

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 01/09/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 08/11/2025, a seguito di un tentativo di frode sull'App di un intermediario terzo, una chiamata riconducibile al numero ufficiale del servizio clienti di tale istituto, nel corso della quale l'operatore veniva a conoscenza dell'ulteriore conto corrente aperto presso l'odierno resistente e gli comunicava che sarebbe stato ricontattato da un operatore di quest'ultimo.

Faceva presente che, effettivamente, avesse ricevuto poco dopo una chiamata riconducibile al servizio clienti dell'intermediario convenuto; sottolineava che, ottenuto l'accesso all'*home banking* senza aver ceduto codici o OTP, l'operatore fosse riuscito ad effettuare un bonifico ordinario da € 4.950,00.

Soggiungeva che, successivamente, fosse stato contattato da un numero attribuibile alla stazione dei Carabinieri di Trieste, nel corso della quale un apparente Maresciallo lo invitava ad autorizzare delle operazioni precedentemente negate (diverse da quelle in contestazione), sostenendo che fosse necessario per recuperare le somme sottratte. A quel punto, dopo aver contattato il Numero Unico di Emergenza 112, si avvedeva di essere stato vittima di una truffa.

Affermava di aver sporto denuncia presso le Autorità e di aver disconoscere le operazioni.

Chiedeva, pertanto, il rimborso dell'importo complessivo fraudolentemente sottratto.

Si costituiva l'odierno resistente il quale rilevava che il ricorrente avesse confessato esplicitamente di aver fornito le credenziali per l'accesso all'*home banking*; riteneva, dunque, non ravvisabile alcun profilo di responsabilità in capo all'intermediario.

Evidenziava comunque che le operazioni fossero state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali e che non fossero stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.

Considerava, di contro, sussistente la colpa grave del cliente – caduto vittima di una truffa ascrivibile al filone dei casi di frode *vishing* – in quanto questi aveva dato seguito alla telefonata e non aveva controllato la sezione apposita a disposizione nell'App che permette di verificare il contatto con l'intermediario tramite un canale sicuro.

Sosteneva che esiste una tecnica con la quale è possibile far visualizzare al destinatario della telefonata nome e numero diversi rispetto a quelli del mittente che fuoriesce dall'ambito di competenza della banca la quale, tuttavia, mette a disposizione dei clienti innumerevoli informative al riguardo.

Rappresentava, peraltro, che l'operazione di bonifico fosse stata eseguita verso un conto corrente aperto presso lo stesso intermediario e, come previsto dalle disposizioni contrattuali, i bonifici tra conti correnti dell'intermediario vengono eseguiti immediatamente e non sono revocabili; affermava di aver comunque tentato di bloccare il conto corrente del beneficiario, operazione che non era andata a buon fine in quanto le somme erano state già trasferite.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale ribadiva di non aver fornito alcun codice, OTP o dato personale ai truffatori e che la banca non avesse assolto l'onere probatorio relativo al dolo o colpa grave dell'utilizzatore, contravvenendo all'obbligo derivante dall'art. 10 del D. lgs. 11/2010 di rimborsare il cliente.

Precisava di essere stato vittima di *spoofing* e non di *vishing*, una tipologia di frode più insidiosa, con la conseguenza che – essendo assente il suo consenso consapevole – l'operazione dovesse qualificarsi come non autorizzata permettendo la piena applicabilità della disciplina PSD2.

Riteneva giustificabile il proprio affidamento a causa dell'ufficialità dei canali di comunicazione con i presunti intermediari nonché con i Carabinieri, mentre considerava insussistente la colpa grave, anche perché non aveva ricevuto alcun messaggio di *alert* per essere preparato a ciò che stava avvenendo. Affermava che in capo all'intermediario fosse imputabile la responsabilità aggravata ex art. 2050 cod. civ.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale reiterava le osservazioni relative alla prova fornita in ordine all'operazione contestata e alla conformità della procedura di autenticazione alla normativa sui servizi di pagamento.

Di contro, ribadiva che lo stesso ricorrente avesse confessato nella denuncia di aver fornito i codici dispositivi, incorrendo in colpa grave; precisava che la tecnica di *spoofing* non è imputabile all'intermediario che infatti ha messo a disposizione un canale apposito e sicuro sull'App.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione di pagamento, successivamente disconosciuta.

La materia, come noto, è regolata dal D. lgs. n. 11/2010 come modificato dal D. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/UE (c.d. PSD2- Payment Services Directive 2).

Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. *Strong Customer Authentication* SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.

Con riferimento alla c.d. SCA gli artt. 97 e 98 della direttiva PSD2, nonché l'articolo 10 bis del C. lgs. n. 11/2010, oltre che le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato UE 2018/389 della Commissione Europea e i criteri interpretativi adottati dalla stessa Autorità (cfr. in particolare il parere dell'EBA del 21 giugno 2019), hanno stabilito che essa 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. In relazione a tutte le predette fasi, la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori, che devono essere reciprocamente indipendenti e appartenere a categorie diverse: conoscenza; inerenza; possesso.

Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa de qua prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Risulta documentalmente che l'operazione in parola consiste in un bonifico eseguito in data 08/11/2025, per un importo di € 4.950,00.

Le tracciate informatiche versate in atti evidenziano che l'accesso all'*home banking* è stato eseguito mediante l'inserimento di username e password (elemento di conoscenza) e la digitazione del codice OTP (elemento di possesso).

Con riferimento alla fase di autenticazione, invece, dall'analisi dei log prodotti risulta che l'operazione sia stata resa possibile dalla contemporanea presenza dell'elemento di possesso, dato dall'inserimento username, della password e dell'OTP, nonché dell'elemento di conoscenza, dato dalla digitazione di due cifre del PIN.

Attesa la conformità a SCA delle operazioni contestate, non resta che verificare se – dalla condotta tenuta dal ricorrente – siano evidenziabili profili di colpa grave, rispetto alla quale la prova di

autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico (cfr. Coll. coord., dec. n. 22745/2019).

A tale proposito, il cliente ha prodotto copia del registro delle chiamate ricevute, di cui ha dato conto sia nella denuncia che nel ricorso; sulla base delle evidenze prodotte risulta effettivamente che la prima chiamata è riconducibile al numero verde dell'intermediario terzo, la seconda è riconducibile all'odierno resistente mentre la terza è riferibile all'Arma dei Carabinieri di Trieste.

Ciò nonostante, la documentazione versata in atti evidenzia che il ricorrente abbia pure ricevuto un SMS *alert* che lo avvertiva dell'importo elevato: dall'insieme di tali risultanze è possibile dedurre che il cliente è stata vittima di una truffa insidiosa, che ben può essere ricondotta alla categoria dello *spoofing* misto a *ID caller spoofing*. Tale tipo di truffa è considerato come potenzialmente più decettivo rispetto al comune *phishing* o *vishing*, che si ritiene possa essere contrastato con l'uso di una diligenza minima, in considerazione della sua diffusione e della sua generalmente scarsa idoneità a trarre in inganno i clienti. Non basta, tuttavia, il ricorrere di una tecnica più sofisticata (che permette di utilizzare numerazioni riconducibili alle utenze ufficiali dell'intermediario) per escludere profili di colpa grave del cliente.

Nel caso di specie, in particolare, il comportamento del ricorrente appare connotato da colpa grave che assume rilievo assorbente, nonostante il legittimo affidamento ingenerato dalla riconducibilità dei numeri all'odierno ricorrente; il contenuto del messaggio, infatti, era tale da mettere sull'avviso il cliente che stava autorizzando un'operazione di pagamento, nella specie un bonifico di elevato importo. Da quanto ammesso in sede di denuncia e nel ricorso, non essendo stato richiesto alcun pagamento, nemmeno da parte dei frodatori, il contenuto del messaggio avrebbe quindi consentito al ricorrente di avvedersi in modo tempestivo che i truffatori (in possesso delle credenziali da lui fornite) stessero eseguendo un'operazione di pagamento da lui non autorizzata; seguendo le istruzioni ivi indicate, quindi, avrebbe potuto bloccarla tempestivamente.

La mancata tempestiva attivazione del cliente, nonostante la chiara informazione ricevuta dall'SMS *alert*, assume dunque rilievo assorbente e determina il rigetto del ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE