ABF Decisione n. 9922 del 13 novembre 2025, Collegio di Torino

ABF – BONIFICO – DISCONOSCIMENTO - ONERE DELLA PROVA – COLPA

MASSIMA

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 tale valutazione 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.

LUCCHINI GUASTALLA, Presidente; GRECO, Membro designato dalla Banca d'Italia; CARATOZZOLO, Membro designato dalla Banca d'Italia; SPENNACCHIO, Membro di designazione rappresentativa degli intermediari; D'ANGELO, Membro di designazione rappresentativa dei clienti.

FATTO

Con ricorso del 26 maggio 2025 parte istante chiede all'ABF il riconoscimento del rimborso della somma di € 17.830,00 corrispondente all'importo di operazioni di pagamento fraudolente eseguite a seguito di una subita truffa.
Afferma la ricorrente di essere stata indotta ad autorizzare diversi bonifici istantanei, nella convinzione di stare stornando delle operazioni di bonifico fraudolenti, da un sedicente operatore antifrode di altro intermediario, presso il quale il marito è titolare di un proprio conto corrente; la truffa è scaturita da un SMS apparentemente proveniente da tale intermediario, al quale il marito ha risposto; nel corso della telefonata il sedicente operatore riferiva la compromissione dell'indirizzo IP del loro computer e della conseguente necessità di provvedere a mettere al sicuro tutti i conti correnti, in quanto in pericolo, inducendo entrambi i coniugi ad utilizzare un software per concedere il controllo da remoto del computer e lasciarlo operare sui conti correnti; le operazioni in contestazione venivano eseguite sia dal conto intestato al marito acceso presso diverso intermediario, sia dai conti a lei intestati accesi presso l'intermediario resistente, e venivano indirizzati allo stesso beneficiario, su conto acceso presso un terzo intermediario; le venivano sottratti complessivamente € 17.830,00 tramite due bonifici istantanei, di € 5.200,00 e di € 9.980,00, il cui ammontare corrisponde all'intera disponibilità presente sul conto a valere sul quale sono stati eseguiti ed un bonifico istantaneo di € 2.650,00 eseguito a valere sul conto corrente cointestato con le aderenti al presente ricorso; avvedutasi della truffa subita, chiedeva all'intermedio convenuto di bloccare il denaro sul conto corrente del beneficiario, nonché il rimborso dei bonifici

eseguiti a causa del raggiro; provvedeva, inoltre, a sporgere denuncia presso le competenti autorità.
Nelle controdeduzioni l'intermediario resistente contesta le richieste di parte avversa e ne chiede il rigetto. In via preliminare eccepisce l'inapplicabilità della normativa dettata dalla PSD2, in quanto tutte le operazioni sono state autorizzate dalla stessa ricorrente; nel merito rileva che tutte le operazioni sono state correttamente autenticate con doppio fattore, previo accesso all'*Home banking* della cliente la quale avrebbe potuto avvedersi della truffa sin dalla prima operazione, in quanto a seguito di ogni autorizzazione le veniva inviata un'e-mail di conferma; afferma che una volta disposti, i bonifici "*instant*" non possono essere bloccati, divenendo il pagamento irrevocabile; contesta il comportamento della ricorrente la quale, con grave negligenza, ha cliccato su un link indicato in un SMS, inserendo le proprie generalità e il numero di telefono a cui essere ricontattata; nulla può essere eccepito all'Istituto di credito resistente, dato che il numero della chiamata ricevuta dal marito della ricorrente non è riconducibile alla resistente, ma a diverso intermediario.
Nelle controdeduzioni e nelle controrepliche entrambe le parti sostanzialmente insistono nelle rispettive richieste e contestazioni, apportando qualche ulteriore precisazione fattuale.

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 tre bonifici, disposti in data 12.04.2025 per la somma complessiva di € 17.830,00, di cui due di importo rispettivamente di € 5.200,00 e di € 9.980,00, effettuati dal conto intestato alla ricorrente (*OMISSIS*) ed un altro di € 2.650,00 eseguito dal conto (*OMISSIS*) cointestato tra la ricorrente e le aderenti al ricorso.
In ordine all'eccezione relativa all'inapplicabilità della normativa vigente alle operazioni in contestazione, essendo state queste eseguite personalmente dalla parte ricorrente e conseguentemente autorizzate, nonostante la subita truffa, il Collegio osserva che dalle evidenze prodotte in atti non è possibile ricostruire, con chiarezza e certezza, se parte ricorrente abbia interamente eseguito le operazioni disconosciute ovvero si sia limitato ad autorizzarle a seguito del preventivo inserimento da parte dei malfattori. Ne deriva che la normativa dettata dalla PSD2 è applicabile al caso di specie in quanto, secondo l'orientamento costante dei Collegi, questa non trova applicazione solo qualora le operazioni siano eseguite per intero dal pagatore, con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione.
Per tali motivi, il Collegio rigetta l'eccezione in esame.
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 riferito che le operazioni contestate sono state autenticate tramite notifica PUSH sul *device* della ricorrente, autorizzata tramite "tap" sulla stessa con inserimento dell'elemento biometrico, previo accesso all' *home banking* via web con PIN e OTP generata da App. Ha affermato che una volta eseguito l'accesso in *Home Banking* i bonifici sono stati correttamente disposti, validati a seguito di riepilogo delle operazioni ed autorizzati: ha trasmesso una notifica PUSH al *device* con specifico ID, abilitato dalla ricorrente, che è stata "tappata" dall'utente; avendo il *device* riconosciuto positivamente l'elemento biometrico dell'utente che ha confermato la notifica PUSH, l'operazione è andata a buon fine.
A supporto delle proprie affermazioni l'intermediario produce evidenze documentali e Log informatici corredati da legende esplicative, che comprovano 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.
Alla luce di tali evidenze, il Collegio ritiene assolto l'onere probatorio gravante sull'intermediario in ordine all'adozione delle prescrizioni normative dettate in tema di autenticazione forte per l'utilizzo dello strumento di pagamento (*Strong Customer Authentication*) sia per l'accesso via web (elemento di conoscenza: codice cliente e PIN; elemento di possesso: OTP generato in App) sia per le singole operazioni (elemento di possesso: notifica *push* in App; elemento di inerenza: biometria).
Si passa, quindi, all'esame dell'ulteriore aspetto relativo alla valutazione del comportamento tenuto dal ricorrente nel corso della vicenda sottoposta a 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, 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."

Si evidenzia che dalla documentazione versata in atti appare chiaro che le operazioni contestate siano scaturite da uno schema illecito articolato, avviato prima con un fenomeno di *smishing* realizzato ai danni del marito della parte ricorrente, seguito da un *caller ID spoofing* (*spoofing* applicato alla chiamata), prima ai danni del marito e poi della moglie, attuale ricorrente, durante il quale veniva concesso il controllo da remoto del proprio pc con download di un'apposita applicazione.

In particolare, nella denuncia, l'istante ha rappresentato quanto segue:

- in data 12.04.2025, alle ore 11:53, il marito riceveva un SMS apparentemente proveniente dalla sua banca (intermediario X), riportante un link ove inserire le proprie generalità e numero di telefono per essere ricontattati e verificare eventuali accessi anomali nel conto;
- il marito procedeva in tal senso e veniva ricontattato dal n. 023****973, da un sedicente operatore dell'intermediario X, che gli riferiva la necessità di intervenire entro le ore 18:00 sul suo conto, ove erano già stati bloccati dei bonifici fraudolenti, per procedere con il rimborso degli stessi;
- poiché si trovava con il marito ad una mezzora da casa, si mettevano in macchina per tornare alla propria abitazione, restando a telefono con il presunto operatore, il quale, nel frattempo, spiegava loro che la frode era partita da un attacco all'IP del wi-fi e che, pertanto, sarebbe stato necessario intervenire su tutti i device collegati alla rete;
- una volta giunti a casa, accedevano da PC alle rispettive aree riservate bancarie e condividevano altresì lo schermo con l'ignoto interlocutore cosicché quest'ultimo potesse guidarli nella procedura idonea a tutelare i conti;
- il sedicente funzionario della banca procedeva, dunque, a fare dei bonifici prima dal suo conto, poi da quello cointestato con le aderenti al ricorso e poi da quello del marito;
- solo dopo l'esecuzione delle operazioni, insospettiti, prendevano contatto con la banca resistente.

A sostegno dei fatti occorsi, parte ricorrente ha altresì allegato screenshot dell'SMS civetta ricevuto e del registro chiamate, evidenza del download dell'applicazione Any Desk per il controllo da remoto del pc e screenshot degli ulteriori sms truffaldini ricevuti nel corso della frode.

In merito a tale documentazione si osserva, innanzitutto, che i primi screenshot si riferiscono a SMS e chiamate ricevute dal marito dell'odierna ricorrente:

- il primo messaggio civetta risulta pervenuto alle ore 11:53 da un numero di telefono cellulare sconosciuto e fa riferimento, nel corpo del messaggio, all'intermediario X – diverso dall'odierna resistente – PSP del marito della ricorrente;

- tale messaggio non contiene punteggiatura e il link ivi contenuto non è riconducibile all'intermediario X;
- la telefonata truffaldina risulta ricevuta alle ore 14:28 da un numero che sembra riconducibile all'intermediario X: l'istante sul punto ha, infatti, allegato una schermata del sito internet di tale intermediario, ove tra i contatti risulta riportato anche il recapito telefonico in questione;
- alle ore 16:05 risulta essere stata scaricata la app AnyDesk.

Gli ulteriori messaggi truffaldini, verosimilmente ricevuti dalla ricorrente mentre era in corso la telefonata con il sedicente operatore dell'intermediario X, riportano come mittente il nome dell'odierna resistente, sono inquadrabili pertanto nello "*spoofing*", e contengono il seguente testo "blocco eseguito 5.200.00" e "blocco eseguito 9.980,00"; nella medesima chat è inserito anche un messaggio che dà atto di un aggiornamento di sicurezza in corso, messaggio – questo – che risulta presente anche in un ulteriore sms proveniente dal mittente "postale".

Alla luce di tale circostanze e tenuto conto anche del tenore dei messaggi truffaldini, della loro provenienza, nonostante l'orientamento dei Collegi ABF rilevi la forte insidiosità del meccanismo di aggressione consistente nell'invio di sms apparentemente dalla stessa utenza dell'intermediario - *spoofing* conclamato - generalmente valutato come idoneo ad escludere la colpa grave del cliente, si rileva che, nel caso di specie, proprio la ricorrente ha collaborato fattivamente con il malfattore al compimento della vicenda truffaldina, seguendo le istruzioni ricevute telefonicamente, inserendo le credenziali richieste ed autorizzando le operazioni e, per di più, concedendo anche l' acquisizione del controllo da remoto del proprio pc e condividendo la schermata dei conti dai quali sono state eseguite le operazioni. Il Collegio ritiene, pertanto, di ravvisare un concorso di colpa tra le parti, in relazione, da un lato, alla grave negligenza dell'utente che ha agevolato il compimento della truffa e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario.

Tale concorso di colpa si ripartisce, nella fattispecie, nella misura di un terzo a carico dell'intermediario e di due terzi a carico della parte ricorrente (conforme Collegio di Torino, decisione 12068/2024).

In conclusione in Collegio accoglie parzialmente le richieste di parte ricorrente e condanna l'intermediario alla restituzione in favore di questa della somma di € 5.943,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.943,00

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.