COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) TOMMASI	Membro designato dalla Banca d'Italia
(BA) BUTA	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - GRAZIA BUTA

Seduta del 26/02/2024

FATTO

Parte ricorrente, nel richiamare il contenuto di tutta la documentazione allegata al ricorso, riferisce che in data 20/03/2023, alle ore 15:20, riceveva un sms da un mittente riconducibile all'IMEL emittente la carta di credito a sé intestata e collegata al conto incardinato presso l'intermediario resistente. Veniva così informata di una limitazione inerente alla "carta/conto per mancata verifica della sicurezza web" con invito a riattivarla mediante un link ivi indicato; soggiunge che alle ore 17:32 riceveva un ulteriore messaggio dallo stesso mittente che la notiziava di una telefonata che avrebbe ricevuto il giorno seguente. In data 21/03/2023, dunque, riceveva la suddetta telefonata da un numero fisso riconducibile all'intermediario convenuto, in cui un sedicente operatore le comunicava l'avvio di una procedura guidata per "aggiornamento della sicurezza". Precisa che nel corso della telefonata non forniva alcun codice o credenziale all'interlocutore il quale, tuttavia, riusciva ugualmente a bloccare l'app invitandola a non utilizzarla per "qualche giorno lavorativo".
Riferisce che alle ore 18:35 del 21/03/2023 contattava una filiale della resistente per ottenere chiarimenti ed apprendeva di essere stata vittima di truffa, per cui procedeva a bloccare il conto; successivamente si avvedeva di un'operazione di bonifico non autorizzata per € 9.998,00 con data valuta 21/03/2023. Lamenta che l'interlocutore telefonico conosceva i suoi dati personali ed era riuscito a mettersi in contatto con lei mediante una chat collegata al conto, senza tuttavia che gli fossero mai stati forniti i codici di sicurezza o altre informazioni riservate. Si duole altresì del mancato storno dell'operazione contestata, rispetto alla quale la resistente, nel caso di specie, si è limitata ad eseguire una richiesta di recall per frode. Menziona l'orientamento della giurisprudenza di legittimità secondo cui sulla banca gravano specifici obblighi di protezione della clientela, escludendo la possibilità di un'utilizzazione dei codici di accesso al sistema di internet banking da parte di terzi non autorizzati.

Chiede dunque la restituzione di € 9.998,00 oltre il danno morale, quantificato in € 5.000,00 con refusione delle spese legali.
Costituitosi, l'intermediario fa presente che l'odierno ricorso ha ad oggetto la richiesta di restituzione dell'importo relativo ad un'operazione di bonifico disconosciuta ed effettuata tramite internet banking.
Illustra in generale: le modalità di accesso all'home banking sia tramite app sia tramite pc; le modalità di disposizione di un bonifico tramite i predetti canali; come eseguire l'enrollment di un token software su nuovo device; come modificare i dati personali a sistema (a titolo esemplificativo, la mail collegata al rapporto di conto corrente). Osserva che ognuna delle citate operazioni richiede un'autenticazione basata su uno o più codici statici, password e pin, nonché su un codice dinamico "OTP o Token Software integrato nell'App", in conformità con i requisiti in materia di SCA previsti dalla direttiva PSD 2.
Tanto premesso riferisce che in data 20.03.2023 parte ricorrente riceveva un sms da un mittente riconducibile ad una società operante nel settore dei pagamenti online e delle emissioni di carte di credito e accedeva ad un link, che peraltro riportava un "insolito indirizzo", per un "fantomatico blocco intervenuto per una presunta mancata verifica di sicurezza".
Soggiunge che, sebbene parte ricorrente in sede di denuncia avesse dichiarato di non aver effettuato l'operazione richiesta nel primo messaggio, è evidente che abbia eseguito l'accesso al link sopra citato con inserimento delle credenziali di accesso al servizio di internet banking; tanto risulta confermato dal fatto che, successivamente, riceveva un ulteriore sms che la preavvisava di una telefonata che avrebbe ricevuto da un operatore.
Afferma dunque che in data 21.03.2023 la ricorrente riceveva una telefonata da un numero fisso riconducibile ad una delle filiali, durata circa venti minuti e nel corso della quale, come si evince dalla denuncia in atti, il frodatore chiedeva il codice presente in app "che appariva cerchiato in rosso" .
Precisa che tale codice è il codice OTP che risultava indispensabile per il frodatore per accedere autonomamente al servizio di internet banking (alle ore 13:27, tramite browser/pc) essendo già in possesso delle altre credenziali di accesso, ottenute mediante il messaggio civetta del giorno precedente.
Alle ore 13:34 del giorno 21.03.2023 la ricorrente riceveva una mail contenente la password dinamica-codice OTP- necessaria per l'attivazione di un nuovo token che, con ogni evidenza, veniva comunicato nel corso della telefonata stessa. Effettuato in questo modo l'accesso alla piattaforma online e in possesso di tutte le credenziali di sicurezza necessarie, il frodatore provvedeva a modificare l'indirizzo mail collegato al rapporto di internet banking così da impedire che la ricorrente ricevesse la mail di notifica automatica dell'esecuzione del bonifico fraudolento.
Il truffatore, dopo aver in questo modo configurato il token software sul proprio dispositivo e modificato l'indirizzo di posta elettronica, si collegava regolarmente al servizio di internet banking dal quale, alle ore 14:59, effettuava l'operazione oggetto di odierno ricorso.
Evidenzia che i sistemi di sicurezza adottati dalla banca non hanno presentato anomalie in quanto l'acquisizione dei codici e l'utilizzo del servizio di internet banking a seguito dell'attivazione del token software erano conseguenza della condotta colposa della ricorrente la quale, nel corso della citata telefonata, forniva le informazioni a tal fine necessarie, in contrasto con gli obblighi incombenti sull'utilizzatore a norma dell'art. 7 del d.lgs. 11/2010. Sottolinea inoltre che nel caso di specie il comportamento della ricorrente risulta ancor più negligente ove si consideri che i messaggi ricevuti ed il link civetta non erano riconducibili alla banca, bensì ad una società terza.
Menziona alcune pronunce dell'Arbitro in materia di phishing e precisa che tale orientamento è stato esteso anche in relazione ai casi di smishing e vishing, escludendo la responsabilità della banca nell'ipotesi in cui il ricorrente comunichi imprudentemente le credenziali di accesso all'home banking a terzi, versando così in colpa grave (cita decisione n. 1191/23 del Collegio di Bologna).
Chiede pertanto il rigetto del ricorso.
In sede di repliche, parte ricorrente ribadisce di non aver comunicato le credenziali di sicurezza ai frodatori, né a seguito della ricezione del primo messaggio civetta, né durante la telefonata intercorsa il giorno seguente. Precisa che in quel periodo stava provvedendo a trasferire il conto corrente proprio presso la filiale da cui apparentemente riceveva la telefonata truffaldina, ragione per cui conosceva quel numero di utenza fissa e confidava nell'affidabilità dell'interlocutore, il quale conosceva a sua volta il suo codice utente e la sua data di nascita, nonché le cifre finali di uno dei numeri di cellulare collegato al rapporto di conto corrente. Ritiene pertanto inadeguati i sistemi di

sicurezza adottati dalla resistente perché, con ogni evidenza, non garantiscono la riservatezza delle informazioni anagrafiche e bancarie dei correntisti. Ribadisce la doglianza relativa al mancato blocco dell'operazione, posto che si trattava di un bonifico ordinario e non istantaneo e che già alle ore 19:00 del giorno della truffa aveva bloccato il conto corrente. Insiste per l'accoglimento delle domande formulate in sede di ricorso.
In sede di controrepliche, l'intermediario ribadisce quanto precedentemente dedotto ed allega un ulteriore documento, curato dalla società a cui all'epoca dei fatti risultavano affidati i servizi di outsourcing informatico, ad integrazione dei log già prodotti in sede di controdeduzioni.
Chiede pertanto il rigetto del ricorso; in via subordinata, chiede che si tenga comunque conto del comportamento incauto della ricorrente.

DIRITTO

La controversia in esame concerne il disconoscimento di un'operazione di bonifico disposta da internet banking per l'importo di € 9.998,00 effettuata in data 21/03/2023.
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 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. La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, co. 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, ai sensi dell'art. 10, d.lgs. n. 11/2010, "qualora l'utilizzatore 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." (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è altresì precisato 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". Al riguardo, 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 […]. Neanche l'apparentemente corretta autenticazione dell'operazione 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). La *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" (Coll. Coord., decisione n. 3947 del 24.6.2014. In senso

conforme: Coll. Coord. Decisione n. 3498/2012; Coll. Coord., decisione n. 991 del 21.2.2014. Da ultimo, cfr. Coll. Coord., decisione n. 22745/19, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, *ex* art. 10, co. 2, d.lgs. n. 11/2010). L'orientamento di questo Arbitro ha trovato riscontro nella sentenza della Corte di Cassazione, 3.2.3017, n. 2950, la quale ha statuito che la disciplina speciale, in tema di strumenti di pagamento, ha esplicitato il principio generale, 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" (Cass., n. 2950/17, sulla scia di Cass., 12.6.2007, n. 13777. In senso conforme, cfr. Cass.,12.4.2018, n. 9158; 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").

Tanto premesso in termini generali, rileva il Collegio che, nella specie, oggetto di disconoscimento è un bonifico di € 9.998,00 disposto il 21/03/2023.

Quanto alle modalità della truffa, la ricorrente in sede di denuncia ha riferito di aver ricevuto, in data 20/03/2023, due sms da un mittente riconducibile alla società emittente la carta di credito collegata al conto corrente: nel primo le veniva richiesto di cliccare su un link per la riattivazione della sicurezza web del "conto/carta" (operazione che non effettuava); nel secondo veniva avvisata di una telefonata che avrebbe ricevuto da un operatore e le veniva confermato un appuntamento telefonico per il giorno seguente. Soggiunge di aver dunque ricevuto tale telefonata da un numero fisso a lei noto e riconducibile ad una delle filiali della resistente, con cui un sedicente operatore, già in possesso del codice utente da lei non comunicatogli, le chiedeva di aprire l'app e di comunicarle il "codice che appariva cerchiato in rosso". La ricorrente, in sede di denuncia, ha precisato di aver riferito tale codice al frodatore. Alle ore 13:37 del 21/03/2023 un messaggio inserito nella stessa chat dei messaggi del giorno precedente la informava dell'avvenuto aggiornamento della procedura di sicurezza, invitandola ad attendere "1-3 giorni lavorativi" prima di riutilizare l'app. Secondo le prospettazioni della ricorrente, la stessa sarebbe stata dunque vittima di una truffa attuata mediante l'utilizzo combinato delle tecniche dello smishing con SMS spoofing e del vishing con caller id spoofing.

Dal canto suo l'intermediario offre innanzitutto una ricostruzione generale dei sistemi di autenticazione, eccependo che l'ordine di bonifico per cui vi è contestazione era stato validato attraverso un sistema di autenticazione forte a due fattori. In generale, questi ricostruisce le modalità di: accesso (tramite App è necessario l'utilizzo congiunto dell'App/token software installata sullo smartphone e delle credenziali statiche, mentre tramite browser/pc è necessario l'utilizzo congiunto della userid-password e del codice OTP generato dal token software, previa digitazione del PIN); disposizione di un bonifico (tramite App è necessario l'utilizzo congiunto dell'App/token software installata sullo smartphone e del codice PIN; segue messaggio di alert di avvenuta esecuzione del bonifico); *enrollment* del token software su un nuovo device (utilizzo congiunto della userid-password e del codice OTP, inviato esclusivamente a mezzo e-mail); modifica dei dati personali (tramite App è necessario l'utilizzo congiunto dell'App/Token Software installata sullo smartphone e del codice PIN; segue messaggio di alert di avvenuta modifica dei dati).

Dalle schermate allegate in atti si evince che il frodatore ha inizialmente eseguito l'accesso tramite proprio dispositivo (web/pc) e abbia in questo modo consultato l'estratto conto della ricorrente e i limiti operativi. L'accesso in esame è avvenuto tramite autenticazione fondata su "*Password*" (fattore di conoscenza) e "*OTP*" (fattore di possesso) che nel caso di specie è stata generata dalla stessa ricorrente tramite il proprio token e comunicata nel corso della telefonata, come riferito da lei stessa in sede di denuncia (cfr., colonna "*DatiZeb*" valore "*Schema=S44*").

Inoltre, dalle schermate prodotte dall'intermediario si evince che alle ore 13:34 il frodatore ha avviato la procedura di *enrollment* sul proprio *device* mediante utilizzo di una "*Password*" (fattore di conoscenza) e di una "*OTP*" (fattore di possesso). Nel rammentare che, secondo le deduzioni dello stesso intermediario, tale OTP viene inviata esclusivamente a mezzo mail, si osserva che non è presente in tali *log* un esplicito riferimento al suo invio. Il Collegio osserva tuttavia che lo stesso potrebbe desumersi dalla dicitura *notificaEmail: true* presente in calce alla schermata concernente l'avvio della procedura di enrollment. Al riguardo l'indirizzo mail che risultava registrato nel momento della configurazione in discorso coincide con l'indirizzo mail indicato dalla ricorrente in sede di denuncia. A seguito dell'avvenuta procedura di *enrollment*, il log di accesso all'app delle 13:35 evidenzia nuovamente e in maniera esplicita l'utilizzo del sistema di autenticazione a due fattori (cfr., colonna "*DatiZeb*" valore "*Schema=S44*").
Quanto alla prova della regolare esecuzione del bonifico, dalle schermate allegate in atti si evince una prima identificazione, verosimilmente finalizzata ad abilitare il nuovo token alle operazioni dispositive, avvenuta mediante identificazione del titolare con SCA basata sull'utilizzo del token installato dal frodatore sul proprio device e di un "PIN mnemonico". Successivamente il bonifico è stato eseguito con SCA (cfr., "SCAPSD2=S") sempre attraverso il token installato dal frodatore sul proprio device e l'inserimento di un nuovo codice PIN appositamente impostato dal frodatore stesso. Successivamente è stata inviata una notifica alert all'indirizzo mail precedentemente modificato dal frodatore, alle ore 13:36 del giorno della frode.
Ciò premesso, il Collegio rileva che le risultanze dei tabulati prodotti dall'intermediario sono idonee a comprovare la S.C.A.
Alla luce delle richiamate disposizioni normative, peraltro, la prova della regolarità formale dell'operazione contestata non è sufficiente ad attribuirne le conseguenze patrimoniali in capo al titolare dello strumento di pagamento, dovendo l'intermediario provare anche i fatti idonei a integrare il dolo o la colpa grave dell'utilizzatore. Questo aspetto risulta enfatizzato, a seguito della novella del 2017 (d.lgs. n. 218/2017), che ha introdotto nell'art. 10, co. 2, la disposizione sopra riportata, in tema di onere della prova del dolo o della colpa grave dell'utente. La prova in questione, evidentemente, non può coincidere con quella della mera regolarità formale delle operazioni, pena un'interpretazione abrogante della disposizione. Sul punto si è, da ultimo, pronunciato il Collegio di Coordinamento, nella menzionata decisione n. 22745 del 10/10/2019, nella quale è stato enunciato il principio secondo cui "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 [....]. Utili informazioni integrative potrebbero, ad esempio, riguardare l'assenza di tentativi falliti di digitazione del PIN, la ricezione della password dinamica tramite cellulare o altro dispositivo del cliente, in assenza di deviazioni o intrusioni nel device, l'accertata assenza di malware, ecc.".
Nel caso di specie, il Collegio rileva che è in atti copia degli sms "civetta" ricevuti dalla ricorrente. Dagli stessi si evince che: il mittente è effettivamente riconducibile ad una società di pagamenti, di cui parte ricorrente riferisce di essere titolare di una carta di credito collegata al conto acceso presso la resistente; il link inserito nel primo messaggio è riconducibile alla stessa società; il messaggio genuino delle ore 20:26 che conferma il blocco della carta, appare all'interno della stessa chat in cui sono presenti i messaggi truffaldini. È in atti, inoltre, la schermata contenente il dettaglio della telefonata truffaldina delle ore 13:21 ed in effetti il numero di utenza chiamante coincide con il numero di una delle filiali dell'intermediario, di cui la ricorrente dichiarava di essere a conoscenza.
Il Collegio ritiene pertanto che le modalità seguite dai truffatori per ottenere le informazioni dalla ricorrente siano riconducibili, in parte, al c.d. vishing con "caller id spoofing", che consiste nella manipolazione dei dati relativi al chiamante per cui la telefonata sembra provenire da un contatto ufficiale dell'intermediario. Secondo l'orientamento condiviso dei Collegi ABF, nelle fattispecie di spoofing non è generalmente ravvisabile la colpa grave del ricorrente, data l'insidiosità del meccanismo di aggressione. Tuttavia, il Collegio ritiene che nel caso in esame possa rilevarsi un concorso di colpa tra le parti, in relazione, da un lato, alla negligenza grave della ricorrente che -

come dalla stessa riferito in sede di denuncia - ha comunicato "il codice che appariva cerchiato in rosso", agevolando così il compimento della truffa e, dall'altro lato, alle criticità organizzative dell'intermediario. Nel caso in esame, infatti, assume rilevanza il fatto che la chiamata ricevuta provenisse da un contatto ufficiale dell'intermediario. Il che induce a ritenere che sebbene il comportamento della ricorrente non sia, per quanto osservato, esente da responsabilità, anche la condotta dell'intermediario non possa andare indenne da censure, quanto meno sotto il profilo della diligenza "organizzativa", per "avere cioè fatto uso di un canale di comunicazione con i clienti suscettibile di essere contraffatto e perciò idoneo ad indurli in errore" (cfr. Collegio di Bari, nn. 84/2021 e 13567/2021). Tanto premesso, ritiene il Collegio che debba riconoscersi un concorso di colpa fra intermediario e ricorrente nella produzione del danno, nella misura, rispettivamente, del 70% (corrispondente all'importo di € 6.998,6 che viene arrotondato per eccesso a 7.000,00) e del 30%.

Relativamente alla doglianza concernente il mancato storno dell'operazione, il Collegio rileva che in sede di reclamo, parte ricorrente ha affermato di essersi avveduta della truffa intorno alle ore 18:35 e di aver richiesto successivamente a tale orario, lo storno dell'operazione disconosciuta. Ebbene, dal sito web della resistente risulta che il c.d. "cut-off" per la lavorazione di questa tipologia di richieste è fissato non più tardi delle ore 16:00.

La ricorrente chiede inoltre la condanna al risarcimento dei danni morali subiti, quantificati in € 5.000,00.

I Collegi territoriali, in conformità con l'orientamento espresso dalla giurisprudenza di legittimità, ritengono non configurabile nel nostro ordinamento il danno in re ipsa, gravando sul ricorrente l'onere di provare sia l'an che il quantum della pretesa risarcitoria (cfr. Collegio di coordinamento, n. 1642/2019). Nel caso di specie tale istanza non è supportata da alcuna evidenza documentale.

Infine, quanto alla richiesta di refusione delle spese legali, la ricorrente non produce alcuna documentazione a supporto della richiesta.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 7.000,00.

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.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI