

COLLEGIO DI TORINO

composto dai signori:

(TO) BARENGHI	Presidente
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) CARATOZZOLO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) PUDDU	Membro di designazione rappresentativa dei clienti

Relatore ROBERTO CARATOZZOLO

Seduta del 27/04/2026

FATTO

Con ricorso del 23 gennaio 2026 parte istante chiede all'ABF il riconoscimento del rimborso della somma di € 200,50, corrispondente all'importo di operazioni di pagamento fraudolenti, oltre alla restituzione del contributo di procedura di € 20,00. Afferma il ricorrente di aver ricevuto un messaggio da un'applicazione di messaggistica istantanea proveniente da un account business apparentemente riconducibile a una struttura alberghiera, presso cui aveva effettuato una prenotazione; tale messaggio richiedeva il completamento di una presunta verifica obbligatoria e gratuita dei dati dell'ospite e conteneva un link che rimandava a un sito graficamente credibile e

apparentemente legittimo; eseguiva quindi le operazioni richieste in quanto convinto della legittimità, senza autorizzare consapevolmente i pagamenti verso terzi; successivamente, notava l'addebito di due operazioni anomale da € 100,25 ciascuna. Nelle controdeduzioni l'intermediario resistente contesta le richieste di parte avversa e ne chiede il rigetto. In particolare afferma che le operazioni contestate sono state personalmente autorizzate dal ricorrente con il device usualmente utilizzato per l'operatività online; il cliente ammette di aver inserito i dati della propria carta di debito sul sito truffaldino, a cui ha avuto accesso mediante un link trasmesso via WhatsApp dal truffatore; le affermazioni del cliente assumono valore confessorio, con conseguente esclusione di responsabilità in capo alla banca; le operazioni disconosciute sono state correttamente autenticate, registrate, contabilizzate ed eseguite, in assenza di malfunzionamenti o altri inconvenienti, tramite commercio elettronico; dopo aver disposto le operazioni mediante l'inserimento delle credenziali della carta sul sito dell'esercente, le transazioni sono state confermate da app con il codice OTP, tramite fattore biometrico; ha trasmesso le notifiche PUSH concernenti l'autorizzazione e l'avvenuto pagamento sul device del ricorrente per tutte le operazioni in contestazione; il ricorrente ha violato con colpa grave gli obblighi a suo carico, fermo restando che avrebbe dovuto bloccarsi ed evitare l'autorizzazione dei pagamenti, a fronte dell'incertezza.

Nelle repliche e nelle controrepliche le parti insistono nelle 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 due pagamenti online da € 100,25 ciascuno – per un totale di € 200,50 – eseguiti con carta di debito n. ***5456, tra le ore 22:48 e le ore 22:49 del 29/12/2025, in favore dell'esercente estero A.

In via preliminare, in ordine all'eccezione di inapplicabilità della normativa richiamata a causa dell'esecuzione personale delle operazioni di pagamento da parte del ricorrente, il Collegio rileva come non è presente, agli atti della procedura, alcun tipo di dichiarazione di carattere confessorio del cliente che possa provare che egli abbia eseguito integralmente e per intero i pagamenti oggetto di ricorso.

In proposito si evidenzia che il ricorrente ha ricevuto un SMS proveniente da un account business apparentemente riconducibile alla struttura alberghiera, presso cui aveva effettuato una prenotazione; ritenuta autentica questa, ha effettuato una presunta verifica gratuita e obbligatoria dei dati dell'ospite al fine di mantenere attiva la prenotazione, mediante il collegamento a un sito Internet apparentemente genuino, ha inserito alcuni dati richiesti e confermato l'operazione mediante fattore biometrico, a seguito del raggio e nella convinzione di completare la procedura di verifica. Alla luce di tali elementi, le operazioni di pagamento oggetto del ricorso sono da considerarsi come non autorizzate e dunque sottoposte al regime normativo sopra richiamato; l'eccezione preliminare va, dunque, rigettata.

Passando al merito della questione, 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 ha sostenuto che le operazioni contestate sono state autenticate tramite notifica PUSH inviata in app e validata con il codice OTP, mediante inserimento del fattore biometrico, previo inserimento delle credenziali della carta sul sito di commercio elettronico.

A supporto delle proprie affermazioni l'intermediario ha prodotto evidenze documentali, Log informatici corredati da legende esplicative e tracciate dell'intermediario N*, in cui risulta che le operazioni sono state disposte con le credenziali della carta di debito n. ***5456 intestata al ricorrente, tramite commercio elettronico 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 loro esecuzione o altri inconvenienti.

Alla luce di tali evidenze, il Collegio ritiene assolto l'onere probatorio gravante sull'intermediario in ordine all'autenticazione delle operazioni contestate e *compliant* con la SCA il sistema di pagamento adottato, tenuto conto dell'utilizzo dei fattori di autenticazione per l'esecuzione delle singole operazioni di bonifico (elemento di inerenza: fattore biometrico - TOUCH; elemento di possesso: notifica PUSH in app installata sul device del ricorrente).

Si passa, quindi, all'esame dell'ulteriore aspetto relativo alla valutazione del comportamento tenuto dal ricorrente nel corso della vicenda sottoposta alla 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, 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 dalla documentazione versata in atti appare chiaro che le operazioni contestate siano scaturite da un fenomeno di *phishing* realizzato a danni del ricorrente. In particolare, dalla denuncia prodotta dallo stesso ricorrente questi ha affermato di aver ricevuto, in data 29/12/2025, tramite app di messaggistica istantanea, un messaggio proveniente da un account business apparentemente riconducibile a una struttura alberghiera, presso cui aveva effettuato una prenotazione; tale messaggio, contenente informazioni corrette e specifiche inerenti la prenotazione effettuata, richiedeva di effettuare una presunta verifica gratuita e obbligatoria dei dati dell’ospite al fine di mantenere attiva la prenotazione; la procedura avveniva mediante il collegamento a un sito Internet riconducibile alla struttura; inseriva alcuni dati richiesti in quanto convinto della legittimità della procedura e provvedeva a confermarla, con la tecnica biometrica.

Sebbene non versata in atti, sulla base delle stesse dichiarazioni di parte ricorrente la messaggistica istantanea tramite la quale il cliente si è collegato ad un sito truffaldino non è riconducibile all’intermediario. Sotto questo aspetto è palese, dunque, come la truffa sia stata attuata mediante un canale del tutto estraneo all’intermediario convenuto e come non sussista alcun presupposto o altro elemento che possa giustificare un radicamento di un’eventuale responsabilità concorrente dell’intermediario.

Pertanto, vi sono elementi tali da escludere qualsiasi responsabilità in capo all’intermediario e, di contro, da configurare in capo al ricorrente una sua condotta colposa, in quanto ha inserito le proprie credenziali accedendo ad un link truffaldino non riconducibile all’intermediario, e, dunque, ha di fatto permesso la realizzazione della truffa, non avendo impiegato quel livello di diligenza medio sufficiente a scongiurare il pericolo e ad impedire la detta truffa.

Alla luce di quanto rilevato, il Collegio conclude per il non accoglimento del ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE f.f.