

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) CARATTOZZOLO	Membro designato dalla Banca d'Italia
(TO) ISAIA	Membro di designazione rappresentativa degli intermediari
(TO) PUDDU	Membro di designazione rappresentativa dei clienti

Relatore ELEONORA ISAIA

Seduta del 30/09/2025

FATTO

Parte ricorrente ha affermato di esser caduta vittima di una truffa in data 04.02.2025, tramite la quale veniva effettuata n. 1 operazione non autorizzata per un importo pari ad € 3.980,00. Ricevuto un sms che la informava dell'associazione di un altro dispositivo e la invitava a chiamare un numero cellulare per disconoscere tale operazione, parte ricorrente ha affermato di aver seguito le indicazioni e, dopo poco, di essere stata ricontattata da un numero fisso che la invitava a restare in linea per ripristinare e bloccare le autorizzazioni in corso. Parte ricorrente "procedeva" e al termine della chiamata, in verità interrotta dall'interlocutore telefonico, riceveva il messaggio di conferma dell'utilizzo di € 3.980,00 presso un sito di scommesse. Ha quindi bloccato la carta, fatto denuncia e aperto la contestazione. Parte ricorrente ha precisato che sia gli sms sia la chiamata erano stati inviati da recapiti riconducibili all'intermediario resistente, in quanto facevano seguito allo storico delle comunicazioni genuine abitualmente inviate alla ricorrente e registrate nella memoria del telefono. Adottando, quindi, l'ordinaria diligenza non avrebbe potuto realizzare di essere oggetto di un tentativo di frode. Parte ricorrente ha, inoltre, rappresentato che l'operazione disconosciuta risultava abnorme e anomala, tenuto conto della natura e dell'importo della disposizione, oltre che dell'abituale utilizzo della carta e dei suoi usuali livelli di spesa. L'eventuale superamento dei limiti di plafond previsti dal contratto determinerebbe una responsabilità dell'intermediario resistente per le somme eccedenti il predetto limite, in mancanza di un'espressa autorizzazione da parte del

titolare. Infine, parte ricorrente ha rappresentato che l'intermediario non ha provveduto ad inviare il codice OTP autorizzativo e l'sms *alert* relativo all'operazione fraudolenta, che avrebbero consentito di richiedere il tempestivo blocco della carta e tentare il recupero delle somme. In ogni caso, parte ricorrente esclude la possibilità di incorrere in colpa grave in quanto la truffa è stata realizzata utilizzando i canali di contatto dello stesso intermediario.

Parte ricorrente in via principale, domanda il rimborso della somma di € 3.980,00, oltre interessi dalla data di deposito e delle spese di procedura del presente ricorso; in via subordinata, nella denegata ipotesi in cui Codesto Collegio ravvisi profili di responsabilità in capo alla ricorrente, chiede di limitare il diritto al rimborso nei limiti di cui all'art 12, comma terzo del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).

Nelle controdeduzioni, l'intermediario resistente ha, *in primis*, precisato che la transazione è stata eseguita tramite *Strong Customer Authentication* (SCA), conformemente al D.Lgs. n. 11/2010. Ha, quindi, affermato che parte ricorrente è stata vittima di una delle ormai note pratiche adottate in occasione di "*phishing/vishing*", in quanto ha dato seguito ad informazioni fornite telefonicamente da un presunto operatore, permettendo così di portare a termine l'operazione di pagamento. La stessa parte ricorrente ha dichiarato di aver ricevuto un SMS, di aver contattato il numero ivi indicato e di aver rilasciato all'interlocutore tutti i codici OTP ricevuti, permettendo al truffatore di accedere al proprio account, associando un nuovo dispositivo. Come noto, l'intermediario non utilizza numeri cellulari per i contatti con i propri clienti né il numero fisso da cui la ricorrente ha ricevuto la telefonata che risulta, invece, riconducibile al recapito di blocco carte per le chiamate in entrata. A differenza di quanto sostenuto da parte ricorrente, l'intermediario ha dichiarato di aver inviato puntuale informativa dell'esecuzione della transazione eseguita. In seguito, ha ricordato di aver messo a disposizione dei clienti un presidio di sicurezza che permette agli stessi di verificare in tempo reale se l'interlocutore telefonico sia realmente un operatore della banca o meno, tramite accesso alla propria applicazione. Ha altresì condotto una massiva campagna informativa al riguardo, anche tramite e-mail che risultano lette dalla stessa parte ricorrente. In ogni caso, l'intermediario ha rappresentato di aver tempestivamente attivato i presidi di sicurezza previsti in relazione alla movimentazione anomala rilevata, cosicché, a seguito della prima transazione eseguita alle ore 17:58, l'operatività del conto è stata immediatamente sospesa e l'operatività della relativa carta di pagamento è stata momentaneamente inibita, in via cautelativa, al fine di consentire gli opportuni approfondimenti con la stessa ricorrente. Non risultano intrusioni non autorizzate nei propri sistemi informatici che abbiano reso possibile l'esecuzione dell'operazione in discussione, transazione che peraltro rientra nei limiti previsti dal contratto sottoscritto da parte ricorrente.

L'intermediario resistente conclude chiedendo il rigetto del ricorso.

DIRITTO

La controversia verte in materia di esecuzione fraudolenta di transazioni online. L'operazione contestata è disciplinata 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.

Sulla base della normativa sopra riportata, l'intermediario resistente deve provare dapprima l'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni sconosciute, e in seguito il dolo o la colpa grave del cliente, uniche ipotesi in cui lo stesso può patire le conseguenze della truffa subita.

Ciò premesso, nel caso in esame, l'operazione consiste in n. 1 transazione online dell'importo di € 3.980,00, effettuata con carta in data 04.02.2025, alle ore 17:58. L'intermediario ha riferito che l'operazione contestata è stata autenticata tramite autenticazione forte, previo *enrollment* di un nuovo dispositivo. Le evidenze informatiche prodotte mostrano che il sistema di pagamento adottato utilizza i fattori di sicurezza stabiliti dalla *Strong Customer Authentication* (SCA) prevista dalla direttiva (UE) 2015/2366. In particolare, l'*enrollment* del nuovo dispositivo è avvenuto a seguito di un accesso eseguito tramite la corretta digitazione dell'indirizzo mail e della password, seguiti da due codici dinamici OTP, ricevuti tramite SMS al riferimento cellulare presente in anagrafica cliente e posseduto quindi dal titolare della carta. In seguito, l'operazione online è avvenuta attraverso l'App installata nel nuovo device e autorizzata tramite la notifica *push* giunta sullo smartphone collegato, con un'azione volontaria ("tap") eseguita sulla medesima notifica tramite parametro biometrico. Si segnala che a fronte di evidenze documentali analoghe prodotte dallo stesso intermediario in controversie della specie, l'ABF è giunto alla medesima valutazione (Collegio di Torino, decisioni n. 2063/2024 e n. 3956/2023; Collegio di Milano, decisione n. 15840/2022).

Assolto quindi l'onere della prova dell'utilizzo di un sistema di sicurezza a due fattori, occorre ora esaminare gli elementi della frode e il comportamento di parte ricorrente. Dalla documentazione agli atti sembra che le operazioni contestate siano scaturite da un fenomeno di *spoofing* realizzato ai danni di parte ricorrente, la quale nella denuncia ha dichiarato di aver ricevuto un sms da parte resistente, di aver contattato il numero di cellulare ivi indicato e di aver ricevuto una nuova telefonata da una utenza fissa riconducibile all'intermediario, comunicando, laddove richiesti, i codici ricevuti per e-mail e via sms. Parte ricorrente, a sostegno di quanto affermato nella denuncia, ha allegato *screenshot* del messaggio civetta e della chiamata ricevuta dal numero indicato in denuncia. Si evidenzia che il messaggio truffaldino - inserito nella chat con l'intermediario resistente – allerta la parte ricorrente dell'avvenuta associazione di un nuovo dispositivo, invitandola a contattare un numero di cellulare nel caso di disconoscimento di tale operazione. Dallo *screenshot* del registro chiamate risultano, inoltre, due telefonate in entrata, alle ore 17:36 e alle ore 17:51, da un numero fisso che corrisponde al numero di blocco della carta messo a disposizione dall'intermediario resistente ai clienti. La modalità di svolgimento della truffa - fenomeno di *phishing*, anche nelle varianti dello *smishing* con l'invio di un sms civetta, o del *vishing* nel caso di telefonata da presunto operatore – è ormai molto diffusa, tanto da portare i Collegi ABF a ritenere che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa. Tuttavia, l'assenza di evidenti indici di anomalia nel messaggio civetta, l'inserimento del messaggio nella chat in cui si sono ricevuti in precedenza altri SMS genuini da parte dello stesso intermediario (c.d. *Spoofing*) rappresentano elementi insidiosi che possono indurre in confusione la vittima (Collegio di Torino, decisioni n. 8970/2022 e n. 6277/2025). Questa, d'altra parte, ha ammesso la collaborazione alla realizzazione della truffa, comunicando i codici e le informazioni

personali che avrebbe dovuto diligentemente custodire. Pertanto, alla luce di tutti i fatti e le circostanze del caso, questo Collegio ritiene che le responsabilità in merito all'operazione fraudolenta debbano essere ripartite fra le parti nella misura del 50%, con il conseguente diritto della parte ricorrente al rimborso della somma di € 1.990,00. Parte ricorrente ha poi eccepito che l'intermediario avrebbe dovuto bloccare l'operazione contestata in quanto anomala rispetto alla sua normale operatività. L'intermediario sul punto ha osservato come l'art. 2 degli RTS Eba (Reg. del. UE n. 389/2018) non preveda un obbligo di monitoraggio *ex ante*, ma solo *ex post*, evidenziando di aver attivato, in ogni caso, i presidi di sicurezza a seguito della transazione disconosciuta; in particolare, ha riferito di aver sospeso l'operatività del conto e di aver inibito momentaneamente l'operatività della relativa carta di pagamento, al fine di consentire gli opportuni approfondimenti con la ricorrente medesima. Quando poi al possibile superamento del plafond sollevato da parte ricorrente, l'intermediario produce il contratto relativo allo strumento di pagamento da cui si evince che l'operazione è stata effettuata entro i limiti di spesa contrattualmente previsti. Da ultimo, parte ricorrente ha domandato la corresponsione degli interessi legali "dal giorno del deposito [del ricorso]". Si richiama che il Collegio di Coordinamento con decisione n. 5304/2013 ha statuito quanto segue: *"Il rimborso, infatti, deve qualificarsi come obbligazione pecuniaria avente natura meramente restitutoria, e non risarcitoria, con la conseguenza che il decorso degli interessi debba essere considerato a partire dal reclamo [e non dalla data dell'operazione], inteso quale atto formale di messa in mora da parte del creditore della prestazione"*.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.990,00 oltre interessi legali dal reclamo al saldo.

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

Firmato digitalmente da
EMANUELE CESARE LUCCHINI GUASTALLA