

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) CARATOZZOLO	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 14/10/2025

FATTO

Parte ricorrente riferisce quanto segue:

- di aver ricevuto, in data 11 dicembre 2024, alle ore 18:22, sulla propria utenza telefonica un messaggio da parte dell'intermediario, apparentemente autentico e posto in coda a precedenti messaggi genuini;
- di aver contattato il numero telefonico indicato nel messaggio e di essersi interfacciata con un sedicente operatore bancario che, spaventandola, le riferiva la necessità di bloccare urgentemente un bonifico che ignoti stavano disponendo a valere sul suo conto corrente;
- che ha seguito le istruzioni ricevute dal malvivente;
- che, in particolare, si è resa conto solo al termine della telefonata di essere stata vittima di un caso di *spoofing*, dal quale era conseguito l'azzeramento del suo conto corrente;
- di aver inviato reclamo e modulo di disconoscimento dell'operazione all'intermediario, ottenendo riscontro negativo e generico;
- di aver ricevuto, quale riscontro al proprio reclamo, in data 6 maggio 2025, un'ulteriore e-mail dall'intermediario, inadeguata ed inconferente, tenuto conto della mancata indicazione dell'indirizzo IP del dispositivo dal quale il truffatore aveva eseguito le operazioni, elemento essenziale per una valutazione completa dell'accaduto;
- che tale reticenza dimostra altresì la scarsa attenzione dell'intermediario rispetto alla questione in esame e un suo maldestro tentativo di nascondere la negligente omessa attuazione dei controlli necessari;

- che tale negligenza risulta ancor più evidente tenuto conto dell'esecuzione di un'operazione di bonifico di € 1.200,00, valore anomalo rispetto alla sua normale operatività e del saldo del suo conto corrente, azzeratosi a seguito della medesima;
- che il finto operatore era riuscito ad entrare nel suo conto corrente senza la sua autorizzazione e a disporre la transazione in esame da un dispositivo appena associato, accreditandola in favore di un IBAN che non era mai stato utilizzato;
- di aver ricevuto riscontro negativo dalla banca sulla base della contestabile affermazione secondo cui l'eventuale dislocazione differente da quella solitamente abbinata al *device* in uso non è di per sé un elemento tale da far scaturire azioni di blocco o sospensive dell'operatività, considerato che per attivare un nuovo *device* è necessaria la presenza contemporanea dei due dispositivi nello stesso luogo, circostanza questa che rende evidente la sua mancata autorizzazione alla modifica del *device*;
- che una spiegazione dell'accaduto è da ricercare nel fatto che i truffatori abbiano avuto accesso ad informazioni specifiche e riservate sfruttando gli scarsi controlli della banca;
- di aver diritto al rimborso di quanto fraudolentemente prelevato in quanto per prevenire frodi della specie non sono sufficienti mere campagne di sensibilizzazione e di formazione in favore della clientela;
- che non è ipotizzabile che, in determinati momenti, i clienti vadano a consultare le e-mail antifrode ricevute dall'intermediario o accertino l'eventuale esistenza del c.d. bollino di sicurezza;
- di non essere stata sprovveduta, in quanto ogni giorno vengono perpetrate moltissime frodi a danno di soggetti che, pur essendo sufficientemente istruiti ed attenti, i truffatori riescono a convincere perché posti in una posizione mentale ed emotiva che abbassa sensibilmente le loro capacità di difesa;
- di aver subito la truffa da parte del finto operatore della resistente perché l'intermediario non ha attivato i necessari presidi tecnologici (ad esempio, verifica del luogo di accesso del nuovo dispositivo, dell'IBAN di destinazione, della coerenza dell'operazione con quelle abitualmente realizzate e blocco di un bonifico istantaneo su un dispositivo appena associato);
- che tutti i presidi tecnologici a disposizione degli istituti di credito debbono comunque essere attuati dall'intermediario, in un'ottica di buona fede e tutela della clientela, anche se non esiste un obbligo per la banca di monitorare e sospendere i pagamenti in caso di anomalia degli stessi.

L'intermediario resistente chiede all'ABF il rigetto del ricorso, sulla scorta dell'autenticazione forte dell'operazione contestata e della colpa grave di parte ricorrente. La parte ricorrente, in sede di repliche alle controdeduzioni, si riporta sostanzialmente a quanto dedotto in sede di ricorso, insistendo per l'accoglimento del medesimo e precisando:

- come la parte resistente dia atto, tramite le proprie controdeduzioni, sebbene implicitamente, di non aver adottato nessuno degli strumenti di controllo menzionati nel ricorso che, se utilizzati, avrebbero evitato la realizzazione della frode;
- che, inoltre, constano precedenti ABF a sé favorevoli, relativi all'assenza di colpa grave della parte ricorrente in casi di operazioni effettuate a seguito di *spoofing*.

L'intermediario resistente, in sede di controrepliche, insiste per il rigetto del ricorso.

DIRITTO

Preliminarmente si osserva che l'operazione fraudolenta consiste in una transazione *e-commerce* d'importo pari ad € 1.200,00, di cui l'intermediario ha negato il rimborso prima della presentazione del ricorso, come pacifico tra le parti. Si tratta di un pagamento effettuato in data 11 dicembre 2024, alle ore 18:38, mediante carta di pagamento, a valere sul conto corrente della ricorrente, in merito al quale sussistono in capo al prestatore di servizi di pagamento obblighi di predisposizione di misure di sicurezza ed autenticazione. Tale operazione risulta dal modulo di disconoscimento e dalla lista delle movimentazioni prodotti. Per completezza, si precisa che la parte ricorrente, in denuncia, riferisce anche della fraudolenta esecuzione di una ricarica telefonica di € 30,00; tale operazione non costituisce, tuttavia, oggetto del ricorso in esame.

L'utilizzo fraudolento è disciplinato dal 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 direttiva (UE) 2015/2366 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. 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. Dalla normativa applicabile e, in particolare, dall'art. 10 del D.Lgs. n. 11/2010 discende che, qualora l'utilizzatore neghi, come nella fattispecie, di aver autorizzato delle operazioni di pagamento, sul prestatore di servizi di pagamento gravi una precisa e graduata sequenza di oneri probatori, in base alla quale il PSP è tenuto a dimostrare, innanzitutto, l'avvenuta autenticazione delle medesime operazioni contestate, la loro corretta registrazione e contabilizzazione, nonché il mancato verificarsi di malfunzionamenti delle procedure necessarie per la loro 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 dell'utente. In secondo luogo, il PSP è tenuto a dimostrare il comportamento gravemente colposo dell'utilizzatore.

In casi come quello in esame, il consolidato orientamento dell'ABF ritiene che l'intermediario è obbligato a fornire la prova che le operazioni siano state autenticate con l'uso di un doppio fattore tra gli elementi di conoscenza, possesso ed inerenza. La definizione di autenticazione forte è data dall'art. 1 del D.Lgs. n. 11/2010, che prevede si tratti di *"un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri"*.

L'intermediario ha riferito che l'operazione contestata è stata autenticata tramite autenticazione forte, previo *enrollment* di un nuovo dispositivo e comunicazione al malfattore dei necessari codici autorizzativi da parte del cliente. Ha dichiarato che: in data 11 dicembre 2024 veniva avviato, a seguito dell'inserimento della mail, un accesso eseguito alle ore 18:35:30; l'inserimento di tali dati dava esito positivo; il sistema rilevava un dispositivo mobile differente da quello utilizzato in precedenza dalla ricorrente e dava, quindi, avvio ad un ulteriore step di autenticazione; a tal fine veniva richiesto l'inserimento del codice dinamico OTP di 6 cifre inviato via sms all'utenza telefonica presente in anagrafica cliente; il corretto inserimento dei dati richiesti consentiva l'accesso in app dal nuovo *device* alle ore 18:35:48. A sostegno di quanto affermato la parte resistente ha allegato i relativi log. Si osserva che il numero di telefono indicato nei suddetti log coincide con quello indicato nella scheda anagrafica del cliente e nel modulo di ricorso.

L'intermediario ha poi affermato che il sistema di sicurezza prevede che laddove il nuovo dispositivo mobile da cui si è fatto accesso venga utilizzato per movimentare la liquidità depositata questo dovrà essere obbligatoriamente autorizzato dal titolare della carta con un ulteriore OTP. Ha quindi riferito di aver inviato un secondo sms OTP al numero di cellulare di parte ricorrente alle ore 18:35:52, allegando in atti la relativa evidenza. Ha prodotto, infine, evidenza recante i dati del *device* associato all'esito della procedura di *enrollment* finora descritta. La resistente ha poi riferito che l'operazione di pagamento contestata è stata autenticata tramite la notifica *push* autorizzativa giunta sul *device* a quel momento associato all'*account*, con un'azione volontaria eseguita sulla medesima notifica tramite parametro biometrico. La parte resistente ha, infine, allegato evidenze a comprova dell'utilizzo del protocollo 3ds.

A fronte delle evidenze documentali prodotte dall'intermediario, il Collegio ritiene provata l'autenticazione dell'operazione contestata e *compliant* con la SCA il sistema di pagamento adottato dal PSP, tenuto conto dell'utilizzo dei seguenti fattori di autenticazione:

- per l'accesso in app ed il contestuale *enrollment*: un elemento di conoscenza, costituito dalla *password*, e un elemento di possesso, costituito da n. 2 sms OTP inviati al numero di cellulare del cliente certificato in anagrafica;
- per l'esecuzione dell'operazione di pagamento: un elemento di possesso, costituito dalla notifica *push* in app (installata sul *device* del malfattore a seguito di *enrollment*), e un elemento di inerenza, costituito da un fattore biometrico.

Dalla documentazione agli atti sembra che l'operazione contestata sia scaturita da un fenomeno di *spoofing* realizzato ai danni di parte ricorrente, la quale, dopo aver ricevuto il messaggio civetta ha contattato il numero ivi indicato, non riconducibile all'intermediario, e ha seguito le indicazioni ricevute da un sedicente operatore dell'intermediario, fornendogli i codici OTP di volta in volta ricevuti (come espressamente dichiarato in denuncia). L'istante ha prodotto in atti copia dell'sms civetta ricevuto nella chat con l'intermediario, in cui risultano anche messaggi genuini. Parte ricorrente non ha prodotto evidenza del registro chiamate del proprio telefono da cui risultino la telefonata al numero telefonico indicato nel messaggio civetta e la successiva chiamata asseritamente ricevuta dal servizio clienti dell'intermediario. Tali circostanze portano ad escludere che la responsabilità dell'accaduto possa essere attribuita esclusivamente all'intermediario medesimo, ai sensi della normativa vigente.

Alla luce di tutti tali elementi il Collegio ritiene, dunque, equo ripartire la responsabilità per l'accaduto e le relative conseguenze pregiudizievoli in parti uguali tra ricorrente ed intermediario.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 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.