

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) COCCIA	Membro di designazione rappresentativa dei clienti

Relatore ROBERTO CARATOZZOLO

Seduta del 29/07/2025

FATTO

Con ricorso del 03/02/2025 parte istante chiede all'ABF il riconoscimento del rimborso della somma di € 3.581,72, corrispondente all'importo di operazioni di pagamento eseguite fraudolentemente da terzi malfattori, non autorizzate e disconosciute.

Afferma la ricorrente di aver ricevuto – alle ore 13:23 del 30/05/2024 – vari sms apparentemente provenienti dal numero ufficiale dell'intermediario, con i quali veniva informata di tre autorizzazioni di pagamento effettuate con la carta di credito n.***380, d'importo rispettivamente di € 500,00, € 1.990,00 ed € 1.870,00, e veniva invitata a contattare il numero telefonico ivi indicato nel caso in cui si fosse trattato di transazioni disconosciute. Riferisce poi che: allarmata, provvedeva immediatamente a contattare tale utenza telefonica al fine di disconoscere le operazioni; riceveva assistenza da parte di un sedicente operatore bancario, il quale le confermava l'effettiva esecuzione delle transazioni e le comunicava che avrebbe provveduto al relativo storno, bloccando la carta di credito ed emettendone una nuova; riceveva alcuni sms dal medesimo numero recanti conferma del blocco della carta n.***380 e dello storno delle transazioni; successivamente si rendeva conto che erano state effettuate sette operazioni mediante carta di credito, del valore complessivo di € 1.648,80, sei transazioni tramite bancomat, del valore complessivo di € 1.782,92, una ricarica telefonica di € 150,00 su un'utenza telefonica sconosciuta; provvedeva, quindi a proporre reclamo in data 28/08/2024, chiedendo l'integrale rimborso della somma di € 3.581,72 in considerazione della totale responsabilità della banca, ricevendo, tuttavia, riscontro negativo. Evidenzia di non aver ricevuto una

semplice e-mail, ma un sms proveniente da un'utenza telefonica recante la denominazione dell'intermediario, da cui aveva sempre ricevuto tutti gli sms *alert* e le proprie comunicazioni e che la lettura degli stessi, ricevuti tra le ore 13:23 e 15:18, non aveva consentito di distinguere i messaggi genuini da quelli fraudolenti.

Chiede il riconoscimento della responsabilità della banca per non aver adottato le misure necessarie ad evitare simili fattispecie truffaldine.

Nelle controdeduzioni l'intermediario convenuto contesta le richieste di controparte e ne chiede il rigetto; in particolare sottolinea il fatto che le operazioni venivano compiute con il contributo determinante di parte ricorrente, che aveva seguito tutte le indicazioni ricevute dal malfattore cui si era espressamente rivolta; contesta la ricostruzione fattuale operata dal ricorrente in quanto carente di elementi certi; afferma che la ricorrente versa in colpa grave, posto che: la stessa ha dichiarato di aver ricevuto un messaggio sospetto e di aver immediatamente richiamato il numero di telefono indicato nell'sms, senza prima disporre alcuna verifica presso i canali ufficiali della Banca; non risultano messaggi di questo tenore inviati alla parte ricorrente nella data in esame, essendo invero stati inviati sms o notifiche *push* in corrispondenza di tutte le operazioni successivamente contestate; seguendo le indicazioni del sedicente operatore antifrode – convinta di stornare delle operazioni – la parte ricorrente autorizzava con notifiche *push* le attività che portavano alla conferma di transazioni *e-commerce* successivamente contestate, anche in questo caso senza effettuare alcun controllo in merito alla veridicità di quanto affermato dall'operatore; tutto ciò avveniva nonostante l'invio di notifiche *push* per tutte le operazioni e i numerosi blocchi delle transazioni disposti dall'istituto a tutela della parte ricorrente.

Nelle repliche e nelle controrepliche, le parti insistono nelle rispettive eccezioni e richieste, che provvedono a specificare ulteriormente.

DIRITTO

Le operazioni oggetto del presente procedimento sono state poste in essere 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), entrato in vigore il 13/01/2018.

Si tratta delle seguenti operazioni, effettuate in data 30/05/2024, tramite carta di debito n.***5020:

- transazione *e-commerce* d'importo pari ad € 278,14, di cui € 4,87 a titolo di commissioni (importo originario USD 300,00), effettuata alle ore 16:56:01;
- transazione *e-commerce* d'importo pari ad € 299,99 effettuata alle ore 17:13:52;
- transazione *e-commerce* d'importo pari ad € 299,98, effettuata alle ore 17:19:04;
- transazione *e-commerce* d'importo pari ad € 299,97, effettuata alle ore 17:31:30;
- transazione *e-commerce* d'importo pari ad € 300,00, effettuata alle ore 17:36:10;
- transazione *e-commerce* d'importo pari ad € 299,97, effettuata alle ore 17:46:42.

Sono ricomprese anche le seguenti operazioni, disposte in data 30 maggio 2024, tramite carta di credito n. ***7643:

- transazione *e-commerce* d'importo pari ad € 299,00, effettuata alle ore 15:25:53;
- transazione *e-commerce* d'importo pari ad € 299,90, effettuata alle ore 15:39:36;
- transazione *e-commerce* d'importo pari ad € 299,98, effettuata alle ore 15:52:08;
- transazione *e-commerce* d'importo pari ad € 100,00, effettuata alle ore 16:12:43;
- transazione *e-commerce* d'importo pari ad € 299,94, effettuata alle ore 16:23:42.
- transazione *e-commerce* d'importo pari ad € 299,98, effettuata alle ore 16:30:32;
- transazione *e-commerce* d'importo pari ad € 50,00, effettuata alle ore 17:45:12.

Con riferimento alla ricarica telefonica di € 150,00 si osserva che:

- la parte ricorrente cita tale transazione nel reclamo e nel ricorso, pur non avendola indicata nel modulo di disconoscimento e nelle denunce;
- l'intermediario non ne fa menzione nei propri atti difensivi, riferendosi unicamente alle altre 13 transazioni e-commerce di cui sopra;
- fermo quanto sopra, risultano in atti evidenze tecniche che sono riconducibili a tale ulteriore operazione.

Si richiamano 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 quindi 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 altri inconvenienti e, per altro verso, l'eventuale frode, dolo o colpa grave dell'utente.

Orbene, sotto il primo aspetto l'intermediario resistente afferma che le 13 operazioni e-commerce contestate sono state autenticate tramite (i) notifica *push* in app (elemento di possesso) attivata su altro dispositivo a seguito di disinstallazione ed *enrollment* e mediante (ii) inserimento del codice *pin (elemento di conoscenza).

Relativamente alle modalità di attivazione dell'app su altro dispositivo, la banca ha affermato che questo avviene secondo i seguenti passaggi:

- viene richiesta una prima autenticazione attraverso l'inserimento del codice adesione (fornito dalla banca ed univoco) e del pin (creato dal titolare del servizio e pertanto noto solo a lui);
- viene svolta una verifica sui recapiti dell'utente (laddove i recapiti non vengano modificati non è previsto l'invio di email, ma unicamente l'invio di un sms OTP per conferma);
- una volta confermati i recapiti, viene inviato un sms OTP da inserire in app;
- è quindi possibile la creazione di un (nuovo) codice *PIN, che può essere utilizzato come secondo fattore di autenticazione delle operazioni in app;
- viene infine richiesto l'inserimento di un ulteriore fattore di sicurezza, rappresentato dal PIN della carta o dal token fisico in possesso dell'utente.

Rispetto all'*enrollment* dell'app su altro dispositivo, la banca ha affermato che questo è stato autorizzato tramite digitazione del "*pin di accesso*", del "*pin della carta*" e dell'OTP ricevuto via SMS.

A riprova di quanto affermato l'intermediario produce evidenze documentali e log informatici corredati da legende esplicative, che comprovano la veridicità delle proprie dichiarazioni sia con riguardo all'accesso tramite app (elemento di inerenza: *fingerprint*; elemento di possesso: app installata su device univocamente associato all'utente), sia per l'*enrollment* dell'app su altro dispositivo (elemento di possesso: sms OTP; elemento di conoscenza: codice pin), sia per l'esecuzione delle singole operazioni *e-commerce* (elemento di possesso: notifica *push* in app; elemento di conoscenza: codice pin) ed infine per la ricarica telefonica (elemento di possesso: *token app; elemento di conoscenza: codice *pin).

Alla luce di quanto sopra, il Collegio ritiene assolto l'onere probatorio in ordine all'adozione delle prescrizioni dettate dalla normativa in tema di autenticazione forte dello strumento di pagamento (SCA) e passa, pertanto, all'esame della valutazione del comportamento tenuto dal ricorrente nel corso della vicenda.

Secondo il principio interpretativo adottato dal Collegio di Coordinamento dell'ABF, infatti, la previsione di cui all'art. 10, co. 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.

A tal proposito si evidenzia che dalla documentazione versata in atti e dalle dichiarazioni confessorie di parte ricorrente, risulta che le operazioni contestate sono state compiute a seguito di un'attività riconducibile ad un fenomeno di *spoofing* seguito da *vishing*, realizzato ai danni di parte ricorrente. Nello specifico, si rileva che: la parte ricorrente riceveva alle ore 13:23 del 30/05/2024 tre messaggi consecutivi con i quali veniva informata di tre operazioni di pagamento – d'importo rispettivamente pari ad € 500,00, € 1990,00 ed € 1870,00 – effettuate mediante sua carta di credito n. ***7463; ogni messaggio riportava il numero da contattare per un eventuale storno o blocco delle transazioni; volendo disconoscere le operazioni indicate, la parte ricorrente contattava immediatamente il numero indicato nei messaggi e s'interfacciava con un asserito operatore bancario, che le riferiva di aver stornato gli addebiti, che avrebbe bloccato la carta di credito e ne avrebbe emessa una nuova; mentre effettuava le operazioni di storno, l'operatore le chiedeva il codice di sicurezza indicato nel retro della carta.

A sostegno di quanto affermato, la parte ricorrente ha versato in atti screenshot degli sms civetta ricevuti, dai quali si evince che: sono posti in coda ad sms genuini e provengono dalla banca resistente; presentano un tenore parzialmente diverso da quello dei precedenti messaggi genuini, in quanto differentemente da questi ultimi, gli sms civetta non recano il nome dell'intermediario del testo e invitano il destinatario a contattare una diversa utenza telefonica rispetto a quella indicata nei messaggi genuini che non è riconducibile all'intermediario; non sembrano contenere errori grammaticali. Se ne deduce che il tenore dei messaggi presenta indici di evidente inattendibilità e di anomalia che avrebbero dovuto far allertare l'utente di una possibile operazione truffaldina. Secondo gli orientamenti condivisi dei Collegi ABF, nelle fattispecie di spoofing che ricorre 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 e nonostante la maggiore diffusione di campagne informative sul tema. Tuttavia, qualora il testo del messaggio civetta presenti indici di evidente inattendibilità o di anomalia è stato ritenuto che possa rilevarsi un concorso di colpa a carico del cliente per

aver agevolato il compimento della truffa. A ciò si aggiunga, con valenza determinante, la circostanza che parte ricorrente ha contattato direttamente il numero telefonico indicato nei messaggi civetta e non riconducibile all'intermediario ed ha seguito le indicazioni provenienti dall'interlocutore.

Pertanto, alla luce di quanto sopra, si configura un concorso di colpa a carico del ricorrente per aver agevolato il compimento della truffa, quantificabile nella misura del 50% delle somme portate dall'operazione contestata, per aver tenuto un comportamento gravemente 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 € 1.791,00.

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

Firmato digitalmente da
EMANUELE CESARE LUCCHINI GUASTALLA