

COLLEGIO DI BARI

composto dai signori:

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

Relatore FRANCESCO GIACOMO VITERBO

Seduta del 17/12/2025

FATTO

Il ricorrente, rinviando al reclamo per la descrizione dell'oggetto della controversia, riferisce di aver subito il furto del telefono cellulare in data 9 maggio 2025 alle ore 13:30 e che i malfattori sono riusciti ad accedere all'app della banca e a disporre numerose operazioni fraudolente.

Rappresenta che, dopo numerosi tentativi, riusciva a contattare la resistente solo alle ore 14:57, chiedendole di bloccare ogni accesso da remoto al conto corrente e ricevendo rassicurazioni in merito. Evidenzia che, ad eccezione di un bonifico di € 2.000,00 eseguito prima della telefonata, a partire dalle 15:50 venivano eseguiti numerosi pagamenti POS, che si protraevano sino ai due giorni successivi al denunciato furto e alla segnalazione prevenuta alla banca.

Afferma che il furto è avvenuto con destrezza e di non aver conservato nel telefono i codici di accesso all'app, come asserito dall'intermediario nel riscontro al reclamo.

Lamenta la grave vulnerabilità dei sistemi di sicurezza adottati dalla banca, atteso che i truffatori tramite il solo telefono sono riusciti ad accedere all'applicazione dell'intermediario, a disporre il bonifico di € 2.000,00, nonché ad attivare da remoto una carta di debito non ancora resa operativa, poiché ricevuta da pochi giorni, e tramite la stessa a eseguire tutti gli acquisti tramite pos.

Precisa che la carta fisica è sempre rimasta nella sua disponibilità.

Sostiene, dunque, che le operazioni contestate sono riconducibili alla negligenza della resistente, la quale non ha provveduto al blocco dell'applicazione, nonostante la segnalazione del furto.

Ritiene, inoltre, incomprensibile la scelta della resistente di rimborsare solo gli addebiti eseguiti dalle ore 14:32 dell'11 maggio 2025 e non anche quelli precedenti.

Chiede, pertanto, il rimborso dell'importo di € 5.655,69.

Costituitosi, l'intermediario afferma che parte ricorrente chiede il rimborso delle somme sottratte in maniera fraudolenta tra il 9 e l'11 maggio 2025, a seguito del furto del cellulare. Precisa che le operazioni contestate consistono in un bonifico di € 2.000,00 e n. 38 operazioni con carta di debito per un totale di € 4.940,79, di cui n. 5 eseguite il 09/05, n. 8 il 10/05 e n. 25 l'11/05.

Afferma di aver provveduto al rimborso delle operazioni eseguite in data 11 maggio 25, a partire dalla n. 8, per un totale di € 1.300,50, giustificando il diniego al rimborso delle altre operazioni per una palese violazione delle disposizioni contrattuali.

In punto di fatto, ripercorre quanto comunicato dal ricorrente nella nota del 14 maggio 2025: questi ha subito il furto alle ore 13:30 del 9 maggio 2025, ha cercato invano di chiamare una filiale della banca alle ore 13:39 in quanto chiusa per la pausa pranzo, è riuscito a contattare tale filiale alle ore 14:57, segnalando l'avvenuto furto e chiedendo il blocco dell'app.

Ciò posto, afferma che il servizio di Internet banking, le operazioni di pagamento contestate e la tokenizzazione della carta di debito hanno rispettato la normativa in materia di SCA, allegando a tal fine una relazione tecnica.

Premette che l'app di home banking, associata al numero di cellulare del ricorrente, è stata attivata in data 1° dicembre 2024 sul dispositivo "s*****6B", tramite inserimento delle credenziali statiche e del codice OTP. Rileva che anche l'app relativa alle notifiche, collegata al numero di cellulare certificato del ricorrente, risulta scaricata già dal 23 novembre 2023.

Precisa che il giorno della truffa l'accesso all'app di home banking è avvenuto mediante l'utilizzo del dispositivo sul quale era presente l'app e inserimento del codice Pin alle 14:22 e alle successive 14:33 è stata inserita la prima operazione di bonifico istantaneo di € 2.000,00, autorizzata mediante codice Pin. Specifica che tale operazione è stata comunicata anche tramite e-mail, nella quale era indicato il beneficiario dell'operazione, l'iban e la sua banca.

Evidenzia che, successivamente, è stata tokenizzata la carta n. *034 in un wallet digitale tramite l'app della banca, illustrandone i passaggi. Afferma che, a tal punto, sono state disposte le operazioni di pagamento POS tramite il wallet, installato sul dispositivo del ricorrente, e inserimento del codice Pin. Quanto alla tokenizzazione, rappresenta che alle 15:01 il sistema ha trasmesso i dati della carta al wallet provider selezionato dall'utente, che ha inviato una richiesta di virtualizzazione della carta a seguito della corretta trasmissione delle credenziali statiche trasmesse dall'app della banca al wallet. Saggiunge che il sistema ha associato al wallet un codice identificativo, rispondendo positivamente alla richiesta di virtualizzazione.

La conferma di virtualizzazione della carta è pervenuta successivamente al sistema e all'app della banca associata all'utenza abilitata.

Segnala che tutte le operazioni contestate sono state eseguite utilizzando il wallet installato sul dispositivo del cliente, secondo i parametri SCA.

Saggiunge che, per le operazioni di importo pari o superiore a € 200,00, è stato inviato al ricorrente il relativo alert tramite SMS.

Quanto alla colpa grave, eccepisce anzitutto la carenza di allegazioni e la mancata ricostruzione dei fatti, in quanto il ricorrente si limita a dichiarare di aver subito l'utilizzo fraudolento della carta di debito a seguito del furto del telefono. Ritiene che la generica rappresentazione dei fatti induca a supporre che il ricorrente abbia incautamente conservato il cellulare nella tasca della giacca o, comunque, in un posto esposto alla pubblica visibilità, nonché abbia conservato al suo interno i codici di accesso e password. Fa presente, difatti, che l'accesso all'app e la tokenizzazione della carta sono stati possibili solo grazie alla negligente custodia dei codici di accesso da parte del ricorrente, nonché del device.

Segnala che il breve lasso temporale tra il furto e l'accesso all'app confermi la violazione degli obblighi di custodia da parte del ricorrente e, dunque, la sua colpa grave.

Richiama, infine, alcune decisioni dei Collegi ABF secondo cui la colpa grave può desumersi anche dal luogo in cui avviene il furto, sottolineando che un luogo pubblico o aperto al pubblico dovrebbe innalzare la soglia di attenzione del cliente.

Conclude, sostenendo che la truffa si è realizzata grazie alla facilità con cui i malfattori hanno avuto accesso ai dati presenti sul cellulare e non alla vulnerabilità del sistema informatico.

Alla luce di quanto ricostruito, chiede preliminarmente di dichiarare la carenza di allegazione e rappresentazione da parte del ricorrente e, nel merito, il rigetto del ricorso; in subordine, di accertare il concorso di colpa del ricorrente nella determinazione del danno.

In sede di repliche, il ricorrente eccepisce anzitutto di aver esaurientemente illustrato tutti i presupposti fattuali della vicenda e le motivazioni sottese alle proprie richieste in sede di ricorso. Saggiunge di aver allegato a tal fine anche copia dell'integrazione di querela del 28 giugno 2025.

Rileva poi, quanto all'autenticazione forte, che i codici OTP sono stati inviati al cellulare che in quel momento si trovava in possesso dei truffatori.

Ribadisce di aver cercato di contattare la resistente per bloccare l'app subito dopo il furto, precisamente alle ore 13:39, e di esserci riuscita solo alle successive 14:57, in quanto prima gli uffici erano chiusi per la pausa pranzo. Afferma che la banca assicurava di aver provveduto al completo blocco di ogni accesso da remoto al conto corrente; tuttavia, le operazioni fraudolente sono state eseguite sino a due giorni dopo il furto e la tempestiva segnalazione dello stesso. Precisa di aver richiesto il blocco totale anche con successive telefonate delle ore 15:07, 16:05 e 16:09 del giorno del furto.

Fa presente che la resistente non ha provveduto nemmeno a bloccare la carta di debito collegata al conto corrente, attivata dagli stessi malfattori. Ribadisce difatti che tale carta, al momento del furto, non era stata ancora da lui attivata in quanto di recente emissione.

Osserva, altresì, che tra il furto e il primo bonifico non è intercorso un breve lasso di tempo, ma circa un'ora, posto che il furto è avvenuto alle ore 13:30 e il bonifico è stato eseguito alle ore 14:33.

Ritiene, al contrario, che proprio il notevole lasso di tempo trascorso tra il furto e la disposizione fraudolenta in parola è sintomatico della circostanza che il pin non fosse stato custodito nel dispositivo, altrimenti il bonifico sarebbe stato eseguito con molta più tempestività.

Segnala che la carta, che si trovava al momento del furto del telefono ancora in busta chiusa presso il domicilio dell'intestatario, distante dal luogo del furto, è stata attivata dai malfattori, senza il supporto fisico, direttamente dall'app del telefono sottratto al ricorrente. Saggiunge che il Pin per l'attivazione della carta di debito era molto banale, consistendo in una sequenza di cinque 2, dunque, facilmente individuabile dai malfattori.

Rileva, infine, che la banca non dimostra l'impossibilità di reperire il pin nelle memorie nascoste del dispositivo come cache, memorie interne.

Tanto premesso, insiste per l'accoglimento del ricorso.

In sede di controrepliche, l'intermediario eccepisce preliminarmente l'inammissibilità delle nuove deduzioni, circostanze di fatto e documentazioni prodotte dal ricorrente in sede di repliche, in quanto volte ad ampliare la domanda iniziale, piuttosto che a puntualizzare difese già svolte.

In particolare, ritiene che siano state sottaciute in sede di ricorso: gli ulteriori tentativi di chiamate; le molteplici richieste di blocco; le contestazioni riguardanti il pin e le ulteriori documentazioni allegate.

Ritiene, difatti, che il ricorrente abbia inteso rimediare all'insufficienza delle allegazioni contenute nel ricorso, solo perché contestata nelle controdeduzioni.

Ad ogni modo, evidenzia che tale documentazione non consente di ricostruire le modalità di custodia delle credenziali e le circostanze che hanno consentito l'uso fraudolento degli strumenti di pagamento. Sostiene di aver bloccato l'accesso all'app non appena ricevuta comunicazione dell'accaduto, *“anche se ciò non ha impedito che i malfattori avessero già eseguito l'operazione di bonifico (alle ore 14:22, a meno di un'ora dal furto del telefono)”*.

Ritiene che sia onere del ricorrente provare l'impossibilità di reperire il pin nelle memorie del telefono e che il pin di attivazione della carta, seppur ritenuto banale, non può fondare alcuna responsabilità della banca, dato che la sua generazione segue procedure standardizzate.

Sottolinea, comunque, che la carta è stata tokenizzata nel wallet solo perché i malfattori avevano avuto accesso all'app.

Ribadisce, infine, che le operazioni sono state eseguite rispettando i parametri SCA, senza anomalie e malfunzionamenti.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto al rimborso dell'importo di € 5.655,69 corrispondente all'ammontare complessivo di n. 21 operazioni, disposte tra il 9 e l'11 maggio 2025, di cui n. 1 bonifico di € 2.000,00, più € 2,00 di commissioni e n. 20 pagamenti POS per un totale di € 3.653,69, tutte successivamente disconosciute.

In via preliminare, il Collegio ritiene priva di pregio l'eccezione opposta in sede di controrepliche dall'intermediario in ordine alla tardività della documentazione allegata dal ricorrente in sede di repliche, al fine di ampliare la domanda iniziale. Difatti, in sede di repliche, il ricorrente ha allegato uno screen shot delle telefonate intercorse con la banca il giorno del furto, una foto della nuova carta di debito con il relativo codice pin e copia dell'integrazione alla denuncia del 28 giugno 2025. Ciò non di meno, sul punto il Collegio richiama l'orientamento dei Collegi territoriali che considera ammissibile la nuova documentazione prodotta in sede di repliche, fermo il divieto di domande nuove (cfr., *ex multis*, Collegio di Bari, decisione n. 4694/23).

Inoltre, il Collegio rileva che la resistente ha prodotto evidenze comprovanti la circostanza di aver già rimborsato al ricorrente un importo di € 1.300,50 corrispondente ad ulteriori 18 operazioni dell'11 maggio 2025, perciò non contestate dal ricorrente, e ad un'operazione del 10 maggio 2025 di € 23,40 che, invece, rientra tra quelle contestate. Segnatamente, il ricorrente dà atto di tale rimborso, ma ricomprende nella somma richiesta di € 5.655,69 anche l'operazione di € 23,40, già rimborsata dall'intermediario. Pertanto, il Collegio procede con l'esame del ricorso limitatamente all'importo di € 5.632,29 (€ 5.655,69 - € 23,40), corrispondente a n. 1 bonifico di € 2.000,00, più € 2,00 di commissioni e n. 19 pagamenti POS (anziché 20).

Nel merito, il Collegio rileva che tali operazioni sono state eseguite 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 gennaio 2018. Inoltre, le operazioni contestate dal ricorrente sono state eseguite successivamente all'entrata in vigore delle disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del 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 dell'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, comma 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento della Banca d'Italia del 5 luglio 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 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".

Ai sensi del successivo art. 12, comma 2 bis, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Per "autenticazione forte" 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" (art. 1, lett. q-bis, d.lgs. 11/2010). Deve, inoltre, ritenersi che gli elementi selezionati devono essere reciprocamente indipendenti, sì che la violazione di un elemento non deve compromettere gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione.

Si deve, altresì, rilevare che l'art. 10-bis, comma 1, d.lgs. 11/2010, stabilisce che "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".

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). 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" (Collegio di Coordinamento, decisioni n. 3947/2014 e, da ultimo, n. 22745/2019, 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, comma 2, d.lgs. n. 11/2010).

Tratteggiato il quadro normativo di riferimento, venendo al caso di specie, ritiene il Collegio che il ricorso possa trovare parziale accoglimento, nei limiti e per le ragioni qui di seguito specificati.

In merito all'autenticazione delle operazioni contestate, deve distinguersi la fase di accesso all'app e di esecuzione del bonifico di € 2.000,00 dal successivo processo di virtualizzazione della carta di debito sul device e di autorizzazione delle successive operazioni di pagamento.

Riguardo alla fase di accesso all'app, l'intermediario eccepisce che essa è stata correttamente autenticata ed autorizzata e, a supporto di quanto affermato, produce: a) i log relativi all'app della

banca, da cui si evince il riferimento al dispositivo utilizzato (SAM***6B), fattore di possesso, che coincide con quello su cui era stata in precedenza installata l'app; b) una relazione tecnica, in cui fa presente che il corretto inserimento del secondo fattore, definito genericamente come "*PIN/biometria*", sarebbe evincibile dalla presenza della "p" nel paragrafo 3.2. Al riguardo, va precisato che, secondo l'orientamento dei Collegi, ai fini della prova della SCA possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione (cfr. Collegio di Bari, decisione n. 13216/2024; Collegio di Torino, decisione n. 11213/2024; Collegio di Milano, decisione n. 12404/2024). Nel caso di specie, l'intermediario ha corredato la produzione documentale relativa ai fattori utilizzati per autorizzare l'accesso all'app con l'esplicazione di quanto ivi riportato, di modo che essi risultano conformi alla SCA, in quanto consistenti in un fattore di possesso (app installata sul device del ricorrente) e un fattore di conoscenza (PIN).

Riguardo alla disposizione del bonifico istantaneo di € 2.000,00, l'intermediario ha prodotto evidenze da cui si evincono i fattori utilizzati per autorizzare tale operazione, che risultano essere l'accesso all'app dal dispositivo su cui era stata in precedenza installata (fattore di possesso) e l'autenticazione tramite PIN (fattore di conoscenza).

Rispetto all'operazione di bonifico, dunque, questo Collegio – in linea con i propri precedenti relativi a casi analoghi (cfr. Collegio di Bari, decisioni n. 7434/2024; n. 6494/2024; n. 12554/22; n. 13718/22) – ritiene che il sistema di sicurezza adottato dall'intermediario sia conforme alla SCA e che la documentazione prodotta sia idonea a dimostrare la corretta autenticazione e la regolarità formale dell'operazione disconosciuta.

Passando all'analisi del profilo attinente alla colpa grave del ricorrente, il Collegio rileva che quest'ultimo ha dichiarato che il furto è avvenuto in una strada pubblica, ove un ladro avrebbe sfilato il telefono dalla tasca della sua giacca tra le 13:13 e le 13:30. Sul punto, si richiama l'orientamento dell'Arbitro secondo il quale, nei luoghi pubblici o aperti al pubblico, ove più elevato è il rischio di furto, è onere dell'utilizzatore adottare adeguate misure di protezione dei propri beni (cfr. Collegio di Roma, decisione n. 2012/2023, che ha ritenuto sussistente la colpa grave del ricorrente che aveva subito il furto dello strumento di pagamento mentre si trovava all'interno di un centro commerciale, per non avere adoperato la necessaria diligenza nella custodia in "luogo pubblico"). Inoltre, dalla documentazione contrattuale in atti, si evince che il ricorrente non ha dimostrato nulla in merito al blocco del telefonino oggetto del furto (cfr. Collegio di Torino, decisione n. 4723/2025) e non ha neppure effettuato il blocco della propria utenza con SMS al numero indicato nel Documento di sintesi, adempimento a cui era tenuto in base al contratto di conto corrente in essere nel caso di impossibilità a contattare la banca telefonicamente (tale impossibilità è stata evidenziata dallo stesso ricorrente). Infine, la circostanza – desumibile dai log dell'app – che l'operazione disconosciuta sia stata eseguita con successo dopo due soli tentativi di accesso non andati a buon fine (alle 14.13 e alle 14.18) e in un arco temporale relativamente breve tra il furto e l'utilizzo fraudolento (la prima operazione disconosciuta è stata eseguita alle 14.33, circa un'ora dopo il furto) costituiscono indizi gravi, precisi e concordanti in ordine al fatto che l'utente non ha custodito diligentemente i codici, agevolando il terzo malfattore nella realizzazione del suo disegno criminoso (cfr. in termini Collegio di Bari, decisioni nn. 2347/22; 3025/2020; e 19816/2019).

Alla luce di tali considerazioni, ritiene il Collegio che la domanda del ricorrente di rimborso dell'importo oggetto della disposizione di bonifico contestata non possa trovare accoglimento.

Può trovare, invece, accoglimento la domanda di rimborso del controvalore complessivo delle operazioni di pagamento tramite POS disconosciute e non rimborsate dall'intermediario, per un importo di € 3.630,29.

Difatti, per eseguire tali operazioni, la carta di debito di titolarità del ricorrente, associata al suo numero di telefono abilitato, è stata registrata su un wallet digitale. Orbene, dalla documentazione in atti e dalle

affermazioni dell'intermediario non sembra evincersi alcun riferimento ai fattori di autenticazione utilizzati per la fase di tokenizzazione, ricavandosi soltanto la trasmissione dei dati della carta dall'app della banca al digital wallet. Nessun riferimento ai fattori impiegati emerge, altresì, dai log dell'app della banca prodotti dalla resistente che, alle ore 15:01 del 9 maggio 2025, recano soltanto riferimenti all'attività A2A, descritta in legenda come trasmissione dei dati della carta (che secondo l'EBA non integrano né un valido elemento di possesso né di conoscenza), ai dati della carta, a più wallet provider (G***pay menzionato dall'intermediario, ma anche S***pay), alla modalità di pagamento "C****-to-**y e ad "authorizationCode" non meglio specificati. Sul punto, il Collegio richiama la recente decisione n. 9559/2024, ove si afferma che "non è in discussione il fatto che sia la tokenizzazione dello strumento di pagamento sia i successivi pagamenti effettuati mediante wallet richiedano, in virtù dell'art. 10-bis, comma 1, d.lgs. 11/2010, la procedura di autenticazione forte"; e la decisione n. 21285/21 del Collegio di Coordinamento, il quale ha ritenuto che, in mancanza di prova dell'autenticazione forte per la digitalizzazione delle carte, l'intermediario sopporta integralmente le conseguenze delle operazioni disconosciute.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 3.630,29.

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