

## COLLEGIO DI NAPOLI

composto dai signori:

|                 |                                                           |
|-----------------|-----------------------------------------------------------|
| (NA) CARRIERO   | Presidente                                                |
| (NA) GIGLIOTTI  | Membro designato dalla Banca d'Italia                     |
| (NA) MARIANELLO | Membro designato dalla Banca d'Italia                     |
| (NA) SANDULLI   | Membro di designazione rappresentativa degli intermediari |
| (NA) VERDICCHIO | Membro di designazione rappresentativa dei clienti        |

Relatore FULVIO GIGLIOTTI

Seduta del 24/03/2026

## FATTO

1. Con ricorso del 7.11.2025 – previo reclamo del 30.7.2025, riscontrato negativamente dall'intermediario – la ricorrente, titolare di conto presso l'intermediario convenuto, ha rappresentato di aver subito un addebito per operazione fraudolenta di € 1.699,50, a seguito di un'operazione di pagamento da lei mai autorizzata

Ha quindi domandato il rimborso della somma a suo avviso indebitamente addebitatale.

2. Si è costituito l'intermediario, chiedendo il rigetto del ricorso.

In particolare, ha evidenziato parte resistente che l'operazione contestata è stata eseguita, nel rispetto delle previste procedure di SCA, utilizzando apposita app precedentemente attivata dalla ricorrente su *device* preventivamente certificato (con *mobile token* generato in data 26/01/2025, alle ore 17:20:44).

In particolare, secondo l'intermediario resistente:

- alle ore 23:04:48 del 19 maggio 2025 è stata installata l'APP, necessaria per l'autorizzazione di disposizioni, sul dispositivo *Iphone 17.1*, tramite inserimento dei dati personali della cliente (codice cliente, data di nascita, PIN) e successivo inserimento del codice OTP ricevuto sul numero di cellulare appartenente alla cliente (si tratta, invero, del medesimo recapito telefonico indicato dalla ricorrente all'interno della denuncia/querela presentata);

- l'operazione oggetto di disconoscimento, del 22.5.2025, è stata correttamente autorizzata, come da *log* prodotti, tramite autenticazione forte;

- la truffa ha potuto giungere a consumazione solo - e proprio - in ragione della condotta attiva della ricorrente, la quale, come risulta dall'analisi dei *log* delle operazioni, ha autorizzato personalmente

l'operazione oggetto di disconoscimento;

- secondo parte ricorrente, le operazioni contestate sarebbero scaturite da un fenomeno di *caller ID spoofing* realizzato ai suoi danni; essa, tuttavia, non ha fornito alcuna evidenza relativa alla pretesa chiamata *spoofed* ricevuta; e non ha provato che la chiamata civetta provenisse da un numero apparentemente riconducibile all'Intermediario sicché, conformemente all'orientamento condiviso dai Collegi, la truffa non può essere considerata come *spoofing* ma come semplice *phishing*, con conseguente colpa grave della ricorrente.

Ha quindi concluso per il rigetto del ricorso.

## DIRITTO

3. Ritiene il Collegio che la domanda della ricorrente sia parzialmente da accogliere, per le ragioni di seguito illustrate.

4. L'operazione contestata è stata posta in essere sotto il vigore del D.lgs. 27 gennaio 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 gennaio 2018; le fonti normative che, nel contesto considerato, regolano la c.d. "autenticazione forte" (in gergo, individuata dall'acronimo SCA: *strong customer authentication*) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10-bis del D. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'eba (*European Banking Authority*) e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare, parere del 21 giugno 2019).

5. Secondo le previsioni normative sopra richiamate, riferibili alla fattispecie, la responsabilità di un Prestatore dei servizi di pagamento (PSP) è esclusa quando, *avendo esso dato prova di utilizzare meccanismi di "autenticazione forte" dell'utente*, sia anche riuscito a dimostrare una condotta dolosa o gravemente colposa dell'utente del servizio (con la precisazione che si intende per "autenticazione forte" 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).

Più in particolare, quando l'utente di servizi di pagamento neghi di aver 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'utilizzatore 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 D. lgs. n. 11/2010.

Piuttosto, sarà onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente: in mancanza di ciò, egli sarà tenuto responsabile dei pregiudizi subiti dall'utente, in ragione del rischio d'impresa sopportato.

Ne consegue che l'intermediario non si libera dalla responsabilità provando la mera regolarità formale delle transazioni, dovendo lo stesso, ai sensi dell'art. 10 del D. lgs. n. 11/2010, documentare elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, anche in via presuntiva, della colpa grave (o del dolo) dell'utente (cfr. Collegio di Coordinamento ABF, n. 22745 del 10 ottobre 2019).

In proposito, peraltro, un orientamento consolidato ritiene che la mancata allegazione delle circostanze di fatto della vicenda (nella specie, asseritamente) fraudolenta, da parte del ricorrente, debba essere intesa quale indizio idoneo a fondare una valutazione in termini di colpa grave della condotta del cliente, qualora il carattere non circostanziato degli utilizzi non autorizzati si sia accompagnato alla prova

dell'autenticazione forte da parte dell'intermediario resistente (in tal senso, da ult., Coll. ABF Torino, n. 8755/2025; ma v., anche, *ex multis*: Coll. ABF Milano, n. 8588/2025; Coll. ABF Bari, n. 8052/2025; Coll. ABF Bologna, n. 7965/2025).

6. Quanto sopra premesso, osserva il Collegio che, alla luce del quadro normativo sopra richiamato, e della connotazione fattuale della vicenda per la quale si procede, per come risultante dalle evidenze in atti, è emerso che:

- la ricorrente, come dalla stessa dichiarato nella denuncia presentata alla competente autorità, e acquisita in atti, ha ricevuto (in data 22.5.2025, ore 15.44 circa) una telefonata nel corso della quale l'interlocutore, qualificatosi come operatore antifrode, le chiedeva conto di una operazione di acquisto di criptovalute per euro 600,00;
- in risposta alla telefonata, la ricorrente dichiarava di non aver posto in essere l'operazione, chiedendo che fosse annullata; l'operatore comunicava l'esistenza di altra operazione per euro 1.699,50, della quale pure essa ricorrente chiedeva l'annullamento. A questo punto, al fine di annullare le operazioni, l'operatore chiedeva di comunicare le cifre centrali della carta, la scadenza e CVV, e la stessa provvedeva in conformità;
- all'esito della telefonata, constatava l'addebito della somma di euro 1.699,50;
- provvedeva, quindi, a contattare operatori dell'intermediario (intorno alle 20.30), bloccando la carta ma senza riuscire ad ottenere lo storno o l'annullamento dell'operazione contestata;
- peraltro, non è stata fornita alcuna evidenza, in atti, della chiamata ricevuta; e non risulta quindi possibile verificare se il numero dal quale è stata contattata fosse effettivamente in apparenza riconducibile all'intermediario;
- dal canto suo, l'intermediario ha dedotto e documentato che in data 19.5.2025 (tre giorni prima dell'operazione fraudolenta), la ricorrente avrebbe attivato la nuova app dell'intermediario su *smartphone* già utilizzato in precedenza (*easy enrollment*) e sul quale era già installata ed attiva altra app L... (Mobile Token); tale *device* sarebbe stato poi utilizzato per autorizzare la transazione disconosciuta;
- il processo di attivazione dell'app, come dedotto dall'intermediario, si è perfezionato alle ore 23:04 del 19.5.2025, mediante utilizzo dei seguenti fattori di sicurezza: codice *pass* (generato dalla app utilizzata in precedenza) inserimento codice OTS inviato via SMS al numero di telefono certificato della cliente (fattore di possesso);
- l'intermediario, a seguito dell'attivazione della nuova app, ha inviato specifico messaggio di alert;
- tuttavia, l'intermediario non ha depositato evidenze attestanti che il *device* certificato, poi utilizzato per autorizzare l'operazione disconosciuta, fosse stato effettivamente già associato al profilo della ricorrente, né ha depositato evidenza del messaggio inviato al numero di telefono certificato della ricorrente: non è quindi possibile stabilire se tale sms indicasse con chiarezza l'attività che con l'utilizzo del codice OTP poteva essere autorizzata;
- l'operazione disconosciuta, secondo parte resistente, sarebbe stata autenticata correttamente, a mezzo di notifica *push* su *device* certificato e digitazione dello *smartcode* (e però, l'intermediario non ha depositato evidenza della notifica *push* inviata al *device* certificato (né, quindi, del relativo contenuto), limitandosi a fornirne una rappresentazione esemplificativa);
- peraltro, non essendo state depositate repliche, le dichiarazioni di parte resistente sono rimaste non contestate.

7. In ragione di quanto sopra, ritiene il Collegio che, pur essendo risultata provata la procedura di SCA richiesta per l'operazione contestata, se, per un verso, la colpa grave della ricorrente appare certamente predicabile, tanto in ragione della mancata allegazione di evidenze relativa alla effettiva provenienza del numero chiamante, che della ingenua cooperazione della stessa alla consumazione della truffa a suo danno (avendo fornito all'ignoto interlocutore telefonico dati indispensabili per il compimento del raggio); per altro verso, anche rispetto alla condotta di parte resistente (ancorché le relative deduzioni siano rimaste non contestate nella procedura) sono residuati profili di incerta

ricostruzione, specialmente in ordine alla effettiva associazione preventiva del *device* poi utilizzato per autorizzare l'operazione disconosciuta al profilo della ricorrente, oltre che al contenuto del messaggio inviato al numero di telefono certificato della ricorrente (rispetto al quale non è possibile stabilire se esso indicasse con chiarezza l'attività che con l'utilizzo del codice OTP poteva essere autorizzata).

La reciproca mancata allegazione di alcune circostanze di fatto relative alla vicenda controversa costituisce, pertanto, a giudizio del Collegio, ragione idonea a riconoscere profili di concorso di colpa nella condotta di ambedue le parti, apparendo equo, conseguentemente, ripartire per metà il carico delle conseguenze economiche della perdita addebitata alla ricorrente.

9. Ne consegue che, in parziale accoglimento della domanda proposta, risulta ragionevole porre a carico dell'intermediario resistente l'ammanto subito dalla ricorrente nella misura del 50%, per cui lo stesso risulta tenuto a corrispondere alla ricorrente la somma di euro 850,00.

**P.Q.M.**

**In parziale accoglimento del ricorso, il Collegio accerta il diritto della ricorrente alla restituzione dell'importo di € 850,00.**

**Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.**

IL PRESIDENTE