

## 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) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore FULVIO GIGLIOTTI

Seduta del 18/12/2025

### FATTO

1. Con ricorso proposto in data 11.9.2025 – previo reclamo del 29.11.2024 – la ricorrente ha esposto di essere stata contattata da un sedicente operatore dell'intermediario, che la avvertiva della necessità di effettuare degli aggiornamenti, per evitare il blocco del conto; avendo dato seguito alle indicazioni dell'operatore, rilevava di non poter più controllare il proprio cellulare (rimasto "in aggiornamento") per circa 50 minuti. All'esito di tale situazione, recuperata la funzionalità del cellulare, constatava di essere stata truffata per oltre 31.000.00 euro, risultando eseguite, sul suo conto, le seguenti operazioni (dalla stessa mai autorizzate):

- 3 pagamenti *on line*, tutti a favore del medesimo beneficiario, del valore, rispettivamente, di euro 1.956,81, euro 1.956,81, euro 1.029,90;
- 1 bonifico istantaneo, di euro 10.000,00;
- 1 bonifico istantaneo, di euro 16.200,00.

Dopo aver precisato che sia il destinatario del pagamento con carta sia i beneficiari dei bonifici istantanei sono a lei sconosciuti, la ricorrente ha quindi richiesto il rimborso delle somme fraudolentemente sottratte, pari a euro 31.143,52.

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

In particolare, ha evidenziato parte resistente che:

- tutte le operazioni contestate (di cui n. 3 addebiti su carta e n. 2 bonifici) sono state correttamente autenticate *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.

In particolare:

- i tre addebiti su carta sono stati autorizzati, dal dispositivo mobile associato al conto della ricorrente rispettivamente alle ore 12:33 UTC (13:33, ora locale), 12:36 UTC (13:36, ora locale) e 12:37 UTC (13:37, ora locale) del 29 novembre 2024;

- i due bonifici sono stati autorizzati dal *device* personale associato al conto della ricorrente rispettivamente alle ore 12:31 UTC (13:31, ora locale) e alle ore 13:11 UTC (14:11, ora locale) del 29 novembre 2024;

- tutte le operazioni sono avvenute previa immissione del codice PIN di conferma dispositivo (fattore di conoscenza) e convalida delle relative notifiche *push* di pagamento inviate all'interno dell'App installata sul dispositivo mobile personale della ricorrente ed associata in via esclusiva al suo conto (fattore di possesso).

Parte resistente ha evidenziato, peraltro, che nel corso della frode i sistemi hanno rilevato indici di anomalia relativamente alle n. 3 operazioni con carta; ciò ha comportato l'invio alla ricorrente di una comunicazione recante l'indicazione dei dettagli delle operazioni segnalate (esercente, importo e data), con l'espresso avviso a verificarne la legittimità; per mezzo di tali comunicazioni, la ricorrente è stata inoltre informata della possibilità di bloccare autonomamente la carta direttamente dall'App, così da prevenire eventuali ulteriori utilizzi non autorizzati; ma solo a frode già consumata, la ricorrente dava seguito al summenzionato avviso, confermando la natura sospetta delle operazioni segnalate.

Ha anche precisato, poi, che nella medesima giornata della frode, la ricorrente contattava il Servizio Clienti per segnalare la frode subita e chiedere lo storno delle operazioni in parola; in tale contesto, la stessa confermava all'operatore di aver condiviso con il frodatore il suo indirizzo e-mail e il PIN (potendosi riferire con tale locuzione sia alla *password* utilizzata per l'accesso al conto nel corso della frode - cfr. allegato n. 1, pag. 2 - sia al PIN di conferma necessario per autorizzare i bonifici oggetto di ricorso creato dalla Ricorrente e di sua esclusiva conoscenza - allegato n. 7).

Ha infine chiarito di aver provato a recuperare le somme in questione, ma senza successo (in particolare, per quanto concerne il bonifico istantaneo dell'importo di 10.000,00 EUR disposto a favore del conto corrente radicato presso altro intermediario, la restituzione della partita richiesta a mezzo “*recall*” non è andata a buon fine giacché la banca controparte non ha provveduto alla relativa pratica di richiamo (allegato n. 8); per quanto riguarda, invece, il tentativo di recupero dell'importo di 16.200,00 EUR disposto a favore di un cliente dello stesso intermediario resistente, tali fondi non risultavano recuperabili in quanto la relativa somma aveva formato oggetto di ulteriori operazioni di pagamento effettuate in stretta successione temporale da parte del beneficiario; per quanto attiene, infine, al tentativo di recupero delle somme relative ai n. 3 addebiti su carta, a conclusione dell'istruttoria interna il dipartimento competente rigettava la richiesta di storno, rilevando che tali operazioni risultavano debitamente autorizzate dal dispositivo certificato della ricorrente mediante sistema di autenticazione multifattoriale e protocollo di sicurezza *3D Secure*, attraverso l'App installata sul dispositivo mobile personale associato al conto corrente).

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. Le operazioni contestate sono state poste 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 le operazioni contestate devono ritenersi correttamente autenticate.

Invero, dalle evidenze informatiche prodotte da parte resistente è emerso che tanto le operazioni con carta che i bonifici disposti sono stati effettuati nel rispetto delle procedure di SCA richieste.

Dai log prodotti, infatti, risulta che:

- il 29 novembre 2024 sono stati registrati 2 accessi al conto, avvenuti tramite SCA, previo utilizzo di un fattore di conoscenza (cf. la stringa "LOGIN\_WITH\_PASSWORD") e di un fattore di possesso (ossia la App installata sul dispositivo certificato: cfr. la stringa "MFA\_OSC" ed il relativo glossario di riferimento)

- i due bonifici contestati sono stati eseguiti con sistema di autenticazione a due fattori (SCA) - modalità di autorizzazione: conferma tramite PIN su device certificato; ed è stata anche data evidenza delle notifiche *push*/richieste di conferma all'utente, con indicazione dell'importo e del beneficiario;

- le operazioni con carta sono state autorizzate su *device* certificato con utilizzo di un elemento biometrico, sebbene l'intermediario non precisi se la modalità di riconoscimento tramite fattore biometrico risultava precedentemente attiva e/o utilizzata dalla ricorrente; anche in tali casi è data evidenza delle notifiche *push* inviate alla ricorrente (sebbene debba rilevarsi, con riguardo a tutte le operazioni poste in essere, che – secondo la prospettazione resa da parte ricorrente, lo smartphone utilizzato sia rimasto sottratto al controllo della ricorrente per tutto il tempo delle operazioni medesime). Se, per un verso, risulta quindi osservata la procedura di SCA, per altro verso è emerso anche – per quanto ammesso dalla stessa parte ricorrente (già nella denuncia presentata) – che la ricorrente ha dichiarato di avere *scaricato un'applicazione* e di avere eseguito le istruzioni impartite dall'ignoto interlocutore.

Per quanto essa abbia pure dichiarato di essere stata contattata da numero già conosciuto perché di supporto ai clienti dell'intermediario, il quale ultimo non ha contestato la circostanza, deve però rilevarsi che viene generalmente riconosciuta la colpa grave in capo all'utente che, dietro indicazioni di un operatore dell'intermediario, installi un'app sul proprio cellulare, che consente al malfattore di carpire le sue credenziali (o, come nel caso di specie, di assumere il controllo del suo device). Non può quindi negarsi l'esistenza di una condotta gravemente colposa di parte ricorrente (cfr., da ult., ad es., Coll. ABF Napoli, n. 2208'5; Coll. ABF Roma, n. 1896/25; Coll. ABF Bologna, n. 7036/25).

7. Occorre anche considerare, tuttavia, che, nel caso di specie:

- i sistemi dell'intermediario – per come emerso in atti – hanno registrato essi stessi rilevanti anomalie delle operazioni compiute, atteso che è stato lo stesso intermediario resistente ad evidenziare che le tre operazioni su carta (nei confronti di un unico esercente: una piattaforma di criptovalute) sono state rilevate come "sospette" dal sistema, benché poi, di fatto, l'intermediario non abbia provveduto a bloccare le predette operazioni (benché classificate ad alto rischio dal sistema) limitandosi, secondo quanto dedotto, ad inviare una comunicazione con la quale invitava la ricorrente a rispondere "sì" nel caso tali operazioni apparissero sospette anche a lei; ma non risulta alcuna evidenza dell'avvenuto tempestivo recapito della comunicazione alla cliente, che infatti ha risposto a frode ormai compiuta (a qual proposito occorre altresì considerare che durante tutta l'operatività delle transazioni compiute il cellulare della ricorrente è rimasto sottratto al suo controllo, secondo quanto dalla stessa dichiarato);

- i due bonifici posti in essere (eseguiti alle ore 13:31 e 14:11, quindi subito prima e dopo le transazioni con carta classificate come sospette; il primo bonifico autorizzato era stato richiesto in modalità istantanea, mentre il secondo era verso conto in essere presso la stessa resistente) risultavano, inoltre, di importo assai elevato, mentre dagli estratti conto disponibili in atti non risulta che la ricorrente abbia mai posto in essere operazioni simili a quelle in contestazione, quanto a importi e beneficiari;

- la ricorrente ha tempestivamente contattato il Servizio clienti dell'intermediario, alle ore 16:46 del 29.11.2024 (giorno stesso delle operazioni), chiedendo di bloccare tutte le operazioni registrate a suo nome nella giornata e segnalando di non averle eseguite (l'assistenza è stata fornita via chat);

- parte resistente, con specifico riguardo al bonifico (non istantaneo) di euro 16.200,00, ha dichiarato di aver provato a recuperare la somma, non essendovi riuscito in quanto la somma medesima aveva già

formato oggetto di ulteriori operazioni di pagamento effettuate in stretta successione temporale da parte del beneficiario (del che, tuttavia, non è stata fornita alcuna evidenza);

- nulla è stato dedotto da parte resistente in relazione all'esistenza/attivazione di un servizio di sms alert (sebbene, comunque, parte ricorrente abbia segnalato di aver perso il controllo del telefono per circa 50 minuti).

8. Sotto altro profilo, poi, occorre pure considerare che, al di là di quanto dettato dall'art. 8 d.m. n. 112/2007 – in tema di prevenzione delle frodi sulle carte di pagamento (con la precisazione che gli indici di frode ivi disciplinati possono costituire, secondo un orientamento condiviso dai Collegi, un parametro di valutazione del comportamento del PSP, ove possibile, anche con riguardo ad operazioni eseguite con altri strumenti di pagamento (ad es. bonifici o ricariche *on line*) in ragione dell'unicità della *ratio* sottesa a tale normativa – il quale considera rilevanti, tra l'altro, *tre o più richieste di autorizzazione sulla stessa carta*, effettuate nelle 24 ore, presso un medesimo punto vendita, una soluzione pacificamente condivisa riconosce che sia certamente consentito, al Collegio, valorizzare anche indici di frode *ulteriori* rispetto a quelli di cui al cit. d.dm. n. 112/2007, 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.

Ed è altrettanto pacifico, al riguardo, che – per quanto concerne la quantificazione del rimborso da riconoscere all'utente – la valutazione della responsabilità del PSP deve essere formulata in un giudizio sintetico che tenga conto della sua condotta complessiva e di tutti gli altri elementi desumibili dal caso concreto: la base di calcolo per la liquidazione della somma oggetto di condanna è costituita dall'intero ammontare degli importi disconosciuti, senza esclusioni, procedendo a una distribuzione in concreto del concorso di colpa tra le parti.

9. Tenuto conto, allora, di tutto quanto fin qui precisato, tanto con riguardo allo svolgimento fattuale della vicenda che con riferimento alle soluzioni correntemente praticate, rileva il Collegio che pur esistendo una condotta gravemente colposa di parte ricorrente, egualmente rilevante e censurabile deve considerarsi il comportamento dell'intermediario convenuto, attese tutte le circostanze sopra segnalate al § 7 (rilevata anomalia e sospetto delle operazioni con carta; mancata evidenza dell'avvenuto tempestivo recapito di avviso alla cliente; numero, rilevanza e importo delle operazioni poste in essere, in discontinuità con il profilo della cliente; mancata evidenza della dedotta impossibilità di recupero di alcune somme disposte; assenza di alert documentati).

Deve perciò giudicarsi concorrente, al 50%, la colpa di parte resistente, la quale dovrà conseguentemente farsi carico, nella misura della metà (oltre interessi), delle somme (euro 31.143,52) fraudolentemente sottratte alla ricorrente.

10. Ne consegue che l'intermediario convenuto risulta perciò tenuto a corrispondere alla ricorrente la somma (arrotondata) di euro 15.572,00, oltre interessi dalla data del reclamo.

### P.Q.M.

**In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente al risarcimento del danno per l'importo di € 15.572,00, 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