



COLLEGIO DI BOLOGNA

composto dai signori:

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

Relatore ANDREA GENOVESE

Seduta del 09/12/2025

FATTO

Insoddisfatta dell'interlocuzione con l'intermediario nella fase del reclamo, con ricorso n. 1316542 del 28.06.2025, la parte ricorrente si rivolge all'Arbitro al quale chiede di voler disporre il rimborso della somma di Euro 950,00, corrispondente all'importo di un'operazione di pagamento fraudolentemente eseguita online.

A sostegno della pretesa, deduce che: (i) è titolare del conto corrente n. **214 acceso presso l'intermediario; (ii) in data 20.03.2025 verso le ore 17:17 veniva contattata da un sedicente operatore dell'intermediario attraverso l'utenza numero +3705**; (iii) contestualmente alla telefonata, riceveva sul proprio cellulare un messaggio apparentemente proveniente dalla parte resistente con il quale le veniva comunicato che stava parlando con un operatore della banca; (iv) nel corso della telefonata, l'interlocutore, dopo avere segnalato alcune operazioni sospette, la invitava a effettuare altre operazioni per annullare le prime; (v) la procedura indicata consisteva nell'invio di alcune transazioni da autorizzare affinché venissero poi annullate; (vi) confidando nella genuinità della conversazione, seguiva tutte le indicazioni fornite dal sedicente operatore e riceveva per ogni transazione un messaggio che comunicava l'esito positivo del blocco di ciascuna operazione; (vii) dopo n. 8

transazioni, il frodatore riusciva a sottrargli la somma di Euro 950,00 dalla carta virtuale collegata al proprio conto corrente e creata su indicazione dello stesso malfattore; (viii) accortasi della frode, in data 21.03.2025 sporgeva denuncia e il successivo 14.04.2025 inoltrava reclamo, riscontrato, tuttavia, negativamente; (ix) a fronte della denuncia del cliente, l'intermediario è obbligato a rimborsargli tutte le somme addebitate ex art. 12 del D.lgs. 11/2010; (x) in virtù degli artt. 8 e 11 del d.lgs. 11/2010, la possibilità di un utilizzo dei codici identificativi da parte di terzi deve essere ricondotta nell'area del rischio professionale del prestatore di servizio, e non al dolo o a comportamenti incauti dell'utilizzatore del servizio di pagamento; (xi) in caso di frode quale il *"caller-id spoofing"*, la condotta del ricorrente non può considerarsi caratterizzata da colpa grave; (xii) le banche svolgono attività professionale e devono adempiere tutte le obbligazioni assunte nei confronti dei propri clienti con la diligenza qualificata dell'accorto banchiere; (xiii) la chiamata ricevuta risultava provenire dall'utenza telefonica riconducibile alla banca. Ciò ha ingenerato fiducia e credibilità nell'interlocutore; (xiv) i messaggi ricevuti, oltre a essere simili per modalità e testo a quelli generalmente spediti dall'intermediario, provenivano tutti dall'utenza intestata allo stesso; (xv) infine, il sedicente operatore aveva libero accesso all'App e la conseguente possibilità di inoltrare al cliente gli estremi delle transazioni da approvare, senza che gli fosse mai stata comunicata alcuna password o codice OTP; (xvi) anche tale circostanza l'ha indotta a riporre la propria fiducia sull'attendibilità delle operazioni compiute con l'interlocutore; (xvii) l'omessa diligenza nella custodia dei dati costituisce nesso causale con l'evento subito e un grave inadempimento contrattuale da parte dell'intermediario; (xviii) applicando i principi espressi dal Collegio di Coordinamento in punto di onere della prova nel caso di utilizzo fraudolento di strumenti di pagamento, i Collegi territoriali hanno precisato che la natura *"sostanzialmente"* della frode subita dall'utente, quand'anche perpetrata tramite c.d. sms *spoofing*, va accertata secondo le circostanze del caso concreto; (xix) in assenza di tale prova è corretta la decisione di imputare all'intermediario il rischio professionale della possibilità che terzi accedano ai profili dei clienti con condotte fraudolente, senza che sia necessario vagliare, pertanto, la propria condotta in occasione della truffa subita; (xx) da quanto accaduto, emerge che la parte resistente non ha diligentemente custodito i suoi dati sensibili e quelli relativi all'utenza telefonica e all'accesso ai software; (xxi) in casi simili, l'orientamento prevalente tra i Collegi Territoriali dell'ABF è quello di imputare all'intermediario la colpa di *"non avere adottato tutti i presidi di sicurezza necessari a impedire che il truffatore potesse chiamare la cliente con un numero riferibile all'intermediario medesimo"*.

Costituitosi, l'intermediario chiede all'Arbitro di rigettare il ricorso perché infondato, sul rilievo che: a) l'operazione contestata dal ricorrente è stata dallo stesso autorizzata e correttamente eseguita nel rispetto delle norme applicabili e delle previste procedure contrattuali, mediante utilizzo della carta di pagamento; b) ai sensi dell'art. 5 del D.lgs. 11/2010, l'operazione non può considerarsi *"non autorizzata"* e non è applicabile il regime di responsabilità previsto dalla PSD2; c) in ogni caso, per l'operazione contestata è stata inviata una notifica *push* sull'App del dispositivo registrato del ricorrente che ha chiesto di confermare la transazione; d) anche l'attivazione della carta è stata effettuata dalla parte ricorrente e autenticata in base a procedure multifattoriali (SCA); e) non è quindi attribuibile alla banca alcuna responsabilità; f) durante l'esecuzione dell'operazione ha inviato notifiche *alert* così avvisando il cliente della potenziale truffa; g) dalle circostanze emerge una condotta gravemente negligente del ricorrente, caduto vittima di una truffa non sofisticata e oramai nota; h) sul proprio sito ha

allestito un'apposita pagina in cui sono elencati i comportamenti che gli operatori non tengono mai, suggerendo ai clienti alcune condotte al fine di evitare truffe; i) la truffa consumata ai danni del ricorrente, quindi, poteva essere evitata tramite l'utilizzo della diligenza media di cui ogni soggetto è dotato; l) nel caso di specie, senza l'attivazione della carta e l'autorizzazione dell'operazione di pagamento fornita dal ricorrente non si sarebbe consumata la truffa; m) peraltro, gli SMS civetta presentano evidenti errori grammaticali e differenze stilistiche rispetto ai messaggi genuini inviati dalla banca; n) il ricorrente ha dato seguito alle richieste dell'interlocutore nonostante le stesse apparissero anomale, come ammesso in sede di reclamo; o) il numero dal quale il ricorrente è stato contattato è utilizzato dalla banca solo per permettere ai clienti di eseguire il blocco delle carte; p) il ricorrente, con colpevole superficialità, ha omesso di verificare l'identità del sedicente operatore e non ha provveduto a contattare la banca mediante la chat presente nell'App, che costituisce il canale ufficiale dell'assistenza; q) la condotta del ricorrente non poteva essere prevista e neppure evitata, costituendo dunque una causa esterna idonea a interrompere qualsivoglia nesso di causalità tra il proprio operato e l'evento dannoso.

In sede di repliche, la parte ricorrente ha affermato che: (i) gli allegati prodotti dalla parte resistente sono inattendibili poiché i documenti informatici sono delle semplici tabelle in formato excel, dunque alterabili; (ii) i documenti D ed E non provano che le operazioni compiute sono state dalla stessa concretamente effettuate e compiute e neppure che gli ID indicati corrispondono al proprio dispositivo registrato; (iii) dai log prodotti non è possibile evincere direttamente l'inserimento della password, poiché gli stessi non sono univoci e uniformi; (iv) i tracciati depositati riportano solo delle mere stringhe di codici e numeri, che nulla dimostrano in merito: 1) all'esecuzione delle operazioni da parte del ricorrente, al dispositivo da cui sono state eseguite e/o all'indirizzo IP; 2) alla comunicazione dei codici OTP; 3) al sistema di doppio controllo; (v) la banca ha consentito l'esecuzione dei bonifici nonostante fosse consapevole della loro natura fraudolenta e non ha adottato un sistema di monitoraggio in grado di rilevare modelli di comportamento anomali del cliente o del dispositivo di accesso del cliente; (vi) il numero di pagamenti eseguiti nell'arco della giornata e la cifra rilevante rispetto all'operatività ordinaria del conto costituiscono un indice di anomalia che avrebbe dovuto insospettire e allertare i sistemi di monitoraggio dell'intermediario; (vii) l'intermediario non ha bloccato il conto nell'immediatezza dell'accadimento dei fatti; (viii) ha creduto a quanto affermato dall'interlocutore perché solo un dipendente della banca poteva avere gli strumenti e gli accessi per effettuare le operazioni svolte.

Con le controrepliche, la parte resistente rileva che: a) la documentazione prodotta rappresenta quella tipica che i Collegi ABF valutano come valida (cfr. Collegio di Torino, decisione n. 635/2024); b) lo stesso ricorrente afferma di aver effettuato l'operazione poi contestata, seppur sulla base di un consenso viziato; c) nella specie, non grava dunque sull'intermediario l'onere di verifica dell'elemento soggettivo sottostante l'operazione; d) in ogni caso, l'operazione è stata eseguita tramite SCA realizzata attraverso una notifica *push* (elemento di possesso) e l'accesso all'App con fattore di inerenza (riconoscimento biometrico facciale); e) non è rinvenibile un obbligo di monitoraggio delle operazioni in capo all'intermediario; f) il sistema di *alert* è risultato perfettamente funzionante nell'ambito della vicenda truffaldina; g) l'attivazione degli *alert* ha impedito al ricorrente di eseguire ulteriori operazioni a suo danno ammontanti a Euro 5.520,00; h) la condotta tenuta dal ricorrente è

connotata da evidenti profili di colpa grave riconducibili a comportamenti caratterizzati da “*inescusabile imprudenza, negligenza o imperizia*”; i) nel caso di specie risultano evidenti e numerosi gli indici di anomalia e inaffidabilità che la parte ricorrente avrebbe dovuto riconoscere o evitare.

DIRITTO

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 950,00, corrispondente all'importo di un'unica operazione di pagamento effettuata online in data 20.03.2025.

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 presunti pagamenti sospetti.

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 raggiri 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 raggiri da parte del sedicente operatore bancario, 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 effettuata da un sedicente operatore della banca, il quale l'ha indotta, con istruzioni manipolative, a disporre il pagamento in questa sede disconosciuto. In base a quanto consta dalla denuncia e dal ricorso, infatti, in data 20.03.2025 verso le ore 17:17, un sedicente operatore bancario contattava la parte ricorrente da un'utenza riferibile all'intermediario recante numero +3705** . Contestualmente, riceveva sul proprio cellulare un messaggio apparentemente proveniente dalla parte resistente, con il quale le veniva confermato che stava parlando con un operatore della banca. In

occasione della telefonata il truffatore la informava che erano stati effettuati alcuni pagamenti e che, per bloccarli, avrebbe dovuto seguire le istruzioni che le avrebbe impartito telefonicamente. In particolare, avrebbe dovuto accedere all'App della banca e autorizzare le transazioni asseritamente fraudolente per consentire al presunto operatore bancario di bloccarle. Fidandosi dell'interlocutore, eseguiva le indicazioni fornite dal sedicente operatore e riceveva per ogni transazione un messaggio che ne comunicava l'avvenuto blocco. Dopo aver presuntamente bloccato n. 8 operazioni di pagamento, le veniva sottratta la somma di Euro 950,00, nonostante avesse creduto di disporre il blocco, attraverso una carta virtuale collegata al suo conto corrente e creata su indicazione sempre del malintenzionato. Insospettitasi, dopo l'invio da parte del truffatore di ulteriori richieste per autorizzare il blocco di altri pagamenti, si avvedeva di essere stata truffata e chiudeva la conversazione. A dimostrazione della frode, parte ricorrente ha allegato la copia degli SMS ricevuti e l'elenco delle chiamate.

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;
- b) i messaggi ricevuti presentano evidenti e numerosi errori grammaticali e sintattici, tanto da essere senza alcun dubbio inattendibili. Il ricorrente, pertanto, non prestando, con grave superficialità, la dovuta attenzione alla forma grammaticale dei messaggi, ha così finito per cooperare alla consumazione della truffa in suo danno, rendendola possibile.

A ciò si aggiunge un ulteriore profilo di colpa grave della parte ricorrente, che emerge tenendo conto del fatto che l'utenza dalla quale sembrava chiamare il sedicente operatore, era in realtà, come si evince dalla documentazione versata in atti dall'intermediario (stralcio del suo sito web ufficiale), il numero dedicato unicamente al blocco della carta, dal quale notoriamente quest'ultima può solo ricevere telefonate, non farle.

Quanto precede permette di formulare un giudizio di colpa grave a carico al 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 una notifica *alert* dell'operazione contestata.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE