Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

## COLLEGIO DI MILANO

composto dai signori:

| | |
|---|---|
| (MI) TINA | Presidente |
| (MI) MODICA | Membro designato dalla Banca d'Italia |
| (MI) BARTOLOMUCCI | Membro designato dalla Banca d'Italia |
| (MI) PERON | Membro di designazione rappresentativa degli intermediari |
| (MI) AFFERNI | Membro di designazione rappresentativa dei clienti |

Relatore (MI) BARTOLOMUCCI

Seduta del 06/05/2026

## FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo (secondo quanto dichiarato nella denuncia alle autorità) di aver ricevuto, in data 05.12.2025, una chiamata da un'utenza sconosciuta, da parte di un interlocutore che si presentava come un operatore dell'intermediario e gli chiedeva informazioni riguardo ad un passaggio di utenza da un dispositivo informatico ad un altro.
Faceva pure presente di essere stato successivamente contattato da un altro operatore, che si presentava come operatore dell'ufficio tecnico che confermava il problema in merito all'utenza, il quale – per rassicurarlo della bontà della chiamata – gli forniva i suoi dati personali e, in seguito, lo faceva accedere ad un sito identico a quello dell'intermediario, salvo poi guidarlo per scaricare un'applicazione e, una volta al suo interno, chiedergli una serie di firme digitali finalizzate a risolvere il problema dell'utenza.
Rappresentava di essersi avveduto, solo a quel punto, di essere stato vittima di una truffa, in quanto il suo telefono era in blocco e si accorgeva che fosse stato effettuato un giroconto di € 7.490,00 sul suo conto presso l'intermediario, che veniva subito impiegata per effettuare 6 transazioni e 1 bonifico istantaneo, in favore di conti esteri, per un totale di € 7.485,10;
Sosteneva di aver tentato il richiamo del bonifico, ma senza successo di aver sporto denuncia presso le Autorità; soggiungeva che, in seguito alla presentazione del reclamo, avesse ottenuto il rimborso di € 0,10.
Chiedeva, pertanto, il rimborso dell'importo complessivo di € 7.485,00.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Si costituiva l'odierno resistente il quale rilevava che le operazioni fossero state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali, mentre il ricorrente non avrebbe allegato alcuna evidenza documentale in merito alle chiamate ricevute né in merito all'utenza telefonica da cui le stesse sarebbero pervenute.

Riteneva sussistente la colpa grave del cliente in quanto avrebbe fatto accesso volontariamente al sito civetta e avrebbe seguito pedissequamente tutte le indicazioni del frodatore; sottolineava, peraltro, che non fosse stata fornita alcuna specifica descrizione della dinamica fraudolenta.

Osservava che, in virtù delle richieste avanzate dai frodatori, le quali erano a tal punto ambigue e controverse, il cliente stesso, utilizzando un minimo di diligenza, non avrebbe dovuto assecondarle e avrebbe dovuto provvedere immediatamente al blocco dello strumento di pagamento e a contattare la banca attraverso i canali di comunicazione ufficiali; di contro, sembrerebbe che durante la conversazione con i frodatori, questi abbia verosimilmente consentito all'acquisizione delle proprie credenziali di sicurezza personalizzate, attraverso il loro volontario inserimento in un ambiente informatico non ufficiale (ossia l'APP).

Con riferimento al giroconto, precisava che gli intermediari non richiedono mai operazioni dispositive per finalità di sicurezza; riteneva, pertanto, che il cliente non avesse adottato alcuna misura volta a mettere in sicurezza il proprio conto, pur avendone la possibilità.

Affermava che non si sarebbe verificato alcun data breach, atteso che gli unici dati del cliente in possesso dei truffatori erano il numero di utenza telefonica e il suo nominativo, informazioni che, di per sé, non sono idonee a compromettere la sicurezza dello strumento di pagamento né a determinare un accesso non autorizzato al conto e che potrebbero essere state acquisite attraverso molteplici canali (es. social network).

Quanto al tentativo di recall del bonifico, poi non andato a buon fine, sottolineava di essersi immediatamente attivato anche senza esplicita richiesta del cliente, il quale aveva chiesto solo un chargeback tramite APP.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale sosteneva che la regolarità formale della SCA non equivale automaticamente ad autorizzazione sostanziale quando l'operazione, come in questo caso, è frutto di inganno idoneo a viziare la volontà del pagatore.

Sosteneva che, alla luce del rimborso dell'operazione di € 0,10 avendone riconosciuto la natura fraudolenta, fosse illogico negare il rimborso per le transazioni successive; soggiungeva, invece, che – di fronte ad un'operatività a tal punto anomala – l'intermediario avrebbe dovuto attivare una misura di blocco cautelativo, anche in virtù del fatto che la giacenza media del conto negli ultimi anni era oscillata tra i € 30,00 e gli € 80,00.

Affermava che i truffatori avessero utilizzato una tecnica di raggiro avanzata e lo avessero indotto a fidarsi di loro in virtù delle conoscenze a priori dei propri dati sensibili; riteneva, dunque, di non aver posto in essere un comportamento gravemente imprudente, anche perché avrebbe agito tempestivamente per bloccare i propri conti correnti, disconoscere le operazioni e sporgere denuncia alle autorità.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Reputava che vi fossero state delle compromissioni esterne, in quanto si sarebbe reso necessario un recupero password in seguito ad un reset delle impostazioni da parte del truffatore; precisava che la mancata allegazione delle chiamate fosse dovuta al reset totale del dispositivo sopra menzionato.

Quanto all'utilizzo del link sul web e non sul canale APP ufficiale dell'intermediario, specificava che il truffatore lo avesse convinto che la procedura potesse avvenire esclusivamente tramite interfaccia web; evidenziava pure che (siccome il link terminava con il suo numero di cellulare) tale estrema personalizzazione lo ha indotto a credere alla bontà dell'operazione.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale specificava che la movimentazione di € 0,10 non costituisse in alcun modo un rimborso, ma si trattasse di una pre-autorizzazione effettuata dall'esercente e in data 05.12.2025, successivamente rilasciata in data 12.12.2025, secondo le ordinarie dinamiche operative dei circuiti di pagamento.

Considerava l'operazione di € 7.490,00 non già come un'anomalia imputabile a soggetti terzi o un ingresso di fondi di provenienza ignota, ma un'operazione volontariamente disposta dal cliente medesimo mediante bonifico proveniente da un proprio ulteriore conto corrente personale.

Nel ribadire che le informazioni personali conosciute dai truffatori sono facilmente reperibili e, in ogni caso, non implicano alcuna compromissione dei sistemi della banca né giustificano l'installazione di applicazione di terze parti su indicazione telefonica di soggetti non verificati, rappresentava che le e-mail sul recupero password non costituiscono prova tecnica di un reset totale eseguita da terzi né di una presa di controllo da remoto del dispositivo da parte dei truffatori.

Da ultimo, rilevava che il fatto che il cliente fosse stato indotto a credere che l'utilizzo del link potesse avvenire solo via web non escludesse affatto la sua colpa grave.

## DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di alcune operazioni di pagamento, successivamente disconosciute.

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 PDS2, nonché l'articolo 10-bis del d. 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 le operazioni in parola consistano in un bonifico istantaneo ed in cinque pagamenti online effettuati il 05.12.2025, per l'importo di € 7.485,00 (con esclusione di quella dell'imporo di € 0,10, che l'intermediario non ritiene essere un'operazione vera e propria e che comunque è stata riaccreditata al cliente che non ne chiede il rimborso).

Parte resistente afferma che le transazioni siano state eseguite all'interno di 2 log-in effettuati dal cliente rispettivamente alle ore 16:18 e 16:23 mediante l'inserimento delle credenziali biometriche e l'utilizzo dell'APP installata sul suo dispositivo mobile personale, associato in via esclusiva al suo conto.

Le tracciature informatiche versate in atti evidenziano che effettivamente i log-in siano stati eseguiti tramite l'inserimento delle credenziali biometriche del cliente (fattore di inerenza), con l'app installata sul dispositivo mobile associato in via esclusiva al conto intestato al ricorrente (fattore di possesso).

Con riferimento alla fase di autenticazione, invece, risulta che – per quanto riguarda il bonifico istantaneo – detta operazione sia stata eseguita attraverso l'uso dell'app sulla quale è stata convalidata la notifica push che riepilogava gli estremi del pagamento (fattore di possesso) ed il corretto inserimento del codice PIN (fattore di conoscenza).

Il ricorrente contesta che detta operazione rientri nel c.d. money muling, nota pratica illegale per la quale tuttavia (indipendentemente dalle modalità con le quali il cliente ignaro presta inconsapevolmente la propria collaborazione per effettuare il trasferimento di denaro ottenuto illecitamente dai malfattori) è pur sempre necessario che le somme siano trasferite da un conto terzo e non, come nel caso di specie, da un altro conto intestato allo stesso cliente; in tal caso, infatti, si tratta di una mera operazione di costituzione della provvista effettuata volontariamente ed autonomamente dal cliente, seppure in conseguenza della frode di cui è caduto vittima.

Per quanto riguarda le altre cinque operazioni di pagamento on line, invece, la documentazione prodotta evidenzia la convalida della notifica push pervenuta sull'app, quale elemento di possesso, ma non rileva in maniera univoca l'inserimento dell'ID biometrico del cliente (fattore di inerenza), che

tuttavia lo stesso cliente ammette di aver inserito, dovendosi quindi ritenere che esse siano state correttamente autenticate.

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 riferisce di aver ricevuto due chiamate da numeri sconosciuti in cui veniva informato, da dei sedicenti operatori dell'intermediario, che fosse stato eseguito un passaggio di utenza da un vecchio dispositivo a quello attualmente in uso. Di tali circostanze, tuttavia, non fornisce alcuna prova documentale.

Secondo il consolidato indirizzo di questo Collegio, la mancata allegazione, da parte del cliente, del registro delle chiamate non consente di verificare se il numero da cui la telefonata truffaldina sarebbe partita possa essere riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la sua genuinità.

Giova pure rilevare che il ricorrente afferma di non aver potuto produrre il registro chiamate in quanto il frodatore avrebbe causato un reset totale del suo telefono e di aver anche dovuto effettuare il ripristino delle proprie credenziali; allega le e-mail delle società informatiche in merito.

Tale circostanza, tuttavia, non appare assumere rilievo ai fini dell'assolvimento dell'onere della prova incombente sul ricorrente e ciò indipendentemente dalla circostanza che essa sia o meno idonea a dimostrare l'avvenuto reset; gli è, infatti, che – pur volendo ammettere che tale operatività sia stata effettivamente eseguita, ciò non consente di considerare provato che il reset sia avvenuto in relazione alla frode subita.

Ciò nonostante, il Collegio non può mancare di rilevare che emergono alcune specifiche circostanze di fatto che assumono rilievo quali indici di una frode (ai sensi delle disposizioni di cui al D. M. n. 112/2007) che avrebbe potuto essere rilevata da parte dell'intermediario; infatti, secondo la posizione più recente condivisa dai Collegi territoriali di questo Arbitro, i principi del suddetto D. M. n. 112/2017 – pur non avendo un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate, ma sono espressione di un generale obbligo di monitoraggio delle operazioni, da valorizzare per valutare la condotta dell'intermediario – possono comunque rappresentare elementi utili per valutare la condotta dell'intermediario, in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario), ove vi sia un'evidenza delle stesse.

In particolare, l'art. 8 del menzionato D.M. prevede che si configura il rischio di frode nel caso di "tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita" e di "sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento".

Nel caso di specie, risulta che le cinque operazioni di pagamento on line siano state effettuate presso il medesimo punto vendita, ossia un noto sito truffaldino di criptovalute. Risultano, pertanto, integrati

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

gli indici di frode previsti dalla normativa ministeriale, con conseguente riconoscimento del diritto della ricorrente ad ottenere la ripetizione del controvalore delle ultime tre operazioni.

**PER QUESTI MOTIVI**

**Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.994,00.**
**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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.**

IL PRESIDENTE