

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 ESTERNI – MAURILIO D'ANGELO

Seduta del 10/12/2025

FATTO

Con ricorso del 3 settembre 2025 (preceduto da rituale reclamo, negativamente riscontrato dall'intermediario), la parte ricorrente ha affermato che in data 20/01/2025, mentre si trovava all'estero, subiva una truffa telefonica, conclusasi con il "furto" della somma di € 851,99.

Sebbene in un primo momento l'intermediario le avesse rimborsato la somma in questione, tuttavia in data 15/05/2025 lo stesso stornava la suddetta somma;

Chiariva di essersi recata nella filiale, dove le operatrici la invitavano ad effettuare un reclamo, che tuttavia aveva esito negativo.

In proposito, rilevava di non aver mai condiviso i PIN delle sue carte con nessuno e che, al contrario, i malfattori erano già autonomamente in possesso dei numeri, scadenze e codici CVV di entrambe le sue carte.

Infatti, questi ultimi le ripetevano più volte che per ragioni di sicurezza non avrebbe dovuto rivelare a nessuno i suddetti numeri, ma limitarsi a confermare i dati letti ad alta voce da loro.

Orbene, pur avendo condiviso un codice "usa e getta" inviatole sul telefono, di fronte alla prima richiesta fatta dagli interlocutori, chiudeva la chiamata, proprio per timore di un inganno.

Precisava di aver acconsentito a seguire le indicazioni solo in quanto i messaggi provenivano dal numero della resistente e solo dopo essere stata ricontatta dal numero verde per le chiamate all'estero della resistente stessa.

Pertanto, concludeva richiedendo che l'intermediario revocasse lo storno della somma di € 851,99.

Nel costituirsi con apposite controdeduzioni, l'intermediario ha rappresentato che la ricorrente avrebbe potuto evitare la truffa se avesse operato con un'attenzione maggiore.

Nel messaggio truffaldino esistevano elementi tali da permettere alla ricorrente di individuare la truffa: la mancanza dell'incipit dell'intermediario, l'indicazione generica dell'operazione e la circostanza che l'intermediario non invita mai a contattare numeri di cellulare. In proposito, la ricorrente avrebbe potuto invece contattare il numero verde e scongiurare la frode.

Dall'SMS ricevuto, la ricorrente poteva intuire che stava autorizzando un acquisto ed ha contattato il servizio clienti solo alle 20:54, dopo essersi resa conto della truffa subita.

L'operazione è stata eseguita per intero dalla ricorrente, con l'autenticazione a due fattori attraverso la ricezione del codice OTP e la digitazione del PIN attraverso una piattaforma esterna, che la parte istante è solita utilizzare.

Ha rilevato che la richiesta del sedicente operatore di inviare una somma ad un soggetto sconosciuto per annullare un'altra operazione è anomala.

Oltretutto l'utilizzo della piattaforma in questione comporta una responsabilità diretta da parte dell'utente nel controllo del beneficiario e dell'operazione stessa ove i numeri con cui la parte ricorrente ha interloquito con il sedicente operatore non erano riconducibili all'intermediario.

Ha, quindi, concluso domandando il rigetto del ricorso.

DIRITTO

L'utilizzo fraudolento per cui è controversia 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.

SuS

Sul punto 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, 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:

- A. 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;

- B. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

L'operazione contestata consiste in una transazione online di € 851,99 avvenuta in data 20.01.2025 alle ore 20:27.

L'operazione risulta dalla denuncia, dal modulo di contestazione e dalla comunicazione di storno dell'operazione contestata da parte dell'intermediario resistente.

In ordine al sistema adottato dall'intermediario ai fini della SCA, parte resistente ha dichiarato che l'operazione contestata è stata autenticata con il codice OTP ricevuto a mezzo sms dalla ricorrente sul suo numero certificato e con la digitazione del codice PIN della carta di sua esclusiva conoscenza.

Quanto alla prova della corretta autenticazione dell'operazione contestata, l'intermediario ha prodotto i relativi log.

La resistente ha altresì allegato il dettaglio del movimento con la relativa legenda esplicativa.

Dalle evidenze prodotte, si evince che il pagamento è avvenuto con OTP SMS inviato al numero di cellulare certificato della cliente, che corrisponde a quello indicato in denuncia, e attraverso l'inserimento del PIN della carta.

In tale contesto, il Collegio rileva che a fronte di evidenze documentali analoghe prodotte dallo stesso intermediario in controversie della medesima specie, l'ABF (cfr. Collegio di Torino, dec. 2807/2023 e dec. 5256/2023) ha ritenuto provata l'autenticazione delle operazioni contestate e compliant con la SCA il sistema di pagamento adottato dall'intermediario, tenuto conto dell'utilizzo dei seguenti fattori di autenticazione per le singole operazioni:

- ✓ elemento di possesso: OTP inviato tramite Sms;
- ✓ elemento di conoscenza: Pin della carta.

Il Collegio ritiene, quindi, alla luce del corredo probatorio sopra richiamato e dei suoi precedenti in merito adeguato a SCA il sistema adottato.

In ordine agli elementi relativi alla frode, secondo quanto riportato in sede di denuncia, appare che le operazioni contestate siano scaturite da un fenomeno di *sms spoofing*, realizzato ai danni di parte ricorrente, seguito da una telefonata effettuata dalla medesima parte ricorrente al numero indicato nell'sms civetta e da successive telefonate.

La parte ricorrente, infatti, dichiara che il 20/01/2025 alle 19:29, mentre era all'estero, riceveva un messaggio da un'utenza che aveva la denominazione dell'intermediario che la invitava a contattare un numero, in quanto era in corso un movimento sospetto sul suo conto. Successivamente, la ricorrente provava a contattare il numero senza ricevere alcuna risposta. Veniva poi ricontattata da un altro numero, al quale il sedicente operatore, presentandosi come appartenente all'ufficio delle consulenze per le truffe online di chi si trova all'estero, informava la ricorrente di un tentativo di accesso sulla carta di credito e di un tentativo di pagamento poi bloccato, informandola, altresì, della necessità di bloccare diversi movimenti online. Ha riferito che in buona fede decideva di seguire le istruzioni dell'operatore e che poi, insospettita, chiudeva la chiamata. Dopo poco, poiché veniva contattata da un sedicente operatore dal numero verde dell'intermediario che la rassicurava e la invitava a continuare le operazioni richieste, facendo affidamento sulla genuinità del contatto acconsentiva a proseguire, avvedendosi successivamente di aver effettuato a sua insaputa un pagamento € 851,99.

Ebbene, le evidenze prodotte comprovano che il messaggio truffaldino veniva ricevuto all'interno della chat che riporta la denominazione dell'intermediario resistente. Lo stesso messaggio dà atto di un'operazione di pagamento e invita a contattare un numero di cellulare per informazioni. In tale direzione, non sembrano risultare evidenti incidi di inattendibilità, sebbene l'intermediario abbia contestato la mancanza dell'incipit del nome della banca, il fatto che l'indicazione dell'operazione sia generica e la circostanza che l'intermediario non invita mai a contattare numeri di cellulare.

Si segnala, peraltro, che dagli screenshot delle chiamate risulta – coerentemente con quanto dichiarato dalla ricorrente - una prima telefonata in uscita al numero riportato nel messaggio civetta, una seconda chiamata da un numero di cellulare della durata di 31 minuti e un terzo contatto alle ore 20:26 da un numero fisso riconducibile alla resistente. Si rammenta, poi, che l'operazione è stata effettuata alle ore 20:27, dopo l'ultima telefonata ricevuta dalla ricorrente dal numero dell'intermediario.

Orbene, dalla disamina della documentazione versata in atti appare chiaro che l'operazione contestata è scaturita da un fenomeno di SMS spoofing seguito da vishing realizzato ai danni del ricorrente, il quale, dopo aver ricevuto il messaggio civetta, ha contattato il numero ivi indicato e seguito le indicazioni ricevute da un sedicente operatore dell'intermediario. Nel caso di specie è lo stesso ricorrente a dichiarare di aver contattato il numero telefonico indicato nell'sms civetta e, quindi, avere autorizzato egli stesso il pagamento. Tali circostanze portano ad escludere che la responsabilità dell'accaduto possa essere attribuita esclusivamente all'intermediario medesimo (che, ad ogni buon conto, ha provato la regolarità della autenticazione della operazione disconosciuta), ai sensi della normativa vigente. Pertanto, alla luce delle considerazioni esposte e delle evidenze presenti in atti, il Collegio ritiene sia

configurabile un concorso di colpa a carico del ricorrente nella misura del 50% per aver agevolato il compimento della truffa attraverso il contatto diretto al numero indicato nell'sms civetta. La domanda di rimborso, pertanto, deve essere accolta per l'importo pari al 50% dell'intero ammontare delle operazioni fraudolenti.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 426,00.

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