

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) VITERBO	Membro designato dalla Banca d'Italia
(BA) NUZZO	Membro designato dalla Banca d'Italia
(BA) BUSSOLI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore CANDIDA BUSSOLI

Seduta del 09/02/2026

FATTO

Il ricorrente dichiara di aver subito una frode informatica il 25 marzo 2025 da parte di persone non identificate. Queste, approfittando della sua età e utilizzando tecniche manipolatorie avanzate, lo hanno convinto che stesse autorizzando, tramite il proprio telefono cellulare, degli accrediti in entrata sul suo conto bancario. In realtà, senza rendersene conto, ha autorizzato bonifici immediati in uscita verso conti intestati a terze persone, presumibilmente complici dei truffatori.

Evidenzia che, nonostante la convalida finale dei bonifici sia riconducibile al dispositivo del cliente vittima di social engineering, l'evento critico risiede in una vulnerabilità tecnica che ha consentito agli aggressori di infiltrarsi nel sistema o di predisporre le operazioni illecite.

Ritiene che ignoti siano *“riusciti ad entrare nel conto corrente”* e a *“disporre i bonifici in contestazione, poi fatti autorizzare a sua insaputa dalla vittima, odierna ricorrente”*.

Afferma che, in seguito alla conclusione delle proprie indagini interne, la banca non ha fornito l'indirizzo IP da cui sono partiti gli ordini di bonifico in contestazione. Segnala che le operazioni in questione partivano da un luogo con un indirizzo IP diverso da quello da cui il proprio smartphone era collegato. Osserva che la Banca, a giustificazione della regolarità dell'operazione, richiama un bonifico di € 25,00 a favore della medesima beneficiaria di quelli contestati, che non è stato disconosciuto. Precisa che tale bonifico era stato disposto in buona fede dal cliente su indicazione dei truffatori, che avevano fatto credere che si trattasse di un versamento iniziale a favore di una società d'investimento. Chiarisce che solo successivamente, dopo il furto integrale dei fondi e dopo aver consultato l'estratto conto, ha scoperto che la beneficiaria non era una società, bensì una persona fisica sconosciuta, prestanome dei truffatori. Riferisce di essere ancora in attesa della conclusione delle indagini preliminari.

Segnala che i tre bonifici di importo pari a € 4.995,00 sono stati effettuati con procedura istantanea e in rapida successione e che, in passato, non aveva mai disposto operazioni analoghe.

Lamenta che la banca ha attivato di default la funzione dei bonifici istantanei, senza ottenere un consenso consapevole e informato da parte del cliente; non ha previsto limiti giornalieri agli importi bonificabili, né blocchi automatici per operazioni anomale; non ha effettuato verifiche di congruità sulle operazioni e non ha attivato alcuna procedura antifrode rafforzata.

Esclude la sussistenza di una sua colpa grave, in ragione della tipologia di frode (vishing) e della mancata condivisione delle credenziali con i truffatori.

Il ricorrente contesta l'operato dell'istituto sotto tre profili principali. In primo luogo, eccepisce la mancata produzione di prove tecniche che escludano l'intervento da remoto sul proprio dispositivo, ritenendo insufficiente la generica affermazione della banca sull'inviolabilità dello smartphone. In secondo luogo, censura la condotta della banca che, dopo un primo riaccredito delle somme, ha effettuato un nuovo addebito unilaterale e senza autorizzazione. Infine, lamenta l'ingiustificato ritardo nella gestione della pratica.

Fa presente che parte della somma complessivamente sottratta (€ 5.000,00) proviene da un fido offertogli dalla banca stessa, la quale, pertanto, può essere considerata vittima di truffa.

Chiede, pertanto, di disporre la restituzione in proprio favore della somma complessiva di € 14.986,86, ovvero di quella ritenuta equa in base alla valutazione dell'illecito, con condanna alle spese di procedura, ove previste.

L'intermediario, costituitosi, evidenzia che, in data 18/02/2025, la controparte, interessata a effettuare investimenti finanziari, durante una navigazione sul web, veniva a conoscenza di un sito che offriva la possibilità di ampi guadagni, censito come rischioso.

Si osserva che il ricorrente ha inizialmente disposto un bonifico istantaneo di € 250,00 con causale 'trasferimento' verso una piattaforma di trading. Tale operazione, inizialmente segnalata come sospetta dai sistemi di sicurezza della banca e posta in stato di sospensione, è stata autorizzata solo dopo le verifiche che hanno confermato l'intenzione d'investimento del cliente. Si evidenzia, inoltre, che la transazione è avvenuta correttamente tramite l'applicazione mobile installata sul dispositivo certificato dell'utente, la cui associazione risaliva al 12/11/2022 e risultava coerente con lo storico operativo e l'indirizzo IP abituale.

Riferisce che il ricorrente veniva contattato da un sedicente consulente finanziario, con il quale, nei giorni a seguire, intratteneva diverse videochiamate e, in data 20/02/2025, seguendo le istruzioni del sedicente consulente, effettuava un secondo bonifico istantaneo di € 25,00 durante una videochiamata, non richiamato (recall), così come quello posto in essere un paio di giorni prima.

Riferisce, inoltre, che il ricorrente richiedeva assistenza telefonica alla presenza del figlio a seguito di alcuni malfunzionamenti riscontrati sulla piattaforma di trading. Durante alcune videochiamate, il ricorrente compiva azioni non precisate sul proprio smartphone. Successivamente, il 25/02/2025, il ricorrente riceveva un'ulteriore chiamata che lo avvisava di un presunto blocco dei conti; insospettito, si recava in filiale, dove risultava l'avvenuta esecuzione di tre bonifici istantanei, pari a € 25,00, a favore dello stesso beneficiario della precedente operazione. Nonostante l'avvio immediato delle procedure di revoca (recall) da parte della banca, le richieste di recupero ricevevano esito negativo.

Evidenzia alcune incongruenze nella ricostruzione della controparte, in quanto, a fronte della telefonata ricevuta alle ore 12:00, i bonifici risultano eseguiti tra le 10:01 e le 10:33. Osserva, inoltre, che i bonifici in questione riportano i medesimi dati tecnici già storicizzati per gli altri eseguiti e non sconosciuti da controparte, come indirizzo IP utilizzato, rete internet e device. Considerati tali dati tecnici e l'operatività della controparte, i bonifici non potevano destare alcun tipo di sospetto, anche solo potenziale, circa l'attività portata avanti in totale autonomia dal ricorrente.

Sostiene, infine, che, trattandosi di operazioni disposte direttamente dal ricorrente, un eventuale sospetto da parte della banca non avrebbe comunque potuto fermarne l'esecuzione. Viene precisato che, anche se la banca fosse stata informata tempestivamente, il suo ruolo si sarebbe limitato a

sconsigliare l'operazione, senza alcuna facoltà di impedirla. Ciò in quanto non sussistevano i presupposti legali per il blocco forzato previsti dall'art. 16 del D.lgs. 11/2010 o dalla normativa antiriciclaggio.

Rileva che, per tutte le attività poste in essere nel frangente incriminato, è presente l'autenticazione a due fattori, che consiste nell'impiego di un user (fattore di conoscenza) e di un device (fattore di possesso).

Aggiunge che, per tutte le operazioni, seguiva l'apposito alert informativo, trasmesso sia tramite push in app sia tramite SMS al numero di cellulare certificato.

Ritiene piuttosto inverosimile che il ricorrente non abbia avuto conoscenza immediata delle operazioni, considerato, tra l'altro, che alle ore 10:57 e 12:04 ha effettuato due ulteriori accessi al servizio di Internet banking tramite il proprio device, potendo visualizzare senza problemi la reale situazione del saldo disponibile.

Richiama la decisione n. 4102/24 del Collegio di Bologna secondo cui l'indirizzo IP è capace di identificare in modo univoco il dispositivo, in quanto è costituito dall'ID di rete (assegnato da un provider di servizi Internet alla rete che si utilizza) e dall'ID host (che è un identificatore univoco assegnato a ogni dispositivo che si connette a quella rete specifica). Aggiunge che, sebbene più di un dispositivo possa condividere lo stesso indirizzo IP esterno (pubblico), ogni dispositivo ha il proprio indirizzo IP locale (privato) che non viene mai condiviso al di fuori della rete domestica privata.

L'intermediario richiama la decisione n. 6732/25 del Collegio di Milano, relativa a casi di truffa legati al trading online. Secondo tale decisione, l'anomalia di un'operazione — sia per l'entità degli importi sia per la novità dei beneficiari — non costituisce di per sé un elemento decisivo per imporre il blocco del conto. Un cliente, infatti, può legittimamente avere la necessità di effettuare pagamenti insoliti o a nuovi soggetti. Inoltre, l'intermediario sostiene l'impossibilità di individuare con precisione il momento in cui avrebbe dovuto sospendere l'operatività, dato che ogni bonifico presentava beneficiari e importi differenti, rendendo difficile l'identificazione della frode.

Fa presente che da tempo attua una massiccia campagna di prevenzione delle frodi al fine di sensibilizzare la clientela.

Chiede, pertanto, in via preliminare, di rigettare nel merito il ricorso, in quanto infondato in fatto e in diritto, e, in via subordinata, in caso fossero ravvisati gli estremi di una concorrenza di responsabilità tra le parti ex art. 1227 c.c., di determinare l'entità delle somme.

Il ricorrente eccepisce di non aver mai disposto o autorizzato i bonifici in contestazione. Sottolinea che i tre bonifici istantanei datati 25 febbraio 2025 sono stati configurati ed eseguiti da terzi malintenzionati. Questi ultimi, attraverso tecniche manipolatorie, hanno indotto il ricorrente in errore, facendogli credere che le autorizzazioni richieste servissero esclusivamente per 'verifiche tecniche' o per ricevere accrediti sul proprio rapporto. Ribadisce, pertanto, la totale assenza di volontà negoziale.

Rileva che la giurisprudenza ABF (Coll. Coord. n. 22745/2019; Milano n. 556/2025) ha chiarito che la regolarità formale dell'autenticazione non prova la volontà dell'utente, né la sua colpa grave.

Sostiene che, ai sensi dell'art. 5 D.Lgs. 11/2010, un'operazione è "autorizzata" solo se il cliente ha espresso un consenso informato e consapevole.

Fa presente di aver provveduto a disconoscere con immediatezza i tre bonifici eseguiti in rapida successione in data 25/02/2025 non appena, recatosi presso la filiale, ne ha constatato la natura fraudolenta.

Segnala che, qualora avesse effettivamente inteso trasferire con urgenza l'intera disponibilità del proprio conto, si sarebbe avvalso di un unico bonifico istantaneo fino all'importo massimo consentito di € 15.000,00, previsto dal contratto di conto corrente per operazioni dirette a un singolo beneficiario. Osserva che la suddivisione della somma totale in tre bonifici distinti da € 4.995,00 ciascuno costituisce una prova inequivocabile di una strategia fraudolenta. Tale frazionamento degli importi è infatti una tecnica tipica dei criminali informatici, utilizzata appositamente per aggirare i sistemi di monitoraggio automatico e evitare che le soglie di allerta dei controlli antiriciclaggio e antifrode facciano scattare il

blocco immediato delle transazioni.

In merito alla tesi dell'intermediario, secondo cui l'uso dell'indirizzo IP abituale confermerebbe la regolarità degli ordini, obietta che tale dato non è idoneo a dimostrare l'identità del reale esecutore. L'indirizzo IP identifica, infatti, esclusivamente il punto di accesso alla rete e non la persona fisica, potendo inoltre essere facilmente manipolato da terzi. Ritiene che il richiamo di controparte alla decisione del Collegio di Bologna n. 4102/2024 sull'identificazione univoca dell'indirizzo IP sia del tutto inconferente con il caso di specie, che attiene a una frode con inganno della volontà del titolare, non ad un accesso tecnico non autenticato.

Insiste pertanto per l'accoglimento del ricorso.

Nelle controrepliche, l'intermediario evidenzia che, in sede di repliche, il ricorrente ha confermato la personale esecuzione dei bonifici, pur non essendone consapevole sul piano volitivo.

L'intermediario sostiene che l'autorizzazione fornita dal cliente sia valida ai sensi dell'art. 5 del D.lgs. 11/2010, nonostante la mancanza di una reale consapevolezza sulla natura delle operazioni. Il fatto che l'inserimento e la convalida dei bonifici siano stati effettuati materialmente dal titolare esclude la possibilità di disconoscere le operazioni come estranee. Si configurerebbe invece una fattispecie di truffa subita dal cliente (citando il precedente del Collegio di Bari, n. 3833/2025), in cui il consenso è tecnicamente esistente, anche se frutto di inganno.

Fa presente di aver chiaramente e inequivocabilmente documentato l'indirizzo IP associato al dispositivo certificato del ricorrente anche in eventi pregressi non disconosciuti dal cliente.

Ritiene inverosimile un'eventuale manipolazione o condivisione dell'indirizzo IP e rileva che il ricorrente non ha in alcun modo contestato gli ulteriori log prodotti in sede di controdeduzioni, che devono conseguentemente ritenersi confermati. Insiste per il rigetto del ricorso.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di n. 3 operazioni di bonifico eseguite in data 25/02/2025 per € 4.995,00= ciascuna. È in atti la denuncia del cliente presentata in pari data.

Preliminarmente va rigettata l'eccezione del ricorrente di illegittima attivazione, da parte dell'intermediario, del servizio di "bonifico istantaneo" per difetto di previo consenso specifico, consapevole e informato, nonché per la dedotta configurazione del servizio in assenza di idonei limiti giornalieri agli importi disponibili.

In merito all'introduzione della funzionalità di bonifico istantaneo si è pronunciato il Collegio di Coordinamento, affermando il principio secondo cui: *"La proposta al consumatore di introduzione della modalità di pagamento tramite bonifico istantaneo, ai sensi dell'art.126-sexies, comma 4-bis, del T.U.B., può essere validamente formulata se corredata da una informazione completa e corretta delle relative caratteristiche. Tale non è quella che si limiti a evidenziare il costo del bonifico istantaneo, a conferma implicita della nuova opportunità offerta al destinatario, senza indicazione della caratteristica della irrevocabilità della operazione, determinativa dell'aumento del rischio in capo all'ordinante"*.

Al riguardo, dalla documentazione versata in atti e dalle stesse dichiarazioni rese dal ricorrente in sede di repliche emerge che la funzionalità di bonifico istantaneo risultava già compiutamente disciplinata nel contratto di conto corrente, con previsione di un limite operativo giornaliero pari ad euro 15.000, così evidenziandosi, da un lato, l'assenza di una modificazione unilaterale delle condizioni contrattuali da parte dell'istituto di credito e, dall'altro, la sussistenza di un predeterminato limite di spesa.

Nel merito, il Collegio rappresenta che le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.1.2010, 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 13.1.2018, nonché delle nuove disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), normate dal Regolamento Delegato (UE) della Commissione, del 27

novembre 2017, n. 2018/389, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (cfr. anche il disposto dall'art. 5, d. lgs. n. 11/2010, come novellato).

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 comma 2 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 viene, altresì, precisato che è *“onere del prestatore di servizi di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente”*.

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, nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Fatte queste premesse, venendo alle operazioni in esame, il Collegio osserva che il presupposto per l'applicazione della suddetta disciplina è che ciascuna operazione disconosciuta dal ricorrente sia un'operazione effettivamente non autorizzata dal medesimo.

Dalla narrazione dei fatti e dalla documentazione in atti risulta che il ricorrente ha autorizzato personalmente le operazioni contestate, seppur inconsapevolmente a causa del raggirio perpetrato da terzi, che lo avevano convinto di dover autorizzare accrediti o verifiche sul proprio conto, mentre in realtà stava disponendo bonifici istantanei in uscita verso un terzo beneficiario.

La documentazione tecnica prodotta dall'intermediario (log SCA, storico device, indirizzo IP, tracciate di login e disposizione) conferma che le operazioni sono state effettuate tramite il device certificato già da tempo associato al cliente, utilizzato anche per operazioni pregresse non disconosciute, e con la medesima combinazione di fattori di autenticazione (user e dispositivo) impiegata nelle altre operazioni lecite.

Orbene, secondo l'orientamento costante dell'Arbitro manifestatosi in casi analoghi, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è, quindi, soggetta al regime di

responsabilità previsto dalla PSD2 (v. ex multis Collegio di Bari, decisioni nn. 4869/2023 e 5468/2022; Collegio di Napoli, decisione n. 1683/2022; Collegio di Milano, decisione n. 3949/2022).

Il Collegio ritiene, tuttavia, che sebbene non sia configurabile – come appena chiarito – una responsabilità oggettiva del PSP, tuttavia, nel caso in cui, sulla base delle evidenze disponibili e secondo le norme di diritto comune, emerga in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode può sussistere una sua responsabilità (così Collegio di Bari, decisione n. 9279/2024; Collegio di Bologna, decisione n. 9454/2024). Tanto può accadere, esemplificativamente, nei casi di:

- a) mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;
- b) mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore;
- c) mancato rilievo di indici di frode nel caso in cui 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 di specie, non sembrano riscontrabili dalle dichiarazioni delle parti tali circostanze.

Tuttavia, con riguardo agli indici di frode appena evocati, l'art. 8 del d.m. 30/04/2007, n. 112 (recante il regolamento di attuazione della l. n. 166/2005, sulla "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento") dispone che "si configura il rischio di frode di cui all'art. 3, co. 1, della legge, quando viene raggiunto uno dei seguenti parametri:

- a) con riferimento ai punti vendita di cui all'art. 7, lett. b):
 - 1) cinque o più richieste di autorizzazione con carte diverse, rifiutate nelle 24 ore, presso un medesimo punto vendita;
 - 2) tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita;
 - 3) richiesta di autorizzazione, approvata o rifiutata, che superi del 150% l'importo medio delle operazioni effettuate con carte di pagamento, nei tre mesi precedenti, presso il medesimo punto di vendita;
- b) riguardo alle carte di pagamento sottoposte a monitoraggio di cui all'art. 7, lett. c):
 - 1) sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento;
 - 2) una ovvero più richieste di autorizzazione che nelle 24 ore esauriscano l'importo totale del plafond della carta di pagamento;
 - 3) due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti".

Nel caso in esame, sono stati eseguiti tre bonifici nell'arco di 24 ore verso lo stesso beneficiario. Il ricorrente in effetti ne contesta il carattere anomalo rispetto alla propria operatività abituale, sostenendo che l'intermediario avrebbe dovuto provvedere a bloccarle.

In un caso del genere, è necessaria una valutazione circa i presidi adottati dall'intermediario, come per esempio l'esistenza di un sistema di monitoraggio. Sul punto, si registrano diverse pronunce dell'ABF che applicano analogicamente i suddetti indici di frode alle operazioni disposte tramite home banking (cfr. Collegio di Milano, decisione n. 16207 del 2021; Collegio di Milano, decisione n. 334 del 2022).

In effetti, non sembra che la conclusione possa mutare in caso di pagamenti online, come avvenuto nel caso di specie.

Sebbene il citato decreto si riferisca alle operazioni effettuate con carta, esso è stato ritenuto applicabile ai bonifici online sulla base dell'unità di ratio (cfr. Collegio di Roma, decisione n. 17037/2020, Collegio di Napoli, decisione n. 15042/2022, Collegio di Milano, decisione n. 13673/2022).

Alla luce degli Orientamenti EBA sui pagamenti via internet e del Regolamento EBA n. 2018/389, nonché dei principi elaborati dai Collegi, il PSP diligente ex art. 1176, comma 2, c.c. è gravato dall'obbligo di predisporre sistemi di monitoraggio in grado di intercettare operazioni anomale per

numero, importo, frequenza, tipologia e beneficiario, attivando – prima dell'autorizzazione definitiva – meccanismi di blocco o verifica aggiuntiva idonei a interrompere il perfezionamento delle transazioni sospette.

Orbene, sulla base di quanto emerso in istruttoria, va evidenziato che l'intermediario risulta aver adottato un sistema di monitoraggio idoneo a intercettare operazioni potenzialmente anomale, come dimostra il blocco iniziale del bonifico di euro 250,00, classificato come operazione "sospetta", nonché il successivo accertamento della volontà del ricorrente di voler effettuare investimenti.

Tale sequenza dimostra che i presidi antifrode e i controlli interni della banca hanno effettivamente funzionato, attivandosi sul primo segnale di rischio e consentendo una verifica diretta con il titolare del rapporto, che ha espressamente manifestato l'intenzione di proseguire nell'operatività; ne consegue che non possono essere imputati all'intermediario né carenze nel sistema di monitoraggio, né omissioni di interventi doverosi rispetto alle operazioni poi oggetto di contestazione.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE