Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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 ENZO SCANNELLA

Seduta del 23/01/2026

FATTO

Dopo aver invano esperito la fase di reclamo, con ricorso pervenuto in data 16.10.2025, il ricorrente chiede la restituzione della somma di € 1.900,00, corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati.
Parte ricorrente riferisce che/di:
-Essere titolare di una carta prepagata n. ***0674;
-In data 25/08/2025 intorno alle ore 15:00, tentava di effettuare pagamento mediante POS ma non andava a buon fine;
-All'interno della carta da lui utilizzata vi era un residuo di circa euro 2.000,00;
-Accedeva quindi all'app di home banking dal suo cellulare per effettuare il pagamento e verificare il conto, ma l'applicazione risultava bloccata;
-Provvedeva a verificare l'estratto conto della carta prepagata sopra indicata e si accorgeva di un bonifico SEPA istantaneo sulla stessa e da lui disconosciuto;
-L'operazione risultava eseguita in data 22/08/2025.
L'intermediario, con le controdeduzioni, eccepisce che/di:
-Non sussiste la sua responsabilità per l'operazione di pagamento in contestazione, risultando approvata correttamente tramite un sistema di autenticazione forte e senza alcuna anomalia, nel rispetto dei requisiti SCA.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

-Alla luce di quanto rappresentato dal cliente e da quanto si evince dagli estratti informatici in possesso, la frode perpetrata ai danni del cliente sembrerebbe essere riconducibile allo schema del “phishing” classico o della manipolazione del pagatore.
-L’operazione risulta correttamente autenticata, registrata e contabilizzata, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi.
In particolare, risulta eseguita mediante “autenticazione a due fattori” appartenenti rispettivamente alle categorie della conoscenza (i.e. qualcosa che solo l’utente conosce, ossia il codice P***Id) e del possesso (qualcosa che solo l’utente possiede), ovvero il device su cui è installata la APP della banca.
-Allo stato non è rinvenibile un obbligo di monitoraggio delle operazioni in capo all’intermediario, il quale non può evitare che i propri clienti dispongano liberamente delle somme di cui hanno la disponibilità sul presupposto – indimostrato ed indimostrabile – che ogni operazione anomala sarebbe di per sé truffaldina.
-Ritiene di aver messo disposizione dei propri clienti e quindi anche dell’odierno ricorrente uno strumento di pagamento rispondente agli attuali standard tecnologici.
-Pertanto, l’operazione disconosciuta, tenuto conto della modalità con cui è stata autorizzata, poteva essere eseguita soltanto dal titolare dello strumento di pagamento, che è in possesso del device su cui è inviata la notifica in APP per l’inserimento del codice di sicurezza “P***ID”, o, in ultima istanza, da un terzo a cui potrebbero essere state fornite, anche inconsapevolmente nell’ambito di uno schema fraudolento di phishing tradizionale, i codici di sicurezza e la password dinamica necessari per l’abilitazione di tale procedura di autenticazione.
-In relazione alle operazioni in oggetto l’utenza telefonica collegata alla posizione del ricorrente non sembra aver ricevuto alcuna modifica.
-Non vi è stato alcun cambio di utenza, dall’enrollment della carta fino alla sua chiusura, conseguenza della presunta frode oggetto della controversia.
-L’assenza di un qualsiasi cenno ad una qualsivoglia operatività online intrapresa in concomitanza dell’illecito addebito, porta a desumere che la presente frode sia riconducibile alla tipologia di phishing classico.
-Il blocco della carta in questione è avvenuto alle ore 08:21, del giorno 28/08/2025 pertanto successivamente alle operazioni per cui è controversia.
-L’orientamento dei Collegi è quello di ritenere che in ipotesi di utilizzi fraudolenti online dello strumento di pagamento, in cui il cliente non ha allegato le circostanze di fatto della frode lamentata, a fronte della prova di autenticazione e in assenza di indici di anomalia e di ulteriori elementi, la colpa grave del cliente si presume.
-Nel caso di specie sono presenti numerosi elementi dai quali emerge la colpevolezza in capo al Ricorrente e l’esonero di qualsivoglia responsabilità in capo allo scrivente intermediario.
-Infine, l’intermediario svolge proattivamente delle azioni volte a rendere consapevole la propria clientela in merito all’evoluzione dei principali schemi di frode agiti dai frodatori, mediante, a titolo esemplificativo, campagne informative sui canali digitale e distribuzione di materiale cartaceo su tutto il territorio.
In conclusione, l’intermediario chiede al Collegio di rigettare il ricorso.

DIRITTO

La domanda del ricorrente è relativa alla restituzione della somma corrispondente all’importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati.
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 13/1/2018.

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:
A. 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.
B. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).
In particolare, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente.
Parte ricorrente lamenta l'esecuzione fraudolenta di una operazione di bonifico istantaneo di importo pari a € 1.900,00, eseguita in data 22/08/2025 alle ore 04:23.
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.
In merito all'autenticazione forte con riferimento alla fase di accesso in app antecedente all'operazione contestata, l'intermediario riferisce che è necessario in via preventiva installare l'app dell'intermediario sul device, associare lo strumento di pagamento e configurare il codice P***ID. Evidenzia al riguardo che l'utenza telefonica collegata all'utenza del cliente non ha subito alcuna modifica prima dell'esecuzione dell'operazione disconosciuta.
Dalla documentazione versata in atti, con riferimento alla data di esecuzione dell'operazione fraudolenta – 22/08/2025 – non sembrerebbero esservi state modifiche relative all'utenza telefonica del ricorrente. PIN e utenza presenti nella documentazione prodotta dall'intermediario sembrano infatti corrispondere con i dati presenti nel modulo di contestazione dell'operazione prodotto dal ricorrente e, dallo storico della carta, non risulterebbero modifiche.
Con riferimento alla fase di accesso in app che ha proceduto il compimento dell'operazione contestata, l'intermediario rappresenta che il ricorrente si sia autenticato in data 22/08/2025 alle ore 04:24 nella propria home banking mediante digitazione del codice P***ID necessario per accedere alla propria area personale.
Sulla base delle evidenze prodotte, risulterebbe quindi che la fase di accesso in app sia avvenuta tramite autenticazione forte e, in particolare, mediante l'inserimento del codice P***ID (fattore di conoscenza) sul proprio device (fattore di possesso).
Al riguardo si ha presente che, per giurisprudenza consolidata dei Collegi ABF (cfr. Collegio di Coordinamento n. 21285/21) devono essere presidiati dalla autenticazione forte a due fattori non solo le singole operazioni dispositive ma anche tutte quelle operazioni (modifica/aggiunta di un device, attivazione di un token, modifica del numero di cellulare e/o della mail associata al conto ecc.) idonee a incidere sulla sicurezza dello strumento e dei pagamenti con questo effettuati.
In merito all'autenticazione forte con riferimento alla operazione di bonifico istantaneo, l'intermediario rappresenta che la transazione è stata disposta tramite la modalità "primaria" di autenticazione, che comporta l'inserimento del codice P***ID in app. Da tali evidenze risulterebbe il device ID, il canale utilizzato e il metodo dispositivo dell'operazione (MOD DISP – PID, il quale indicherebbe l'utilizzo del codice P***ID).

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Sulla base delle evidenze prodotte e sopra riportate, risulterebbe che il ricorrente abbia autenticato correttamente la transazione e, in particolare, sembrerebbe che l'autorizzazione sia stata fornita mediante inserimento del codice P***ID – fattore di conoscenza – inserito sul device in uso al ricorrente – fattore di possesso –.
Preliminarmente, il Collegio precisa che la colpa grave del ricorrente assume rilievo solo se l'intermediario fornisce la prova di autenticazione delle operazioni che – secondo l'orientamento condiviso dai Collegi – rappresenta, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente (cfr. Collegio di Coordinamento, con decisione n. 22745/2019).
In merito alle modalità della truffa e alla sussistenza degli indici di colpa grave in capo all'utilizzatore, dalla documentazione versata in atti e dall'analisi di tutta l'ulteriore documentazione prodotta dal ricorrente, non risulta in maniera chiara quale sia stata la modalità con la quale sia stata perpetrata la truffa ai danni del ricorrente, il quale si limita a riferire di aver notato l'addebito in oggetto il 25/08/2025 (quindi tre giorni dopo la sua esecuzione), al momento di effettuare un altro pagamento.
Si osserva che, secondo l'orientamento condiviso dai Collegi territoriali, nel caso in cui:
i. l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute;
ii. il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA);
iii. non risultano indici di anomalia delle operazioni e/o ulteriori elementi;
le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo.
In merito al blocco dello strumento, risulterebbe che in data 28/08/2025, alle ore 08:21, sia avvenuto il blocco dello strumento di pagamento. Si precisa che non sono state eseguite operazioni in seguito al blocco.
Parte ricorrente non ha contestato il superamento del plafond.
Circa l'attivazione di idoneo sistema di alert, dalla documentazione in atti non risulta l'attivazione di un servizio di notifiche; tuttavia, si tratta di un'unica operazione.
Al riguardo si ha presente che, secondo gli orientamenti condivisi dai Collegi, la mancata attivazione ovvero il mancato funzionamento del servizio di sms-alert (o servizio assimilabile) possano essere ritenuti irrilevanti nell'ipotesi in cui le operazioni risultino effettuate a breve distanza di tempo l'una dall'altra ovvero si tratti di una sola operazione, in quanto l'invio dell'sms non avrebbe potuto, in concreto, impedire o contenere la perdita relativa alle operazioni non autorizzate dal titolare dello strumento di pagamento.
Parte resistente non ha domandato l'applicazione della franchigia.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE