

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) NUZZO	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore NICOLA CIPRIANI

Seduta del 16/03/2026

FATTO

A. Il ricorrente si rivolge all'Arbitro rappresentando di aver ricevuto una telefonata proveniente dal numero fisso della resistente alle ore 17:00 del 24/10/2024, a seguito della quale sono stati sottratti € 22.501 dal suo conto corrente. Pertanto, il ricorrente chiede il rimborso della somma sottratta, oltre il ristoro delle spese sostenute per aver dovuto fare ricorso all'ausilio di un consulente di parte, specializzato in "informatica forense".

B. Costituitosi, l'intermediario osserva che "il "raggiro" subito dal ricorrente è stato di agevole esecuzione", visto che ai frodatori è bastato chiedere al ricorrente di scaricare un'App (rendendo così possibile l'accesso di un soggetto terzo al suo dispositivo) e di eseguire le istruzioni da loro ricevute. In particolare, l'intermediario eccepisce la "perdita di controllo" dell'App bancaria da parte del ricorrente, precedentemente funzionante, solo dopo aver installato quella indicata dai malfattori e precisa che l'istante è stato raggirato tramite una telefonata di phishing. Pertanto, il resistente conclude per il rigetto del ricorso.

C. In sede di repliche, il ricorrente ribadisce la domanda, chiedendo in particolare di "accertare il concorso di responsabilità dell'intermediario", "in ragione "dell'esecuzione oltre cut-off con contabile/valuta coincidenti, della mancata revoca/recall nonostante richiesta entro 16 minuti, dell'inefficacia dei presidi di monitoraggio e customer protection contro spoofing/vishing, della mancata contestazione su app fake e reset suggerito dalla filiale, della mancata prova di assenza di malfunzionamenti e della condotta abnorme del cliente".

DIRITTO

1. La controversia concerne una vicenda di utilizzo non autorizzato di uno strumento di pagamento (artt. 9 ss. d.lgs. 27 gennaio 2010, n. 11), nella specie consistente in un bonifico ordinario di € 22.501,00, addebitato il 24/10/2024 (data contabile e data valuta coincidenti) sul conto corrente allo stesso intestato e aperto presso l'intermediario resistente.

2. Orbene, il Collegio rileva innanzi tutto che l'operazione contestata è stata eseguita sotto il vigore del d.lgs. 27.1.2010, 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), entrato in vigore il 13.1.2018. Inoltre, l'operazione contestata è stata eseguita successivamente all'entrata in vigore delle nuove disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del Regolamento Delegato (UE) della Commissione, del 27 novembre 2017, n. 2018/389, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (cfr. anche il disposto dell'art. 5, d. lgs. n. 11/2010, come novellato).

3. La disciplina appena richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore (artt. 7 e 12, co. 4, d.lgs. n. 11/2010).

In particolare, "qualora l'utente 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" (ai sensi dell'art. 10, d.lgs. n. 11/2010). Inoltre, ove l'utente neghi di avere 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'utente 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. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente" (art. 10 comma 2, d.lgs. cit.).

Ai sensi del successivo art. 12, co. 2 bis, d.lgs. cit., "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Per "autenticazione forte" si intende "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" (art. 1, lett. q-bis, d.lgs. 11/2010).

I prestatori di servizi di pagamento sono tenuti a utilizzare l'autenticazione forte "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" (art. 97, comma 1, direttiva UE 2015/2366; art. 10-bis, comma 1, d.lgs. 11/2010).

In relazione alla disciplina richiamata, il Collegio di Coordinamento ha in più occasioni precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che

l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro). La ratio di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coord., decisione n. 3947 del 24.6.2014. Più di recente, cfr. Coll. Coord., decisione n. 22745/2019, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, ex art. 10, co. 2, d. lgs. n. 11/2010).

4. Fatte queste premesse, venendo al caso di specie, il Collegio ritiene che, da un lato, l'intermediario abbia fornito adeguata prova del corretto svolgimento delle procedure di autenticazione, registrazione e contabilizzazione; dall'altro lato, debba reputarsi sussistente la colpa grave del ricorrente, il quale ha fornito una decisiva cooperazione affinché le operazioni fraudolente potessero compiersi.

In particolare, con riferimento alle modalità di accesso, l'intermediario rappresenta che il ricorrente, tra le ore 17:07 e le ore 17:42 del 24/10/2024, ha effettuato n. 3 login, mediante l'inserimento di ID Utente e PIN (fattore di conoscenza) e utilizzando, per ognuna di esse, l'OTP generato da Mobile Token (fattore di possesso). A sostegno di quanto affermato, l'intermediario produce apposita evidenza informatica, dalla quale risulta che tutte le attività riportate relativamente alla fase di autenticazione sono state compiute dal cellulare in uso al ricorrente, anche se l'indirizzo IP del primo accesso (delle ore 17:07, quindi anteriore rispetto al momento in cui il ricorrente avrebbe scaricato l'App indicata dai truffatori) risulta essere diverso da quelli successivi.

Quanto alla fase di predisposizione e autorizzazione dell'operazione di bonifico, essa risulta essere inserita alle successive ore 17:44 ed autorizzata mediante l'inserimento del PIN (fattore di conoscenza) e del codice OTP (96033419) generato da Mobile Token (fattore di possesso).

Ciò rilevato, ritiene il Collegio che l'intermediario abbia adottato un sistema di sicurezza multifattoriale che appare conforme ai requisiti di SCA, di modo che può ritenersi assolto l'onere della prova richiesta ai sensi dell'art. 10, d.lgs. n. 11/2010, in merito all'autenticazione e alla corretta registrazione delle transazioni contestate (Collegio di Bari, decisione n. 11542/2023; decisione n. 32/2023).

5. Passando all'esame della condotta del ricorrente, in sede di denuncia egli ha dichiarato di aver ricevuto una chiamata da un numero riconducibile all'intermediario, nel corso della quale è stato informato di un tentativo di accesso da parte di presunti malfattori nell'App bancaria installata sul suo smartphone e che, per poterli rintracciare, era necessario installare una seconda e diversa. Al fine di procedere al download dell'app, il sedicente operatore ha chiesto al ricorrente di proseguire la conversazione sul numero fisso. Pertanto, seguendo le istruzioni fornite dal frodatore, il ricorrente ha scaricato sul suo device una App, non riconducibile a quelle ufficiali dell'intermediario. Il giorno successivo, dopo aver riscontrato l'assenza sul suo device delle app bancarie e aver tentato di accedere al suo home banking, il ricorrente si è infine accorto dell'avviso "manutenzione con sospensione temporanea" e, quindi, si è rivolto alla sua filiale.

Orbene, le dichiarazioni di natura confessoria riportate nella denuncia allegata confermano che il ricorrente, assecondando le istruzioni ricevute al telefono dal suo sconosciuto interlocutore, abbia seguito le istruzioni ricevute, cliccato su di un link sconosciuto (la cui modalità di trasmissione è stata

omessa dal ricorrente) e consentito l'installazione di app "malevola" – disconosciuta dalla Banca - rendendo così possibile l'accesso al suo dispositivo da soggetto terzo.

Inoltre, dalla perizia tecnica prodotta in atti dal ricorrente, emerge che il link sul quale il ricorrente è stato indotto a cliccare non è riconducibile in nessuna sua parte alla Banca resistente e che, effettuando una semplice ricerca online, si può apprendere che non si tratta di un sito affidabile.

Per di più, l'intermediario ha dimostrato di avere tempestivamente trasmesso un alert riguardante l'esecuzione dell'operazione contestata al cliente con un SMS e con notifica push (cfr. evidenze allegate da intermediario).

Ciò premesso, il Collegio ritiene che l'esito fraudolento della vicenda sia stato reso possibile essenzialmente dalla condotta gravemente incauta del ricorrente, che ha dato seguito alle richieste inviategli, consentendo l'installazione sul suo device dell'app malevola suggerita dal truffatore. Pertanto, il Collegio ritiene che la domanda del ricorrente non sia meritevole di accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE