

COLLEGIO DI BARI

composto dai signori:

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

Relatore FRANCESCA BARTOLINI

Seduta del 18/02/2026

FATTO

Il ricorrente, esaurita la fase del reclamo, si rivolge all'Arbitro chiedendo l'accertamento del proprio diritto alla restituzione dell'importo di 1.200 euro, corrispondente al valore un bonifico che disconosce perché effettuato fraudolentemente da terzi non autorizzati.

Nel ricorso e nella denuncia a questo allegata afferma di aver ricevuto un'e-mail l'8 luglio 2025 e di aver cliccato sul link ivi contenuto; si accorgeva il giorno successivo del bonifico istantaneo in uscita in favore di un terzo ignoto e avvisava l'intermediario convenuto. Lamenta di non aver ricevuto alcuna notifica. L'intermediario, costituitosi, eccepisce che l'operazione è stata eseguita con autenticazione forte (e pieno rispetto dei parametri della *Strong Customer Authentication – SCA –*), sia per la fase di accesso all'area riservata dell'home banking, sia per l'autorizzazione. Eccepisce la colpa grave del ricorrente, che non avrebbe offerto una ricostruzione dei fatti adeguata, considerati anche i numerosi indici di inattendibilità dell'e-mail c.d. civetta ricevuta. Eccepisce di aver inviato un alert, via e-mail, sull'installazione dell'app su un altro device e di aver comunque avviato la procedura di recall, pur vanamente. Chiede pertanto il rigetto del ricorso.

DIRITTO

1. Il Collegio è chiamato a esprimersi sul diritto del ricorrente a vedersi rimborsato dall'intermediario resistente l'importo di 1.200,00 euro, corrispondente al valore di un'operazione di bonifico che disconosce perché effettuato fraudolentemente da terzi non autorizzati.
2. Il ricorso non merita accoglimento per le ragioni che seguono.

3. L'operazione disconosciuta – un bonifico istantaneo – è stata disposta online il 9 luglio 2025, nella vigenza del d.lgs. n. 11/2010, così come modificato dal d.lgs. n. 218/2017, che ha recepito la nuova Direttiva sui servizi di pagamento nel mercato interno – 2015/2366/UE (c.d. PSD 2) – e del Regolamento Delegato (UE) n. 2018/389, nonché successivamente all'emanazione dell'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019 in tema di autenticazione forte, appunto, *Strong Customer Authentication*, o SCA.

4. Si impone dunque, anzitutto, la verifica sul sistema di autenticazione predisposto dall'intermediario resistente e sul rispetto dei requisiti di cui alla predetta disciplina, la quale pone proprio sull'intermediario l'onere di 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» e che il sistema di autenticazione e autorizzazione delle operazioni di pagamento è conforme alla SCA, secondo cui è necessaria un'autenticazione cd. a doppio fattore (un fattore "di possesso" e uno "di conoscenza").

5. Sul punto l'intermediario afferma che l'operazione è stata disposta a seguito dell'installazione dell'app su un nuovo dispositivo attraverso l'accesso all'app tramite il nuovo device con inserimento di un codice personale, la data di nascita e il codice pin (fattore di conoscenza), la ricezione di un sms con una OTP sul recapito telefonico registrato sull'anagrafica del ricorrente e l'inserimento del codice OTP (fattori di possesso); riferisce che questi passaggi possono esser stati effettuati direttamente dal ricorrente o in ragione di una sua cooperazione con il frodatore; produce a supporto delle proprie affermazioni copia delle schermate tratte dal proprio sistema informatico, dall'esame delle quali emerge come l'installazione del nuovo device sia avvenuta con l'inserimento di due fattori di autenticazione (il codice pin per l'accesso all'app e l'OTP inviato al numero di telefono del ricorrente). In questo senso il Collegio si è già espresso, con un orientamento dal quale non vi è ragione di discostarsi (vd., ad esempio, le decisioni nn. 13339/2022 e 6695/2022).

Quanto alla fase dell'autorizzazione dell'operazione l'intermediario resistente produce copia di un ulteriore log dal quale emerge l'autenticazione nell'app di home banking con l'inserimento del codice segreto dal nuovo device, lo smart code (fattore di conoscenza) dal device su cui è stata installata l'app (fattore di possesso). L'operazione risulta autorizzata digitando il codice personale (fattore di conoscenza) dal suo device (fattore di possesso).

Alla luce della documentazione agli atti, così come rapidamente sopra descritta, il sistema di autenticazione del cliente e autorizzazione delle operazioni impiegato dall'intermediario resistente appare al Collegio compatibile con i requisiti SCA.

6. Resta allora da vagliare l'eccezione di colpa grave formulata in controdeduzione dall'intermediario resistente. Sul punto va rammentato che la colpa grave dell'utente può ritenersi provata anche attraverso il combinarsi di più elementi indiziari, e anche, quindi, in via presuntiva, sulla base delle risultanze agli atti del procedimento in relazione alle modalità con le quali l'operazione truffaldina è stata posta in essere.

7. Nel caso di specie il ricorrente non allega altre circostanze in relazione alla frode subita oltre all'ammissione, nella denuncia, di aver cliccato sul link contenuto in una e-mail apparentemente proveniente dall'intermediario; non offre, in altri termini, alcun elemento utile al Collegio per valutare possibili elementi di particolare sofisticatezza dell'inganno subito, che potrebbero incidere sul grado di diligenza richiesto al cliente nella custodia delle proprie credenziali; anzi, risulta chiaramente che l'indirizzo e-mail del mittente dell'e-mail non è riferibile al resistente, e che nel corpo del messaggio compaiono ulteriori indizi di inattendibilità (ad esempio, la resistente è indicata come «[s]ocietà di brokeraggio assicurativo». Alla luce di questi elementi, il Collegio ritiene nel caso di specie di ravvisare la colpa grave del ricorrente per negligente custodia delle credenziali personali.

8. D'altra parte, non coglie nel segno la doglianza relativa alla mancanza di alert in relazione all'operazione *de qua*, perché nei di un'unica operazione fraudolenta l'avviso non avrebbe potuto comunque limitare il danno.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE