

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) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) QUARTA	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCA BARTOLINI

Seduta del 23/03/2026

FATTO

Il ricorrente, esaurita la fase del reclamo, si rivolge all'Arbitro chiedendo l'accertamento del proprio diritto al rimborso dell'importo complessivo di 691,50 euro, corrispondente al valore di un'operazione di pagamento che disconosce perché eseguita fraudolentemente da terzi non autorizzati; nel ricorso riferisce di essersi avveduto, il 15 gennaio 2025, dall'esame dell'estratto conto relativo ai movimenti della propria carta di credito del dicembre 2024, di quell'addebito, mai da lui autorizzato, datato 17 dicembre 2024. Riferisce di aver denunciato l'operazione alle autorità e di aver contattato l'intermediario convenuto, che inizialmente ha disposto un riaccredito provvisorio in attesa di verifiche, salvo poi respingere il rimborso sostenendo che la transazione fosse stata autorizzata con riconoscimento biometrico. Ricostruzione che contesta, negando di aver ceduto le credenziali o autorizzato in qualsiasi altro modo l'operazione.

Costituitosi, l'intermediario eccepisce che il ricorrente non abbia fornito elementi concreti per dimostrare la frode, limitandosi a negare l'autorizzazione, mentre ritiene provata l'autenticazione forte e la riconducibilità dell'operazione al dispositivo del ricorrente. Sostiene che le modalità delle operazioni, anche precedenti e successive, escludono intrusioni esterne e fanno presumere che il pagamento sia stato effettuato dal cliente, eventualmente ingannato tramite phishing; eccepisce infine la responsabilità al ricorrente per negligenza grave, evidenziando il ritardo nel blocco della carta, la mancata adozione di misure di sicurezza disponibili e la violazione dell'obbligo di custodire diligentemente le proprie credenziali. 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 691,50 euro, corrispondente al valore di un'operazione di pagamento online con carta eseguita il 17 dicembre 2024, che disconosce perché effettuata da terzi non autorizzati.
2. Il ricorso non merita accoglimento per le ragioni che seguono.
3. La vicenda ricade 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 *Strong Customer Authentication* – SCA –, secondo cui è necessaria un'autenticazione cd. a doppio fattore (un fattore "di possesso" e uno "di conoscenza").
5. Sul punto l'intermediario resistente afferma che la certificazione del device del ricorrente, univocamente associato alla sua App, era stata eseguita il 17.8.2024 con accesso all'area personale alle ore 11:56 e inserimento di username e password statica (fattore di conoscenza), nonché della OTP inviategli sul cellulare (fattore di possesso); aggiunge che il riconoscimento biometrico era invece stato abilitato successivamente – il 18.8.2024, alle ore 10:47 –, in seguito all'accesso all'area personale con inserimento delle credenziali statiche (fattore di conoscenza) e della OTP inviata al ricorrente via S.M.S. (fattore di possesso). A supporto di quanto affermato produce agli atti copia delle schermate tratte dal proprio sistema informatico relative all'invio degli S.M.S. necessari a finalizzare le operazioni di login e di registrazione del fattore biometrico; risulta che il numero di cellulare ivi indicato coincide con quello indicato dal ricorrente in sede di denuncia. Quanto alla fase di autorizzazione della singola operazione di pagamento, l'intermediario resistente afferma che il pagamento e-commerce è stato convalidato con riconoscimento biometrico (fattore di inerenza), precedentemente "registrato" su device abilitato (elemento di possesso). A supporto di quanto affermato, produce in atti un log dal quale emerge che, per l'operazione disconosciuta dal ricorrente, è stata richiesta l'autenticazione, ottenuta poi con riconoscimento biometrico da web-browser. Su quest'ultimo aspetto, va richiamato l'orientamento dell'Arbitro, cui il Collegio intende qui dar continuità, secondo cui un web browser o un App possono essere considerati elemento di possesso per la SCA se risulta rispettato un processo di device binding, ovvero un legame univoco tra il browser/App ed il device (PC/smartphone) utilizzato dall'utente (in questo senso, ad esempio, ABF Palermo, n. 8852/2025 e ABF Milano, n. 3329/2025). Infine, quanto alle notifiche in App, la copia del log prodotto agli atti mostra come per l'operazione *de qua* sia stata inviata la notifica per autorizzare il pagamento tramite Biometria, e poi l'avvenuto riconoscimento biometrico; emerge altresì che le notifiche erano state inviate al device in uso al ricorrente.
6. Alla luce di quanto sopra, il Collegio, in continuità con l'orientamento dell'Arbitro, ritiene dimostrata la corretta autenticazione e la regolarità formale delle operazioni disconosciute ex art. 10, c. 1, del d.lgs. n. 11/2010 con un sistema *SCA-compliant* (ad es., in tal senso, ABF Palermo n. 1338/2026).
7. Resta da vagliare l'eccezione di colpa grave del ricorrente formulata in controdeduzione dall'intermediario. 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, ricostruite sulla base delle evidenze disponibili. Nel caso di specie il ricorrente non allega alcuna circostanza relativa alla frode subita, limitandosi a segnalare di essersi avveduto dell'addebito non voluto consultando l'estratto conto. Tuttavia, la carenza di allegazioni della parte ricorrente non consente al Collegio di ravvisare un contesto di frode particolarmente sofisticato, che possa giustificare un abbassamento della soglia di diligenza del ricorrente che se ne afferma vittima. In assenza di qualsivoglia elemento, allora, il Collegio riscontra, in via presuntiva, la condotta gravemente colposa del ricorrente per negligente custodia delle credenziali personali.

8. Né, ancora, risultano, nel caso di specie, gli indici di frode di cui all'art. 8 del D.M. n. 112/2007 [ovvero: *i*) 7 o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento, *ii*) tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita, *iii*) due o più richieste di autorizzazione provenienti da Stati diversi, effettuate con la stessa carta, nell'arco di sessanta minuti], che avrebbero potuto innescare una responsabilità dell'intermediario.

9. Infine, quanto alla carenza del servizio di alert, secondo le posizioni condivise dai Collegi territoriali dell'Arbitro, la mancata attivazione ovvero il mancato funzionamento del servizio di alert (o di servizio assimilabile) sono irrilevanti nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta perché la ricezione dell'alert non avrebbe potuto in concreto limitare il pregiudizio dell'utente.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE