

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) GENOVESE	Membro di designazione rappresentativa degli intermediari
(BO) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore ANDREA GENOVESE

Seduta del 03/02/2026

FATTO

Insoddisfatta dell'interlocuzione con l'intermediario nella fase del reclamo, con ricorso n. 1900937 del 02.10.2025, la parte ricorrente si rivolge all'Arbitro al quale chiede di voler disporre il rimborso della somma di Euro 3.900,00, corrispondente all'importo di n. 1 operazione di pagamento fraudolentemente eseguita mediante bonifico. A sostegno della pretesa, deduce che: (i) è titolare del conto corrente n. **202 acceso presso l'intermediario resistente; (ii) in data 15.09.2025, alle ore 17:13, riceveva una telefonata proveniente dal numero 02**, che, da una verifica effettuata, risultava riconducibile all'intermediario; (iii) in occasione della telefonata, un messaggio preregistrato le comunicava che era in atto un tentativo di esecuzione di un bonifico sospetto e che sarebbe stata contattata da un operatore del servizio antifrode dall'utenza recante numero 347**; (v) alle 17:14 dello stesso giorno riceveva la telefonata preannunciata, in occasione della quale l'interlocutore le riferiva che sarebbe stata contattata dai Carabinieri per attuare una procedura di ricerca del truffatore ed evitare la perdita della somma di Euro 3.900,00; (vi) durante la telefonata, al fine di rintracciare il truffatore, avrebbero dovuto simulare l'operazione di bonifico contestata; (vii) seguiva quindi le istruzioni dal sedicente operatore, senza materialmente confermare alcuna operazione di pagamento. Tale operazione veniva confermata dal

sedicente operatore, riuscito a entrare in maniera fraudolenta nell'home banking; (viii) riceveva, poi, un SMS di conferma dell'operazione simulata e uno di conferma del blocco del bonifico simulato; (ix) terminata la telefonata, durata circa mezz'ora, contattava la stazione dei carabinieri precedentemente indicata dall'interlocutore. Le veniva riferito che non vi era un carabiniere con il nominativo indicato; (x) resasi conto di essere stata vittima di una frode, alle 17:59 contattava il numero verde dell'intermediario per chiedere il blocco dell'operazione, riuscendo a parlare con un operatore solo alle 18:07; (xi) l'operatore si rifiutava di annullare il pagamento nonostante fosse ancora possibile intervenire; (xii) esaminando gli ultimi 20 mesi di entrate e uscite dal conto corrente, non risultano bonifici in uscita superiori a Euro 1.000,00; (xiii) l'operazione doveva essere considerata anomala per importo e frequenza, ma la banca non ha effettuato le dovute verifiche prima di consentirne l'esecuzione. Inoltre, quando ha chiesto il blocco del bonifico, l'intermediario non ha provveduto.

Costituitosi, l'intermediario chiede all'Arbitro, in via preliminare, di dichiarare inammissibile il ricorso poiché il ricorrente non ha atteso la risposta del reclamo (inviata il 14.10.2025), presentando quasi contestualmente sia il reclamo (26.09.2025) che il ricorso (02.10.2025). Nel merito chiede disporsi il rigetto del ricorso perché infondato, sul rilievo che: a) il ricorrente ha effettuato un bonifico su indicazione di un terzo sconosciuto; b) in sede di denuncia, di compilazione del modulo di contestazione e in occasione del colloquio con il personale della filiale, il ricorrente ha ammesso di avere eseguito il bonifico contestato; c) anche la documentazione tecnica conferma che il bonifico ordinario è stato effettuato tramite l'App installata sul dispositivo della parte ricorrente e autorizzato tramite fattore biometrico; d) non risultano nuove attivazioni dell'App nel giorno in cui è stato effettuato il bonifico in questione; e) l'operazione di pagamento è stata eseguita dal dispositivo del ricorrente su cui l'App è installata, a seguito dell'accesso avvenuto alle ore 17:24, autorizzata mediante fattore biometrico; f) nessuna ulteriore utenza risulta collegata alla banca multicanale del ricorrente; g) di conseguenza, all'operazione disconosciuta non è applicabile il regime di cui alla PSD 2 (Payment Services Directive 2, Direttiva UE 2015/2366), in ragione delle dichiarazioni confessorie rese dal ricorrente; h) non ha alcuna responsabilità per quanto riguarda la telefonata ricevuta dal ricorrente in occasione della quale è stata consumata la frode; i) sebbene l'elenco degli SMS prodotti dalla parte ricorrente non è completo, tanto basta per dimostrare che l'unico dei messaggi fraudolenti visibili, con scritto "*bonifico bloccato con successo*", non è conforme a quelli genuini inviati in precedenza; l) i messaggi non autentici erano immediatamente riconoscibili in quanto privi di incipit, di riferimenti al conto corrente interessato e del numero telefonico da contattare per ricevere le informazioni; m) presso di esso è radicato il conto corrente del beneficiario del bonifico, che, per tale motivo, è stato accreditato immediatamente, quindi non più revocabile; n) il bonifico non poteva in nessun caso essere annullato; o) è provata la colpa grave del ricorrente per avere eseguito l'operazione sotto dettatura di un sedicente operatore dei carabinieri; p) infine, durante la giornata in cui si è consumata la truffa, il ricorrente ha eseguito numerosi accessi all'home banking tramite l'App sino a qualche minuto prima dell'esecuzione del bonifico. Avrebbe, quindi, potuto verificare la totale assenza di notifiche relative a operazioni di pagamento da autorizzare nonché l'assenza di operazioni indesiderate; q) ha dato seguito a un ordine

di bonifico correttamente impartito e autenticato tramite SCA; r) supporta i clienti nel riconoscimento e nella prevenzione delle frodi come quella subita dalla parte ricorrente.

DIRITTO

L'intermediario, in via preliminare, eccepisce l'inammissibilità del ricorso, sul rilievo del mancato decorso del termine di quindici giorni tra la proposizione del reclamo e il deposito del ricorso.

L'eccezione è infondata.

Dall'esame della documentazione prodotta dalla parte ricorrente, si evince che quest'ultima ha presentato il reclamo in data 25.09.2025 e ha ottenuto dalla banca riscontro negativo quasi nell'immediatezza, ossia il 26.09.2025. Il ricorrente ha, quindi, proposto il ricorso in data 02.10.2025, a intervenuto rigetto della doglianza; e questo fatto rende legittima e rituale la proposizione del ricorso, a nulla valendo in contrario il fatto dell'omesso spirare del termine di 15 giorni dall'inoltro del reclamo.

Ciò posto, nel merito, l'operazione contestata è stata posta in essere sotto il vigore del d.lgs. 27.01.2010, 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), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

La presente controversia ha ad oggetto la richiesta di rimborso della somma di Euro 3.900,00, corrispondente all'importo di un'unica operazione di pagamento mediante bonifico eseguita, in data 15.09.2025, dal dispositivo del ricorrente su cui la App dell'intermediario è installata.

Parte ricorrente, in sede di ricorso e di denuncia, ammette di avere seguito le istruzioni impartite dal malfattore e di aver eseguito l'operazione di pagamento contestata, nella convinzione di procedere al blocco di un presunto pagamento sospetto.

Secondo l'orientamento consolidato dei Collegi ABF, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dal D.lgs. n. 11/2010; ciò anche se tale operazione è realizzata sulla base di un consenso viziato dagli artifici e raggiunti posti in essere da un truffatore (cfr. *ex multis* Collegio di Bologna, n. 2290/2023).

Tanto premesso, poiché, effettivamente, l'operazione di pagamento è stata eseguita direttamente dalla parte ricorrente, ancorché a ciò indotta con raggiiri da parte del sedicente carabiniere, non trova applicazione il regime di speciale protezione previsto dall'art. 10, comma 1, D.lgs. 11/2010.

Ciò non impedisce però al Collegio di valutare se possa venire in rilievo un'eventuale responsabilità dell'intermediario, sulla base delle evidenze disponibili e secondo le norme di diritto comune.

Sul punto, questo Arbitro osserva che la parte ricorrente è stata vittima di una frode denominata dai Collegi ABF *social hacking*, realizzata con la tecnica del c.d. *vishing caller id spoofing*, che ha avuto origine da una chiamata proveniente da un'utenza apparentemente riconducibile all'intermediario. In base a quanto consta dalla denuncia e dal ricorso, infatti, in data 15.09.2025, alle ore 17:13, riceveva una telefonata proveniente dal numero 02**, che, da una verifica effettuata, risultava riconducibile all'intermediario. In occasione della telefonata, un messaggio preregistrato le comunicava che erano in corso alcuni tentativi di esecuzione di bonifici sospetti e che sarebbe stata contattata da un operatore del servizio antifrode dall'utenza recante numero 347***. Riceveva, quindi, la telefonata da tale utenza telefonica e il sedicente operatore del servizio antifrode dell'intermediario la avvisava che sarebbe stata contattata dai Carabinieri che le avrebbero impartito le istruzioni per procedere al blocco di tali operazioni. Prima di concludere la conversazione, il ricorrente, su richiesta del truffatore, comunicava alcuni dati personali, tra i quali l'indirizzo mail e il codice fiscale. Veniva, poi, effettivamente contattata da un'utenza apparentemente riconducibile ai Carabinieri (numero 054***). In occasione della telefonata, il sedicente carabiniere le chiedeva di entrare nell'home banking e di effettuare un bonifico in modalità simulata, al fine di bloccare i bonifici sospetti. Rassicurata sia dal fatto che l'operazione di annullamento era presuntamente gestita dai Carabinieri, sia dalla ricezione di SMS apparentemente provenienti dalla banca che la informavano che era stata attivata in App la modalità simulazione e che i bonifici (simulati) effettuati sarebbero stati annullati, eseguiva le indicazioni fornite dal truffatore e disponeva il bonifico di Euro 3.900,00. Riceveva, poi, un SMS di conferma del bonifico e del suo blocco. Terminata l'operazione, cadeva la linea. Il ricorrente chiamava quindi l'utenza da cui aveva ricevuto la telefonata dal sedicente carabiniere, entrava in contatto con il Comando dei Carabinieri di Fa***. La parte ricorrente apprendeva, quindi, di essere stata truffata poiché, durante la telefonata, le veniva riferito che presso quel Comando non prestava servizio alcun carabiniere con il nominativo con cui si era presentato il truffatore. Contattava il servizio assistenza clienti della banca per segnalare la truffa subita e chiedere l'annullamento del bonifico.

Ciò posto, se, con riguardo alla fattispecie di "*vishing caller id spoofing*" (consistente nell'invio di sms o nella effettuazione di chiamate da un'utenza apparentemente riferibile all'intermediario) l'orientamento dei Collegi ABF è nel senso di escludere, in linea generale, la colpa grave dell'utente in ragione dell'insidiosità di tale tecnica fraudolenta, d'altro canto, la stessa colpa grave deve essere, invece, ravvisata tutte le volte in cui, come nella specie:

a) il ricorrente ha incautamente e pedissequamente seguito le istruzioni del truffatore impartite telefonicamente, nella fattispecie un presunto carabiniere, così finendo per cooperare alla consumazione della truffa in suo danno, rendendola possibile, nella convinzione inverosimile di eseguire un bonifico per bloccarne altri.

b) i messaggi truffaldini ricevuti, anche se collocati nella chat ove sono presenti anche quelli genuini precedentemente inviati dalla banca, erano riconoscibili poiché presentavano evidenti errori ortografici, tanto da essere senza alcun dubbio inattendibili. Il ricorrente, pertanto, non ha prestato, con grave

superficialità, la dovuta attenzione alla forma grammaticale dei messaggi. Inoltre, il ricorrente avrebbe dovuto accorgersi che tali messaggi, a differenza di quelli genuini, sono privi di incipit, di riferimenti al conto corrente interessato e dell'indicazione del numero da contattare per ricevere informazioni.

A ciò si aggiunge un ulteriore profilo di colpa grave della parte ricorrente, che emerge tenendo conto del fatto che l'utenza mobile 347*** dalla quale ha ricevuto la seconda telefonata non era riconducibile al servizio antifrode dell'intermediario.

Infine, come eccepito e documentato dall'intermediario, la parte ricorrente, poco prima dell'esecuzione del bonifico sconosciuto, aveva effettuato numerosi accessi all'home banking, con la conseguenza che era nella condizione di potersi avvedere dell'assenza di movimenti anomali sul proprio conto.

Quanto precede permette di formulare un giudizio di colpa grave a carico del ricorrente.

Per converso, nessuna responsabilità è ravvisabile nel comportamento dell'intermediario resistente, anche tenuto conto che: i) l'operazione non integra alcun parametro di cui all'art. 8, rubricato "*Rischio di frode*", del D.M. 112/2007, recante il "*Regolamento di attuazione della legge 17 agosto 2005, n. 166, recante «Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento»*"; ii) ha inviato un SMS *alert* dell'operazione contestata; iii) il *recall* non è stato possibile in quanto il bonifico era indirizzato a un beneficiario con conto corrente radicato presso l'intermediario stesso e ciò ha comportato la sua esecuzione immediata, con la conseguenza della sua irrevocabilità.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE