Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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

Relatore ELEONORA ISAIA

Seduta del 19/12/2025

FATTO

Parte ricorrente ha rappresentato di essere stata vittima di un'operazione di spoofing scaturita da un messaggio ricevuto nella chat utilizzata abitualmente dall'intermediario resistente. Ha riferito che il messaggio la avvertiva di "un'operazione di sicurezza dati" e riportava il nominativo e il codice numerico dell'operatore incaricato. Contattata dal presunto operatore del servizio anti-truffa, tramite un numero di telefono cellulare, parte ricorrente è stata informata di un'operazione sospetta dell'importo di € 2.567,00 e invitata a collaborare trasferendo una serie di dati personali, tra cui quelli della carta di credito, per bloccare la transazione truffaldina. Ha quindi ricevuto da parte dell'intermediario una prima notifica push con cui veniva richiesta la conferma dello storno del pagamento di € 2.567,00 a favore di tale J*.it. e, una volta confermato, una seconda notifica riportante il blocco della carta di credito. Insospettiva, parte ricorrente ha contattato il numero fisso dell'intermediario resistente, venendo a conoscenza della truffa e provvedendo immediatamente a bloccare lo strumento di pagamento.
Parte ricorrente domanda il rimborso della somma di € 2.567,00, oltre alle spese sostenute per la presentazione del ricorso.
Nelle controdeduzioni, l'intermediario resistente ha affermato che parte ricorrente ha proceduto al rilascio delle proprie credenziali e all'approvazione dell'operazione,

attraverso le notifiche push inviate sul suo device. L'operazione disconosciuta è stata, infatti, eseguita mediante l'utilizzo delle credenziali di sicurezza personalizzate su sito "3d secured", attraverso il codice OTP generato dal dispositivo in possesso di parte ricorrente. Il servizio di cui è intestataria prevede un sistema di autenticazione forte sia per effettuare il login all'app e per le operazioni di inquiry, sia per disporre le operazioni. L'intermediario resistente ha pertanto sottolineato di aver posto in essere tutte le misure di sicurezza e prevenzione idonee a tutelare il cliente e che la frode è stata resa possibile esclusivamente dalla negligente custodia delle credenziali da parte dello stesso. Ha, in seguito, affermato che non si deve riporre troppa fiducia nel "caller ID" che appare su telefono fisso o mobile poiché è possibile per chiunque modificare il numero visibile al momento delle telefonate/sms. I clienti sono stati oggetto di molteplici campagne informative per il riconoscimento e la prevenzione dei fenomeni fraudolenti. In ogni caso, parte ricorrente è venuta meno all'onere della prova, non allegando il numero chiamante in entrata. L'intermediario resistente ha concluso chiedendo il rigetto del ricorso, in quanto il caso di specie è escluso dall'applicazione del regime di protezione previsto dal d.lgs. n. 11 del 2010, poiché trattasi di operazioni di spesa autorizzate da parte ricorrente, come da sua stessa ammissione.
In sede di repliche, parte ricorrente ha precisato che il truffatore era a conoscenza di operazioni da lei precedentemente effettuate, a dimostrazione che una o più persone avevano effettuato un accesso illecito e non autorizzato ai sistemi dell'intermediario.
In sede di controrepliche, parte resistente ha sostenuto che la domanda relativa al disconoscimento di altre n. 3 operazioni di spese è improcedibile in quanto le operazioni sono state eseguite con un sistema di autenticazione forte, come provato dalle evidenze informatiche prodotte agli atti. Dai Log è possibile evincere che il Device name e lo UserAgent hanno cambiato nomenclatura nei giorni antecedenti e successivi alla frode per poi, però, ripetersi a conferma della genuinità delle credenziali di accesso utilizzate. Inoltre, l'indirizzo IP dal quale è stata autorizzata l'operazione è localizzato nella città in cui parte ricorrente ha il domicilio.

DIRITTO

La controversia verte in materia di esecuzione fraudolenta di transazioni online. Le operazioni contestate sono disciplinate 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, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, anche 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 contestata consiste in n. 1 transazione online dell'importo di € 2.567,00 eseguita il 28/10/2024 alle ore 15:17. L'intermediario ha riferito che da gennaio 2020, sia nel caso in cui si disponga un pagamento (tramite carte) su sito sicuro, oppure un accesso all'home banking, le modalità autorizzative non prevedono più che venga inserito manualmente il codice OTP, ma richiedono che il titolare delle carte e dei canali diretti autorizzi il pagamento e/o l'accesso all'home banking tramite la app, attraverso la ricezione notifica push e successivo "tap" sulla

stessa e autorizzazione, oppure accedendo all'home banking (login), cliccando sulla lista delle autorizzazioni e poi autorizzando l'operazione. In entrambi i casi, si viene indirizzati nella sezione di autorizzazione della transazione e/o accesso in caso di accesso all'home banking; il cliente quindi, inserendo il PIN o utilizzando il touch/face ID (se abilitato), darà la conferma con la quale sarà generato anche una OTP transazionale "silente" (non visibile al cliente) legata a quella e solo a quella specifica operazione, come disposto dalla PSD2. Il testo "parlante" della notifica push e dell'autorizzazione indica in chiaro l'operazione che si sta autorizzando. Posto quanto sopra, con riferimento al caso in esame, la banca ha riferito che l'operazione contestata è stata autenticata con PIN e OTP generato dal Mobile Token attivo sull'app, previo accesso all'home banking tramite credenziali di sicurezza (Id utente e PIN) e OTP, sempre generato da Mobile Token. Le evidenze documentali prodotte dall'intermediario sono ritenute compliant con la SCA, analogamente a quanto valutato in altre controversie della stessa specie (Collegio di Torino, decisione n. 669/2024: Collegio di Roma, decisione n. 4981/2024).

Assolto quindi l'onere della prova dell'utilizzo di un sistema di sicurezza a due fattori da parte dell'intermediario – elemento che costituisce l'antecedente logico rispetto alla prova della colpa grave del cliente –, occorre ora esaminare gli elementi della frode e il comportamento di parte ricorrente. Si sottolinea che, come riportato nella documentazione agli atti, parte ricorrente ha riferito di aver comunicato al sedicente operatore bancario i numeri centrali della propria carta e di aver dato seguito alla notifica push per lo storno del bonifico in contestazione. L'intermediario eccepisce che parte ricorrente abbia eseguito personalmente le operazioni disconosciute, con conseguente inapplicabilità della "PSD2". Sul punto si rappresenta che secondo l'orientamento condiviso dei Collegi l'operazione può essere considerata autorizzata solo quando la stessa è interamente eseguita dal pagatore. Nel verbale di denuncia, parte ricorrente afferma di aver confermato il pagamento, ma non di averlo disposto e allega i messaggi ricevuti da cui si evince che sono stati incanalati nella chat utilizzata con l'intermediario, sono privi di errori grammaticali, menzionano una attività di sicurezza dati con un operatore, richiedono di "autorizzare lo storno", e, infine, confermano l'avvenuto storno del pagamento. Dal registro chiamate allegato, emerge come la telefonata del sedicente operatore provenisse da un numero privato, non riconducibile all'intermediario.

Secondo gli orientamenti condivisi dei Collegi ABF, nelle fattispecie di spoofing – ricorrente sia nel caso di sms che si inserisca in una "conversazione" o "chat" precedente con l'intermediario, sia quando sussista un singolo messaggio civetta che sembri provenire dall'intermediario - non è generalmente ravvisabile la colpa grave del ricorrente, data l'insidiosità del meccanismo di aggressione, nonostante la maggiore diffusione di campagne informative sul tema. Nel caso poi di messaggi di storno, il Collegio di Torino ha più volte ritenuto la presenza di una particolare insidiosità della frode, poiché il contenuto del messaggio induce ad una incolpevole abbassamento della soglia di attenzione (Collegio di Torino, decisioni n. 7214/2024; n. 965/2022; n. 6052/2021; n. 10578/2021; n. 10870/2021). Occorre tuttavia considerare la colpevole collaborazione di parte ricorrente al completamento dell'operazione fraudolenta, violando gli obblighi di custodia delle credenziali. Valutate tutte le circostanze, il Collegio rileva un concorso di colpa a carico del cliente per aver agevolato la truffa e ripartisce la responsabilità in misura paritetica fra le parti (in merito al concorso di colpa si richiama il Collegio di Torino, decisioni n. 7214/2024 e n. 7430/2023).

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.284,00.
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