

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 del 9.8.2025 – previo reclamo del 26.3.2025, riscontrato negativamente dall'intermediario in data 14.4.2025 – il ricorrente ha esposto quanto segue:

- in data 12/03/2025, alle ore 14:08, riceveva un sms, che si inseriva nella chat già in precedenza intrattenuta con l'intermediario; il messaggio lo avvisava di un tentativo di pagamento per € 2.750,00 a valere sul suo conto e lo invitava a contattare un numero telefonico, pure indicato;

- preoccupato per la situazione, provvedeva quindi a contattare tale utenza; nel frangente, l'operatore, qualificatosi come operatore dell'intermediario, nel confermare il tentativo di pagamento, lo invitava a bloccare le proprie credenziali per salvaguardare il proprio conto; seguiva quindi un ulteriore sms recante un *link* che lo indirizzava ad una pagina *web* dalle sembianze identiche a quella dell'intermediario, nella quale provvedeva ad inserire le proprie credenziali; una volta effettuata questa operazione gli giungevano degli OTP che l'operatore gli chiedeva di comunicare.

A questo punto riceveva notifica dell'avvenuta installazione di un *wallet*, da lui mai voluta, e poi del perfezionamento di un pagamento di € 4.000,00, a mezzo POS, da lui mai autorizzato.

Quanto sopra premesso, ha quindi richiesto il rimborso della somma fraudolentemente sottrattagli.

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

In particolare, ha evidenziato parte resistente che in base a quanto descritto nella denuncia ed alla ricostruzione degli eventi, è evidente che il ricorrente, per sua stessa ammissione, è rimasto vittima di una truffa realizzata attraverso *smishing* mista a *vishing*, consistente nell'invio di sms fraudolenti che sembrano provenire dal proprio intermediario (sms *spoofing*) ma che, in realtà, mirano a carpire dati riservati per poter effettuare operazioni dispositive.

Ha quindi sottolineato che

- il ricorrente ha contattato imprudentemente una utenza mobile non riconducibile all'intermediario, fornendo poi, incautamente, dati strettamente segreti e confidenziali, di sua esclusiva conoscenza;
- l'operazione disconosciuta è stata effettuata previo accesso all'internet banking del cliente;
- l'accesso è avvenuto attraverso credenziali di sicurezza in esclusivo possesso del ricorrente, ovvero digitazione di *username* (codice utente), *password* (elemento di conoscenza) e *password* temporanea (OTP, elemento di possesso), ricevuta sul proprio cellulare tramite SMS, in relazione all'operazione da autorizzare (nel caso di specie accesso all'area privata).

Più in dettaglio, parte resistente – producendo i relativi log informatici – ha rilevato che l'intera procedura si è svolta secondo questa sequenza:

- avvio sessione di *login* (da App) in data 12/03/2025 alle ore 14:21:51, tramite l'inserimento a sistema di codice utente e *password* (*session_id* -1602764339 – colonna *browser_type* "yaSApp" e colonna *logintype*: "*password*");
- invio codice OTP, via SMS, per validazione della modalità di accesso, sempre sul recapito di cellulare del ricorrente (**030) alle ore 14:21:52;
- inserimento a sistema del codice OTP, alle ore 14:22:22, per finalizzazione accesso ("OTP-PagAcc" *session_id* -1602764339).

Durante detta sessione di accesso veniva attivato, in relazione alla carta di debito, il servizio *Wallet* G***p**, tramite codice OTP specifico, pervenuto sul numero del cliente. L'attivazione del servizio *wallet* veniva finalizzata tramite l'inserimento in procedura dello specifico codice OTP inoltrato via SMS in data 12/03/2025 alle ore 14:23:34, sul recapito di cellulare del ricorrente: di tale attivazione, il ricorrente riceveva apposita notifica, via SMS, sul recapito indicato, alle ore 14:24:38.

A seguito dell'attivazione del servizio, veniva poi finalizzata la transazione, a distanza di tre minuti circa, alle ore 14:26.

Tanto premesso, parte resistente ha evidenziato che la regolare abilitazione di un dispositivo *smartphone* all'uso del servizio attivato, come per il caso di specie, prevede che lo *smartphone*, contenente l'applicazione dell'intermediario dove sia stato comunque effettuato almeno un primo accesso, venga utilizzato come una carta di pagamento *contactless* (elemento di possesso), insieme alla *password* selezionata e conosciuta esclusivamente dal possessore del dispositivo autorizzato ad emulare la carta (elemento di conoscenza).

Conseguentemente, nell'esecuzione delle operazioni contestate, sono stati rispettati i parametri ed i requisiti della cd. autenticazione forte, mediante la richiesta di più fattori per l'accesso all'*internet banking*, per l'*enrollment* del dispositivo al servizio *Wallet* e l'esecuzione dell'operazione di pagamento. Su tali premesse, parte resistente ha chiesto il rigetto del ricorso.

DIRITTO

3. Ritiene il Collegio che la domanda del 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. Con specifico riguardo, poi (come nella specie), a operazioni di pagamento tramite *wallet*, è stato precisato che «nell’autenticazione di operazioni di pagamento tramite *digital wallet*, il codice di sblocco del dispositivo utilizzato (ovvero, in alternativa, il riconoscimento biometrico) può valere come secondo fattore rilevante ai fini della SCA, purché esso sia stato in via preventiva associato univocamente all’utente, mediante uso nella fase di *tokenizzazione* dello strumento all’interno del *wallet*, con procedura conforme a SCA» (Coll. coordin. ABF, n. 9559/2024).

In proposito, proprio con riferimento a caso del tutto simile, riferibile al medesimo intermediario oggi convenuto – premesso che possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di

autenticazione – è stato deciso che l'utilizzo della carta *tokenizzata* costituisce un fattore di possesso secondo la *Question ID*: 2019_4827 dell'EBA; mentre con riguardo al secondo fattore, la dicitura "Tipo oper.: AUT", per quanto desumibile dalla *legenda* dell'intermediario (esattamente come nel caso di specie), consente di evincere l'uso dell'ulteriore elemento di conoscenza (in tal senso, espressamente, Coll. ABF Roma, n. 8676/2025).

Dalle evidenze prodotte in atti, quindi, può ritenersi provato il rispetto della procedura di SCA richiesta.

7. Nondimeno, 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, sebbene le operazioni contestate debbano ritenersi correttamente autenticate, deve tuttavia rilevarsi un concorso di colpa di parte resistente idoneo a sorreggerne, parzialmente, la responsabilità.

Invero, per quanto parte ricorrente, eseguendo le istruzioni impartite dall'ignoto interlocutore, abbia posto in essere una condotta gravemente colposa, deve però considerarsi, altresì, che l'associazione di una carta di pagamento ad un *wallet* digitale rientra certamente tra quelle azioni che possono comportare un rischio di frode nei pagamenti o altri abusi (cfr. Q&A EBA del 25.9.2020), tale da suggerire, cautelativamente, di non consentire operazioni *immediatamente successive* a tale associazione, considerato che le stesse potrebbero ragionevolmente essere fraudolente: nel caso di specie, invece, l'operazione di pagamento disconosciuta è avvenuta dopo poco più di un minuto, soltanto, dall'avvenuta *tokenizzazione* della carta tramite *wallet* (e quindi, è proprio immediatamente successiva), così rivelandosi una condotta indubbiamente incauta dell'intermediario resistente (condotta che deve essere apprezzata, in termini di concorso di colpa, in eguale misura (50%) rispetto a quella di parte ricorrente). Ne consegue, pertanto, che l'intermediario convenuto deve rispondere della perdita fraudolentemente subita dal ricorrente nella misura appena indicata del concorso di colpa.

9. In ragione di quanto precede, quindi, reputa il Collegio che l'intermediario convenuto dovrà farsi carico del 50% della somma (euro 4.000,00) indebitamente sottratta al ricorrente, risultando perciò tenuto a corrispondere a quest'ultimo la somma di euro 2.000,00, 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 € 2.000,00, 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