

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) MIOLA	Membro di designazione rappresentativa degli intermediari
(NA) MAFFEO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - ADRIANO MAFFEO

Seduta del 10/03/2026

FATTO

Con ricorso del 21/10/2025, il ricorrente, insoddisfatto dell'interlocuzione intercorsa con l'intermediario in sede di reclamo, si rivolge all'Arbitro, al quale chiede il riconoscimento in capo al convenuto dell'obbligo di restituzione della somma di € 3.140,00, a suo dire fraudolentemente sottratta mediante l'esecuzione di diverse operazioni ("Pagamento POS") non autorizzate a valere sulla carta di prepagata dotata di IBAN.

Dalla documentazione versata in atti è dato rilevare che il ricorrente ha, prima, ricevuto un SMS apparentemente proveniente dall'intermediario resistente, con il quale lo si invitava a verificare presunte anomalie di sicurezza sul conto corrente e, successivamente, è stato contattato da un sedicente operatore che lo informava della possibilità di bloccare l'operazione anomala attraverso un'applicazione da scaricare mediante un link all'uopo condivisogli. Una volta conclusa la procedura, il ricorrente veniva invitato dall'operatore ad inquadrare con il cellulare la carta di debito e, successivamente, ad accedere all'applicazione dell'intermediario per verificare il codice di sicurezza. A questo punto, resosi conto di essere stato vittima di una truffa, provvedeva a chiudere l'applicazione e a bloccare lo strumento di pagamento.

L'intermediario, costituitosi, conferma l'effettuazione di n. 7 operazioni di pagamento in modalità contactless, con successivo inserimento del PIN, per un importo totale di € 3.140,00.

Contesta il diritto al rimborso degli importi richiesti dal ricorrente assumendo il pieno rispetto delle obbligazioni in tema di Strong Customer Authentication. Chiede pertanto il rigetto del ricorso.

DIRITTO

In via preliminare occorre rilevare che l'operazione contestata è stata eseguita 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 13/01/2018. In particolare, le fonti normative che regolano la c.d. *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10-bis del D. Lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA 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 (v. in particolare il parere dell'EBA del 21 giugno 2019). Nel merito, dalle risultanze del fascicolo, emerge che le operazioni contestate sono in totale sette prelievi cardless, effettuati il 02/10/2025 in un arco temporale di tre minuti, dalle ore 18:15 alle ore 18:18, e tutte effettuate presso il medesimo punto vendita (POS), per un importo complessivo di € 3.140,00.

Lo schema della truffa risulterebbe riconducibile al c.d. "Card Relay Attack", nel quale il cliente viene inizialmente ingaggiato attraverso un phishing tradizionale, e, poi, attraverso l'installazione sul device di un'applicazione malevola, viene effettuata una transazione contactless sfruttando la tecnologia NFC del dispositivo.

Tanto evidenziato, giova rilevare che dalle risultanze documentali del fascicolo emerge che le operazioni risultano autorizzate tramite un elemento di possesso, nella specie la carta, letta in modalità contactless, ed uno di conoscenza, il PIN, peraltro oggetto di recupero poco prima dell'inizio dei prelievi sconosciuti tramite l'App dell'intermediario.

Sotto il profilo formale le operazioni risultano pertanto correttamente autenticate e la procedura conforme alla SCA.

Tuttavia, giova rilevare che nella specie sussistono gli indici di frode identificati dall'art. 8 del D.M. 112/2007 che, come noto, pur non avendo un valore precettivo diretto, rappresentano utili indicatori per identificare anomalie e scenari di raggiri anche ai sensi dell'art. 2 del Regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente.

Nel caso in questione viene in rilievo ciò che la norma prevede per i punti vendita (terminali POS), configurando il rischio di frode allorché vengano effettuate "tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita". Nella fattispecie in oggetto sono state effettuate sette richieste presso lo stesso punto vendita, nell'arco di pochi minuti.

A quanto rilevato si aggiunge l'ulteriore rilievo che, per quanto l'intermediario asserisca di disporre di un sistema di notifiche sui movimenti in uscita, non fornisce evidenza alcuna dell'invio dei c.d. messaggi alert.

Tali elementi inducono il Collegio a ritenere addebitabile all'intermediario un concorso di colpa, nella misura del 50%, nella determinazione del danno lamentato dal ricorrente, al quale va riconosciuto, quindi, l'importo di euro 1.570,00, oltre interessi legali a decorrere dalla data del reclamo.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente al risarcimento del danno nella misura di € 1.570,00 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