

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) PUDDU	Membro di designazione rappresentativa dei clienti

Relatore GIANNI PUDDU

Seduta del 09/02/2026

FATTO

Riscontrato negativamente il reclamo, in data 18.10.2025, parte ricorrente proponeva ricorso avanti l'ABF.

Essa parte, in sede di ricorso, contestava che era stata compiuta una transazione *e-commerce* in maniera fraudolenta contro il suo consenso e la sua volontà a causa di gravi falle nel sistema di gestione dei dati bancari da parte dell'intermediario convenuto. Precisava di non aver fornito il PIN per l'accesso al conto corrente, di non aver mai installato alcuna app e sosteneva che dal momento in cui l'intermediario aveva cominciato a collaborare con alcune aziende di dubbia reputazione, essa parte aveva iniziato a ricevere informazioni sulla disponibilità dei dati legati al proprio conto sul dark web. Sottolineava che l'operatore inviava e-mail e messaggi identici a quelli inviati dall'intermediario. Domandava, il rimborso della somma di € 530,00.

L'intermediario, in sede di controdeduzioni, eccepiva che il cliente aveva con la propria condotta, connotata da colpa grave, consentito al truffatore di perfezionare la frode, avendo rilasciato le credenziali di accesso alla sua *home banking*. Allegava di aver attuato, da molto tempo, una campagna per avvertire la clientela in merito a tale fenomeno. In ordine all'operazione oggetto di ricorso rappresentava, altresì, che essa risulta eseguita mediante l'utilizzo delle credenziali di sicurezza personalizzate, su sito

“3d secured” e validata attraverso l'utilizzazione del codice OTP generato dal dispositivo in possesso del cliente. Precisava che la mail allegata al ricorso, che il cliente definisce fraudolenta, non è altro che la prima comunicazione (genuina) inviata, contenente il codice per l'attivazione del Mobile Token, che l'operazione disconosciuta risulta stata eseguita *online* attraverso l'utilizzo del numero della carta di credito abbinata al relativo Pin e che il cliente ha ricevuto sul proprio numero di cellulare, il messaggio SMS relativo all'attivazione del Mobile Token, nonché i messaggi relativi all'operazione contestata. Sottolineava che nessuna falla nel sistema di sicurezza ha permesso a terzi di venire a conoscenza dei dati sensibili del cliente. Domandava, quindi, il rigetto del ricorso.

L'operazione contestata consiste in una transazione *e-commerce* dell'importo di € 530,00, eseguita in data 16.10.2025 alle ore 12:04. Sono in atti l'estratto conto relativo e la denuncia.

DIRITTO

Il fraudolento utilizzo di servizi di pagamento è disciplinato 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 al mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

La normativa appena richiamata prevede che qualora l'utilizzatore neghi di aver autorizzato un'operazione di pagamento (il consenso del pagatore è un elemento necessario per la corretta esecuzione di un'operazione di pagamento, in assenza del quale essa non può considerarsi autorizzata- art. 5), grava sull'intermediario provare che l'operazione stessa è stata autenticata, correttamente registrata, contabilizzata, e che durante la sua esecuzione non si siano verificati malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti (art. 10). Quanto precede trova un limite nella circostanza che l'utilizzatore abbia agito mancando di osservare in modo fraudolento o gravemente colposo gli obblighi di corretto utilizzo e di custodia degli strumenti di pagamento, situazione nella quale l'art. 12, comma 4, del d.lgs. n. 11/2010, prevede che l'utilizzatore sopporti per intero le perdite subite.

Nel caso che ci occupa, il Collegio rileva come l'intermediario alleggi producendo le relative evidenze informatiche, che l'operazione disconosciuta è stata correttamente autenticata e autorizzata con l'utilizzo dei seguenti fattori: per l'attivazione del Mobile Token: elemento di conoscenza, PIN; elemento di possesso, OTP ricevuto via SMS; per l'accesso all'app propedeutico all'operazione: elemento di conoscenza, PIN; elemento di possesso: OTP (silente) generato in App; per l'operazione: elemento di conoscenza, PIN; elemento di possesso, OTP (silente) generato in App.

Alla luce di quanto sopra esposto, sulla scorta delle evidenze documentali prodotte dall'intermediario resistente, può, quindi, sostenersi che la procedura seguita dall'intermediario sia conforme alla SCA (Strong Customer Authentication) (si richiamano, tra le altre, le Decisioni del Collegio di Torino n. 1137/2024 e n. 4653/2023).

Avendo fornito l'intermediario, la prova posta a suo carico dall'art. 10 d.lgs. 11/2010 è, dunque, necessario passare alla valutazione del comportamento dell'utente, nei

confronti del quale parte resistente ha eccepito una condotta contraddistinta da colpa grave, ai fini dell'applicazione delle previsioni del successivo art. 12 del suddetto d.lgs.. Dalla documentazione agli atti emerge come le operazioni contestate siano scaturite da un fenomeno di *spoofing* e *vishing*, realizzato ai danni di parte ricorrente, la quale riferisce di aver ricevuto, un sms riconducibile all'intermediario che la informava di un presunto pagamento di € 985,00, invitandola, per evitarne l' esecuzione, a contattare un' utenza mobile, di aver chiamato il numero indicato, interloquendo con un sedicente operatore bancario e seguendone le istruzioni, per accorgersi solo successivamente di essere stata vittima di una frode.

Sulla base delle produzioni in atti si può rilevare che il documento indicato da parte ricorrente quale messaggio civetta, non appare essere il messaggio civetta da cui, secondo quanto riferito dalla stessa nella denuncia, sarebbe scaturita la frode, non sussiste, tra l' altro, in seno al medesimo, alcuna menzione del presunto pagamento di € 985,00 che avrebbe indotto la ricorrente a contattare telefonicamente il truffatore. Quanto allo screenshot relativo alla chiamata del truffatore, esso proviene da un numero di cellulare non riconducibile all' intermediario ma coincidente, invece, con quello indicato nella denuncia come contatto della chiamata truffaldina ricevuta dall'istante.

Sulla base delle circostanze emerse e del materiale probatorio in atti, deve, quindi, concludersi, che la condotta della ricorrente sia stata connotata da colpa grave avendo, essa parte, dato seguito ad un messaggio sms di incerta provenienza, dal contenuto scarsamente verosimile ed avendo seguito acriticamente, le direttive di un sedicente operatore dell'intermediario, attraverso un'utenza telefonica mobile non riconducibile all' intermediario medesimo (si richiamano, ex multis, Collegio di Torino, Decisioni n. 5143/2022 e n. 7063/2022). Inoltre, parte ricorrente neppure ha allegato il messaggio civetta, si rammenta in merito che secondo gli orientamenti condivisi dai Collegi, tale mancata allegazione determina, di per sé, il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e pertanto risulti possibile un legittimo affidamento dell'utente circa la genuinità del messaggio (si richiama ex multis Collegio di Torino, Decisione n. 1440/2024)

Per gli esposti motivi, il ricorso non può, pertanto, essere accolto.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE