

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

Relatore ROBERTO CARATOZZOLO

Seduta del 23/03/2026

FATTO

Con ricorso dell'1 dicembre 2025 parte istante chiede all'ABF il riconoscimento del diritto al rimborso della somma di € 1.796,21, corrispondente all'importo di operazioni di pagamento fraudolenti eseguite a seguito di una subita truffa.

Afferma la ricorrente di aver appreso dell'esecuzione di alcune operazioni di pagamento, effettuate a sua insaputa, dalle notifiche provenienti dall'app di home banking; contattava immediatamente il servizio clienti della banca per bloccare gli strumenti di pagamento, presentava denuncia e compilava la modulistica di disconoscimento delle operazioni; da un successivo estratto conto veniva a conoscenza di ulteriori operazioni non autorizzate e provvedeva ad integrare la precedente denuncia e a disconoscere le stesse; ritiene che

la sottrazione del denaro sia imputabile alla banca, per insufficienza dei sistemi di sicurezza informatica e per mancanza di adozione di adeguati presidi di controllo.

Nelle controdeduzioni l'intermediario resistente contesta le richieste di parte avversa e ne chiede il rigetto. In particolare eccepisce la mancata diligenza della ricorrente la quale avrebbe dovuto impedire l'esecuzione delle operazioni fraudolente; afferma di adottare procedure conformi alla normativa in tema di autenticazione forte sia per l'accesso ai sistemi di pagamento sia per la disposizione delle singole operazioni; contesta la non adeguata descrizione delle modalità della presunta truffa da parte della ricorrente, la quale si è limitata ad un mero disconoscimento delle operazioni contestate.

Nelle repliche e nelle controrepliche, le parti si riportano, sostanzialmente, alle rispettive deduzioni, eccezioni e richieste.

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. Si tratta di un pagamento di € 454,35 delle ore 01:56 e di un pagamento di € 37,83 delle ore 02:23 effettuati con carta ***1449 il 26/08/2025; di un pagamento di € 699,50 delle ore 01:50, di un pagamento di € 489,65 delle ore 01:53, di un pagamento di € 70,70 delle ore 02:06, di un pagamento di € 44,18 delle ore 02:07 effettuati con carta ***569 sempre in data 26/08/2025.

Vanno richiamate le fonti normative che regolano la *Strong Customer Authentication* (SCA), rinvenibili negli artt. 97 e 98 della PSD2, 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 ha riferito che in data 25/08/2025 alle 20:01 è stato effettuato un enrollment dell'App su un nuovo smartphone, specificando che, per poter accedere a tale app, l'utente deve inserire il codice cliente (codice composto da 7 cifre che viene assegnato dalla banca al cliente al momento della conclusione del contratto) e la data di nascita, il PIN, l'OTP, per procedere all'attivazione della nuova App.

Relativamente alla disposizione delle operazioni, ha affermato che, in linea generale, l'autenticazione forte del cliente deve avvenire verificando almeno due fattori: il primo è soddisfatto laddove il cliente abbia ricevuto la PUSH inviata al suo device registrato, del quale lui solo è in possesso. Il secondo è soddisfatto laddove il cliente abbia autorizzato la PUSH con dati di sola sua conoscenza (S***Code) o che lo caratterizzano (impronta digitale/riconoscimento facciale).

Nel caso di specie sono stati effettuati diversi accessi a dei portali on-line e predisposti gli acquisti: all'atto del pagamento è stato digitato il numero di carta, mese e anno di scadenza, nome e cognome del Titolare, codice di sicurezza (CVV) ed è stata autorizzata l'operazione digitando lo S***Code/impronta digitale/faceID (secondo fattore SCA: conoscenza o inerenza) all'interno dell'APP.

L'intermediario ha infine rappresentato che, nel caso in esame, prima dell'esecuzione delle operazioni contestate, è stato effettuato un accesso all'app al fine di visualizzare il PAN e il CVV di entrambe le carte.

A supporto delle proprie affermazioni l'intermediario produce evidenze documentali e Log informatici corredati da legende esplicative, che comprovano che le operazioni di pagamento in contestazione sono state autenticate, correttamente registrate e contabilizzate e che non hanno subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o altri inconvenienti.

Alla luce di tali evidenze, il Collegio ritiene assolto l'onere probatorio gravante sull'intermediario in ordine all'autenticazione dell'operazione contestata e compliant con la SCA il sistema di pagamento adottato, tenuto conto dell'utilizzo dei fattori di autenticazione sia per l'enrollment della App (elemento di conoscenza: codice cliente e data di nascita, elemento di possesso: OTP inviato tramite sms), sia per l'accesso in App e per la visualizzazione dei dati della carta (elemento di conoscenza: S***Code, elemento di possesso: app installata sul nuovo device) sia, infine, per l'esecuzione delle singole operazioni (elemento di conoscenza: S***Code, elemento di possesso: app installata sul nuovo device).

In virtù di tale adempimento, si passa alla valutazione del comportamento tenuto dalla ricorrente. 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, la decisione del Collegio di Coordinamento n. 24366/19 secondo la 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." Si evidenzia che la parte ricorrente afferma che le operazioni contestate sono state eseguite a sua insaputa e senza autorizzazione e di averne appreso l'esistenza solo a

seguito della ricezione delle notifiche sull'app di home banking. Tuttavia, a supporto di tale ricostruzione, non produce alcun elemento che possa provare le circostanze di fatto dell'asserita frode subita. Sul punto si richiama il costante orientamento dei Collegi ABF per il quale, l'assenza di allegazioni da parte del ricorrente relative alle modalità con le quali si sarebbe perpetrata la truffa, allorché l'intermediario assolva al proprio onere probatorio inerente l'autenticazione delle transazioni e la conformità alla SCA, è un elemento da cui il Collegio può trarre il proprio convincimento circa la colpa grave del ricorrente medesimo. Nella fattispecie a fronte della prova fornita dall'intermediario, la domanda di parte ricorrente, del tutto carente sotto il profilo delle allegazioni, si risolve nel semplice, formale disconoscimento delle operazioni, senza alcuna concreta ed ulteriore contestualizzazione fattuale, così da impedire di valutare il grado di insidiosità della truffa ovvero l'eventuale colpevolezza del suo comportamento (si vedano ex multis Collegio di Torino, decisioni n. 9395/2025, n. 1802/2025, n. 6623/2024, n. 5133/2022, n. 11710/2021; Collegio di Milano, Decisione n. 19237/2020).

Alla luce di quanto sopra considerato, nonché dell'irrilevanza delle contestazioni sia in tema di mail-alert, dato l'arco temporale ristretto di esecuzione delle transazioni in controversia, sia in tema di anomalia delle disposizioni disconosciute, non potendosi ritenere configurabile in capo all'intermediario un obbligo generale di monitoraggio preventivo delle operazioni di pagamento, il Collegio conclude per il non accoglimento del ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE f.f.