

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) IMBURGIA	Membro di designazione rappresentativa degli intermediari
(PA) PLATANIA	Membro di designazione rappresentativa dei clienti

Relatore ANTONINO FRANCESCO PLATANIA

Seduta del 14/04/2026

FATTO

Il ricorrente chiede la restituzione della somma di euro 600,00, corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati affermando che l'intermediario non ha rimborsato un'operazione di pagamento non autorizzata, nonostante la presentazione di formale reclamo. IL ricorrente lamenta di essere stato vittima di una truffa di tipo smishing/vishing che ha determinato l'esecuzione di un bonifico istantaneo fraudolento. Afferma che ai sensi del D.Lgs. 11/2010 (attuativo della direttiva PSD2), l'intermediario è tenuto a rimborsare le operazioni di pagamento non autorizzate salvo prova del dolo o della colpa grave del cliente, che nel caso di specie non ricorre. Costitutosi l'intermediario convenuto eccepisce che il ricorrente ha fornito una ricostruzione parziale e approssimativa della vicenda: tale condotta rappresenta un'ipotesi di colpa grave; che non è stata prodotta copia dell'SMS ricevuto e che l'operazione contestata è stata correttamente autenticata mediante un sistema conforme alla SCA, utilizzando l'APP dell'intermediario. Con repliche del 9/03/2026 parte ricorrente produce evidenza della chiamata ricevuta dal frodatore, infine evidenzia il carattere sofisticato della truffa di cui è stato vittima e rileva di essersi immediatamente attivato al fine di bloccare il prelievo fraudolento. Con controrepliche del 19/03/2026 parte resistente conferma il contenuto delle proprie controdeduzioni, insistendo per il rigetto del ricorso.

DIRITTO

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.

Con riferimento all'autenticazione delle operazioni e alla valutazione di conformità ai requisiti della SCA si rammenta che 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. 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 un'operazione fraudolenta posta in essere in data 01.12.2025, ossia un bonifico istantaneo di euro 600,00. L'intermediario sostiene che l'operazione oggi contestata sia stata correttamente autenticata, registrata e contabilizzata. Fornisce evidenze a riprova della propria ricostruzione, producendo due allegati alle controdeduzioni che si procede da analizzare. Il primo relativo all'enrollment dell'app sul device del ricorrente da cui si rileva che tale operazione è avvenuta in data 27.09.2025, quindi circa due mesi prima della truffa. E tuttavia risulta essere un antecedente logico necessario per la ricostruzione della vicenda. In particolare, con riferimento a tale operazione parte resistente produce: Log antifrode corredato di legenda; evidenza della chiamata Securecall al numero certificato del cliente; log autorizzativo corredato da legenda esplicativa. Si rammenta che secondo l'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019 il codice PIN rappresenta un elemento di conoscenza. Inoltre, secondo l'orientamento dei Collegi ABF, la securecall sul numero certificato del ricorrente costituisce un valido fattore di autenticazione inquadrabile nella categoria del possesso- Collegio di Bologna, decisione n. 4737/2024 e Collegio di Milano, decisione n. 12602/2024. 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.

Con riferimento all'autenticazione forte dell'operazione contestata si rileva che trattasi di bonifico istantaneo e che l'intermediario a supporto di tale ricostruzione produce Log antifrode corredato di legenda e log autorizzativo corredato da legenda esplicativa.

Sulla base delle evidenze prodotte e sopra riportate, risulta quindi che l'operazione oggi contestata sia stata effettuata tramite inserimento del PIN (elemento di conoscenza) sull'app installata sul device riconosciuto del ricorrente (elemento di possesso).

Si richiama anche quanto affermato dal ricorrente in sede di repliche: "Seguendo le indicazioni ricevute durante tale conversazione, il ricorrente disponeva un'operazione di bonifico che si è successivamente rivelata fraudolenta". I Collegi Abf, hanno precisato che eventuali dichiarazioni confessorie del cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c.. I Collegi Abf, nei casi in cui dalla tracciatura informatica non risulti in modo esplicito uno dei fattori di autenticazione inseriti (conoscenza, possesso o inerenza), si sono interrogati sulla valenza da attribuire alle informazioni presenti nei log prodotti dagli intermediari per provare l'autenticazione forte del cliente nelle operazioni di pagamento sconosciute (artt. 10, comma 1 e 10-bis del D.lgs. 11/2010).

Tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte, i Collegi hanno concordato che, per valutare l'assolvimento dell'onere della prova della SCA, 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*. Si segnala che a fronte di evidenze documentali analoghe prodotte dallo stesso intermediario in controversie della specie, l'ABF ha ritenuto provata l'autenticazione delle operazioni contestate e compliant con la SCA il sistema di pagamento adottato dal PSP decisioni: Collegio di Torino, decisione n. 4753/2025 , Collegio di Torino, decisione n. 3898/2023, che richiama, in termini, Collegio di Bologna, decisione n. 13422/2022.

Con riferimento alla sussistenza degli indici di colpa grave in capo all'utilizzatore il ricorrente sostiene di aver ricevuto un SMS fraudolento ma non produce evidenza dello stesso .Il ricorrente afferma di avere ricevuto un sms apparentemente proveniente dall'intermediario e pertanto riconducibile alla tipologia dello spoofing; tuttavia, non ne produce evidenza. Al riguardo si rappresenta che secondo le posizioni dei Collegi, nel caso di spoofing, la mancata allegazione, da parte del cliente, del messaggio civetta, determina il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e pertanto possibile un legittimo affidamento dell'utente circa la genuinità del messaggio.

Il Collegio per quanto sopra pertanto ritiene non meritevole di accoglimento la domanda proposta dal ricorrente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE