

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 GIANNI PUDDU

Seduta del 27/04/2026

FATTO

All'esito infruttuoso del reclamo, in data 10.11.2025, veniva proposto ricorso avanti all'ABF.

Parte ricorrente allegava di aver subito, in data 30.10.2025, una frode informatica, a seguito della ricezione di una telefonata da un numero riconducibile ai contatti ufficiali dell'intermediario, nell'ambito della quale l'interlocutore, identificatosi come addetto del dipartimento antifrode dell'intermediario la aveva informata di una presunta clonazione delle proprie credenziali legate all'applicazione di home banking e dell'effettuazione di due bonifici fraudolenti, rispettivamente per € 5.000,00 ed € 15.000, da un telefono agganciato ad una cella nella zona del Friuli. Il presunto operatore le aveva poi indicato la necessità di eseguire una specifica procedura per bloccare tale tentativo fraudolento. Parte ricorrente precisava, inoltre, che nel corso della predetta telefonata, aveva, altresì, ricevuto sul proprio cellulare una serie di sms nella cronologia di messaggistica già esistente e riportante la denominazione dell'intermediario, i quali sembravano confermare il reale intervento della banca e che, inoltre, riceveva da parte dell'interlocutore un ulteriore sms dal contatto '*alertmedio*' contenente un nuovo codice cliente. Quindi riferiva come, seguendo le istruzioni fornite dall'interlocutore e nella convinzione di eseguire un'operazione di blocco automatico, avesse disposto un bonifico di € 20.000,00, pari alla cifra asseritamente

sottratta, recante causale “*b / c auto*”. Allegava, altresì, che, dal proprio conto, non erano mai stati fatti bonifici di valore superiore ad € 10.000,00, come attestato dagli estratti conto versati in atti e che, su indicazione dell’operatore, aveva anche proceduto ad installare un antivirus sul telefono per effettuare una scansione, e successivamente, ad installare un ulteriore antivirus per rimuovere eventuali bug. Sempre su richiesta dell’interlocutore, rispondendo alle mail ricevute per l’annullamento del bonifico, gli aveva inviato uno screenshot dell’operazione effettuata e un estratto conto degli ultimi tre mesi. Alle ore 19 circa, insospettita da tali richieste, aveva verificato l’indirizzo e-mail da cui provenivano le comunicazioni, che si rivelava non essere quello ufficiale dell’intermediario, quindi alle ore 19:30, aveva contattato telefonicamente la parte resistente, al fine di verificare quanto riportato dall’interlocutore e ricevuto conferma, da un operatore autentico, che si era trattato di una truffa, concludeva, quindi, la telefonata con l’operatore fraudolento e contattava l’intermediario per disconoscere formalmente l’operazione e richiedere il richiamo del bonifico di € 20.000,00. La mattina successiva presso la filiale dell’intermediario, apprendeva che, nonostante la sua tempestiva richiesta, il richiamo del bonifico era stato disposto solo alle ore 7:00; su indicazione dell’operatrice della filiale, presentava denuncia alle autorità per aver diritto al risarcimento da parte dell’assicurazione, dal canto suo l’intermediario le comunicava telefonicamente di aver concluso la pratica di recall del bonifico, riferendo che l’unico modo per recuperare la cifra in questione era tramite vie legali. Precisava parte ricorrente che la frode subita non consisteva in un semplice caso di phishing, ma in una truffa perpetrata con tecniche combinate di SMS spoofing e caller ID spoofing, modalità riconosciute dalla giurisprudenza dell’ABF come sofisticate e particolarmente insidiose e quindi idonee ad escludere la colpa grave del cliente (cfr. Milano n. 6156/2025, Palermo n. 5652/2025, Milano n. 5401/2025) e che, come più volte rilevato dall’ABF, l’attività bancaria è soggetta a un obbligo di diligenza professionale qualificata (art. 1176, co. 2, c.c.), che impone l’adozione di sistemi di sicurezza tecnologicamente avanzati, capaci di prevenire le frodi e di monitorare le operazioni per rilevarne le anomalie: nel suo caso la banca non si sarebbe avveduta dell’evidente anomalia dell’operazione controversa rispetto all’operatività storica del conto, così contribuendo alla produzione del danno. Contestava, altresì, che l’intermediario sarebbe stato negligente nella gestione successiva alla segnalazione della frode: nonostante la richiesta di richiamo del bonifico fosse stata avanzata alle ore 19:40 del 30 ottobre 2025, infatti, la banca avrebbe atteso fino alle 07:00 del giorno successivo per inoltrarla. Nel replicare alle controdeduzioni, la parte ricorrente, ulteriormente precisava che, sebbene avesse personalmente disposto il bonifico, il proprio consenso era stato chiaramente carpito in modo ingannevole e che l’operazione sarebbe, quindi, da intendersi sostanzialmente “non autorizzata”. La banca non avrebbe, inoltre, adottato presidi di sicurezza ulteriori e specifici alla luce delle anomalie dell’operazione. Parte ricorrente avrebbe agito in un contesto di rapido e concitato susseguirsi delle richieste del truffatore, la chiamata dal numero ufficiale della banca e la ricezione di SMS nella chat autentica avrebbero ridotto, oggettivamente, la propria capacità critica ed in ogni caso, la propria condotta non potrebbe qualificarsi come gravemente colposa. Contestava, inoltre, nuovamente la violazione da parte dell’intermediario dell’obbligo di monitoraggio delle operazioni anomale e che le campagne informative condotte non risulterebbero attinenti al caso concreto. Domandava, quindi, in via principale, il rimborso della somma di € 20.000,00; in via subordinata, richiedeva il riconoscimento del concorso di colpa dell’intermediario e il rimborso parziale dell’importo sottratto.

L'intermediario, in sede di controdeduzioni, rilevava come, dalle dichiarazioni fornite dall'istante, emergesse che la vicenda in contestazione fosse parte al filone delle frodi compiute tramite la tecnica di social hacking, il caso di specie non rientrerebbe, quindi, nell'ambito delle frodi perpetrate mediante la tecnica di phishing, poiché l'operazione risulta eseguita personalmente dalla ricorrente, né, peraltro, l'interlocutore telefonico era in possesso delle credenziali personali di accesso all'Home Banking. Di conseguenza, la responsabilità sarebbe da ascrivere interamente alla parte ricorrente, che dichiara di aver eseguito personalmente e interamente l'operazione. Allegava, altresì, che la parte ricorrente avrebbe prestato una collaborazione attiva "all'altrui macchinazione fraudolenta" e che la chat, avente presunta denominazione dell'intermediario, non sarebbe invero riconducibile alla parte resistente: parte ricorrente risultava aver ricevuto altri sms su un'altra chat non genuina e con un nominativo non attribuibile all'intermediario con una visualizzazione chiaramente inusuale, inoltre, ulteriore prova dell'evidente inattendibilità delle comunicazioni ricevute sarebbe fornita dai messaggi di alert recapitati, le uniche comunicazioni confluite all'interno della chat con denominazione dell'intermediario. Eccepiva, altresì, che l'operazione di bonifico disposta dalla parte ricorrente risulta effettuata in favore di un conto sconosciuto, presso un intermediario terzo estraneo alla banca e che il beneficiario risulta ignoto alla ricorrente e corrisponde all'effettivo titolare del conto corrente di destinazione in base alle verifiche VOP (verification of payee). Sottolineava, inoltre, che l'indirizzo di posta elettronica dal quale parte istante ha ricevuto le e-mail era evidentemente anomalo e che il cliente provvedeva a mettersi in contatto con la banca solo alle ore 20:04. Rappresentava di condurre un'assidua campagna informativa a cadenza periodica al fine di sensibilizzare i propri clienti sulla sicurezza digitale e di non aver potuto rilevare la presunta anomalia nell'operazione in oggetto in quanto non è possibile escludere a priori che la propria clientela abbia la necessità di effettuare operazioni diverse dalle proprie abitudini per far fronte ad esigenze tempo per tempo manifestate, l'operazione di bonifico in oggetto risulterebbe, inoltre, correttamente autenticata, registrata e contabilizzata senza anomalie e mediante il corretto inserimento del doppio fattore di autenticazione in possesso solo all'istante. Precisava di essersi attivata al fine di recuperare l'importo illegittimamente sottratto alla ricorrente, informando l'istituto beneficiario della frode in questione e inserendo richiesta di richiamo di tale disposizione, che la banca beneficiaria, tuttavia, rifiutava. In sede di controrepliche insisteva sulla circostanza che la parte ricorrente ha confermato di aver disposto e autorizzato personalmente il bonifico, escludendo, quindi, nella fattispecie, applicazione dell'art. 10 del d.lgs. 11/2010. Domandava, quindi, il rigetto del ricorso.

L'operazione contestata consiste in un bonifico, recante causale "*b / c auto*", di € 20.000,00 eseguito alle 18:02 del 30/10/2025, tramite home banking. E' in atti il relativo estratto conto, così come 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 il medesimo sopporti per intero le perdite subite.

Nelle proprie controdeduzioni l'intermediario ha eccepito l'inapplicabilità, alla fattispecie, della PSD2 in ragione delle dichiarazioni confessorie rese dalla ricorrente, tali da escludere per l'operazione disconosciuta, il difetto di autorizzazione. L'eccezione è da ritenersi fondata e deve essere accolta con valore assorbente di tutte le altre doglianze articolate in ricorso. La parte ricorrente ha, infatti, riferito, con dichiarazioni in atti di natura confessoria che, pur vittima di un raggirio da parti di terzi, ha personalmente disposto l'operazione oggetto del presente ricorso. Più precisamente ha allegato di aver ricevuto una telefonata dal numero ufficiale della banca con la quale un presunto operatore dell'intermediario paventava la fraudolenta disposizione di bonifici dal suo conto corrente e di aver, per sventare tale frode, seguito le indicazioni del presunto operatore predisponendo un bonifico, con causale "b / c auto", pari a € 20.000 (lo stesso importo delle presunte operazioni fraudolente) verso un beneficiario ed un conto corrente del tutto ignoti, persuasa di mettere, così, in sicurezza la somma, accorgendosi solo successivamente di aver che si trattava di una truffa.

Le circostanze, pacifiche in atti, sopra descritte determinano, quindi, l' inapplicabilità, nella fattispecie, della normativa c.d. "PSD2", la quale concerne i mezzi di pagamento e il loro uso indebito da parte di terzi, ma non può estendersi alle operazioni direttamente e personalmente disposte dal ricorrente, che come tali sono regolarmente autorizzate: *"l'esplicita ammissione del cliente di aver personalmente eseguito le operazioni, per quanto sotto la pressione truffaldina, esclude già in radice l'esistenza del presupposto necessario ai fini del preteso rimborso, vale a dire il difetto di autorizzazione delle operazioni medesime"* (Collegio di Torino Decisione n. 10900/2024, nello stesso senso, ex multis, Collegio di Torino, Decisioni n. 8802/2024, n. 10071/2024, n.10067/2024; Collegio di Roma, Decisione n. 1414/2023; Collegio di Milano, Decisione n. 2038/2023).

Peraltro, non risultano, in ogni caso, provate circostanze tali, da indurre il Collegio a ritenere il sussistere di un apporto causale alla frode da parte dell'intermediario ed anche il tentativo di recall appare effettuato conformemente alla normativa, si rammenta, in merito, che l'art 5, comma quarto, D. lgs. 11/2010 prevede la revocabilità di un ordine di pagamento *"purché' ciò avvenga prima che l'ordine di pagamento diventi irrevocabile ai sensi dell'articolo 17"* e che a norma del successivo art. 17, comma 1: *"..... una volta ricevuto dal prestatore di servizi di pagamento del pagatore, l'ordine di pagamento non può essere revocato dall'utente"*. Né ha, l' intermediario, obblighi di monitoraggio ex ante delle operazioni di pagamento (Collegio di Torino, decisione n. 3546/2026) ed anzi la condotta della parte ricorrente che, senza operare

verifica alcuna, ha disposto il pagamento oggetto di ricorso a beneficio di un soggetto terzo estraneo, appare connotata da colpa grave.

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

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE