

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) MIRABELLI	Membro di designazione rappresentativa degli intermediari
(BO) TRAVERSI	Membro di designazione rappresentativa dei clienti

Relatore ELEONORA MIRABELLI

Seduta del 13/01/2026

FATTO

Il ricorrente, anche per mezzo della documentazione allegata al ricorso, riferisce di essere titolare di un conto corrente acceso presso l'intermediario convenuto e che, in data 12/12/2024, alle ore 10:30 circa, riceveva una telefonata dal numero verde della banca dove, un sedicente operatore dell'ufficio antifrode lo informava che la sua App era stata associata ad un altro telefono. Apparendo la conversazione telefonica disturbata, il sedicente operatore lo invitava a fornirgli un altro numero di telefono su cui richiamarlo e veniva così richiamato sul cellulare aziendale ed invitato a scaricare sul telefono personale una applicazione antivirus da Playstore. Terminata la telefonata, con l'avvertenza che sarebbe stato richiamato più tardi per installare insieme l'applicazione scaricata, chiamava ripetutamente il proprio consulente finanziario al numero di cellulare, per avere conferma di ciò che stava accadendo, ma scattava la segreteria telefonica che segnalava l'indisponibilità dell'operatore chiamato. Verso le ore 13:00 riceveva una seconda telefonata dal sedicente operatore della convenuta, il quale gli forniva indicazioni per procedere all'installazione ed alle ore 18:30 circa, il truffatore effettuava una terza telefonata per sapere se fosse andata a buon fine la procedura di installazione dell'app antivirus. Il giorno seguente, dopo aver cercato nuovamente e senza successo il proprio consulente, chiamava il numero verde della convenuta ed apprendeva di essere stato vittima di una truffa. In particolare, in data 12/12/2024, era stato effettuato un bonifico ordinario di € 5.967,00, da lui non autorizzato, a favore di un beneficiario sconosciuto. Riferisce il ricorrente a questo riguardo, di non aver comunicato né inserito sul telefono codici OTP, pin o password, né impronte digitali o altro per

autorizzare l'operazione di bonifico disconosciuta e lamenta il fatto che la truffa sia avvenuta proprio nei giorni in cui il consulente finanziario era in ferie e quindi senza che potesse beneficiare di una persona all'interno della banca "*fisicamente presente*"; ciò dimostra una falla nel sistema di protezione dei clienti predisposto dalla convenuta. Conclude dunque il ricorrente chiedendo che codesto Arbitro adito accerti l'obbligo della banca di rimborsare la somma di euro 5.967,00 oltre interessi, illegittimamente sottrattagli.

L'intermediario, nelle proprie deduzioni, afferma che dal registro delle telefonate in uscita, allegato al ricorso, relativo al cellulare in uso al cliente, si evincono tre tentativi di telefonate di cui 2 ad un numero corrispondente al gestore del ricorrente ed una, di soli 11 secondi, verso il numero verde della convenuta. Tale condotta mostra una scarsa diligenza prestata dal cliente, data l'operatività costante del servizio clienti della banca. Il cliente inoltre, non ha depositato alcuna evidenza a supporto delle responsabilità della banca, disattendendo di fatto al principio dell'onere della prova ex art. 2697 c.c. ed inoltre, la condotta tenuta da parte ricorrente è connotata da colpa grave, per aver dato seguito a comunicazioni con evidenti profili di anomalia (*more solito* la richiesta di conoscere quale fosse il suo modello di telefono, la richiesta di riavvio del cellulare, la richiesta di passare su un'altra linea per meglio eseguire la procedura impartitagli) e per aver scaricato, seguendo le istruzioni del truffatore, un'APP malevola sul proprio telefono. Così facendo, il cliente ha perso il controllo dell'APP, consentendo ai malfattori di agire indisturbati su di essa e disporne a proprio piacimento. La banca, da tempo, raccomanda la massima attenzione e cautela nell'utilizzo dei canali telematici; tra l'altro, dalle verifiche effettuate, non è emerso alcun malfunzionamento o compromissione dei sistemi e le operazioni risultano correttamente autenticate, registrate e contabilizzate. Chiede dunque l'intermediario il rigetto del ricorso in quanto infondato in fatto ed in diritto.

Nelle repliche, parte ricorrente precisa che il giorno 12/12/2024, tra le ore 11:11 e le ore 11:28, effettuava tre telefonate nel tentativo di parlare con la sua banca: dopo due tentativi a vuoto di parlare col proprio consulente (unico soggetto all'interno della banca col quale aveva un "rapporto umano"), provava a chiamare il numero verde dove scattava la segreteria telefonica; sperava così di essere richiamato dal consulente, come era sempre accaduto nel corso degli anni. Precisa, inoltre, che il truffatore chiamava da un numero riconducibile alla convenuta ed era perfettamente a conoscenza del suo nominativo e numero di telefono, nonché del fatto che aveva un conto in essere e che aveva l'App installata sul cellulare; il truffatore poteva aver appreso tutti i suoi dati soltanto a causa di una falla nel sistema di protezione dei dati della banca, unico soggetto che doveva conoscere e custodire tali dati sensibili del ricorrente. A questo riguardo, l'art. 82 del GDPR, prevede che chiunque subisca un danno, materiale o immateriale, causato da una violazione del GDPR, ha diritto al risarcimento del danno. Ritiene inoltre di aver assolto pienamente il proprio onere probatorio, mentre la convenuta non ha provato le misure adottate per prevenire la frode informatica. Nel caso di specie, il ricorrente riferisce di aver scaricato un'app malevola ma di non aver comunicato a terzi alcun codice e/o password e che se anche la banca ha dichiarato che tutte le operazioni sono state eseguite dal medesimo IP e dallo stesso device, utilizzato anche per accessi ordinari, tale identità non prova la volontà dispositiva del cliente ma, al contrario, è compatibile con la duplicazione remota del dispositivo mediante software di remote access. Tra l'altro, la banca non produce screenshot, timestamp o hash dell'evento di approvazione, ma solo il codice OTP generato automaticamente dal Mobile Token, senza che risulti un'azione dell'utente e la rapidità e linearità delle operazioni effettuate (accesso alle 15:36:10, bonifico completato alle 15:39:59; logout alle 16:40:04) sono tipiche di un'operazione automatizzata o eseguita tramite malware, non di digitazione manuale da parte di un utente reale, anche perché dai log emerge l'attivazione di un nuovo Mobile Token il 13 dicembre 2024, indizio di problemi di sicurezza nell'utilizzo del vecchio token. Ribadisce inoltre (i) che l'operazione disconosciuta era del tutto anomala rispetto alle

altre operazioni da lui effettuate sul conto e doveva essere automaticamente segnalata o bloccata, tanto che l'accesso immediatamente antecedente il bonifico è avvenuto tramite Pin, diversamente dagli altri accessi eseguiti mediante autenticazione biometrica e (ii) che la banca non documenta come sia avvenuta la conferma attiva del cliente.

Nelle controrepliche, parte resistente si riporta a quanto già contro dedotto, evidenziando che con riferimento alla contestata violazione delle regole sulla protezione dei dati personali, nel caso di specie non è presente l'evento dannoso richiamato dall'art. 82 del GDPR (non v'è stata alcuna violazione dei sistemi bancari), né vi è alcun indizio che imputi una partecipazione della banca all'asserita frode subita; gli stessi dati, asseritamente già a conoscenza del frodatore, potrebbero esser stati attinti da molteplici fonti, anche su web. Rileva poi l'intermediario, che il valore dei Log è riconosciuto dai Collegi ABF e che nell'operazione disconosciuta non vi erano elementi tali da poter essere letti o percepiti come costitutivi di una possibile frode in corso. La comprovata condotta colposa del ricorrente risulta predominante rispetto all'evento dannoso, avendo avuto un'efficienza causale autonoma e prevalente nel processo attraverso il quale si è verificato l'illecito produttivo dell'evento e, per quanto concerne la contestata uniformità anomala di device e IP, rileva che dal file Log si evince che l'IP è cambiato nel corso del periodo in esame (+/- 15 giorni dalla disposizione), per cui si ritiene pacifico e non contestato che non vi sia stata duplicazione remota del dispositivo né alcuna anomalia sistemica. Da ultimo, eccipisce che l'attivazione di un nuovo Mobile Token eseguita il giorno dopo la frode, non è un indizio di forte compromissione in quanto rientra, così come previsto dal contratto di Home Banking, nella libertà del cliente poter attivare fino a n. 2 Mobile Token contemporaneamente su n. 2 dispositivi.

DIRITTO

La presente controversia ha ad oggetto il disconoscimento di un bonifico ordinario di € 5.967,00 (comprensivo di € 1,00 di commissione), effettuato tramite *home banking* in data 12/12/2024 alle ore 15:39 del quale il ricorrente chiede il rimborso.

A questo riguardo, il Collegio rileva che l'operazione contestata è stata posta in essere 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), 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.

Per consolidato orientamento dei Collegi ABF, a fronte del disconoscimento dell'operazione da parte del cliente, è onere dell'intermediario provare che l'operazione sia stata correttamente autenticata, registrata e contabilizzata, ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010 che così statuisce: *“Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti”*. In mancanza di tale prova, dunque, l'intermediario sopporta – in ogni caso – integralmente le conseguenze delle operazioni disconosciute.

0 bis del medesimo D.Lgs. n. 11/2010 prevede: “Conformemente all'articolo 98 della direttiva (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi”. L'art. 1, lettera q bis del medesimo decreto chiarisce, conformemente alla suddetta direttiva, che la c.d. autenticazione forte consiste in “un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione”. Sul punto, è intervenuta l'EBA con la “Opinion” del 21 giugno 2019 (richiamata espressamente dal Regolamento UE/2018/389 del 27.11.2017), nella quale sono stati passati in rassegna alcuni dei più comuni sistemi di autenticazione predisposti dagli intermediari per valutare se possano o meno annoverarsi tra i presidi di autenticazione forte.

Occorre dunque verificare se, nel caso di specie, l'operazione contestata è stata autenticata mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d. “autenticazione forte”.

A questo riguardo, l'intermediario deduce la corretta esecuzione, registrazione e contabilizzazione della transazione contestata, senza alcuna anomalia e con doppio fattore SCA mediante l'utilizzo del device in uso al ricorrente. In particolare, dallo stralcio delle evidenze Log trasmesse dall'intermediario, si evince che sia l'accesso all'home banking sia il bonifico sono stati autorizzati con Pin (elemento di conoscenza) ed OTP da Mobile Token (elemento di possesso).

Come però previsto dall'art. 10, comma 2, del d.lgs. n. 11/2010 “Quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7”.

Giacché, a tal riguardo, il Collegio di coordinamento con decisione n. 22745/2019, pronunciandosi su quesiti interpretativi in tema di onere della prova del dolo o della colpa grave dell'utente, posto a carico del prestatore di servizi di pagamento, ha formulato il principio interpretativo secondo il quale: “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 volta a provare l'“autenticazione” e la 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”.

Da quanto sopra ne emerge che l'intermediario, dopo aver fornito prova della corretta autenticazione, registrazione e contabilizzazione dell'operazione, è chiamato ad indicare una serie di elementi di fatto circa la condotta del ricorrente dai quali possa trarsi prova della colpa grave della stessa.

Passando quindi alla valutazione della colpa del cliente, lo stesso riferisce di aver ricevuto delle telefonate provenienti dal numero verde della convenuta, con le quali un sedicente operatore dell'ufficio

antifrode gli faceva installare sul telefono una applicazione antivirus scaricata da *Playstore*, senza però fornire, né per le telefonate ricevute né per l'applicazione scaricata, alcuna evidenza documentale.

Tra l'altro, il ricorrente – come dichiarato dallo stesso – ha dato seguito a comunicazioni con evidenti profili di anomalia, come la richiesta da parte dei malfattori di conoscere il modello del suo telefono, quella di riavvio del cellulare e la richiesta di passare su un'altra linea, financo a quella di installare sul proprio device una applicazione sconosciuta che ha consentito agli stessi di avere il pieno controllo del suo telefono.

Il pregiudizio lamentato dal ricorrente, a causa della truffa subita, è pertanto da ascriversi esclusivamente a sua negligenza e superficialità, tenutosi altresì conto della frequenza con la quale vengono perpetrate truffe *online* (cfr. Collegio di Bologna decisione n. 4162/2023) e del fatto che lo stesso ha scaricato sul suo dispositivo un'applicazione che ne consentiva l'utilizzo da remoto da parte di terzi.

Per tali motivi, il Collegio ritiene che il ricorso sia da rigettare tenuto conto della colpa grave della ricorrente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE