

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) NUZZO	Membro designato dalla Banca d'Italia
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) QUARTA	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - GABRIELE NUZZO

Seduta del 15/09/2025

FATTO

1. Con ricorso in data 9 maggio 2025, la Ricorrente, titolare del conto corrente n. ***226 intrattenuto presso l'Intermediario, riferisce che, in data 16 settembre 2024, riceveva un SMS recante un invito a contattare l'assistenza clienti chiamando un numero di telefono. Seguiva un secondo SMS, ricevuto a valle della cronologia di precedenti messaggi genuini inviati dall'Intermediario, contenente l'invito a seguire le indicazioni di un operatore per disporre il blocco di un bonifico non autorizzato.

In assenza di riscontro telefonico al numero del servizio clienti dell'Intermediario riportato nell'APP dell'*home banking*, rappresenta di aver contattato il numero indicato nell'SMS e che il presunto operatore era a conoscenza dei suoi dati personali e di quelli del conto corrente, compreso il saldo. In particolare, il sedicente operatore riferiva che erano stati impartiti due bonifici (uno di Euro 400,00 e uno di Euro 4.100,00) dei quali doveva essere eseguito il blocco. Al termine della conversazione telefonica, la Ricorrente riscontrava dal proprio *home banking* che era stato effettuato un bonifico di Euro 4.100,00 a favore di un beneficiario sconosciuto.

Fa presente che, il giorno seguente, recatasi presso una filiale dell'Intermediario per revocare il bonifico, riceveva rassicurazioni senza ricevere alcun rimborso.

Evidenzia che, se non avesse ricevuto l'SMS dall'Intermediario che la invitava a contattare il presunto operatore, non avrebbe mai telefonato al numero indicato nel messaggio.

Ritiene di avere diritto alla ripetizione delle somme e al risarcimento dei danni subiti, pari all'importo del bonifico non autorizzato, in ragione dell'inadempimento da parte dell'Intermediario ai propri obblighi di diligenza professionale previsti dalla disciplina di settore (d.lgs. 27 gennaio 2010, n. 11), dall'art. 2050 c.c. e dalla normativa sulla protezione dei dati personali.

Afferma la responsabilità dell'Intermediario e, in particolare, la violazione da parte di quest'ultimo degli obblighi di protezione che gli imporrebbero di rifiutare l'esecuzione di operazioni anomale e non rispondenti agli interessi del correntista.

Tanto premesso, afferma di non aver mai eseguito bonifici di importo rilevante e ritiene che l'operazione disconosciuta fosse per questo anomala rispetto alla normale operatività del conto. Rileva, inoltre, che l'Intermediario non avrebbe previsto un limite giornaliero e mensile di utilizzo, per evitare prelievi e pagamenti oltre la soglia stabilita.

Pertanto, chiede la condanna dell'Intermediario alla rifusione delle somme indebitamente sottratte, pari a Euro 4.100,00.

2. Costitutosi nel presente procedimento, l'Intermediario precisa, in primo luogo, che l'operazione contestata, essendo un bonifico istantaneo, non sarebbe revocabile, come comunicato con proposta di modifica unilaterale inviata alla Ricorrente a giugno 2022.

Ciò posto, rappresenta che al conto è collegato il servizio di "*home banking*", che consente al cliente di effettuare le operazioni informative e dispositive utilizzando il telefono o *internet*.

Osserva che, nella prima delle due denunce, intervenute a distanza di due mesi, la Ricorrente ha sostenuto di avere contattato immediatamente il numero indicato nell'SMS truffaldino; mentre nella seconda ha affermato di avere, in un primo momento, tentato invano di contattare il numero del servizio clienti dell'Intermediario. Inoltre, ritiene che la ricorrente abbia fornito una ricostruzione incompleta dell'accaduto, non avendo chiarito se ha eseguito un'operazione sotto dettatura del frodatore o ha scaricato un'applicazione terza che ha consentito al presunto operatore di inserire l'operazione.

In ordine alla prova dell'autenticazione forte, osserva che, per effettuare il *login* e le operazioni di *inquiry*, è previsto l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) e del codice OTP; per disporre le operazioni, dopo avere effettuato il *login*, è prevista la conferma con codice PIN e OTP. Specifica che il codice OTP viene generato in modo silente dal *mobile token* attivato sullo strumento/device utilizzato dal cliente e che il testo della notifica, sul quale l'utente deve fare "*tap*" per autorizzare, indica chiaramente l'operazione che si sta disponendo. Rileva inoltre che l'attivazione del *mobile token* è resa possibile solo attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente a mezzo *e-mail* e SMS al cellulare collegato all'*home banking* (indipendentemente dall'attivazione del servizio di SMS *alert*).

Afferma che tale sistema di autenticazione è riconosciuto come "forte" dall'orientamento diffuso dei Collegi ABF e che, dalle verifiche effettuate, non è emerso alcun malfunzionamento o compromissione dei sistemi. Al contrario, tutte le operazioni di *login* e di bonifico risultano correttamente autenticate, registrate e contabilizzate con le credenziali di sicurezza della Ricorrente.

Fa presente che la riconducibilità dell'operazione alla Ricorrente sarebbe confermata dal codice cliente utilizzato sia per il *login*, sia per autorizzare l'esecuzione del bonifico (tale codice è riportato in chiaro nei *log* versati in atti); per contro, la digitazione del codice PIN, risulta nel *log* dalle colonne attività, laddove viene indicato "pin inviato" e "pin verificato".

Fa inoltre presente di non aver rilevato indici di anomalia dell'operazione che, per causale e importo, non appariva difforme da altre precedentemente poste in essere dalla cliente.

Rileva, inoltre, che per i bonifici istantanei eseguibili tramite *APP*, è fissato un limite di Euro 15.000,00.

Infine, sottolinea di avere inviato alla ricorrente SMS e notifica *push* relativi all'operazione, nonché di avere tentato il richiamo delle somme oggetto di frode, con esito negativo.

Chiede, pertanto, il rigetto del ricorso.

3. In sede di repliche, la Ricorrente ribadisce di avere ricevuto una comunicazione proveniente dal canale ufficiale dell'Intermediario, contenente l'invito a seguire le istruzioni del presunto operatore; di non aver confuso il servizio indicato negli SMS con quello dell'Intermediario, sottolineando che le operazioni eseguite con il proprio strumento di pagamento sono gestite dalla società terza indicata nell'SMS; di avere tentato di contattare tempestivamente l'Intermediario; di non aver fornito alcun codice al presunto operatore contattato in seguito al mancato riscontro da parte dell'Intermediario.

Richiama la normativa di settore a sostegno della responsabilità dell'Intermediario e precisa che l'operazione disconosciuta ha riguardato tutte le somme presenti sul proprio conto corrente, anomalia che l'Intermediario avrebbe dovuto riconoscere.

4. In sede di controrepliche, l'Intermediario osserva che la ricorrente non si è allertata della provenienza degli SMS da due soggetti giuridici differenti, rilevando l'assenza di connessione della società terza con l'Intermediario.

Evidenzia, inoltre, che la Ricorrente non ha provato l'asserito mancato riscontro alle sue telefonate, che l'avrebbe indotta a contattare il numero riportato nel messaggio ricevuto.

DIRITTO

1. Il Collegio rileva preliminarmente che l'operazione contestata è stata eseguita sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 (entrato in vigore il 13 gennaio 2018), che ha recepito la direttiva (UE) n. 2015/2366, relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2).

Con riguardo a detta disciplina, il Collegio rammenta che, ai sensi dell'art. 10 d.lgs. n. 11/2010, «[q]ualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti».

Il secondo comma del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento eseguita, «l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7» (: obblighi di custodia e di corretta utilizzazione dello strumento di pagamento).

Sempre il secondo comma stabilisce che «è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente».

La disciplina relativa all'autenticazione e alle misure di sicurezza da adottare nel caso di operazioni elettroniche di pagamento a distanza è contenuta nell'art. 10-*bis* d.lgs. n. 11/2010, secondo il quale:

- (i) «i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente:
 - a) accede al suo conto di pagamento on-line;

- b) dispone un'operazione di pagamento elettronico;
- c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi» (1° comma);
- (ii) «[n]el caso dell'avvio di un'operazione di pagamento elettronico di cui al paragrafo 1, lettera b), per le operazioni di pagamento elettronico a distanza, l'autenticazione forte del cliente applicata dai prestatori di servizi di pagamento comprende elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico» (2° comma).

Ai sensi dell'art. 1, 1° comma, lett. q-bis), d.lgs. n. 11/2010, per “autenticazione forte del cliente” (di seguito, “SCA”) si intende «un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione».

Il Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce “*un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema*”. Il Collegio di Coordinamento ha, peraltro, precisato che “*l'apparentemente corretta autenticazione dell'operazione [non] è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 50 euro)*”. Secondo il Collegio di Coordinamento, “[l]a ratio di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento” (così Collegio di Coordinamento, decisione n. 3947/14; in senso conforme, Collegio di Coordinamento, decisioni nn. 3498/12, 991/14; cfr. anche Collegio di Coordinamento, decisione n. 22745/19, con particolare riguardo all'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, ex art. 10, 2° comma, d. lgs. n. 11/2010).

Il menzionato orientamento ha trovato riscontro nella giurisprudenza di legittimità (Cass. 3 febbraio 2017, n. 2950), secondo cui la disciplina speciale relativa agli strumenti di pagamento ha esplicitato un principio generale applicabile in tema di onere probatorio a carico del debitore professionale nelle azioni di risoluzione contrattuale, risarcimento del danno o adempimento, “*in quanto si è ritenuto che non può essere omessa la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire la sicurezza del servizio [...]; infatti la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi come parametro la figura dell'accorto banchiere*” ((in senso conforme, cfr. Cass., 12 aprile 2018, n. 9158; Cass. 12 febbraio 2024, n. 3780; v. anche Cass., 26

novembre 2020, n. 26916, anche per l'importante statuizione, secondo cui *“al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento – prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente – la possibilità di un'utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo”*).

2. Tanto premesso in termini generali, in ossequio ai principi in tema di riparto dell'onere probatorio sopra enucleati, è necessario innanzitutto verificare la conformità delle operazioni disconosciute alle prescrizioni normative in tema di SCA.

L'operazione disconosciuta consiste in un bonifico istantaneo di Euro 4.100,00, disposto il 16 settembre 2024 alle 17:00.

L'intermediario deduce che l'operazione contestata è stata eseguita mediante l'utilizzo del PIN (fattore di conoscenza) e della OTP generata dal *mobile token* (fattore di possesso). Al riguardo, fa presente che la OTP è generata in modo silente dal *mobile token*, integrato nell'APP di *home banking*, che la Ricorrente ha attivato sul proprio *device*. Precisa che il testo della notifica, che appare sul *device* e sul quale l'utente deve fare *“tap”* per autorizzare, indica quale operazione/attività si sta autorizzando. Rileva, inoltre, che l'attivazione del *mobile token* è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all'*home banking*.

Produce il *log* relativo alle attività effettuate da APP il giorno dell'esecuzione dell'operazione contestata con l'“*Id Utente*” della Ricorrente (cfr. colonna “*Id Utente*” n. ***435), corrispondente a quello indicato nei “*dati cliente*”.

Dal *log* si evince che:

- in data 16/09/2024, alle 16:56:30, è stato eseguito un *log-in* mediante inserimento di *Id Utente* e PIN dall'indirizzo IP ****a302 con il dispositivo “iPh***15,4” e verifica a 2 fattori con OTP generato dal *mobile token*;
- dal medesimo dispositivo e indirizzo IP è stato inserito il bonifico alle 17:00:26 firmato con SCA (PIN + OTP generato da *mobile token*).

L'Intermediario ha altresì prodotto evidenza della notifica *push* e dell'SMS inviati alla Ricorrente a valle dell'esecuzione dell'operazione contestata.

Dalla documentazione depositata dall'Intermediario risulta altresì che le attività riportate nei *log* dal 2 settembre 2024 al 25 settembre 2024, sia antecedenti che successive al giorno della truffa (16 settembre 2024), risultano eseguite dal medesimo *device* impiegato per l'autenticazione dell'operazione contestata (“iPh***15,4”, colonna descrizione “*device*”). Inoltre, dal *log* sembra evincersi che sia l'inserimento del bonifico disconosciuto che la sua autenticazione tramite PIN e OTP sia avvenuta tramite l'APP installata su tale *device*, presumibilmente in possesso della Ricorrente.

Questo Collegio, sulla base della documentazione in atti e in linea con il proprio consolidato orientamento (Collegio di Bari, decisioni nn. 3343/2025, 10734/2024 e 4225/2024; cfr. anche Collegio di Bologna, decisione n. 11648/2024, Collegio di Napoli, decisione n. 5452/2024), ritiene pertanto integrata la prova che il sistema di sicurezza adottato dall'intermediario sia conforme alla SCA. La documentazione tecnica allegata alle controdeduzioni risulta, infatti, idonea a dimostrare la corretta autenticazione e la regolarità formale delle operazioni disconosciute ex art. 10, 1° comma, d.lgs. n. 11/2010.

3. Sulla base dei principi elaborati dal Collegio di Coordinamento (v. sopra, n. 1), l'accertamento della conformità della procedura di autenticazione alla definizione di SCA contenuta nel d.lgs. n. 11/2010 non è di per sé dirimente per escludere la responsabilità

del cliente, che sussiste, invece, nei «casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato» (Collegio di Coordinamento, decisione n. 3947/14, cit.).

Più di recente, il medesimo Collegio di Coordinamento ha chiarito che «la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente» (decisione n. 22745/19).

Nel caso in esame, l'Intermediario ha eccepito che la Ricorrente ha fornito una ricostruzione incompleta della frode subita, essendosi limitata a narrare le modalità di "aggancio" senza allegare nulla circa la materiale esecuzione dell'operazione.

In effetti, nelle denunce e nel ricorso, la Ricorrente non descrive le modalità con cui sarebbe avvenuta la truffa, ma si limita ad affermare che *"le transazioni promesse sono risultate essere un unico bonifico a loro favore"*.

Va peraltro osservato che la condotta della Ricorrente appare connotata da colpa grave anche tenuto conto del fatto che il primo SMS:

- (i) stato ricevuto da un numero non riconducibile all'Intermediario (e, anzi, espressamente riferito a un soggetto diverso da questo);
- (ii) contiene errori grammaticali (*"se non e lei chiama assistenza clienti"*; sic);
- (iii) invita a chiamare un numero di cellulare, asseritamente qualificato come *"assistenza clienti"*, non riconducibile all'Intermediario.

Pure il secondo SMS, peraltro, per quanto collocato nella cronologia genuina di precedenti messaggi dell'Intermediario, contiene errori grammaticali e di punteggiatura (*"Segua le istruzioni del nostro operatore ... per il blocco del bonifico da lei non autorizzato da lei cordiali saluti"*).

Tanto avrebbe dovuto fare insospettire la Ricorrente che, consapevole che non si trattasse del numero del servizio clienti dell'Intermediario, ha comunque chiamato il numero di cellulare indicato nel primo SMS.

In relazione ad un siffatto quadro probatorio, questo Collegio, nel solco del suo precedente orientamento, ritiene che dagli elementi di prodotti in atti dalle Parti emergano modalità esecutive dell'operazione da cui si può evincere la prova, in via presuntiva, della colpa grave della Ricorrente, che non può non avere fornito, anche solo inconsapevolmente, cooperazione affinché le operazioni fraudolente potessero compiersi (cfr. Collegio di Bari, decisioni nn. 7144/23; 8552/22, 6517/22, 3157/22 e 21785/2021; v. anche Collegio di Bologna, decisione n. 10036/22; Collegio di Roma, decisione n. 6169/22).

4. In casi come quello oggetto del presente procedimento non è generalmente configurabile una responsabilità dell'Intermediario, salvo che, sulla base delle evidenze disponibili, emerga in concreto un suo apporto causale alla produzione del danno e al compimento della frode (così Collegio di Bari, decisione n. 9279/2024; Collegio di Bologna, decisione n. 9454/2024).

Tanto può accadere, a titolo di esempio, nei casi di:

- a) mancata disponibilità (anche temporanea) del numero del servizio clienti dell'intermediario, che impedirebbe al cliente di accertare in via preliminare la genuinità della chiamata ricevuta dal frodatore;
- b) mancata identificazione del tentativo di frode in corso da parte del dipendente dell'intermediario, cui il pagatore si sia rivolto esponendo le richieste del frodatore;

- c) mancato rilievo di indici di frode, quando il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere.

Nel caso oggetto del presente procedimento:

- con riguardo all'ipotesi di cui sopra, sub a), sebbene la ricorrente abbia dedotto di avere tentato, subito dopo la ricezione del messaggio civetta, di contattare il numero verde del servizio clienti dell'Intermediario senza riuscire a parlare con un operatore, non ha però prodotto alcuna evidenza tratta dal proprio registro chiamate;
- non ricorre l'ipotesi di cui sopra, sub b);
- con riguardo all'ipotesi di cui sopra, sub c), la Ricorrente si duole del carattere anomalo del bonifico, in considerazione della rilevanza e significatività dell'importo sottratto rispetto alla normale operatività del proprio conto corrente. Al riguardo, in atti sono presenti un estratto conto trimestrale dal 1° aprile 2022 al 30 giugno 2022 e un estratto conto dal 28 agosto 2024 al 17 settembre 2024, da cui si evince l'assenza di operazioni di pagamento di importo superiore a Euro 1.000,00.

Sulla base della documentazione in atti, risulta quindi che l'importo dell'operazione contestata è anomalo rispetto alla usuale operatività della Ricorrente (per la valorizzazione di questo elemento, v. Collegio di Bari, decisione n. 1690/2023; Collegio di Milano, decisione n. 5346/2022; Collegio di Roma, decisione n. 595/2023) e di tale anomalia avrebbe dovuto avvedersi l'Intermediario.

Non coglie nel segno, invece, la doglianza della Ricorrente, secondo cui l'Intermediario non avrebbe previsto alcun limite giornaliero ai pagamenti, né avrebbe proposto alla Ricorrente di fissarlo. Al riguardo, infatti, l'Intermediario allega due proposte di modifica unilaterale inviate alla ricorrente a gennaio del 2019 ed a giugno 2022, da cui si evince che il limite per i bonifici istantanei è fissato in Euro 15.000,00 per operazione.

Alla luce di quanto precede, ad avviso del Collegio, ferma la grave negligenza della Ricorrente, che con la propria condotta ha agevolato il compimento della truffa, nella verifica del danno può ritenersi sussistente un contributo causale della condotta dell'Intermediario che avrebbe potuto (e dovuto) apprestare presidi organizzativi adeguati e funzionali ad evitare l'esecuzione di operazioni "sospette" rispetto alla usuale operatività della propria clientela.

Per questi motivi, il Collegio ritiene il ricorso meritevole di accoglimento parziale, con imputazione in capo all'Intermediario di una quota di responsabilità che stima equo riconoscere in Euro 2.000,00.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 2.000,00.

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 al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.



Decisione N. 8614 del 30 settembre 2025

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI