamento gravemente colposo dell'utilizzatore.

L'operazione contestata consiste in un bonifico di €. 9.800,00=, disposto in data 28 maggio 2025, alle ore 16:29. Tale operazione risulta dal dettaglio del pagamento.

A fronte di evidenze informatiche e documentali prodotte dall'intermediario, il Collegio ritiene che l'autenticazione dell'operazione contestata sia stata debitamente provata e che il sistema di pagamento adottato dal PSP, tenuto conto dell'utilizzo dei fattori di autenticazione indicati in atti, sia conforme a quanto normativamente richiesto in relazione all'autenticazione forte del cliente. Nel caso di specie, infatti, l'intermediario ha riferito e comprovato che l'operazione contestata è stata autenticata tramite *username* e *password* (elemento di conoscenza), nonché codice OTP inviato via sms (elemento di possesso), previo accesso, a sua volta completato tramite le suddette credenziali personali di sicurezza (elemento di conoscenza) e codice OTP, anche in questo caso inviato via sms al numero di cellulare certificato del cliente (che integra l'elemento di possesso).

Nello specifico, sulla prova della corretta autenticazione dell'operazione contestata, l'intermediario ha prodotto le seguenti evidenze. Alle 16:08:16 è stato registrato accesso da web con autenticazione forte mediante inserimento di *username*, *password* e codice OTP (come si evince dalla colonna "*Auth Method Code*"), ricevuto tramite sms sul numero di cellulare univocamente associato al conto corrente del ricorrente.

Alle 16:29:28 veniva disposto ed eseguito un bonifico di €. 9.800,00=, tramite accesso con autenticazione forte all'area riservata, mediante inserimento di *username*, *password* e codice OTP (colonna "*Auth Method Code*") ed autorizzazione e conferma codice OTP (come si evince dalla colonna "*Strong Auth Code*"), ricevuto tramite sms sul numero di cellulare univocamente associato al conto corrente del cliente.

Senonché la prova dell'autenticazione, registrazione e contabilizzazione dell'operazione disconosciuta non esenterebbe di per sé sola l'intermediario da responsabilità: la previsione di cui all'art. 10, comma 2, d.lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretata nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente ad indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione, dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente.

Dalle dichiarazioni della parte ricorrente sembrerebbe che l'operazione contestata sia scaturita da un fenomeno di asserito *spoofing* applicato alla telefonata (c.d. *Caller ID spoofing*), realizzato ai danni della medesima. Il ricorrente nel ricorso ha dichiarato, in

sintesi, di aver ricevuto una telefonata dalla banca con cui gli veniva comunicato un accesso anomalo al suo conto e veniva informato che sarebbe stato contattato da un operatore della Polizia Postale.

Il Collegio rileva, altresì, che a sostegno di quanto dichiarato il ricorrente non ha fornito né la denuncia sporta alle autorità (cui le parti fanno riferimento) né eventuale evidenza delle chiamate ricevute.

Dalle evidenze in atti risulta che il blocco completo dell'accesso al conto corrente è avvenuto in data 28 maggio 2025, alle ore 22:03. Il blocco temporaneo dello stesso risulta, invece, avvenuto alle ore 17:50, come risulta dai log e dalla copia della notifica via e-mail allegata dal ricorrente.

Parte resistente ha dichiarato di offrire un sistema di *alert* alla propria clientela. L'operazione contestata è una soltanto, in quanto i due successivi tentativi di bonifico risultano negati.

Secondo la posizione condivisa dei Collegi, che si fonda su un'interpretazione sostanzialistica, è irrilevante la mancata attivazione ovvero il mancato funzionamento del servizio di *sms alert* (o di servizio assimilabile) nei casi in cui la ricezione dell'*alert* non possa in concreto limitare il pregiudizio dell'utente, ossia nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più transazioni ma a distanza di pochi minuti l'una dall'altra e, complessivamente, in un arco di tempo limitato.

Per completezza, si evidenzia che parte ricorrente ha inoltre lamentato la violazione, da parte dell'intermediario, della normativa *privacy*, avendo la banca consentito l'accesso a terzi ai dati del cliente. In merito si evidenzia che, da quanto dichiarato dalla parte ricorrente, risulta che la stessa ha risposto ad una telefonata civetta ed ha poi seguito le indicazioni del truffatore.

Vero è, dunque, che nel ricorso parte ricorrente sostanzialmente ammette di aver "abboccato" al raggio, comunicando al truffatore i codici di accesso alle funzionalità bancarie da remoto e che, da quanto appena riepilogato, la manovra fraudolenta eseguita a suo danno non risulta aver raggiunto un grado elevato di insidiosità.

Secondo gli orientamenti condivisi dei Collegi ABF, nelle fattispecie di *spoofing*, ricorrente sia nel caso di sms o telefonata che si inseriscano in una "conversazione" o *chat* precedente con l'intermediario, sia quando sussista un singolo messaggio civetta o una singola chiamata che sembri provenire dall'intermediario, non è generalmente ravvisabile la colpa grave del ricorrente, data l'insidiosità del meccanismo di aggressione e nonostante la maggiore diffusione di campagne informative sul tema. Tuttavia, qualora il testo del messaggio civetta o la provenienza della chiamata presentino indici di evidente inattendibilità o di anomalia (che portino ad una inequivoca non riconducibilità all'intermediario), che dovrebbero far allertare l'utente avveduto, è stato ritenuto che possa rilevarsi un concorso di colpa a suo carico per aver agevolato il compimento della truffa.

Differentemente, la mancata allegazione del messaggio civetta ovvero del registro chiamate, da parte del cliente (come nel caso di specie), determina il rigetto del ricorso, in quanto non consente di verificare se il mittente o il chiamante risultino riconducibili all'intermediario e, pertanto, possibile un legittimo affidamento dell'utente circa la genuinità del contatto.

Nel caso di cui si tratta, dunque, valutate tutte le circostanze, il Collegio ritiene che al cliente vada interamente attribuita la responsabilità per la somma indebitamente sottratta.

P.Q.M

Il Collegio non accoglie il ricorso.

IL PRESIDENTE