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 PAOLO DI STEFANO

Seduta del 23/01/2026

FATTO

Il ricorrente il 4 agosto 2025 veniva contattato telefonicamente da un soggetto che, simulando l'identità di un operatore della Polizia Postale (attraverso un numero apparentemente riconducibile alla Questura di M***), allo scopo di prevenire una frode, lo invitava a trasferire la somma di € 1.589,00 dal proprio conto F** ad altro conto del ricorrente. L'operazione veniva indotta anche tramite l'invio di SMS appartenente riconducibili alla banca, volti a confermare l'attendibilità del sedicente agente. Solo successivamente constatava che, dal conto di destinazione, era stato disposto un ulteriore bonifico in uscita di pari importo a favore di un terzo ignoto. Accertata la frode, il ricorrente provvedeva a sporgere denuncia e a disconoscere formalmente l'operazione bancaria. Ritenuta la responsabilità della banca rispetto ai fatti contestati, il ricorrente, con ricorso depositato il 14.10.2025, chiede che gli venga corrisposta la somma di € 1.589,00.
L'intermediario contesta il ricorso rilevando che l'operazione è stata regolarmente contabilizzata ed eseguita nel rispetto del quadro normativo e contrattuale. Il sistema di autenticazione a più fattori utilizzato per l'esecuzione dell'operazione è risultato conforme ai requisiti di Strong Customer Authentication (SCA) e senza anomalie. Assume che l'operazione sia stata disposta ed autorizzata direttamente dal ricorrente (come dallo stesso ammesso in sede di denuncia) e, trattandosi di un'operazione volontariamente autorizzata, sebbene frutto di un raggiro, ritiene inapplicabile la disciplina della PSD2 in materia di operazioni non autorizzate. Precisa di avere tentato

tempestivamente il recupero delle somme, non andato a buon fine a causa dell'irrevocabilità dell'ordine di pagamento. Imputa, quindi, alla colpa grave del ricorrente la causa e le conseguenze della frode.
Con repliche del 2.12.2025 il ricorrente contesta il diniego di rimborso opposto dall'intermediario, ritenendolo generico e ribadendo l'applicabilità della tutela prevista dalla PSD2 in quanto operazione non autorizzata. Nello specifico, l'istante deduce che il raggiro è stato realizzato tramite tecniche avanzate (caller ID spoofing e SMS spoofing), che hanno permesso ai malfattori di simulare i canali ufficiali della banca e della Polizia Postale. Tale manipolazione ha ingenerato nel cliente il legittimo affidamento sull'attendibilità delle comunicazioni ed ha comunque reso la frode non riconoscibile tramite l'ordinaria diligenza. Parte ricorrente nega di aver comunicato PIN, password o codici OTP e di aver eseguito operazioni "sotto dettatura", avendo piuttosto assunto una posizione meramente passiva rispetto all'intrusione informatica, che non può essergli imputata. Evidenzia che l'attività truffaldina deve rientrare nel rischio d'impresa dell'intermediario, al quale contesta la mancanza di sistemi di alert tempestivi e l'inadeguatezza delle misure di sicurezza adottate.
In sede controrepliche, parte resistente ribadisce quanto eccepito in sede di controdeduzioni, confermando che l'operazione contestata è stata personalmente autorizzata dal ricorrente, che è stata inviata una notifica *push* di *alert*, riepilogativa dell'ammontare della disposizione, che non esiste un obbligo generale di monitoraggio e di sospensione dei pagamenti in caso di anomalia degli stessi, che la colpa grave del ricorrente ha determinato la frode.

DIRITTO

La controversia rientra nell'ambito della disciplina dettata dal 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, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta. In particolare, 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).
Il ricorrente disconosce il bonifico di importo pari ad euro 1.589,00 effettuato in data 04/08/2025 alle ore 18:41.
Dai log in atti emerge che l'operazione sia stata compiuta alle ore 16.41, orario riferibile al diverso fuso orario, considerato che l'alert dell'operazione riporta le ore 18.41.
Le operazioni di pagamento sono state precedute da uno spostamento di fondi.
In particolare, parte ricorrente riferisce che, in seguito ad una telefonata, apparentemente proveniente dalla Questura di M***, egli abbia disposto, su indicazione del malfattore, un bonifico istantaneo, pari all'intero ammontare disponibile sul conto F** (intestato al ricorrente) di euro 1.589,00 verso il conto R** (altresì a lui intestato).
Tale operazione di provvista è stata personalmente autorizzata dal ricorrente, come da lui stesso riferito sia in sede di reclamo sia di denuncia sia di ricorso.
Il bonifico effettuato fraudolentemente verso un soggetto terzo, sconosciuto al ricorrente, non sembra che sia stato disposto ed autorizzato dal ricorrente.
Occorre quindi verificare se tale ultima operazione di bonifico sia stata autenticata nel rispetto della normativa sopra citata, attraverso l'analisi dei documenti prodotti dall'intermediario.
Dalle videate informatiche in atti si ricava che: l'accesso all'app del ricorrente è avvenuto alle ore 16:41:34 tramite riconoscimento biometrico (impronta digitale); il bonifico è stato disposto alle ore

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

16:41:45, autorizzato tramite riconoscimento biometrico (impronta digitale) e tramite l'invio sul dispositivo del ricorrente di un token di verifica dell'operazione. L'inserimento di entrambi i fattori ha dato esito positivo e, in conseguenza di ciò, l'operazione è stata correttamente effettuata.
Il sistema di autorizzazione ha così previsto l'utilizzo del doppio fattore di autenticazione: quello di inerenza (dato dal fattore biometrico, i.e. l'impronta digitale) e di possesso (dato dall'invio al dispositivo del ricorrente di un token di verifica dell'operazione).
In particolare, con riferimento al dispositivo utilizzato, risulta che il device registrato e abitualmente utilizzato dal ricorrente sia unico; inoltre, con riferimento ai momenti in cui si è consumata la frode, le risultanze informatiche non attestano alcun malfunzionamento. Ciò si desume dall'analisi dei log allegati, indicati nella "colonna M", dai quali emerge come il dispositivo su cui si è operato durante la truffa sia sempre lo stesso e, in particolare, sia quello in uso al ricorrente, identificato con un codice univoco "****bba".
Il metodo di accesso all'app è registrato in modalità "*fingerprint".* L'autorizzazione del bonifico è caratterizzata, anch'essa dall'impronta digitale (*fingerprint*) e dall'inserimento del token (cfr. log, allegati dal resistente, dotati di legenda esplicativa).
L'intermediario ha quindi dato prova della procedura di autenticazione conforme alla c.d. SCA (strong customer authentication).
Occorre pertanto esaminare, anche al fine di valutare la sussistenza di indici di colpa grave di parte ricorrente le modalità della truffa che, invero, trovano riscontro nella denuncia, oltre che nei fatti esposti in ricorso, dai quali si desume che l'attacco informatico è assimilabile alla tecnica del c.d. spoofing che ha consentito di simulare i numeri di telefono della banca in relazione sia alla chiamata sia all'sms.
Tuttavia, avuto riguardo alla telefonata che il ricorrente ha riferito di avere ricevuto dallo stesso numero della banca (Caller ID Spoofing), non vi sono elementi che consentano di ritenere provata la circostanza, dal momento che non vi è in atti copia del registro delle chiamate che il ricorrente avrebbe ricevuto in occasione dell'evento in questione.
Quanto agli sms spoofing, dei quali è stata fornita evidenza, è vero che sono inseriti nel canale di comunicazione della banca, ma è altrettanto vero che gli errori grammaticali contenuti all'interno dei messaggi avrebbero dovuto indurre il ricorrente ad allarmarsi circa la loro attendibilità.
L'intermediario ha anche provato di avere inviato una notifica *push* di *alert* al ricorrente, riepilogativa dell'operazione effettuata.
Infine, non si rilevano indici di anomalia ex D.M. 112/2007, considerato peraltro che il ricorrente non ha depositato documentazione a sostegno della presunta difformità dell'operazione rispetto al normale utilizzo del conto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE