

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

Relatore GIANNI PUDDU

Seduta del 09/02/2026

FATTO

Ricevuto riscontro negativo al reclamo in data 03.09.2025, veniva proposto ricorso avanti all'ABF.

Parte ricorrente allegava di aver ricevuto, in data 15.05.2025, una chiamata da presunti carabinieri che l'avvertivano di essere stata vittima di una frode informatica e che sarebbe stata contattata dalla propria banca per bloccare i relativi pagamenti, di averne poi ricevuto un'altra, da un soggetto che credeva essere un operatore della propria banca, che la informava di alcuni pagamenti sospetti e la convinceva ad effettuare una particolare procedura per bloccarli. Riferiva poi che, solo al termine della procedura di "falso blocco", si rendeva conto di essere stata vittima di una truffa e scopriva che tramite la propria carta erano stati effettuati due pagamenti, per un totale di € 1.002,00.

Riferiva, quindi, di aver sporto denuncia la mattina stessa, precisando che la chiamata della banca si collocava automaticamente tra quelle ricevute precedentemente o quantomeno, l'ID chiamante indicava "BANCA", circostanza tale da generare affidamento sulla genuinità sia del mittente sia dell'azione richiesta e di essere, perciò, stata vittima di *caller id spoofing* e di *vishing*. Allegava, altresì, di aver contattato, tempestivamente l'intermediario e che lo stesso, in data 19.05.2025, le aveva accreditato nuovamente sul conto la somma fraudolentemente sottratta, per poi il 03.09.2025, riaddebitare la cifra di € 501,00, pari ad una sola delle transazioni contestate. Riteneva del tutto ingiustificato l'accredito della sola transazione delle 10:04 e non anche di quella delle 10:08, atteso che il prestatore di servizi è tenuto all'adozione di preventive e idonee misure atte a evitare l'utilizzo da parte di terzi non autorizzati di codici e dati personali, che l'intermediario stesso non avrebbe, nel caso di specie, fornito la prova della violazione degli obblighi di custodia dei dati identificativi e dispositivi personalizzati e che le misure tecnologiche di sicurezza adottate dall'intermediario non hanno impedito ai truffatori di inserirsi nel circuito bancario. I log non dimostrerebbero, peraltro, se l'arruolamento del dispositivo sia stato preceduto da un accesso fraudolento o se l'OTP sia stato intercettato o generato su un terminale compromesso e in ogni caso, l'eventuale uso dei codici di accesso al sistema da parte di terzi rientrerebbe nel rischio professionale del prestatore dei servizi di pagamento, trovando applicazione il regime di responsabilità in tema di attività pericolose ex art. 2050 c.c. e dall'art. 82 GDPR. La parte ricorrente domandava, quindi, il rimborso della somma di € 501,00. In sede di repliche domandava, oltre al rimborso dell'importo di € 501,00, gli interessi legali e la rivalutazione monetaria.

L'intermediario, nelle proprie controdeduzioni, allegava che il caso in esame sarebbe da ascrivere al fenomeno del *phishing*, nella sua variamente denominata *vishing* con la tecnica del "*caller id spoofing*" e precisava di sensibilizzare continuamente i propri clienti sulla tematica tramite un'assidua campagna a cadenza periodica. Eccepiva che la ricorrente stessa aveva informato i frodatori di essere titolare di un conto presso l'intermediario resistente e di non aver mai richiesto, nelle interlocuzioni con i propri clienti, la comunicazione di dati relativi alle credenziali di accesso: le strane richieste del sedicente operatore avrebbero dovuto immediatamente allarmare la ricorrente. Allegava, altresì, che l'operazione di pagamento oggetto del ricorso risultava eseguita grazie all'inserimento dell'apposito codice OTP inviato sul recapito censito della cliente, che il messaggio contenente la password dinamica riportava un riepilogo dell'operazione di pagamento da autorizzare, oltre all'espressa indicazione di non comunicare a terzi quanto ricevuto e che la cliente aveva fornito il codice dinamico segreto ai malfattori, prestando la propria collaborazione attiva al perfezionamento della frode in atto; rappresentava, poi, di aver correttamente inviato il relativo messaggio di *Alert* a conclusione delle operazioni disconosciute e che la password dinamica veniva inviata all'interno della medesima chat in cui si inseriscono anche i messaggi di *Alert* rendendo, così, certo che la cliente aveva preso visione anche dell'alert, posto che, se così non fosse stato, l'operazione non sarebbe andata a buon fine. Aggiungeva che i malfattori avevano disposto un'operazione di pagamento immediatamente precedente a quella oggetto di ricorso, rimborsata dall'intermediario resistente, in relazione alla quale era stato inviato il messaggio riepilogativo solo due minuti prima del perfezionamento della seconda operazione ma che, nonostante ciò, la

cliente non si era avveduta di quanto in corso e aveva comunicato la password dinamica ricevuta sui propri sistemi nel messaggio immediatamente successivo, consentendo così ai frodatori di perfezionare anche la seconda operazione fraudolenta. Precisava, altresì, che l'operazione contestata risulta essere stata disposta ben 32 minuti prima dell'asserito blocco. Contestava che il mascheramento dell'utenza attuato dai malfattori non sarebbe stato particolarmente sofisticato, rilevando come sarebbe da ritenersi priva di fondamento la domanda formulata in merito alla condanna ai sensi dell'art. 2050 c.c. e all'art. 82 GDPR. Domandava, quindi, il rigetto del ricorso.

L'operazione oggetto della domanda consiste in un pagamento *e-commerce* dell'importo di € 501,00, eseguito in data 15.05.2025, alle ore 10:07. Dalle allegazioni e produzioni in atti risulta altresì un altro pagamento sconosciuto per le medesime ragioni, eseguito alle ore 10:04 del medesimo giorno, di pari importo, rimborsato dall'intermediario. Sono in atti il modulo di disconoscimento e la denuncia.

DIRITTO

Il fraudolento utilizzo di servizi di pagamento 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 al mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

La normativa appena richiamata prevede che qualora l'utilizzatore neghi di aver autorizzato un'operazione di pagamento (il consenso del pagatore è un elemento necessario per la corretta esecuzione di un'operazione di pagamento, in assenza del quale essa non può considerarsi autorizzata- art. 5), grava sull'intermediario provare che l'operazione stessa è stata autenticata, correttamente registrata, contabilizzata, e che durante la sua esecuzione non si siano verificati malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti (art. 10). Quanto precede trova un limite nella circostanza che l'utilizzatore abbia agito mancando di osservare in modo fraudolento o gravemente colposo gli obblighi di corretto utilizzo e di custodia degli strumenti di pagamento, situazione nella quale l'art. 12, comma 4, del d.lgs. n. 11/2010, prevede che il medesimo sopporti per intero le perdite subite.

Per ciò che attiene, quindi, all'onere probatorio gravante su parte resistente, il Collegio rileva come l'intermediario abbia allegato e documentato, producendo le relative evidenze informatiche, che l'operazione contestata è avvenuta in assenza di anomalie ed è stata correttamente autenticata, registrata e contabilizzata, tenuto conto dell'utilizzo dei seguenti fattori di autenticazione: elemento di possesso, OTP sul recapito telefonico censito della cliente; elemento di conoscenza: password *K**6*.

Con riferimento ad evidenze analoghe a quelle prodotte nel presente ricorso, conformemente ai precedenti dell'ABF, si ritiene, quindi, provata l'autenticazione delle operazioni contestate e conforme alla SCA il sistema di pagamento adottato dall'intermediario (si veda, tra le altre, Collegio di Roma, Decisione n. 5233/2023).

Avendo fornito l'intermediario, la prova posta a suo carico dall'art. 10 d.lgs. 11/2010 è, dunque, necessario passare alla valutazione del comportamento dell'utente ai fini dell'applicazione delle previsioni del successivo art. 12 del suddetto d.lgs..

Sulla base dell'esame della documentazione agli atti, emerge come le operazioni contestate siano scaturite da un fenomeno di *Caller ID spoofing* realizzato ai danni di parte ricorrente, la quale dichiara aver ricevuto, una chiamata con numero sconosciuto da un operatore della sua vecchia banca che la avvisava di alcuni prelievi che stavano avvenendo a sua insaputa, di aver comunicato al presunto operatore di non avere più un conto presso quella banca, ma presso la resistente e di essere, successivamente, stata chiamata prima da un sedicente carabiniere e poi da un presunto operatore dell'intermediario resistente che la inducevano, al fine di sventare una asserita frode, ad accedere all'applicazione della propria banca e a comunicare i relativi codici, permettendo loro di eseguire due movimenti per un totale di € 1.002,00. Si rileva, in merito, come, in base alle produzioni della ricorrente, le chiamate ricevute provenissero da numeri effettivamente riconducibili ai carabinieri ed all'intermediario. Gli orari indicati negli screenshot risultano compatibili con la vicenda truffaldina esposta nella denuncia.

In conclusione, alla luce delle circostanze emerse e della documentazione in atti, sulla scorta dell'orientamento dei Collegi ABF, i quali rilevano in generale la forte insidiosità del meccanismo di aggressione consistente nell'invio di sms o telefonate dalla stessa utenza dell'intermediario, valutando lo spoofing- caller ID conclamato, quale quello che connota la complessiva vicenda occorsa, come idoneo ad escludere la colpa grave del cliente, si ritiene, nella fattispecie, il sussistere, in ordine alla complessiva vicenda occorsa, una colpa concorrente tra le parti, nella misura del 50% (ex multis, Collegio di Torino, Decisioni n. 7763/2024 e n. 7606/2024) in relazione, da un lato, alla negligenza dell'utente che, con la propria condotta, ha agevolato il compimento della truffa e, dall'altro lato, alle criticità organizzative relative al servizio di pagamento offerto dall'intermediario.

L'intermediario, prima del ricorso ha, tuttavia, pacificamente, provveduto al rimborso di 501,00 relativo alla prima delle due operazioni di pagamento portate a termine durante la medesima vicenda truffaldina e parimenti disconosciuta. In fattispecie analoghe il Collegio si è già pronunciato computando la ripartizione di responsabilità rispetto al complessivo importo sottratto alla parte ricorrente e scomputando poi dalla somma posta a carico dell'intermediario il rimborso dallo stesso già operato (si richiama Collegio di Torino, Decisione n. 4726/25). Nel caso che ci occupa, quindi, considerato che il complessivo ammontare delle operazioni fraudolente è pari ad € 1.002,00, la quota del 50% già rimborsata dall'intermediario alla ricorrente deve ritenersi soddisfattiva.

Quanto, infine, alla domanda di parte ricorrente, formulata per la prima volta in sede di replica, volta ad ottenere la corresponsione degli interessi e della rivalutazione monetaria, essa sulla base delle Disposizioni ABF – Sez. VI, par. 1, deve ritenersi tardiva e non meritevole, quindi, di accoglimento (si veda Collegio di Torino, decisione n. 11247/2024).

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE