

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) VITERBO	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 09/03/2026

FATTO

A. Il ricorrente si rivolge all'Arbitro affermando che, in data 02/08/2025, è stato disposto un bonifico istantaneo di € 15.000,00 dal suo conto corrente, da lui mai autorizzato. L'istante precisa che, accedendo al proprio account online per eseguire alcune operazioni, si è accorto dell'esecuzione di un'operazione non autorizzata e, pertanto, ha contattato il servizio clienti per chiedere il blocco del conto e la modifica delle credenziali di accesso, nonché la sostituzione del numero di telefono registrato. Il ricorrente fa presente di non aver ricevuto alcuna chiamata o SMS in merito all'operazione contestata e di aver sempre custodito con diligenza le proprie credenziali e i dispositivi abilitanti. Inoltre, egli lamenta che l'intermediario non abbia adottato misure idonee a prevenire l'illecita intrusione nel conto, né abbia fornito prova della regolarità dei propri sistemi di sicurezza e della corretta autenticazione della operazione. Per di più, il ricorrente rileva che l'operazione in questione presenta chiari caratteri di anomalia che avrebbero dovuto essere intercettati dall'intermediario, ossia l'importo particolarmente elevato, la natura istantanea del bonifico, la causale palesemente incongrua, la fascia oraria e un destinatario sconosciuto. Infine, il ricorrente evidenzia che dai log dell'intermediario non risulta alcun accesso all'home banking nella data dell'operazione e precisa di non aver ricevuto il codice OTP al momento dell'operazione, né alcun SMS alert. Pertanto, il ricorrente chiede il rimborso della somma integrale sottratta, oltre interessi e rivalutazione monetaria.

B. Costituitosi, l'intermediario fa presente che in data 02/08/2025 veniva disposto tramite app un bonifico istantaneo per un importo di € 15.000,00, a valere sul conto corrente del ricorrente. L'intermediario precisa che, nella denuncia del 04/08/2025, il ricorrente ha dichiarato di aver subito una truffa informatica, senza fornire informazioni al riguardo, limitandosi a presupporre che ignoti malfattori

abbiano disposto il bonifico istantaneo in questione tramite l'apposita modalità presente all'interno dell'area privata. In particolare, l'intermediario evidenzia che l'operatività sul conto corrente non può finalizzarsi senza essere in possesso delle credenziali di accesso all'internet banking (username e password, dati strettamente riservati e confidenziali) e l'inserimento in procedura dei codici OTP autorizzativi inoltrati, esclusivamente, al titolare del rapporto bancario stesso. Invero, l'operazione disconosciuta è stata effettuata dopo un accesso all'home banking, avvenuto mediante la modalità di autenticazione forte e digitazione di codice utente, password alfanumerica di esclusiva conoscenza del cliente e digitazione dell'OTP inviato per SMS sull'utenza telefonica del ricorrente. Nel caso in esame, l'OTP non è stata richiesta perché l'accesso risulta effettuato tramite l'utilizzo del device abitualmente utilizzato dal ricorrente; durante la medesima sessione di login è poi stato disposto il bonifico istantaneo, verosimilmente autorizzato dallo stesso ricorrente. Inoltre, l'intermediario precisa che il device utilizzato per l'operatività contestata è lo stesso utilizzato nelle sessioni di login effettuate in precedenza, nel periodo dal 1° luglio al 15 luglio 2025, ed evidenzia che la transazione è stata autorizzata con un sistema di autenticazione forte. Infine, l'intermediario segnala di aver inviato tempestivamente opportune notifiche via mail e SMS in merito all'operazione in questione. Pertanto, il resistente conclude per il rigetto del ricorso.

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 una operazione di bonifico istantaneo di € 15.000,00 disposto il 02/08/2025.

2. Preliminarmente, il Collegio osserva che l'operazione contestata non può tecnicamente essere considerata quale operazione autorizzata dal cliente. Infatti, nella specie, sebbene l'operazione risulti autorizzata con l'inserimento delle credenziali e dei codici di sicurezza, la successiva disposizione di pagamento sembrerebbe essere avvenuta ad opera dei truffatori. Orbene, conformemente all'orientamento consolidato dell'Arbitro, deve ribadirsi che, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale, la transazione non può intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP.

3. Nel merito, il Collegio rileva 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).

4. 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).

5. Fatte queste premesse, venendo al caso di specie, il Collegio ritiene che il ricorso non possa trovare accoglimento, in quanto da un lato l'intermediario ha fornito adeguata prova del corretto svolgimento delle procedure di autenticazione, registrazione e contabilizzazione; dall'altro deve ritenersi sussistente la colpa grave del ricorrente, il quale ha fornito una decisiva cooperazione affinché le operazioni fraudolente potessero compiersi.

In particolare, l'intermediario chiarisce che l'operazione disconosciuta dal ricorrente è stata effettuata previo accesso all'area privata dell'home banking da App. Con riferimento alla fase di accesso all'area

privata dell'home banking, l'intermediario afferma che tale accesso avviene attraverso credenziali personali che garantiscono la riconoscibilità del cliente e la massima sicurezza, ovvero:

- a) la digitazione di un codice utente;
- b) la digitazione di una password alfanumerica di esclusiva conoscenza del cliente (elemento di conoscenza);
- c) la digitazione di una password temporanea (One Time Password o OTP), ricevuta tramite SMS (elemento di possesso) sullo smartphone/cellulare, univoca, dell'operazione da autorizzare.

Nel caso in esame, il resistente rileva che, in sede di login, non è stata richiesta OTP in quanto l'accesso risultava effettuato tramite l'utilizzo del device abitualmente in uso al ricorrente. Tale circostanza trova conferma nella documentazione in atti, dalla quale risulta che il device utilizzato per il login e la successiva operazione di bonifico fosse quello del ricorrente.

Inoltre, l'intermediario riporta le evidenze documentali attestanti l'applicazione dell'autenticazione forte per autorizzare il bonifico in esame, mediante l'inserimento del codice OTP ricevuto tramite Sms alle ore 09:50:30. In particolare, il convenuto produce in atti:

- 1) evidenza relativa alla operazione di bonifico, specificando che la dicitura "it.bol.security.OtpSmsHandler" nella colonna "authorization_handler" indica l'inserimento dell'OTP;
- 2) evidenza relativa al codice OTP inviato tramite Sms il 2/08/2025, alle ore 09:50:30 al numero di telefono del ricorrente (coincidente con quello riportato in denuncia).

Sulla base della documentazione prodotta, si può dedurre che l'operazione di bonifico è stata autorizzata tramite la password statica utilizzata per il login al conto corrente (sessione **000205) e il codice OTP inviato a mezzo Sms al numero di telefono del ricorrente.

Ciò premesso, il Collegio ritiene che il sistema di sicurezza adottato dall'intermediario sia conforme alla SCA e che la documentazione tecnica allegata alle controdeduzioni, sia idonea a dimostrare la corretta autenticazione e la regolarità formale dell'operazione disconosciuta.

6. In ordine alla colpa grave, deve rilevarsi che il ricorrente non allega alcuna evidenza sulle circostanze di fatto della truffa che afferma di aver subito. Invero, il ricorrente si limita ad affermare che ignoti avrebbero "violato" il suo telefono e che, prima della operatività contestata, vi sono stati due tentativi di accesso all'app della banca, rispettivamente alle ore 08:45 e alle 08:46. Ebbene, secondo il consolidato orientamento dell'Arbitro, la reticenza del ricorrente in ordine alle circostanze della truffa costituisce un elemento dal quale il Collegio può trarre il proprio convincimento circa la sussistenza della colpa grave (cfr. Collegio di Bari, decisione n. 9006/2024).

Pertanto, alla luce delle considerazioni svolte, il Collegio ritiene che la domanda del ricorrente non sia meritevole di accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE