



COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) CORRADI	Membro di designazione rappresentativa degli intermediari
(BO) TRAVERSI	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO VELLA

Seduta del 02/12/2025

FATTO

Parte ricorrente, legalmente assistita, premesso di essere titolare di conto corrente nr. *762, acceso presso una filiale dell'intermediario resistente, come di seguito ricostruisce i fatti accaduti.

In data 02/09/2024 alle ore 17:15 circa, effettuava due pagamenti tramite carta bancomat n. *974 presso due esercizi commerciali e riceveva, alle ore 17:31, un SMS proveniente dal medesimo profilo dal quale abitualmente riceve comunicazioni dall'intermediario, con cui veniva segnalata l'autorizzazione di un pagamento dell'importo di € 4.900,00. Contattava l'esercizio presso il quale aveva precedentemente effettuato gli acquisti, ritenendo che fosse stato commesso un errore nella digitazione dell'importo, ottenendo tuttavia riscontro negativo. Contattava quindi il numero per il blocco della carta indicato nell'SMS, ricevendo risposta da un sedicente addetto dell'“Ufficio Prevenzione Frodi” dell'intermediario, il quale gli richiedeva l'invio dei propri dati personali e della copia dei documenti d'identità. Veniva successivamente contattato dal medesimo numero tramite WhatsApp e trasmetteva, su tale canale, la fotografia del proprio documento d'identità. Era poi informato telefonicamente dal suddetto sedicente operatore che l'importo del pagamento fraudolento era aumentato a € 25.000,00 e che l'unico modo per bloccarlo consisteva nell'effettuare un bonifico della medesima somma su un conto di storno, somma che sarebbe poi stata riaccreditata sul suo conto personale al termine della presunta procedura tecnica. Riceveva, nella medesima data, tra le ore 14:00

e le ore 14:30, due bonifici per l'importo complessivo di € 38.155,50 — circostanza della quale i malfattori dovevano essere a conoscenza e che con ogni probabilità li aveva indotti a rilanciare — somma che gli ha consentito, alle ore 19:21, di effettuare un bonifico di € 25.000,00 sull'IBAN indicatogli telefonicamente. Riceveva, alle ore 19:23, un ulteriore SMS proveniente da un profilo riconducibile all'intermediario, nel quale venivano fornite le istruzioni su come procedere al blocco del bonifico di € 25.000,00.

Essendosi insospettito, contattava con il cellulare della figlia, tra le 19:45 e 19:48, mentre era ancora al telefono con il sedicente operatore, il numero verde ufficiale dell'intermediario ove un complice confermava la versione del primo interlocutore (il quale, a conferma dell'intrusione nelle linee dell'intermediario, riferiva di vedere dai propri dispositivi che stava tentando di contattare il numero verde). Si recava quindi a denunciare la truffa e tentava il blocco del bonifico, sia tramite canali formali sia tramite conoscenti dipendenti dell'intermediario. Conclude precisando che l'operazione effettuata si è rilevata essere un bonifico internazionale con accredito a favore di un conto corrente in Estonia.

Disconosciuto il pagamento senza esito, chiede all'ABF di condannare parte resistente a consegnare la documentazione inerente tutte le richieste di accesso ai suoi dati bancari dal 15/08/2024 al 15/09/2024, comprensive "degli identificativi dei dispositivi ed account di provenienza", nonché al risarcimento del danno subito, pari ad € 25.000, ovvero l'operazione fraudolenta subita, oltre alle spese legali per 3.000 oltre al 15% quale rimborso forfettario spese generali, CPA 4% e IVA 22%.

L'intermediario nella controdeduzione eccepisce che la parte ricorrente è caduta vittima di una truffa ormai consolidata nota come *spoofing* e che l'accesso e le disposizioni sono avvenuti con corretto riconoscimento delle credenziali e delle *password* dispositive e, inoltre, il cliente si è collegato *ex novo* alle ore 19:43, quando il bonifico era ancora da lui direttamente annullabile. Con riferimento alle chiamate effettuate al numero verde dalle 19:45 alle 19:48, osserva che agli atti non è allegato il registro chiamate, risultando dall'utenza del cliente un tentativo di chiamata alle ore 20:25 e una chiamata alle ore 21:12. Precisa che è stato effettuato un tentativo di *recall*, che è stato rifiutato.

Argomenta quindi che la frode è stata possibile con la fattiva collaborazione del ricorrente che, seguendo le indicazioni di un sedicente operatore, ha autonomamente disposto l'esecuzione di un bonifico ordinario per bloccare un asserito pagamento autorizzato. Di conseguenza, non viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate di cui alla direttiva 2015/2366/EU (PSD2) e al D.Lgs. n. 11/2010. Peraltro,

la responsabilità del cliente è evidente e grave poiché ha seguito le istruzioni di un sedicente operatore nonostante gli evidenti indizi di anomalia. Osserva ancora che agli atti non è presente né l'SMS né il registro delle chiamate e il numero contattato dal cliente non è riconducibile all'intermediario e viene segnalato online come "potenziale truffa".

Ribadisce di aver eseguito la disposizione di pagamento autorizzata dal ricorrente conformemente alle disposizioni impartite, previo superamento dei presidi di sicurezza, e non poteva essere a conoscenza di un'eventuale frode. Dichiara, peraltro, di aver attivato molteplici campagne informative per supportare i clienti nel riconoscimento e nella prevenzione dei fenomeni fraudolenti.

Infine, dichiara di aver provveduto a consegnare alla controparte i Log (comprensivi di indirizzi IP) relativi agli accessi/autorizzazioni effettuati/ottenute in banca multicanale relativi al periodo di interesse.

Conclude in merito alla domanda di parte ricorrente sulle spese legali, osservando che non era stata avanzata in sede di preventivo reclamo e risulta pertanto non accoglibile, oltre a non avere alcuna giustificazione in quanto non è previsto il patrocinio di un legale per un ricorso ABF e a non risultare neanche supportata dalla prova dell'effettivo pagamento della fattura allegata.

Chiede al Collegio di respingere il ricorso.

Parte ricorrente, in sede di repliche, lamenta che la documentazione relativa alle richieste di accesso ai dati bancari è stata trasmessa dall'intermediario solo pochi giorni prima del deposito delle controdeduzioni, circostanza che conferma la fondatezza del ricorso. Tali documenti, oltre a contenere oscuramenti mediante righe in neretto, evidenziano accessi all'account di *home banking* del ricorrente non solo tramite il suo dispositivo, ma anche tramite altri apparecchi a lui non riconducibili e non collegati al suo telefono, pur riferendosi al medesimo account: ciò dimostra l'intrusione dei truffatori attraverso vulnerabilità del sistema di sicurezza dell'intermediario e, conseguentemente, una responsabilità – o quantomeno corresponsabilità – dell'intermediario per avere consentito o agevolato la truffa e i relativi danni.

Insiste che il sistema di sicurezza approntato dall'intermediario si è rivelato inidoneo e/o del tutto inefficace, poiché ha consentito l'accesso a soggetti terzi non autorizzati. Argomenta ancora che l'intermediario non ha fornito prova di essersi attivato tempestivamente per bloccare o richiamare il bonifico, intervento che – secondo quanto confermato anche dalla banca estone – avrebbe consentito il recupero delle somme.

Richiama la più recente giurisprudenza di legittimità, che afferma che gli istituti di credito sono tenuti ad adottare misure idonee a prevenire l'uso fraudolento dei sistemi elettronici di pagamento, nel rispetto del principio di buona fede nell'esecuzione del contratto ed eccepisce che non può essere ravvisata una colpa grave a carico dell'utente, avendo egli ricevuto comunicazioni provenienti integralmente da account e numeri identici a quelle dell'intermediario. Aggiunge che spetta all'intermediario dimostrare la riconducibilità esclusiva e integrale dell'operazione contestata al cliente truffato.

L'intermediario, in sede di controrepliche, sostiene che, poiché si tratta di chiamate o messaggi in entrata, l'Istituto non avrebbe la possibilità di intervenire, non essendo attività originate al suo interno né riconducibili a vulnerabilità della propria infrastruttura di sicurezza. Aggiunge che il bonifico SEPA ordinario poteva essere annullato direttamente dal cliente oppure tramite contatto con il numero verde ufficiale della banca; che l'onere della prova risulterebbe assolto, avendo l'intermediario dimostrato – anche mediante la produzione della documentazione tecnica – che il bonifico ordinario è stato eseguito nel rispetto della normativa vigente; che è stato comunque effettuato un tentativo di richiamo del bonifico, come confermato anche dalla banca estone; che risulterebbe incontrovertibile che l'operazione contestata sia stata eseguita dalla stessa parte ricorrente e, pertanto, non potrebbe qualificarsi come “non autorizzata”; che il fatto che un soggetto riceva una chiamata o un SMS apparentemente provenienti da un determinato mittente non implica né un coinvolgimento di quest'ultimo, né una compromissione del relativo sistema di sicurezza.

DIRITTO

La presente controversia ha ad oggetto la richiesta di restituzione dell'importo di un bonifico fraudolento per una somma pari € 25.000,00, posto che la resistente ha provveduto a consegnare al ricorrente

documentazione in ordine ai Log (comprensivi di indirizzi IP) relativi agli accessi/autorizzazioni effettuati/ottenute in banca multicanale relativi al periodo di interesse.

L'operazione contestata risulta eseguita personalmente dal ricorrente, a seguito di truffa perpetrata in suo danno.

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. 27 gennaio 2010, n. 11. In questi casi, non è dunque configurabile una responsabilità oggettiva del PSP. Il Collegio potrà comunque rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode come, ad esempio, nei casi di: a) mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore; b) mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore; c) mancato rilievo di indizi di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere. Si tratta di principi recentemente ribaditi anche dal Collegio di Coordinamento (Collegio di coordinamento, decisione n. 8671/2024) e di ipotesi di cui non vi è in atti prova alcuna.

Nel caso in esame, dalla documentazione in atti emerge come la dinamica della truffa sia assimilabile a quella delle truffe c.d. di "*social hacking*". Da quanto in atti emerge infatti che il ricorrente, ricevuto un SMS fraudolento nel quale gli veniva segnalata l'esecuzione, dal proprio conto corrente, di un bonifico di € 4.900,00, contattava per il blocco il numero indicato nel messaggio ricevuto, appunto fraudolento, e un sedicente operatore lo informava che l'operazione fraudolenta risultava ormai aumentata a € 25.000,00 e che la procedura di storno prevedeva l'effettuazione di un bonifico di pari importo verso l'IBAN che gli veniva dettato telefonicamente. Confidando nella veridicità di tali indicazioni, il ricorrente eseguiva personalmente un bonifico ordinario dal proprio conto corrente, con conseguente inapplicabilità della disciplina in tema di responsabilità nel caso di operazioni non autorizzate. In merito alla colpa grave del ricorrente, per quanto come evidenziato non sia qui applicabile il regime favorevole previsto dal d. lgs. 11/2010 in tema di operazioni non autorizzate, l'intermediario rileva che il numero indicato nell'SMS truffaldino per il blocco non è a lui riconducibile e viene anzi segnalato online come "potenziale truffa".

Avendo parte ricorrente eseguito personalmente l'operazione e, troppo ingenuamente, dato seguito ad un messaggio truffaldino, non ravvisando altresì il Collegio ulteriori elementi che possano indicare vi sia stato un apporto casuale dell'intermediario nel compimento della frode

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE