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 ROBERTO CARATOZZOLO

Seduta del 19/12/2025

FATTO

Con ricorso del 9 luglio 2025 parte istante chiede all'ABF il riconoscimento del diritto al rimborso della somma di € 1.592,43, corrispondente all'importo di operazioni di pagamento fraudolente non autorizzate.
Afferma la ricorrente di aver ricevuto una telefonata, apparentemente proveniente da un numero riconducibile al gestore della propria carta prepagata di pagamento, con la quale un operatore le comunicava la presenza di asseriti movimenti sospetti sulla stessa carta e della necessità di effettuare alcune verifiche; di aver comunicato all'operatore, su sua espressa richiesta, l'indirizzo mail collegato alla carta nonché due codici ricevuti tramite sms, dall'utenza da cui solitamente giungono le comunicazioni da parte dell'odierna resistente, nella convinzione che fossero necessari per stornare i pagamenti e terminare la gestione della pratica; di non essere più riuscita, di lì a poco, ad operare sul proprio conto dal suo device in quanto l'app risultava disabilitata.
Nelle controdeduzioni l'intermediario resistente contesta le richieste di parte avversa e ne chiede il rigetto. In particolare afferma che le operazioni di pagamento sono state eseguite tramite autenticazione forte, nel rispetto dei presidi SCA e in conformità alla

normativa di settore ed eccepisce la colpa grave della ricorrente, rimasta vittima di un caso "phishing/vishing", in quanto non conforme agli obblighi prescritti dall'art. 7 del D.Lgs. n. 11/2010.

DIRITTO

Le operazioni oggetto del presente procedimento sono state compiute sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), efficace dal 13/01/2018; esse consistono in due pagamenti e-commerce, disposti alle ore 16:43 e 16:44 del 23/10/2024, rispettivamente di € 1.284,98 e di € 307,45, per un valore complessivo di € 1.592,43.
Vanno richiamate le fonti normative che regolano la Strong Customer Authentication (SCA), rinvenibili negli artt. 97 e 98 della PDS2, negli articoli 10 e 10-bis del d.lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare il parere del 21 giugno 2019).
Rileva, in primo luogo, per l'intermediario, ai sensi del richiamato art. 10 d.lgs. 11/2010, l'onere di provare per un verso che le operazioni di pagamento sono state autenticate, correttamente registrate e contabilizzate e che non hanno subito le conseguenze del malfunzionamento delle procedure necessarie per la loro esecuzione o di altri inconvenienti e, per altro verso, l'eventuale frode, dolo o colpa grave dell'utente.
Sotto il primo aspetto l'intermediario resistente dichiara che le operazioni contestate sono state autenticate nel rispetto dei presidi SCA, previo *enrollment* di un nuovo dispositivo. In particolare l'intermediario ha dichiarato che in data 23/10/2024 veniva avviato, a seguito dell'inserimento dell'e-mail e della password, un accesso eseguito alle ore 16:36:22; 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 per il quale veniva richiesto l'inserimento del codice dinamico OTP di 6 cifre inviato via sms all'utenza telefonica presente in anagrafica cliente alle ore 16:36:22; il corretto inserimento dei dati richiesti consentiva l'accesso in app da nuovo device alle ore 16:36:59.
L'intermediario ha poi affermato che il sistema di sicurezza prevede che nel caso in cui il nuovo dispositivo mobile da cui si è fatto accesso venga utilizzato per movimentare la liquidità depositata, questo dovrà essere obbligatoriamente autorizzato dal titolare carta con un'ulteriore OTP, correttamente inserita e verificata; inoltre ha riferito che le operazioni contestate sono state autorizzate tramite la notifica push autorizzativa giunta sullo smartphone collegato, con un'azione volontaria ("tap") eseguita sulla medesima notifica tramite parametro biometrico.
A supporto delle proprie affermazioni l'intermediario produce evidenze documentali e Log informatici corredati da legende esplicative, che comprovano che le operazioni di pagamento sono state autenticate, correttamente registrate e contabilizzate e che non hanno subito le conseguenze del malfunzionamento delle procedure necessarie per loro esecuzione o altri inconvenienti. In particolare è provato l'utilizzo dei fattori di autenticazione sia per l'accesso in app e contestuale *enrollment* (elemento di conoscenza: password; elemento di possesso: due sms OTP inviati al numero di cellulare del cliente certificato in anagrafica) sia per le singole operazioni (elemento di

possesso: notifica push in app installata sul device del malfattore a seguito di enrollment; elemento di inerenza: fattore biometrico).
Alla luce di quanto sopra, il Collegio ritiene assolto l'onere probatorio gravante sull'intermediario in ordine all'adozione delle prescrizioni dettate dalla normativa in tema di autenticazione forte per l'utilizzo degli strumenti di pagamento (Strong Customer Authentication).
Si passa, quindi, all'esame dell'ulteriore aspetto relativo alla valutazione del comportamento tenuto dal ricorrente nel corso della vicenda sottoposta a cognizione di codesto Collegio.
Secondo il principio interpretativo adottato dal Collegio di Coordinamento dell'ABF, infatti, la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale relativa all'"autenticazione" ed alla formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente (Collegio di Coordinamento, decisione n. 22745 del 10 ottobre 2019).
Si richiama, sul punto, l'orientamento del Collegio di Coordinamento (decisione n. 24366/19) secondo il quale "*Con riguardo alla prova della colpa grave dell'utente, non ogni contegno imprudente può far ritenere integrato questo grado di colpa, ma solo quello che appaia abnorme ed inescusabile: una valutazione siffatta deve essere compiuta alla luce di tutte le circostanze di fatto che, di volta in volta, caratterizzano il caso di specie, tenendo in considerazione la sussistenza della stessa sia con riferimento agli obblighi di custodia dello strumento di pagamento, sia quelli di memorizzazione del codice identificativo (Coll. Coord., decisione n. 5304/2013)*" . La prova della colpa grave – che costituisce onere dell'intermediario ai sensi dell'art. 10, comma 2 del decreto – consiste nella prova dei fatti che, in connessione tra loro, possono ragionevolmente condurre a ritenere gravemente negligente la condotta del cliente. Questa prova può essere fornita anche per mezzo di presunzioni, purché queste siano gravi, precise e concordanti, ai sensi dell'art. 2729 c.c."
Dalla documentazione versata in atti si evidenzia che le operazioni contestate sono scaturite da un fenomeno di *Caller ID Spoofing*, realizzato ai danni di parte ricorrente, la quale ha espressamente affermato di aver ricevuto una chiamata dal numero dell'intermediario ed aver comunicato al malfattore i codici autorizzativi ricevuti sul proprio device ed utilizzati per l'associazione di un nuovo dispositivo. Il numero del mittente appare riconducibile all'intermediario, sebbene questi abbia espressamente dichiarato che serva unicamente a consentire ai clienti di chiedere il blocco delle proprie carte di pagamento e non anche ad essere contattati dall'intermediario medesimo, come specificato sul proprio sito web.
Orbene, nonostante in simili ipotesi non sia generalmente ravvisabile la colpa grave del ricorrente, data l'insidiosità del meccanismo di aggressione nonostante la diffusione di campagne informative sul tema, tuttavia, il quadro fattuale ricostruito sulla base delle allegazioni e delle offerte di prova provenienti da entrambe le parti, induce a ritenere che nel caso di specie siano ravvisabili indici di evidente colpa del cliente, per aver comunicato a terzi le proprie credenziali personali relative al servizio pagamento utilizzato agevolando il compimento della truffa; pertanto, alla luce di quanto sopra, si configura un concorso di colpa quantificabile nella misura del 50% delle somme portate dalle operazioni contestate, a causa del comportamento del ricorrente gravemente

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

colposo e contrario agli obblighi di correttezza e diligente custodia delle proprie credenziali.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 796,00.
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