

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) RUSSO	Membro designato dalla Banca d'Italia
(PA) SCANNELLA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO MELI

Seduta del 14/05/2026

FATTO

Con ricorso pervenuto il 9.02.2026 il ricorrente riferisce che in data 29.09.2025 riceveva un messaggio SMS apparentemente proveniente dal servizio antifrode dell'intermediario, con il quale veniva segnalata una presunta operazione sospetta sulla carta a lui intestata e gli veniva richiesto di contattare con urgenza il numero telefonico indicato nel messaggio. La comunicazione, per contenuto e modalità di presentazione, risultava idonea a simulare una comunicazione ufficiale dell'intermediario. Preoccupato dalla possibile compromissione dello strumento di pagamento, contattava il numero indicato e veniva messo in comunicazione con un soggetto che, qualificandosi falsamente come operatore del servizio antifrode, lo induceva a compiere attività presentate come necessarie alla messa in sicurezza della carta. Nel corso della conversazione non comunicava codici dispositivi, PIN o OTP, né autorizzava alcuna operazione di pagamento. Successivamente, contattando il reale servizio clienti, apprendeva che era stato eseguito un pagamento non autorizzato, per l'importo di € 979,00. Egli, quindi, si recava immediatamente presso un ufficio dell'intermediario per segnalare l'accaduto e richiedere il blocco della carta compromessa. In tale sede, tuttavia, l'operatore, anziché procedere al blocco immediato dello strumento, disponeva l'estinzione della carta e il trasferimento del saldo residuo (pari ad € 4.113,34) su una nuova carta. Tale errata procedura consentiva ai malintenzionati di reiterare la frode, con l'esecuzione di ulteriori cinque operazioni di pagamento non autorizzate, per un importo complessivo di € 3.489,96.

Il ricorrente sporgeva tempestiva denuncia presso la Polizia Postale e attivava tutte le iniziative previste dalla normativa vigente, senza tuttavia ottenere alcun rimborso delle somme indebitamente sottratte, nonostante la natura manifestamente non autorizzata delle operazioni contestate e le gravi criticità riscontrate nella gestione dell'evento da parte dell'intermediario.

Con il ricorso chiede che l'Arbitro voglia:

- accertare e dichiarare la natura non autorizzata delle operazioni di pagamento contestate, eseguite sulla carta intestata al ricorrente;
- accertare e dichiarare la responsabilità dell'intermediario per la violazione della normativa di cui al D.lgs. n. 11/2010 (PSD2), per il difetto di prova dell'effettiva applicazione della *Strong Customer Authentication*, per le carenze dei presidi antifrode e per la condotta colposa del proprio dipendente ai sensi degli artt. 1228 e 2049 c.c.;
- per l'effetto, disporre la condanna dell'intermediario al rimborso integrale in favore del ricorrente dell'importo complessivo di € 3.489,96, corrispondente alle operazioni fraudolente contestate;
- con ogni conseguente statuizione in ordine agli interessi e alle spese di procedura, secondo quanto previsto dal Regolamento ABF.

Con le controdeduzioni, l'intermediario chiede il rigetto del ricorso. Afferma che, da quanto emerge dagli atti, la frode perpetrata ai danni del cliente sembrerebbe essere riconducibile allo schema del "phishing" classico, nel quale il malcapitato, comunicati i propri codici (ricevuti anche per SMS), consente al frodatore di predisporre operazioni dispositive, partecipando in tal modo, seppur inconsapevolmente, alla truffa in suo stesso danno.

Riporta evidenza contabile delle operazioni disconosciute da parte ricorrente e documenta che l'operazione contestata di € 979,00 eseguita con carta di pagamento n. ***837 è stata restituita alla parte ricorrente in data 1.10.2025.

Parte ricorrente contesta n. 5 operazioni di pagamento online eseguite con Token con la carta n. ***914. Le operazioni contestate risultano correttamente autenticate, registrate e contabilizzate, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi. Più precisamente, come si evince dalla documentazione – costituita da estratti dei gestionali interni della Società – risultano regolarmente avvenute:

- la fase di *enrollment* della carta di pagamento n. ***914 di titolarità della parte ricorrente al sistema autorizzativo di tipo dinamico funzionante mediante invio con sms della password dinamica sul numero di cellulare altresì indicato dal cliente nella denuncia in atti;
- la fase di tokenizzazione della carta sul wallet con procedura SCA;
- la fase dispositiva delle operazioni oggetto di ricorso, per le quali fornisce evidenza informatica che dimostra la modalità autorizzativa con Token secondo procedura SCA di ciascuna delle stesse.

Il blocco della carta in questione è avvenuto alle ore 19:11 del giorno 29.09.2025. Pertanto, successivamente alle operazioni per cui è controversia.

Con replica e controreplica le parti hanno sostanzialmente ribadito le loro posizioni.

DIRITTO

La controversia attiene ad una richiesta di rimborso di somme che sono state fraudolentemente sottratte al ricorrente, attraverso operazioni non autorizzate.

Le operazioni contestate sono state eseguite 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. Ai sensi

dall'art. 10 del d.lgs. 11/2010, a fronte del disconoscimento di una operazione di pagamento da parte dell'utente, il prestatore di servizi di pagamento (PSP) ha l'onere di provare:

- l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione contestata e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti;
- il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

In sintesi, secondo gli orientamenti condivisi dei Collegi (cfr. Collegio di Coordinamento, dec. n. 22745/2019), la prova di autenticazione rappresenta, in aderenza al dato normativo l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente.

Le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del dlgs. 10/2011, 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).

Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Parte ricorrente lamenta l'esecuzione fraudolenta di 5 operazioni dispositive, eseguite con una carta il 1°.10.2025, per un totale di € 3.489,96. Si tratta di operazioni di pagamento eseguite attraverso il wallet, nel giro di due minuti, ad un'impresa di onoranze funebri.

L'intermediario sostiene che le operazioni sono state autorizzate mediante un sistema di autenticazione forte. Afferma che il sistema ha registrato, alle 16:32, l'*enrollment* dell'app su un altro dispositivo, effettuata inserendo username e password e successiva conferma con l'inserimento di un codice OTP inviato mediante SMS. Alle 16:48 la prima carta è stata tokenizzata nel wallet di tale dispositivo, mediante inserimento del pin (elemento di conoscenza). Successivamente (ma non vengono indicate né l'ora, né le modalità), è stata tokenizzata la seconda carta (attivata in sostituzione della prima). Con quest'ultima, dalle 18:25 alle 18:27, sono state effettuate attraverso il wallet digitale le cinque operazioni disconosciute. Non viene indicato come queste siano state autenticate e l'intermediario non produce alcuna documentazione.

Alla luce delle dette evidenze, si deve ritenere mancata la prova della SCA, proprio con riferimento alla tokenizzazione della carta con la quale sono state effettuate le cinque operazioni disconosciute (e non rimborsate, a differenza di quella che era stata effettuata con la prima carta) e all'effettuazione delle medesime operazioni.

Il ricorso deve, pertanto, trovare accoglimento, senza necessità di condurre ulteriori valutazioni.

PER QUESTI MOTIVI

In accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla corresponsione dell'importo complessivo di € 3.489,96, oltre interessi dalla data del reclamo.

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