

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 11/05/2026

FATTO

Il ricorrente, titolare di una carta di credito e di un conto corrente presso la resistente, riferisce che, in data 23 marzo 2025, riscontrava sul proprio conto tre operazioni di pagamento da lui non autorizzate (un pagamento del valore di € 243,00 in data 10 marzo 2025 e due pagamenti del valore di € 1.000,00 e di € 1.200,00 in data 18 marzo 2025).

Fa presente di aver presentato denuncia in data 20 marzo 2025 e di aver contestualmente disconosciuto tali operazioni.

Riferisce che la banca accreditava sul c/c le somme relative alle operazioni oggetto di disconoscimento salvo poi procedere al riaddebito delle stesse, comunicandogli che non erano state riscontrate anomalie e che le operazioni risultavano essere state eseguite con la “*conoscenza*” del ricorrente.

Rileva che la banca sostiene di aver inviato, in data 18 marzo 2025, una notifica per l’attivazione dell’app su un nuovo dispositivo, a seguito della quale sarebbero state effettuate le transazioni disconosciute; tuttavia, il ricorrente nega di aver ricevuto SMS o OTP in merito e ribadisce di non aver mai fornito le proprie credenziali.

Contesta la violazione degli obblighi di sicurezza e vigilanza posti in capo alla banca, previsti dalla normativa in materia di autenticazione forte e prevenzione delle frodi (cita gli artt. 8-10 del D.Lgs.

11/2010, artt. 97–98 della Direttiva PSD2 e Linee Guida EBA/GL/2022/06).

Aggiunge che la banca non ha fornito alcuna prova concreta dell'effettiva autenticazione delle operazioni contestate, mancando elementi tecnici quali i log di accesso, gli indirizzi IP, l'identificativo del dispositivo o i *timestamp* delle operazioni, che avrebbero potuto dimostrare la reale provenienza delle stesse e che l'affermazione che le transazioni siano state eseguite “con le credenziali del cliente” è priva di valore probatorio.

Inoltre, sostiene che la banca non ha adottato misure preventive adeguate e che l'assenza di tali cautele dimostra una carenza nel sistema di monitoraggio delle operazioni sospette.

Riferisce che è la stessa banca a riconoscere che l'app del cliente è stata attivata su un nuovo dispositivo, sostenendo quindi che tale evento costituisce un’*“anomalia comportamentale”* che richiede l'adozione di misure di sicurezza rafforzate, come la sospensione automatica delle funzionalità dispositive o una doppia verifica dell'identità tramite canale alternativo.

Richiama: la decisione del Collegio di Palermo n. 4292 del 30 aprile 2025 secondo cui gli obblighi di “*strong customer authentication*” non riguardano soltanto le operazioni dispositive, ma anche l'*enrollment* o l'attivazione dell'app su un nuovo dispositivo; la decisione del Collegio di Bari n. 3432 del 2 aprile 2025, che ha riconosciuto la responsabilità della banca in assenza di prove tecniche idonee a dimostrare la riconducibilità delle operazioni al cliente, per cui la semplice attestazione dell'invio di un codice OTP non prova l'effettivo utilizzo da parte dell'utente, potendo lo stesso essere stato intercettato da soggetti terzi; la decisione del Collegio di Milano n. 324 del 14 gennaio 2025, in tema di diligenza dell'utente nell'attivazione di un “*Mobile Token*” su nuovo dispositivo, precisando che la responsabilità del cliente sussiste solo quando sia provata una condotta manifestamente negligente o contraria alla comune prudenza; la decisione del Collegio di Roma n. 3052 del 21 marzo 2025 che ha confermato l'obbligo dell'intermediario di fornire prova tecnica completa e verificabile dell'autenticazione, mediante produzione di log di sistema, dati di rete e identificativi dei dispositivi coinvolti.

Per ultimo, richiamando l'art. 11, comma 2, del D.Lgs. 11/2010 che impone all'intermediario di conservare e fornire al cliente le prove dell'autenticazione delle operazioni di pagamento, sostiene che il rifiuto della banca di consegnare la documentazione, subordinandone la visione a un provvedimento dell'autorità giudiziaria, costituisce violazione del principio di trasparenza sancito dall'art. 117-bis del T.U.B. e dalle Disposizioni della Banca d'Italia in materia di gestione dei reclami.

Chiede il rimborso delle somme sottratte pari a € 2.443,00, oltre interessi legali dal 27 ottobre 2025 fino all'effettivo rimborso.

Costitutosi, l'intermediario osserva che l'importo del *petitum* va decurtato della somma di € 243,00 corrispondente all'operazione di pagamento del 10 marzo 2025, che nelle more della presentazione del ricorso è stata rimborsata al ricorrente.

Circa le modalità di funzionamento del servizio *Internet banking*, afferma che, per poter accedere ai servizi online, è richiesto l'inserimento simultaneo di password statiche (PIN e codice Titolare) e password dinamica (OTP), nello specifico impiegata per l'autorizzazione di operazioni dispositive, generata via APP o via SMS.

Precisa che, nel caso di generazione via APP, è necessaria la selezione della notifica ricevuta sullo smartphone associato e la digitazione del PIN o, se abilitati, l'utilizzo dell'impronta digitale o del riconoscimento facciale.

Circa la corretta autenticazione, ritiene che le operazioni in esame, disconosciute dal cliente, siano state eseguite dopo essere state autenticate, correttamente registrate e contabilizzate e non abbiano subito le conseguenze del malfunzionamento delle procedure necessarie per la loro esecuzione o altri

inconvenienti. A sostengo di tale affermazione, produce l'estratto delle registrazioni elettroniche effettuate in occasione dell'operatività disconosciuta dal ricorrente.

Evidenzia che il ricorrente si connette solitamente tramite APP dal proprio *device* identificato con il codice univoco "8b0***26d". Aggiunge che, in data 18 marzo 2025 alle ore 11:40, è stata riscontrata da app un'attività di *enrollment* di un nuovo dispositivo identificato dal codice univoco "F88***53B" in sostituzione del precedente, autorizzato mediante l'inserimento delle credenziali statiche del ricorrente (user e pin) e del codice OTS, inviato a mezzo di sms al numero certificato del ricorrente dal seguente tenore: *"NON CEDERE IL CODICE. Se qualcuno te lo chiede è una frode! Per attivare l'app su "I***", solo se in tuo possesso, usa il codice ***"*, (v. Foglio sms, Riga 3, doc.7 ctd.), che viene inserito (v. Foglio Tracciatura, riga 229, doc.7 ctd.). Aggiunge che, successivamente, il ricorrente ha ricevuto una *push* relativa all'attivazione dell'APP da un nuovo dispositivo, dal testo: *"Stai attivando l'App su "I****". SE QUESTO DISPOSITIVO NON È IN TUO POSSESSO È UNA FRODE! Contatta la Filiale Digitale"*. (v. Foglio push, Riga 12, doc.7 ctd.).

Fa presente che l'operazione di *enrollment* è stata resa possibile solo perché il truffatore era a conoscenza delle credenziali del cliente.

Soggiunge che, in data 18 marzo 2025, alle ore 11:54 e alle ore 11.58, sono stati disposti da APP due pagamenti con carta di credito, rispettivamente di € 1.000,00 e di € 1.200,00, e le transazioni risultano essere state validate con codice OTP previa digitazione del PIN, così come confermato dalla tracciatura fornita dal *provider* (v. colonna O 3DS= S2 che, secondo la legenda significa: transazioni effettuate su commercio elettronico sicuro con autenticazione del titolare nessuna anomalia).

Per quanto attiene alla condotta del ricorrente, evidenzia che quest'ultimo non ha fornito elementi utili alla ricostruzione dei fatti e che la mancata allegazione da parte del cliente di documentazione atta a dimostrare la frode asseritamente patita rappresenta un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la sua colpa grave (richiama *ex multis* le seguenti decisioni: Collegio di Milano n.4016/2025; Collegio di Roma nn .5446/2025, 11050/2024 e 7663/2023; Collegio di Napoli n. 66/2023).

Fa presente, inoltre, che il ricorrente non ha denunciato la perdita di possesso della carta di credito o il malfunzionamento del proprio dispositivo.

Osserva, altresì, che la prima operazione di € 243,00 del 10 marzo 2025, rimborsata, è stata eseguita prima dell'*enrollment* e in tale occasione il ricorrente ha ricevuto una *push* con importo e beneficiario del pagamento.

Da ultimo, segnala che il ricorrente nel novembre 2022 aveva disconosciuto quattro operazioni di pagamento sempre a favore di siti di *bitcoin*.

Sostiene, altresì, di aver adeguatamente informato la clientela sulle tipologie di truffe assimilabili a quella occorsa nel caso di specie e sui comportamenti da adottare per evitarle.

Sostiene, quindi, che deve escludersi ogni responsabilità dell'intermediario, ai sensi degli artt. 7, comma 2, e 12, comma 3, del D. Lgs. n. 11/2010.

Chiede, pertanto, di rigettare il ricorso e, nella denegata ipotesi che il Collegio ritenga di poter ravvisare profili di responsabilità nell'accaduto in capo all'intermediario, di definire la ripartizione fra le parti del danno ai sensi dell'art. 1227, primo e secondo comma c.c., con l'applicazione della franchigia di € 50,00 contemplata dalla normativa in materia di servizi di pagamento.

In sede di repliche, il ricorrente ribadisce di non aver ricevuto, in data 18 marzo 2025, l'OTP per l'attivazione dell'APP sul presunto nuovo dispositivo.

Sostiene che le tracciature fornite dalla resistente in formato 'foglio di calcolo' sono inidonee a dimostrare l'effettiva ricezione del codice e la colpa grave, essendo prive di certificazione tecnica.

Sostiene che l'intermediario avrebbe dovuto monitorare l'associazione del nuovo dispositivo, specialmente alla luce della precedente operazione fraudolenta del 10 marzo 2025 (già rimborsata). Rileva, inoltre, che le operazioni eseguite dal nuovo dispositivo recano un indirizzo IP anomalo e geograficamente incoerente rispetto allo storico del cliente, nonché modalità d'accesso diverse, tramite *fingerprint*.

Aggiunge che, prima delle operazioni del 18 marzo 2025, vi sono stati ripetuti tentativi di accesso, inizialmente dal sito *web* della banca e successivamente finalizzati all'associazione di un presunto nuovo cellulare "I***", come si desume dalle tracciatore di accesso e dalle notifiche *push* prodotte.

Ritiene significativo il fatto che, dopo l'esecuzione delle operazioni di € 1.200,00 e di € 1.000,00, la carta è stata bloccata automaticamente.

Soggiunge che l'assenza di transazioni come quelle disconosciute nella cronologia web, unitamente alla totale estraneità del ricorrente ad acquisti *online* di tale entità, conferma che l'operazione non è a lui riconducibile, evidenziando una falla nei sistemi di sicurezza della banca piuttosto che una negligenza del cliente.

Insiste per l'accoglimento del ricorso.

In sede di controrepliche, l'intermediario precisa che l'allegato 7 alle controdeduzioni reca l'estratto delle registrazioni elettroniche effettuate in occasione dell'operatività disconosciuta dal cliente e riporta i log estratti dagli archivi informatici della banca. Evidenzia l'attendibilità del file prodotto sulla base dell'orientamento condiviso dei Collegi territoriali.

Sostiene che l'importo di € 243,00 relativo all'operazione del 10 marzo 2025 è stato rimborsato in "*un'ottica commerciale*", senza riconoscimento di responsabilità da parte della banca, precisando che il ricorrente ha ricevuto una *push* con riferimento all'operazione effettuata nella predetta data.

Circa il presunto obbligo di vigilanza da parte della banca, richiama la decisione del Collegio di Torino n. 12843/2024 che ha escluso l'esistenza un obbligo generale di monitoraggio *ex ante* in capo all'intermediario.

Insiste per il rigetto del ricorso.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di tre operazioni di pagamento effettuate mediante carta di credito – rispettivamente, di € 243,00 effettuata in data 10 marzo 2025 e di € 1.000,00 ed € 1.200,00 effettuate il 18 marzo 2025, per un valore complessivo di € 2.443,00 –, successivamente disconosciute.

Il Collegio rileva preliminarmente che le operazioni contestate 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, tali operazioni 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 carpirlo 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" (Coll. 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, occorre premettere che il 14 gennaio 2026 l'intermediario ha rimborsato al ricorrente l'importo di € 243,00, riferito all'operazione del 10 marzo 2025. Risultano, perciò, oggetto di controversia soltanto due operazioni di pagamento con carta di credito, rispettivamente di € 1.000,00 ed € 1.200,00 del 18 marzo 2025, per complessivi € 2.200,00. Inoltre, dalla documentazione depositata in atti e dalle dichiarazioni delle parti risulta che la carta è stata bloccata all'esito delle operazioni contestate, per ragioni cautelative, tra le ore 12.05 e 12.07 del 18 marzo 2025 (l'ultima operazione disconosciuta risale alle 11.58 dello stesso giorno). Il blocco risulta definitivamente effettuato il 20 marzo 2025.

L'intermediario, al fine di dimostrare che le operazioni contestate sono state eseguite conformemente alla SCA, ha allegato alle controdeduzioni un file excel di "tracciature informatiche" – che, secondo l'orientamento di questo Arbitro, è mezzo idoneo a fornire la prova della genuinità delle operazioni ivi registrate, considerata anche l'impossibilità per questo Arbitro di disporre CTU – relative all'autenticazione, registrazione e contabilizzazione dell'operazione contestata.

Trattasi di un file composto da cinque fogli, così denominati:

- 1) "anagrafica" (sui dati anagrafici del cliente reperiti nell'archivio del servizio Internet banking);
- 2) "accessi" (sull'elenco degli accessi al servizio effettuati dall'utenza del cliente);
- 3) "tracciatura" (sulla tracciatura informatica delle operazioni disconosciute);
- 4) "sms" (sull'elenco dei messaggi sms inviati al cliente tra il 10 ed il 19 marzo 2025);
- 5) "push" (sull'elenco delle *push notification* inviate all'APP).

Ha prodotto, inoltre, un *file* di tracciature relative alla carta di credito, estratto dal *provider*.

L'intermediario ha fatto, altresì, presente che il ricorrente si connetteva abitualmente all'*home banking* da un determinato *device* identificato con il codice univoco "8b0***26d" e che, tuttavia, in data 18 marzo 2025 alle ore 11:40, è stato riscontrato l'*enrollment* di un nuovo dispositivo, identificato dal codice univoco "F88 *** 53B", in sostituzione del precedente. Al riguardo, ha precisato che, in via generale, per l'*enrollment* di un nuovo *device* sono previsti i seguenti passaggi:

- download e installazione dell'app dallo *store* ufficiale dello smartphone;
- avvio dell'app ed inserimento del codice titolare comunicato dalla banca (presente sul contratto);
- inserimento del pin – codice creato dal cliente;
- inserimento dell'ots – inoltrato al numero di cellulare certificato del cliente;
- secondo inserimento pin a conferma;
- alert inoltrato al cliente che notifica l'avvenuto *enrollment*.

Ciò premesso, nel caso di specie, dalle tracciature prodotte si evince che, alle ore 11:40 del 18 marzo 2025, è stata riscontrata un'attività di *enrollment* tramite inserimento di user e PIN (pin, v. foglio "tracciatura", riga 226-229, colonne I e J, doc.7) e del codice OTS, trasmesso alle ore 11:40:37 al numero di cellulare certificato del ricorrente (+39337***04) a mezzo sms (v. foglio "sms", riga 3, doc.7). Sebbene il ricorrente neghi di aver ricevuto tale SMS, il Collegio rileva, tuttavia, che l'utenza telefonica riportata in tale *log* coincide con quella indicata nel foglio "anagrafica" e che il ricorrente non ha indicato

né in denuncia né nel modulo di ricorso il proprio numero di cellulare. Dal foglio *“push”* (riga 12) risulta, altresì, che, in corrispondenza dell’*enrollment*, il ricorrente ha ricevuto sul proprio *device* (n. ***26d) una *push* di alert, dal testo: *“Stai attivando l’App su “I***”. SE QUESTO DISPOSITIVO NON È IN TUO POSSESSO È UNA FRODE! Contatta la Filiale Digitale”*.

Quanto all’autenticazione delle operazioni di pagamento, dalle tracciature e schermate in atti si evince che:

- le operazioni contestate sono state autorizzate mediante codice OTP (cfr. foglio *tracciatura*, “checkotpmobile”, riga 347 e 398, col. “API_SRV”), generato a mezzo *push* (cfr. foglio *push*, riga 15 e 16), previa digitazione del PIN (cfr. foglio *tracciatura*, riga 347 e 398, colonna MSG_INPUT, “authType”: “PIN”);
- le operazioni contestate sono state eseguite *“su commercio elettronico sicuro”* con *“autenticazione del titolare”* senza anomalie;
- tra le 12:33:23 alle 12:33:25, risulta il tentativo di esecuzione di altre quattro operazioni con la stessa carta, non andate a buon fine per *“carta sospesa”* (presumibilmente si tratta del blocco cautelativo apposto dall’intermediario).

All’esito dell’esame delle dichiarazioni rese dall’intermediario e della documentazione prodotta, il Collegio ritiene che l’intermediario abbia dato prova della conformità alla SCA del sistema di autenticazione utilizzato e della formale regolarità delle operazioni contestate.

Tuttavia, secondo il consolidato orientamento di questo Arbitro, “[...] 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” (Collegio di Coordinamento, pronuncia n. 22745/19).

Circa i possibili profili di colpa grave del cliente, l’intermediario in sede di controdeduzioni, evidenzia che il ricorrente non ha fornito alcun elemento utile che possa contribuire a ricostruire le circostanze dalle quali è scaturito l’evento fraudolento.

Al riguardo, secondo il condivisibile e consolidato orientamento arbitrale, nelle contestazioni di utilizzi fraudolenti *on line* di strumenti di pagamento in cui:

- l’intermediario ha offerto la prova dell’autenticazione delle transazioni disconosciute,
- il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA),
- non risultano indizi di anomalia delle operazioni e/o ulteriori elementi,

le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo (cfr. Collegio di Bari, decisioni n. 8247/2024 e n. 7144/2023).

Nel caso di specie, il Collegio rileva che, a fronte della dimostrazione da parte dell’intermediario resistente della regolarità formale dell’operazione disconosciuta, eseguita in difetto di indizi di anomalia, il ricorrente – né nella fase prodromica al ricorso, né successivamente – ha offerto alcun elemento utile alla ricostruzione della truffa asseritamente patita.

Priva di pregio è la doglianza del ricorrente in merito all’asserita clonazione dello strumento di pagamento – lamentata nel modulo di disconoscimento – in quanto le operazioni disconosciute sono state eseguite tramite app, dunque, senza l’utilizzo della carta fisica.

Il Collegio osserva, altresì, che nella specie non risulta integrato alcuno degli indici di frode previsti dall'art. 8 del D.M. 112/2007. Al contrario, la carta di credito del ricorrente risulta essere stata bloccata cautelativamente dall'intermediario prima che si verificasse l'indice di frode cui al punto 2 della lett. a) del citato art. 8 (tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita): infatti le due operazioni oggetto di ricorso sono state eseguite lo stesso giorno verso il medesimo beneficiario e il tentativo di esecuzione di altre quattro operazioni con la stessa carta non è andato a buon fine.

Va pure rilevato che non vi è alcun riconoscimento di responsabilità da parte dell'intermediario, avendo lo stesso affermato di aver rimborsato l'operazione del 10 marzo 2025 in "*un'ottica commerciale*"; e che il ricorrente, sebbene lamenti l'assenza sul proprio dispositivo di tracce di navigazione verso i portali *e-commerce* interessati dalla frode e l'assenza di acquisti online di entità pari agli importi delle operazioni contestate nel proprio storico dei movimenti, non ha allegato alcuna evidenza della cronologia delle proprie navigazioni online né dei movimenti sulla carta.

Infine, sebbene dalle tracciatore in atti non risultino *push* o SMS di alert relativi alle due operazioni oggetto di ricorso, deve evidenziarsi che le stesse sono state eseguite a distanza di quattro minuti l'una dall'altra. Secondo le posizioni condivise dai Collegi, la mancata attivazione ovvero il mancato funzionamento di tale servizio (o di servizio assimilabile) sono ritenuti irrilevanti nelle ipotesi di esecuzione di più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, in quanto la ricezione dell'*alert* non potrebbe in concreto limitare il pregiudizio dell'utente. Inoltre, con riferimento all'operazione disconosciuta del 10 marzo 2025 (rimborsata), il ricorrente ha ricevuto sul proprio device e sul numero di cellulare associato al suo profilo, rispettivamente, due *push* autorizzative e un SMS con OTP recanti l'importo e il beneficiario del pagamento; mentre le due operazioni contestate del 18 marzo 2025 sono state precedute dall'invio al cellulare del ricorrente dell'SMS contenente l'OTP per l'*enrollment* sul nuovo device, nonché di una *push* di alert al dispositivo del cliente relativa a tale *enrollment*. Tali circostanze sembrano a questo Collegio sufficienti per ritenere accertata l'irrilevanza, nel caso di specie, di un sistema di alert *ex post*.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE