

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) GENOVESE	Membro di designazione rappresentativa degli intermediari
(BO) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore ANDREA GENOVESE

Seduta del 03/02/2026

FATTO

Insoddisfatta dell'interlocuzione con l'intermediario nella fase del reclamo, con ricorso n. 1872824 del 29.09.2025, la parte ricorrente si rivolge all'Arbitro al quale chiede di accertare il proprio diritto al risarcimento del danno patrimoniale di Euro 49.618,00, corrispondente all'importo di numerose operazioni di pagamento fraudolentemente, eseguite mediante bonifici non autorizzati, tra il 07.08.2025 e il 20.08.2025, oltre alla refusione delle spese di assistenza legale di Euro 200,00. A sostegno delle pretese, deduce che: (i) è titolare del conto corrente n. *263 radicato presso la banca resistente; (ii) è stata vittima di un attacco informatico nel mese di agosto 2025, che le ha causato un danno patrimoniale di Euro 49.618,00; (iii) nel periodo compreso tra il 07.08.2025 e il 20.08.2025, terzi ignoti hanno disposto n. 70 bonifici non autorizzati per un importo di Euro 69.472,00, di cui solo n. 20 sono stati bloccati e riaccreditati dall'intermediario; (iv) il tentativo di frode è iniziato il 24.07.2025 con la ricezione di un SMS di *smishing* che segnalava alcune irregolarità sul conto, in un primo momento ignorato con diligenza; (v) il 07.08.2025, mentre si trovava in aeroporto per prendere un volo per la Cina, ha ricevuto una chiamata da un'utenza apparentemente riconducibile alla banca da parte di un sedicente operatore dell'intermediario; (vi) indotta in errore dall'apparente genuinità della chiamata, ha seguito le istruzioni dell'operatore, accedendo a un sito web clone e inserendo le proprie credenziali;

(vii) durante la chiamata, ha ricevuto un'e-mail di attivazione dell'App all'indirizzo d*@gmail.com, sebbene non lo avesse comunicato all'operatore. In tale occasione le è stato suggerito anche di eliminare l'applicazione dal proprio dispositivo; (viii) al suo rientro in Italia, il 20.08.2025, ha riscontrato la perdita di una rilevante somma dal conto corrente e ha provveduto al disconoscimento delle operazioni e alla denuncia presso i Carabinieri; (ix) è evidente la responsabilità oggettiva della banca per non aver impedito la consumazione della truffa; (x) la condotta dell'intermediario non è stata improntata alla diligenza qualificata propria dell'operatore professionale, che comporta l'accettazione del rischio d'impresa relativo ai collegamenti telematici; (xi) non ha agito con colpa grave, poiché la strategia persuasiva posta in essere dal truffatore e l'uso del numero ufficiale della banca hanno generato un affidamento incolpevole; (xii) è mancata l'autenticazione forte (SCA), con conseguente violazione del combinato disposto della direttiva PSD2 (Direttiva UE 2015/2366) e del Regolamento Delegato (UE) n. 2018/389, che rende l'intermediario responsabile per la mancanza di un secondo elemento dinamico di sicurezza; (xiii) la banca ha adottato solo misure di "tutela passiva", consistenti in informative e avvertimenti, omettendo invece la tutela attiva, che avrebbe dovuto portare alla sospensione dei bonifici in ragione dell'anomala frequenza e dell'importo seriale degli stessi; (xiv) l'intermediario stesso si era accorto della violazione, avendo stornato parte dei bonifici, ma avrebbe dovuto procedere all'accertamento dell'identità di chi stava compiendo tali operazioni sin dall'inizio.

Costituitosi, l'intermediario chiede all'Arbitro di rigettare il ricorso perché infondato, sul rilievo che: a) vi è stata piena conformità del servizio "Rapporti a distanza tra Banca e Cliente" ai requisiti della "Strong Customer Authentication" (SCA), previsti dalla normativa europea PSD2 (Direttiva UE 2015/2366); b) il sistema di sicurezza adottato prevede un'autenticazione "a due fattori": uno statico (numero cliente e codice PIN, noto solo all'utente) e uno dinamico (codice OTP generato in modo silente dal Mobile Token installato sul dispositivo certificato); c) dalle evidenze dei LOG di sistema, risulta che in data 07.08.2025, alle ore 10:51, è stato attivato un secondo Mobile Token (seriale *024) sul dispositivo *669; d) l'attivazione di tale strumento di pagamento è tecnicamente impossibile senza il concorso del titolare, in quanto richiede l'inserimento delle credenziali personali (PIN) e di un codice riservato inviato tramite SMS o e-mail al cliente; e) la parte ricorrente ha ammesso, in sede di denuncia, di essere stata vittima di un raggio telefonico (*vishing*), durante il quale ha fornito le proprie credenziali e il codice OTP a un sedicente operatore; f) la condotta della parte ricorrente, consistita nel seguire istruzioni fornite da terzi, accedere a link sospetti non riconducibili alla banca e disinstallare l'App ufficiale dal proprio device, è qualificabile alla stregua di "colpa grave" ai sensi dell'art. 7, comma 2, del D. Lgs. n. 11/2010; g) la parte ricorrente ha violato gli obblighi di custodia e protezione delle credenziali di sicurezza. La diligenza media dell'utente sarebbe stata sufficiente a scongiurare la frode; h) ha adempiuto ai propri doveri di informazione e prevenzione attraverso la pubblicazione di avvisi di sicurezza sul portale web, sull'App e sugli schermi ATM, nonché mediante comunicazioni allegate agli estratti conto; i) in ossequio all'art. 10 del D. Lgs. n. 11/2010, le operazioni sono state correttamente autenticate e contabilizzate, con esclusione di qualsivoglia malfunzionamento o compromissione dei sistemi informatici; l) è infondata la richiesta di rifusione delle spese legali, per Euro 200,00, in quanto la procedura ABF non richiede assistenza professionale obbligatoria e, per orientamento consolidato, tale voce non è oggetto

di rimborso; m) si è attivato per il recupero delle somme (procedura di “recall”) presso le banche corrispondenti, con esito tuttavia negativo; n) ha formulato una proposta transattiva in data 10.11.2025, al solo fine di chiudere bonariamente la vicenda e senza riconoscimento di alcuna responsabilità, offrendo il rimborso di Euro 31.760,00 a fronte della sottoscrizione di una manleva e della rinuncia agli atti del giudizio.

In sede di repliche, la parte ricorrente ha affermato che: (i) l'intermediario avrebbe dovuto adottare tutte le misure idonee a garantire la sicurezza del servizio ai sensi dell'art. 1176, comma 2, c.c.; (ii) l'intermediario può escludere la propria responsabilità solo provando di aver predisposto ogni strumento necessario a tutelare la sicurezza e l'inviolabilità del conto corrente, e al contempo dimostrando il dolo o la colpa grave in capo al cliente; (iii) l'adeguatezza dei sistemi di sicurezza non può desumersi dalla mera pubblicazione delle procedure sul sito web; (iv) poiché la banca non ha assolto all'onere di provare l'idoneità dei propri sistemi, la stessa è tenuta al risarcimento integrale della perdita patrimoniale subita; (v) la propria condotta non è stata colposa né tantomeno gravemente colposa; (vi) la truffa ha avuto origine da un messaggio “civetta” proveniente dal canale ufficiale della banca, al quale ha fatto seguito una chiamata da un numero apparentemente proveniente da quest'ultima, in occasione della quale un presunto operatore la avvisava di alcune irregolarità sul proprio conto corrente; (vii) ha prontamente disconosciuto le operazioni eseguite da terzi ignoti; (viii) spetta al prestatore dei servizi l'onere di dimostrare che l'utilizzatore abbia agito con frode, come confermato dalla Corte di Cassazione e dalle decisioni del Collegio di Roma; (ix) la comunicazione delle credenziali a terzi malfattori è considerata un “evento fisiologico” nel fenomeno del *phishing* e non integra l'elemento della colpa grave se indotta da modalità particolarmente insidiose che non consentano di rilevare l'inattendibilità del messaggio; (x) le modalità della truffa non erano tali da permettere a chiunque di avvedersi dell'inganno, e ciò esclude la colpa grave necessaria per sollevare la banca dalla responsabilità; (xi) le operazioni contestate sono soggette alla normativa del d.lgs. 11/2010, come modificata dalla direttiva PSD2 (Direttiva UE 2015/2366); (xii) in caso di disconoscimento, l'intermediario deve provare che l'operazione è stata autenticata, registrata e non influenzata da malfunzionamenti; (xiii) l'art. 10 bis del d.lgs. 11/2010 impone l'applicazione dell'autenticazione forte (SCA) per l'accesso ai conti online e per le operazioni a distanza; (xiv) nel caso specifico, non è stata fornita la prova dell'autenticazione forte; (xv) non ha mai ricevuto l'SMS con il codice OTP per l'attivazione del mobile token sul proprio telefono e la banca non ha dimostrato il contrario mediante idonee tracciature informatiche; (xvi) dalle evidenze prodotte risulta che il 07.08.2025 terzi ignoti hanno effettuato l'accesso dalla città di N** (tramite identificazione IP) attivando un nuovo token seriale “*0024”, con un dispositivo differente da quello della ricorrente; (xvii) la banca non ha provato l'invio o la ricezione dell'SMS OTP di associazione del token sul numero della cliente; (xviii) la parte ricorrente ha digitato esclusivamente un “codice di attivazione” (*263) su un sito contraffatto, diverso dal codice OTP (*625) indicato dalla banca; (xix) l'intermediario non ha chiarito l'appartenenza del dispositivo su cui è stata reinstallata l'App, elemento fondamentale per provare il fattore di possesso; (xx) secondo la giurisprudenza dell'ABF, la prova dell'autenticazione forte deve riguardare sia l'operazione sia i passaggi precedenti e funzionali, come l'*enrollment* dell'App; (xxi) emerge la responsabilità della banca per non avere intercettato operazioni anomale effettuate in meno di due settimane, per importi elevati e verso i medesimi beneficiari; (xxii) tali circostanze costituivano

indici di anomalia che avrebbero dovuto allertare i sistemi di monitoraggio della banca; (xxiii) respinge la proposta di pagamento parziale avanzata dalla banca, e insiste per l'accoglimento pieno della domanda risarcitoria.

Con le controrepliche, la parte resistente rileva che: a) l'attivazione di un secondo Mobile Token, in data 07.08.2025, è avvenuta correttamente, essendosi l'operazione perfezionata esclusivamente mediante l'inserimento di codici di sicurezza riservati nella disponibilità del solo ricorrente; b) la parte ricorrente ha ricevuto regolarmente sul proprio dispositivo mobile sia l'SMS che la notifica *push* comprovanti l'attivazione del predetto strumento di autenticazione; c) il sistema consente l'associazione del Mobile Token fino a due dispositivi distinti e l'utente può procedere alla sostituzione degli stessi in totale autonomia; d) il sistema di autenticazione "a due fattori" (SCA), qualificato come sistema di sicurezza "forte", conformemente agli orientamenti consolidati della giurisprudenza dell'Arbitro Bancario Finanziario, è ritenuto idoneo a tutelare la sicurezza delle transazioni; e) in virtù della sicurezza del sistema e dell'assenza di anomalie tecniche, è evidente la negligenza del ricorrente nella custodia delle credenziali personalizzate; f) la parte ricorrente, per sua stessa ammissione, ha interagito con un sedicente operatore fornendogli il codice OTP necessario per l'abilitazione ad operare; g) il comportamento della parte ricorrente è gravemente colpevole, avendo proceduto anche alla disinstallazione dell'applicazione ufficiale dal proprio *device* seguendo le istruzioni del truffatore; h) la condotta è connotata da colpa grave, integrando la violazione dei doveri di diligenza, custodia e protezione degli strumenti di pagamento previsti dalla normativa di settore; i) ha adempiuto a ogni onere di prevenzione e sicurezza, ritenendo che l'imprudenza della parte ricorrente abbia reso inefficaci i presidi tecnici adottati; l) è inammissibile la domanda di rifusione delle spese legali, pari a Euro 200,00, stante la natura della procedura ABF che non richiede assistenza professionale obbligatoria; m) in via subordinata e *pro bono pacis*, rinnova la propria proposta transattiva per un importo di Euro 31.760,00, condizionata alla sottoscrizione di una manleva e alla contestuale rinuncia a ogni ulteriore pretesa oggetto del ricorso.

DIRITTO

Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.01.2010, 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), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Le operazioni non autorizzate consistono in n. 70 bonifici, eseguiti tra il 07.08.2025 e il 20.08.2025, per un importo complessivo di Euro 69.472,00. Di tali operazioni, l'intermediario ha provveduto al blocco e al riaccredito di n. 20 bonifici, per cui l'importo delle operazioni oggetto di contestazione è pari a Euro 49.618,00.

Per quanto riguarda l'autenticazione delle operazioni, l'intermediario ha riferito e documentato mediante produzione in atti delle evidenze informatiche che la parte ricorrente ha attivato il secondo Mobile Token con seriale ***024, in data 07.08.2025, alle ore 10:51, tramite il dispositivo ***6L1 (***669), con inserimento del codice Pin (elemento della conoscenza) e del codice OTP ricevuto via SMS (elemento del possesso).

Inoltre, dalle allegazioni della parte resistente, sempre comprovate dalle tracciate informatiche in atti (Log), si osserva che: a) per quanto concerne gli accessi all'App, l'autenticazione è avvenuta mediante l'utilizzo del codice "Id Utente" e l'inserimento del codice PIN (elemento della conoscenza), seguito dall'utilizzo del codice OTP, generato nell'App della banca installata sul secondo dispositivo ***6L1 (***669) (elemento del possesso); b) le operazioni di pagamento mediante bonifico sono state eseguite tutte con la stessa modalità. Nello specifico, anche in questo caso, attraverso l'autenticazione forte a due fattori (SCA), mediante l'inserimento del codice PIN (elemento della conoscenza) e successivo utilizzo del codice OTP generato in App installata sul secondo dispositivo ***6L1 (***669) (elemento del possesso).

Per quanto osservato, è possibile affermare che l'intermediario ha assolto al proprio onere di dimostrare che le operazioni contestate, compresa l'attivazione del secondo Mobile Token e gli accessi in App, sono state correttamente autenticate, eseguite e contabilizzate, ex art. 10, comma 1, D.lgs. 11/2010 (per un precedente, relativo allo stesso processo di autenticazione, cfr. Collegio di Bologna, decisione n. 10470/2024).

È ora opportuno scrutinare la condotta serbata dalle parti in occasione dei fatti che conducevano al compimento delle operazioni contestate perché - come sancito dal Collegio di Coordinamento, con la decisione n. 22745/19 - *"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"*.

Sul punto, si osserva che la parte ricorrente è stata vittima di una frode denominata dai Collegi ABF *social hacking*, realizzata con la tecnica del c.d. *vishing caller id spoofing*, che ha avuto inizio con l'invio di un SMS civetta inseritosi nella chat delle conversazioni genuine con l'intermediario. In base a quanto consta dalla denuncia e dal ricorso, in data 24.07.2025, la parte ricorrente riceveva il detto SMS con il quale veniva avvisata che si erano verificate alcune irregolarità sul proprio conto e, al contempo, la avvisava che avrebbe dovuto premere sul link ivi presente per risolvere il problema. Tuttavia, non fidandosi, non dava seguito a quanto richiesto nel messaggio. Successivamente, in data 07.08.2025, mentre si trovava in aeroporto, riceveva una chiamata proveniente da un'utenza apparentemente riconducibile alla banca. In tale occasione, un sedicente operatore bancario le chiedeva se avesse ricevuto il messaggio di segnalazione delle irregolarità riscontrate nel conto corrente e, a fronte della sua risposta affermativa, ma dubbiosa sulla genuinità del messaggio, la rassicurava, dicendole che era

appena stata contattata dal numero ufficiale della banca. La pregava di intrattenersi telefonicamente qualche minuto, nonostante fosse vicina la partenza del volo, al fine di eseguire le operazioni necessarie a ristabilire la regolarità del conto corrente, altrimenti lo avrebbe dovuto chiudere, divenendo inutilizzabile. Fidandosi della situazione, ossia del fatto di aver ricevuto il precedente SMS nella chat in essere con la banca e di essere stata contattata telefonicamente da un'utenza apparentemente ufficiale, la parte ricorrente a quel punto seguiva le istruzioni fornite dal truffatore. Quindi, entrava tramite il suo dispositivo nell'App della banca e inseriva il codice PIN del conto corrente. Subito dopo le veniva fornito un link che la reindirizzava ad un sito web apparentemente uguale a quello dell'intermediario, ove inseriva le proprie credenziali, ossia codice cliente e PIN di accesso all'home banking. Appena fatto l'accesso al sito, riceveva una mail al proprio indirizzo di posta elettronica, nonostante non lo avesse comunicato al sedicente operatore, contenente un codice di attivazione dell'App della banca. Dopo aver dato seguito alle istruzioni impartite dal sedicente operatore bancario, quest'ultimo le suggeriva di disinstallare l'App precedentemente registrata sul suo *device* e le dava appuntamento telefonico per il 20.08.2025, alle ore 12:00, il giorno successivo al suo rientro in Italia, al fine di reinstallare l'App. Prima di terminare la conversazione, il truffatore la rassicurava che le presunte irregolarità erano state risolte. Rientrata in Italia, non riceveva alcuna telefonata ma solo un messaggio che la avvisava che non era stato possibile eseguire un bonifico del 20.08.2025 di Euro 993,00. Insospettitasi, poiché non aveva disposto alcun bonifico, contattava il numero assistenza clienti dell'intermediario (060***) e, nell'occasione, veniva invitata a recarsi in filiale. Quivi apprendeva di essere stata truffata, poiché tra il 07.08.2025 e il 20.08.2025 erano stati eseguiti n. 70 bonifici, per un importo di Euro 69.472,00, di cui n. 50 erano andati a buon fine e n. 20, invece, erano stati annullati e riaccreditati dalla banca.

A dimostrazione della truffa, la parte ricorrente ha allegato la copia dell'SMS civetta e della chiamata ricevuta.

Ciò posto, se, con riguardo alla fattispecie di "*vishing caller Id spoofing*" (consistente nell'invio di sms o nella effettuazione di chiamate da un'utenza apparentemente riferibile all'intermediario) l'orientamento dei Collegi ABF è nel senso di escludere, in linea generale, la colpa grave dell'utente in ragione dell'insidiosità di tale tecnica fraudolenta, d'altro canto, la stessa colpa grave deve essere, invece, ravvisata tutte le volte in cui, come nella specie, il ricorrente abbia incautamente e pedissequamente seguito le istruzioni del truffatore impartite telefonicamente, consentendogli di effettuare l'*enrollment* dell'App su un secondo dispositivo, così finendo per cooperare attivamente alla consumazione della truffa in suo danno.

La conclusione così raggiunta deve dirsi confermata anche tenuto conto che: i) l'SMS civetta, anche se inseritosi nella chat dell'intermediario, è, da un punto di vista grammaticale, anomalo rispetto a quelli genuini (passaggio dal "tu", contenuto nei messaggi della banca al "lei" presente nel messaggio fraudolento). Il ricorrente, pertanto, qualora avesse prestato la necessaria attenzione, avrebbe potuto rendersi conto che era in corso un tentativo di truffa a suo danno. Questa conclusione deve dirsi avvalorata dalla circostanza che l'SMS fraudolento contiene un'inusuale richiesta di accedere ad una pagina web, tramite un link ivi presente, per risolvere una presunta irregolarità del conto corrente; ii) inoltre, il numero dal quale sembrava chiamare il sedicente operatore bancario coincide con il numero

verde del servizio clienti della banca, dal quale, tuttavia, notoriamente quest'ultima può solo ricevere telefonate, non farle.

Quanto precede permette di formulare un giudizio di colpa grave a carico al ricorrente.

Da altra angolazione, non si può però fare a meno di notare come, dalle evidenze prodotte dall'intermediario, numerose operazioni di pagamento mediante bonifico contestate apparivano oggettivamente anomale. Infatti, nel periodo di tempo preso in considerazione, dal 07.08.2025 al 20.08.2025, molti bonifici venivano effettuati in rapida sequenza, in un brevissimo lasso di tempo nell'arco di 24 ore, per importi di circa Euro 990,00, di volta in volta verso uno stesso IBAN riferito ad un conto corrente intestato ad un determinato beneficiario. Ad es., il 07.08.2025 venivano eseguiti in rapida sequenza n. 6 bonifici di Euro 991,00, 998,00, 996,00, 994,00, 997,00 e 993,00, a favore del medesimo beneficiario, sig. P*** F***, e ciò avrebbe dovuto sollecitare l'apposizione di un blocco del conto da parte della banca, giacché oggettivamente anomale, e non a caso riconducibili nella fattispecie, debitamente interpretata in via estensiva, del rischio di frode di cui all'art. 8, D.M. 30.04.2007, n. 112, lettera a) n. 2, (tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita).

Per quanto visto, il Collegio reputa sussistere un concorso di colpa delle parti nella causazione del danno ed accerta, pertanto, in via equitativa il diritto della parte ricorrente ad ottenere dall'intermediario il rimborso della somma di Euro 35.000,00.

Infine, con riguardo alla domanda di refusione delle spese legali, quantificate dal ricorrente in Euro 200,00, questo Arbitro osserva che, in una recente pronuncia, il Collegio di Coordinamento (decisione n. 4580/2025), pur ribadendo che la difesa legale in sede di ABF costituisce una mera facoltà, con la conseguenza che, di regola, l'intermediario eventualmente soccombente non è tenuto al rimborso delle spese legali, ha, tuttavia riconosciuto che in *“presenza di determinate circostanze, da valutarsi secondo il prudente apprezzamento del Collegio giudicante, è però talora possibile riconoscere al ricorrente, la cui richiesta sia stata totalmente o parzialmente accolta, i costi sostenuti per essersi dovuto avvalere di un'assistenza professionale per la proposizione del ricorso ovvero per lo svolgimento della successiva attività procedurale innanzi all'Arbitro. Tali esborsi rappresentano, invero, un danno emergente per il cliente, risarcibile in base alle regole di diritto comune [...]”*. In particolare, ad avviso del Collegio di Coordinamento *“[...] Il riconoscimento di una somma a titolo di risarcimento del danno implica che risulti dimostrato il comportamento gravemente scorretto, oppure significativamente e ingiustificatamente dilatorio od ostruzionistico tenuto dall'intermediario nella gestione della controversia, che abbia reso oggettivamente necessaria la presenza di un professionista; in tale prospettiva, può assumere rilievo anche il carattere particolarmente difficile e complesso delle questioni oggetto di controversia. Quanto alla prova del danno, consistente nei costi connessi all'assistenza di un professionista, il ricorrente può produrre ogni evidenza documentale da cui si possa evincere l'effettività, la funzionalità e la rilevanza di tale presenza nella gestione del procedimento”*. La quantificazione del danno, secondo il Collegio di Coordinamento, non può che essere equitativa (art. 1226 c.c.) e, in quanto tale, affidata alla prudente valutazione del Collegio giudicante, anche in ragione

del carattere sommario della procedura innanzi all'ABF e della sua natura di sistema di risoluzione alternativa delle controversie".

Per quanto visto, nel caso di specie, ricorre il presupposto individuato dal riferito orientamento del Collegio di Coordinamento per dichiarare l'intermediario tenuto al rimborso delle spese legali domandate dalla parte ricorrente, ossia il carattere particolarmente complesso della controversia, che ha reso necessario il ricorso all'assistenza tecnica di un difensore.

PER QUESTI MOTIVI

Il Collegio – in parziale accoglimento del ricorso – dichiara l'intermediario tenuto, in favore della parte ricorrente, alla restituzione dell'importo complessivo di Euro 35.000,00 (trentacinquemila/00), oltre al rimborso di Euro 200,00 a titolo di risarcimento del danno derivante dalla sopportazione dei costi connessi all'assistenza professionale.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE