

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) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCA BARTOLINI

Seduta del 23/04/2026

FATTO

La ricorrente, esaurita la fase del reclamo, si rivolge all'Arbitro chiedendo l'accertamento del proprio diritto al rimborso dell'importo complessivo di 980,00 euro, corrispondente al valore di un'operazione di pagamento che disconosce perché eseguita fraudolentemente da terzi non autorizzati.

Si costituisce l'intermediario convenuto, eccependo che il bonifico disconosciuto risulta correttamente autenticato, registrato e contabilizzato, senza evidenza di malfunzionamenti o compromissioni dei sistemi, disposto mediante un sistema di autenticazione pienamente rispettoso dei parametri della *Strong Customer Authentication* – SCA – basato su elementi appartenenti alle categorie della conoscenza (codice personale) e del possesso (uso del device associato alla ricorrente); eccepisce inoltre la colpa grave della ricorrente e aggiunge di aver messo a disposizione strumenti di controllo (SMS alert) e di non essere assoggettato ad alcun obbligo generale di monitoraggio delle operazioni. Chiede pertanto il rigetto del ricorso.

In sede di repliche la ricorrente integra la documentazione acclusa al ricorso.

DIRITTO

1. Il Collegio è chiamato a esprimersi sul diritto della ricorrente a vedersi rimborsato dall'intermediario resistente l'importo di 980,00 euro, corrispondente al valore di un bonifico istantaneo eseguito l'11 gennaio 2026, bonifico che disconosce perché effettuato da terzi non autorizzati a seguito di una frode.
2. Il ricorso non merita accoglimento per le ragioni che seguono.

3. Il bonifico risulta disposto 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 l'operazione contestata è stata eseguita con un sistema di autenticazione forte a doppio fattore, attraverso una notifica push nell'app e l'inserimento del codice personale; precisa che per attivare tale procedura è necessario preliminarmente installare l'app sul device, per poi procedere con l'associazione dello strumento di pagamento (carta di pagamento o conto corrente) e con la configurazione del codice personale tramite l'inserimento delle credenziali di accesso ai servizi di internet banking (username e password), dei dati dello strumento di pagamento utilizzato per effettuare i pagamenti online (nel caso della carta, PAN, CVV2 e data di scadenza), e una password dinamica "usa e getta" – OTP – inviata via SMS sul numero di cellulare associata al cliente; nel caso di specie le operazioni risultano effettuate dal device associato alla ricorrente. L'intermediario produce agli atti copia delle schermate tratte dal proprio sistema informatico dalle quali emerge la procedura di enrollment sul menzionato dispositivo dal 20 novembre 2024, senza modifiche successive. Quanto alla specifica operazione, produce copia delle schermate dalle quali si evince prima l'autenticazione della ricorrente alla propria home banking il giorno della truffa alle ore 12:12 (poco prima della esecuzione dell'operazione *de qua*), mediante l'inserimento del codice personale (fattore di conoscenza) e l'utilizzo del device a lei associato (fattore di possesso) e poi l'autorizzazione del bonifico attraverso, ancora, l'utilizzo dell'app installata sul suo device (fattore di possesso) e l'inserimento del codice personale (fattore di conoscenza).

6. Alla luce di quanto sopra, il Collegio, in continuità con il proprio orientamento, ritiene dimostrata la corretta autenticazione e la regolarità formale dell'operazione disconosciuta ex art. 10, c. 1, del d.lgs. n. 11/2010 con un sistema *SCA-compliant* (ad es., in tal senso, può vedersi la decisione n. 224/2025).

7. Resta da vagliare l'eccezione di colpa grave della 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 la ricorrente non allega alcuna circostanza relativa alla frode subita, limitandosi a contestare l'operazione fraudolentemente disposta; solo in sede di denuncia allude a una telefonata ricevuta da un numero non riconducibile alla convenuta, senza meglio specificare; anche l'integrazione offerta in sede di repliche (copia delle schermate contenenti alcuni messaggi relativi a tentate operazioni di pagamento), priva di una descrizione, non aiuta a decifrare le circostanze di fatto. In questo contesto, le mancate allegazioni della ricorrente non consentono al Collegio di ravvisare un contesto di frode particolarmente sofisticato, che possa giustificare un abbassamento della soglia di diligenza della ricorrente che se ne affermi vittima. In assenza di qualsivoglia elemento, allora, il Collegio riscontra, in via presuntiva, la condotta gravemente colposa della ricorrente per negligente custodia delle credenziali personali.

8. Infine, quanto alla carenza, nel caso di specie, del servizio di alert, occorre richiamare il noto approccio sostanziale per cui sebbene «[f]ra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene», poiché «[g]li effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto», la mancata attivazione del servizio, considerata la sua natura di presidio di sicurezza *ex post*, è irrilevante nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta, perché l'alert non avrebbe comunque potuto eliminare, né ridurre, il danno.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE