Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	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 02/12/2025

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 04/06/2025, una chiamata da un interlocutore che si presentava come un operatore dell'intermediario, sostenendo che risultasse un pagamento sospetto da Bolzano effettuato con un telefono.
Faceva presente che, non essendo proprietario di alcun telefono del modello indicato, si fosse convinto della veridicità della chiamata e fosse stato indotto a collaborare per "bloccare la frode", inducendolo a comunicare i codici OTP; precisava, tuttavia, di non essersi collegato personalmente all'home banking, né di aver autorizzato consapevolmente alcuna operazione.
Sottolineava che, a seguito della sua tempestiva segnalazione alla banca, avesse recuperato l'importo di € 1.420,00, mentre la somma di € 1.100,00, spesa con la carta di credito, inizialmente riaccreditata sul conto corrente, veniva successivamente stornata.
Così ricostruita la vicenda, rappresentava di non aver autorizzato consapevolmente queste operazioni, disposte da terzi con modalità fraudolente mediante un inganno sofisticato, con tono ufficiale e pressante, simulando una collaborazione con la banca.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Affermava che la percezione del contesto truffaldino lo avesse indotto a fornire i codici, nella convinzione errata di difendersi da una frode, senza che ciò possa essere qualificato come colpa grave; osservava, peraltro, di essere stato diligente nell'aver segnalato tempestivamente la frode.
Soggiungeva, invece, che l'intermediario avesse omesso di realizzare controlli adeguati, in quanto le operazioni risultavano eseguite da dispositivo non abituale, e che non lo avesse mai informato in modo chiaro sulle comunicazioni via messaggio ricevute in app, che in ogni caso non sostituiscono l'obbligo di SCA né esonerano la banca dall'obbligo di prevenire o bloccare frodi sofisticate.
Rilevava pure che – seppure l'intermediario limita l'importo massimo giornaliero per i bonifici istantanei ad € 1.000,00 – l'operazione disconosciuta ammontasse ad € 4.900,00.
Chiedeva, pertanto, la ripetizione delle somme fraudolentemente sottratte, oltre alla rettifica del saldo negativo per € 1.034,89 e al blocco dell'addebito di ulteriori oneri e spese, nonché di fornire dettagli su IP e modalità di accesso al sistema operativo. Domandava, inoltre, di accertare l'esistenza di sistemi di adeguata verifica dell'identità del beneficiario dei pagamenti, oltre che di blocco tempestivo delle operazioni fraudolente successivamente alla segnalazione del cliente.
Costituitosi ritualmente, l'intermediario evidenziava che in data 04/06/2024 fossero stati eseguiti un bonifico e la stipula di contratto di carta di credito dall'area riservata del cliente, nonché alcuni pagamenti online sia con la carta di debito che con la carta di credito intestate al ricorrente.
Osservava che tali operazioni fossero state correttamente autorizzate, mediante l'utilizzo delle credenziali statiche e dinamiche in possesso del cliente, registrate e contabilizzate; riteneva, pertanto, sussistente la colpa grave del ricorrente, che aveva ammesso di aver fornito, su indicazione del sedicente operatore, i codici OTP ricevuti tramite SMS, in seguito ad una telefonata che aveva affermato di aver ricevuto senza fornirne alcuna prova.
Sottolineava, di contro, la correttezza e diligenza del proprio operato, dopo essere venuto a conoscenza dell'accaduto, essendosi immediatamente attivato per bloccare il conto corrente del beneficiario e tentare il recupero delle somme (riuscito solamente per la somma di € 1.420,00).
Considerava la truffa subita non particolarmente sofisticata, in quanto non si sarebbe potuta concretizzare senza il negligente e colpevole apporto del ricorrente stesso.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale rappresentava di essere una persona anziana, con difficoltà visive e uditive: circostanze che avevano di certo agevolato il compiersi della truffa.
Riteneva che si fossero verificate numerose anomalie nel caso di specie come accessi da IP, reti e dispositivi sconosciuti, con nessuna notifica inviata nei canali sicuri dell'app né blocco dell'attività sospetta; una carta di credito creata, firmata e usata in pochi minuti e l'associazione di un wallet di pagamento sul dispositivo del truffatore.
Ribadiva di aver fornito i codici OTP esclusivamente perché convinto di bloccare una frode e che la funzionalità di avviso dell'intermediario in messaggistica, per confermare la genuinità della chiamata in ingresso, non fosse stata chiaramente illustrata e non fosse immediatamente percepibile come quella in uso presso altri intermediari.
Faceva presente che, in data 10/09/2025, avesse ricevuto una telefonata dall'Ufficio legale dell'intermediario per una proposta transattiva, effettuata da un numero di cellulare non ufficiale e senza alcuna notifica preventiva nella sezione 'I miei messaggi'; sottolineava, in ogni caso, che non vi fosse prova che le notifiche di avviso di contatto fossero state effettivamente inviate al cliente o che questi avesse avuto la possibilità di prenderne visione prima o durante la frode.
Considerava, pertanto, la truffa subita come una frode sofisticata, non avendo neppure ricevuto SMS alert.
In sede di repliche il ricorrente chiedeva di accertare la responsabilità dell'intermediario, con conseguente riconoscimento del rimborso dell'importo complessivo di € 5.580,00 oltre interessi e

rivalutazione monetaria; reiterava poi la richiesta di effettuare verifiche sul conto del beneficiario dei pagamenti.
Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale reiterava le proprie considerazioni, osservando che il ricorrente avesse ammesso più volte di aver comunicato i codici OTP e che non fosse mai stato alcun malfunzionamento o compromissione dei sistemi di sicurezza dell'intermediario né alcun apporto causale alla truffa da parte della stessa.
Precisava di non poter essere a conoscenza di come i truffatori avessero ottenuto i dati e le informazioni personali e bancarie del ricorrente (con collaborazione volontaria o involontaria, telefonicamente, durante o prima la truffa), rilevando si aver eseguito correttamente le disposizioni di bonifico contestato, nel rispetto delle tempistiche massime previste dalla normativa, secondo quanto previsto dall'art. 17 del D .Lgs. n. 11/2010.
Sottolineava che le comunicazioni di messaggistica in app fossero accessibili e che la richiesta della carta di credito fosse stata sottoscritta con Firma Elettronica Avanzata (FEA), rilasciata dalla Banca al proprio cliente ai sensi dell'art. 55, lett. a), del DPCM 22 febbraio 2013.
Da ultimo, osservava che la telefonata da cellulare ricevuta dal Cliente il 10 settembre 2025 fosse una chiamata di cortesia proveniente da un dipendente dell'Ufficio Legale dell'intermediario, al fine di provare a raggiungere un accordo con il ricorrente e, per questo motivo, non era stata preceduta da un avviso nella sezione "I miei messaggi".

DIRITTO

La domanda proposta dal ricorrente è relativa – previo accertamento della responsabilità dell'intermediario resistente – al riconoscimento del proprio diritto alla restituzione del controvalore di una serie di operazioni, successivamente disconosciute.
Pur in assenza di una specifica eccezione di parte, il Collegio rileva che le ulteriori domande spiegate dal ricorrente non possano essere ritenute ammissibili, sia con riguardo a quelle relative alla corresponsione degli interessi e della rivalutazione monetaria, sia a quelle relative all'accertamento sui sistemi di adeguata verifica circa l'identità del beneficiario dei pagamenti stessi. Vale per tutte la circostanza che esse non siano state formulate nel preventivo reclamo; con riguardo alle prime, inoltre, va pure rilevato che esse sono state formulate tardivamente in sede di repliche, in violazione di quanto stabilito dalle Disposizioni della Banca d'Italia che regolano il presente procedimento, le quali per un verso richiedono che vi sia corrispondenza tra reclamo e ricorso e, per altro verso, escludono un ampliamento della domanda in sede di repliche.
Passando al merito del ricorso deve rammentarsi che 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 contestate consistono in un bonifico ed in tre pagamenti *online* mediante carta, effettuati in data 04/06/2025, per il complessivo importo di € 7.000,00; il ricorrente, tuttavia, chiede la restituzione di € 5.580,00, in ragione dell'avvenuto recupero della somma di € 1.420,00 da parte della banca.

Dai log informatici versati in atti emerge che sia stato effettuato un accesso all'area riservata dall'applicazione presente sul dispositivo del cliente, autorizzato in modalità conforme a SCA mediante inserimento di username e password (elemento di conoscenza) e digitazione del codice OTP ricevuto tramite SMS sul numero di cellulare del cliente (elemento di possesso).

In tale sessione si sono registrati la creazione del wallet, con la disposizione dei due pagamenti di € 500,00, ed il pagamento tramite bonifico.

Quanto alla creazione del wallet, l'intermediario ha affermato che questa sia stata preceduta dalla creazione di un CVV dinamico generato, in modalità conforme a SCA, tramite accesso all'area riservata con username, password e OTP (che costituirebbe il fattore di conoscenza o di inerenza), oltre che mediante una conferma mediante un ulteriore OTP inviata via SMS sul device del cliente (che costituirebbe il fattore di possesso).

A fronte di tale descrizione, i log informatici versati in atti mostrano che siano stati effettivamente inseriti l'username e la password personali, a cui ha fatto seguito la digitazione del codice OTP inviato tramite SMS al dispositivo autenticato del cliente. La generazione del CVV dinamico risulterebbe quindi avvenuta mediante l'inserimento delle credenziali (elemento di conoscenza) e il possesso del dispositivo mobile autenticato (elemento di possesso).

Tuttavia, alla luce delle evidenze in atti, se il codice OTP SMS rappresenta – ai fini dell'autenticazione delle operazioni disconosciute – il fattore di possesso, si pone il problema di individuare il secondo fattore di autenticazione. In particolare, è necessario stabilire la valenza attribuibile al codice CVV dinamico, che l'intermediario qualifica come elemento di "conoscenza".

Non può sottacersi, infatti, che – alla luce delle indicazioni fornite dall'EBA nell'Opinion del 21 giugno 2019 – il CVV dinamico debba essere definito come elemento di possesso; l'orientamento condiviso dei Collegi appare conforme a tali indicazioni, così come pure la decisione di questo Collegio in merito alla medesima fattispecie (cfr. dec. n. 4510/25).

Ne deriva, pertanto, che un doppio fattore di possesso non risulta conforme alla SCA in quanto, in base alla citata Opinion dell'EBA, l'autenticazione forte presuppone il ricorso a due fattori di autenticazione appartenenti a categorie diverse.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

La mancanza anche parziale della prova del rispetto dei presidi di sicurezza in tutte le fasi dell'operazione di pagamento, e quindi sin da quella di accesso al sistema, è risolutiva e dirimente tanto rispetto al processo di autenticazione delle singole operazioni di pagamento (tre delle quali sono state effettuate utilizzando un CVV dinamico) quanto alla valutazione di eventuali profili di colpa ascrivibili al cliente, costituendo, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente (cfr. Coll. coord., dec. n. 22745/2019).
Deve, pertanto essere riconosciuto il diritto del ricorrente ad ottenere il rimborso del controvalore delle operazioni contestate.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.580,00.
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