

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) SPAGNOL	Membro di designazione rappresentativa degli intermediari
(TO) COCCIA	Membro di designazione rappresentativa dei clienti

Relatore ALESSANDRA SPAGNOL

Seduta del 08/04/2026

FATTO

Dopo aver presentato, in data 29.9.2025, reclamo non riscontrato dall'intermediario, la parte ricorrente ha proposto reclamo all'ABF affermando:

- di aver subito, in data 17.09.2025, alle ore 20:05, una frode bancaria per un importo di € 4.992,00;
- di essere stata ingannata da una notifica verosimile, inviata da un'applicazione software con logo identico a quello della banca;
- di aver agito prontamente, bloccando il conto corrente e la carta di debito ad esso associata;
- di aver presentato denuncia alle autorità in data 18.09.2025 alle ore 11:17;
- di aver posto in essere tutte le azioni che oggettivamente escludono la colpa grave;
- di aver avuto - dall'apertura del conto corrente fino al momento della frode - una spesa media mensile sul conto corrente di € 627,24;

- che l'operazione bancaria fraudolenta risultava oggettivamente anomala, essendo superiore di ben otto volte a tale importo;
- che non ha ricevuto alcun sms, né di conferma specifica dell'operazione né di alert;
- che la tecnica fraudolenta perpetrata è nota ai prestatori dei servizi di pagamento;
- che la banca deve adottare tutte le misure necessaria alla prevenzione delle frodi con appropriate misure tecniche per garantire la sicurezza del sistema;
- che l'istituto, non inviando l'sms di alert, è venuto meno ad un dovere di base di informazione e prevenzione;
- che tali eventi sono da ricondurre al rischio di impresa.

Su tali assunti parte ricorrente ha chiesto il rimborso della somma di € 4.992,00 ed il ristoro di € 20,00 per le spese di procedura.

Nelle proprie controdeduzioni l'intermediario ha contestato la pretesa della ricorrente osservando ed eccependo che:

- la banca ha tentato, in data 19/09/2025, il recupero delle somme sottratte, ricevendo tuttavia il cut off delle richieste da parte della banca ricevente, in data 24/09/2025, per mancanza fondi;
- che la frode rientra in una tipologia di truffa diffusa, riconducibile allo spoofing/SMS phishing, non imputabile a falle dei sistemi bancari;
- che il cliente ha riferito di aver contattato, volontariamente, un numero di telefono non riconducibile alla banca e di aver parlato con un sedicente operatore del quale ha seguito le istruzioni telefoniche, autorizzando così l'operazione di bonifico;
- che non sono state fornite prove documentali (SMS o chiamate) utili a verificare l'effettiva dinamica dei fatti;
- che è onere della parte ricorrente identificare con estrema chiarezza e con la dovuta allegazione l'oggetto della contestazione;
- che la mancata produzione del messaggio "civetta" è motivo di rigetto del ricorso;
- che, presumibilmente, la parte ricorrente è rimasta vittima di sms spoofing;
- che, nei mesi di aprile e settembre 2025, aveva inviato ai propri clienti una notifica push relativa alle frodi "autoinflitte" e che le medesime informazioni sono reperibile sul sito della banca nella sezione "Sicurezza";
- che il cliente, pur convinto con un raggirio, ha eseguito autonomamente l'operazione tramite il proprio internet banking;
- che il bonifico è risultato formalmente regolare, con corretta autenticazione, validazione, registrazione e contabilizzazione, e senza che siano state riscontrate anomalie;
- che, nello specifico, il bonifico è stato regolarmente eseguito previo accesso all'App ufficiale della banca, attiva sullo smartphone del cliente, validato tramite Pin applicativo e confermato con MPIN;
- che, trattandosi di bonifico SEPA eseguito alle ore 19:28, lo stesso era annullabile direttamente dal cliente fino al cut off (ore 20) o chiamando il numero verde riportato nell'SMS inviato;
- che, realisticamente, l'intenzione del ricorrente era quella di effettuare la disposizione di bonifico sulle coordinate iban che gli sono state fornite seguendo le indicazioni del sedicente operatore, il tutto senza porsi il minimo dubbio in corso d'opera sulla correttezza della disposizione che stava eseguendo;

- che, alla luce di quanto esposto, non sussiste alcun elemento o mancanza imputabile alla banca tale da determinare una responsabilità della stessa per l'accaduto denunciato e per la perdita patrimoniale verificatasi, tenuto anche conto che il sistema di autenticazione in uso risulta conforme alla PSD2.
L'intermediario ha, quindi, concluso chiedendo il rigetto del ricorso.

DIRITTO

Va, anzi tutto, inquadrato il paradigma normativo in cui si inserisce la questione sottoposta al Collegio. L'utilizzo fraudolento è disciplinato dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta. 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, essendo "ispirata al principio del "rischio d'impresa", e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi" (così Collegio di coordinamento, decisione n. 3498/2012).

In particolare, l'art. 10 del d.lgs. 11/2010 prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento (PSP), una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare: (i) l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti. In particolare, 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 (o dolo) dell'utente; (ii) il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni). Chiarito ciò, l'operazione contestata consiste in un bonifico ordinario di € 4.992,00 eseguito in data 17/09/2025 alle ore 19:28 e l'intermediario ha riferito e dimostrato che l'operazione contestata è stata autenticata tramite l'App di Mobile Banking ed autorizzate con l'inserimento del PIN da dispositivo genuino, secondo un sistema a doppio fattore di autenticazione come richiesto dalla PSD2. In particolare, in linea con gli orientamenti dei Collegi sul punto (cfr. Collegio di Bologna, decisione n. 6207/25, Collegio di Milano, decisione n. 1867/23, Collegio di Bari, decisione n. 1691/2023 e Collegio di Torino, decisione n. 2624/24), è stato provato per l'accesso in App (1) l'elemento di possesso: App Mobile installata sul device certificato e (2) l'elemento di conoscenza: codice PIN in App e per quanto attiene alle singole operazioni (3) l'elemento di possesso: App Mobile installata sul device certificato e (4) l'elemento di conoscenza: codice PIN in App.

Dalla documentazione agli atti risulta che l'operazione contestata è scaturita da un fenomeno di sms spoofing realizzato ai danni di parte ricorrente. Nel ricorso, infatti, la stessa, pur non producendo il messaggio civetta, ha riferito di essere stata ingannata

da una “notifica verosimile inviata da un’applicazione software con logo replicato identico a quello ufficiale dell’Istituto di Credito” a seguito della quale la parte (i) ha contattato il numero indicato nel messaggio ricevuto (ii) ha seguito le indicazioni impartite dal sedicente operatore, fornendogli anche un codice richiesto (iii) al termine della chiamata, si accorgeva dell’esecuzione del bonifico in contestazione (iv) il giorno successivo, dopo essere stata ricontattata dal medesimo soggetto, che le riferiva che era in corso un ulteriore bonifico, si insospettiva e contattava la propria banca, redendosi conto soltanto a quel punto di essere stata vittima di una truffa. Va detto, inoltre, che, oltre a non essere stato prodotto da parte della ricorrente il messaggio civetta come già precisato (circostanza che secondo l’orientamento dei Collegi determina il rigetto del ricorso, cfr. Collegio di Torino, decisioni nn. 1041/2022, 6054/21, 10578/21, 10870/21), il numero di telefono che sarebbe stato indicato da detto messaggio e che parte ricorrente ha utilizzato nel caso in esame non è affatto riconducibile all’intermediario. Inoltre, come eccepito dall’intermediario, è pacifico che l’operazione dispositiva è stata correttamente autorizzata, inserita e finalizzata direttamente dal cliente sul device a lui associato in maniera univoca e che, per ciò, l’operazione non può essere considerata “non autorizzata”: secondo gli orientamenti pacificamente condivisi dai Collegi (Collegio di Torino, decisione n. 10900/24, Collegio di Torino, decisione n. 10071/2024, Collegio di Roma, decisione n. 2414/23, Collegio di Milano, decisione n. 2038/2023, Collegio di Bologna, decisione n. 4499/2023), quando l’operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione) deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2 e rientrano in questa fattispecie anche le operazioni eseguite seguendo le indicazioni del frodatore senza la consapevolezza di disporre una transazione (ad esempio, le operazioni cd. “sotto dettatura”). Il ricorso conseguentemente deve essere rigettato. Le ulteriori contestazioni e domande della parte ricorrente risultano, pertanto, assorbite.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE F.F.