

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) VERDICCHIO	Membro di designazione rappresentativa dei clienti

Relatore FULVIO GIGLIOTTI

Seduta del 13/01/2026

FATTO

1. Con ricorso del 25.7.2025 – previo reclamo del 3.7.2025, riscontrato negativamente dall'intermediario – la ricorrente ha esposto di avere ricevuto, in data 31.7.2024, un sms apparentemente proveniente dall'utenza associata al servizio clienti dell'intermediario convenuto, che indicava un numero di telefono da contattare, al fine dell'aggiornamento dei dati della cliente; contattava l'utenza indicata e l'interlocutore la induceva a disinstallare l'*app* dell'intermediario dal cellulare, senza però dover fornire le proprie credenziali all'operatore (ovvero, senza inserire alcun ID o *password* nell'*app* stessa); l'operatore, altresì, contestualmente la invitava ad installare la nuova *app token* dell'intermediario, apparentemente identica alla precedente, senza comunicare o farsi comunicare alcun codice.

Solo successivamente comprendeva che l'interlocutore le aveva fatto scaricare un'applicazione malevola, con la quale esso era in grado di assumere la capacità di agire operativamente da remoto, sul conto corrente della stessa, per porre in essere operazioni fraudolente (nella specie, un bonifico, dalla ricorrente mai autorizzato, di euro 8.820,00).

Ha chiesto, quindi, il rimborso della somma fraudolentemente sottrattale.

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

In particolare, ha evidenziato parte resistente che:

- il bonifico contestato è stato correttamente autenticato in *app* tramite il dispositivo mobile in esclusivo possesso della ricorrente ed unicamente associato al suo conto, ovvero in conformità con i requisiti previsti dalla c.d. “*Strong Customer Authentication*” o *SCA*; segnatamente, l’operazione di pagamento contestata è stata autorizzata alle ore 11:51 UTC (13:51 ora locale) del 31 luglio 2024 in seguito a:

- immissione del codice PIN di conferma dispositivo (fattore di conoscenza), nonché
- convalida della relativa notifica *push* di pagamento inviata all’interno dell’*app* installata sul dispositivo mobile personale della Ricorrente ed associata in via esclusiva al suo conto (fattore di possesso);

L’operazione avveniva all’interno della sessione *in app* per l’accesso al conto avviata in data 31 luglio 2024, alle ore 11:46 UTC (13:46 ora locale), sempre tramite *SCA*, vale a dire per mezzo dell’inserimento dell’*ID* biometrico della ricorrente (fattore di inerenza: cf. la stringa “*LOGIN_WITH_REFRESH_TOKEN*”) nell’*app* installata sul dispositivo mobile personale della stessa, associato in via esclusiva al suo conto (fattore di possesso).

Tanto premesso, parte resistente ha rilevato la colpa grave della ricorrente, per la condotta posta in essere in violazione delle disposizioni di legge e contrattuali, dando seguito alle indicazioni del frodatore (precisando, comunque, che, a differenza di quanto espresso nel testo del ricorso, il frodatore non può aver chiesto alla ricorrente di disinstallare l’*app* dal momento che – come si evince chiaramente dall’allegato n. 4 – tale dissociazione è avvenuta solo successivamente alla consumazione della frode, vale a dire il giorno 2 agosto 2024; infatti, il giorno 31 luglio 2024 il conto della ricorrente risultava ancora correttamente associato al suo dispositivo mobile personale; piuttosto, seguendo le istruzioni impartite dal frodatore la ricorrente ha installato una *app* non ufficiale nel suo *smartphone*, ma l’operazione di pagamento successivamente disconosciuta è stata autorizzata tramite sistema di autenticazione multifattoriale dal *device* personale della ricorrente, associato al suo conto (*SCA*)).

Su queste premesse, parte resistente ha chiesto 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), fermo restando che in caso di mancanza di prova dell'avvenuto rispetto delle procedure di SCA richieste la responsabilità dell'intermediario andrà comunque dichiarata.

Qualora, poi, si trattasse di operazioni eseguite personalmente dal cliente, non potrebbe farsi applicazione della disciplina richiamata, e il PSP potrebbe rispondere solo in caso di apporto causale proprio, secondo il diritto comune.

6. 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, rileva il Collegio che l'operazione contestata deve ritenersi correttamente autenticata.

Invero, dalle evidenze informatiche prodotte da parte resistente è emerso che:

- l'accesso al sistema dell'intermediario ha avuto luogo mediante inserimento dell'ID biometrico della ricorrente (fattore di inerenza) all'interno dell'*app* installata sul dispositivo univocamente associato al suo conto (fattore di possesso), ancorché non risulti chiaramente lo specifico tipo di fattore effettivamente utilizzato nel caso di specie (impronta digitale, riconoscimento facciale...) e quando tale modalità autorizzativa sia stata abilitata dalla cliente:

- l'operazione dispositiva è stata eseguita con sistema di autenticazione a due fattori (SCA), a mezzo digitazione di PIN su *device* certificato, già associato al profilo della ricorrente (in particolare l'associazione del *device* risaliva al 5 febbraio 2024; mentre il codice PIN utilizzato è quello impostato dalla cliente in data 1 giugno 2021, mai modificato).

7. Per altro verso, è pacificamente emerso che parte ricorrente ha eseguito le istruzioni impartite dall'ignoto interlocutore, scaricando un programma (nuova *app*) che ha reso possibile le disposizioni fraudolente: il che, secondo un pacifico orientamento dei Collegi (da ult. cfr., ad es., Coll. ABF Napoli, n. 2208"5; Coll. ABF Roma, n. 1896/25; Coll. ABF Bologna, n. 7036/25) integra una condotta gravemente colposa del ricorrente.

Occorre anche considerare, tuttavia, la condotta di parte resistente.

Invero, sebbene non sia normativamente previsto in capo agli intermediari uno specifico obbligo di monitoraggio preventivo delle transazioni (cfr. Q&A 4090/2018 dell'EBA, nonché, *ex multis*, la decisione del Collegio di Roma, n. 16114/21), è tuttavia opinione condivisa dai Collegi quella secondo la quale (oltre agli specifici indici di anomalia di cui al d.m. n. 112/2007, e anche al di fuori del più ristretto ambito (considera dal d.m. citato) delle frodi su carte di pagamento: e così, ad es., per

operazioni di bonifico o ricariche *on line*) sia ben possibile valorizzare indici di frode ulteriori, in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario), ove vi sia un'evidenza delle stesse.

Nel caso di specie, il bonifico contestato non risulta in linea con le abitudini di spesa della ricorrente, come attestate dall'estratto conto depositato, considerato anche l'importo rilevante del pagamento, che ha di fatto azzerato le disponibilità esistenti, e l'IBAN di destinazione, riferibile a conto radicato all'estero (Spagna), ma in essere presso l'intermediario resistente.

Peraltro, lo stesso intermediario resistente (in sede di risposta al reclamo) ha chiarito che già in data 1° agosto 2024, *quindi prima di ricevere la segnalazione da parte della cliente*, aveva svolto "controlli sul conto corrente di destinazione" e aveva messo "in sicurezza" il conto della ricorrente, bloccando quest'ultimo in via cautelativa; parte resistente, tuttavia, non ha chiarito se al momento dello svolgimento dei suddetti controlli sul conto del beneficiario (suo stesso cliente) i fondi fossero stati già distratti (ciò in relazione alla possibile utilità di un tempestivo blocco anche del conto di destinazione); né ha fornito alcuna evidenza del tentativo effettivamente svolto per il recupero delle somme, limitandosi unicamente a dichiarare che, al momento del primo contatto della cliente, tali somme erano ormai già state sottratte tramite ulteriori operazioni di pagamento realizzate in stretta successione temporale

Conseguentemente, tenuto conto degli elementi fattuali appena evidenziati, e dell'orientamento condiviso dai Collegi, neppure il comportamento di parte resistente appare esente da censure.

Invero, alla luce delle considerazioni che precedono, la stessa condotta di parte resistente, oltre che della ricorrente, risulta egualmente censurabile, con la conseguenza di dover considerare assolutamente predicabile un concorso di colpa, *in pari misura*, di ambedue le parti; per cui l'intermediario dovrà farsi carico delle somme fraudolentemente sottratte alla ricorrente nell'ordine della metà, oltre interessi dalla data del reclamo.

8. Ne consegue che l'intermediario convenuto, dovendo farsi carico del 50% della somma indebitamente sottratta alla ricorrente, risulta tenuto a corrispondere a quest'ultima la somma di euro 4.410,00, oltre interessi dalla data del reclamo.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto della ricorrente al risarcimento del danno per l'importo di € 4.410,00, oltre interessi legali dalla data del reclamo nei sensi di cui in motivazione.

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