

COLLEGIO DI BARI

composto dai signori:

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

Relatore FILIPPO BOTTALICO

Seduta del 30/03/2026

FATTO

Nella denuncia in atti, alla quale il ricorrente rinvia nel modulo di ricorso per la ricostruzione dell'oggetto della controversia, il medesimo ricorrente afferma che, in data 15/12/2025, pubblicava su un portale *online* un annuncio per la vendita di alcuni articoli e, alle ore 09:56 del medesimo giorno, riceveva un'e *mail* con l'ordine di tali articoli e la specificazione che l'acquirente ne attendeva la spedizione.

Dichiara di aver ricevuto "*immediatamente dopo*" dei messaggi sul portale *online* con i quali un'interlocutrice richiedeva delle verifiche per il versamento del denaro.

Dichiara di aver quindi fornito, in un primo momento, i dati di una carta di debito di altro intermediario, rifiutata dall'interlocutrice, per poi fornire quelli della carta prepagata riferibile all'intermediario odierno resistente, che invece veniva accettata.

Gli veniva quindi chiesto di accettare due operazioni, una di € 424,00 (alle ore 11:34) e un'altra di € 377,00 (alle ore 12:37).

Richiedeva quindi il rimborso di tali somme, non quanto pattuito per la vendita, ma gli veniva risposto che il rimborso sarebbe avvenuto su altro strumento di pagamento, che non possedeva.

A seguito di quest'ultima comunicazione, realizzava di essere rimasto vittima di una frode.

Sostiene che le operazioni sono non autorizzate e che l'intermediario non ha fornito alcuna prova del suo comportamento doloso o gravemente colposo.

Domanda l'accertamento della natura non autorizzata delle operazioni ed il rimborso della somma sottratta pari a € 801,00.

Si costituisce nel presente procedimento un IMEL in luogo dell'intermediario originariamente convenuto, osservando che il ricorrente è titolare della carta prepagata n. *** 736 e ha reclamato il rimborso della somma di € 801,00 a seguito di due operazioni di pagamento *e-commerce* autorizzate da *app* in data 15/12/2025.

Fa presente che, così come dichiarato dal ricorrente, le suddette operazioni risultano interamente da costui autorizzate e, pertanto, il relativo addebito è esclusivamente ascrivibile alla condotta di parte ricorrente nell'ambito della vicenda.

Ritiene che la frode in esame sia riconducibile allo schema della manipolazione del pagatore, nel quale il malcapitato dispone operazioni di pagamento convinto da un abile frodatore.

Evidenzia che le operazioni sono state correttamente autenticate, registrate e contabilizzate, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi.

Osserva che le procedure di autenticazione forte adottate per operazioni eseguite attraverso canali digitali sono due: procedura "primaria" con *push notification* in *app* e codice *****ID, e procedura "secondaria" con *One Time Password* (OTP) via SMS e *password*.

Fa presente che nel caso in esame le operazioni sono state autorizzate dal ricorrente tramite *app* in data 15/12/2025 utilizzando il codice *****ID, ovvero mediante "*autenticazione forte del cliente*".

Precisa poi che, ai fini dell'utilizzo della citata procedura di autenticazione forte, è necessario in via preventiva installare l'*app* dell'intermediario sul *device*, associare lo strumento di pagamento (carta di pagamento o conto corrente) e configurare il codice *****ID, attraverso l'inserimento delle credenziali di accesso ai servizi di *internet banking* (*username* e *password*); dei dati dello strumento di pagamento utilizzato per effettuare i pagamenti *online* (ossia, nel caso della carta ad esempio PAN, CVV2 e data di scadenza); della *password* dinamica "usa e getta" (OTP) inviata via SMS sul numero di cellulare certificato fornito dal cliente e associato allo strumento di pagamento in modo sicuro. Illustra dunque il funzionamento del codice *****ID.

Fa presente che, per operazioni *e-commerce* come quelle oggetto di ricorso, il cliente accede sul *merchant* attraverso il quale vuole effettuare l'acquisto e, dopo aver inserito i dati dello strumento di pagamento e la propria *password*, per autorizzare l'operazione può ricevere una notifica in *app* e inserire come mezzo autorizzativo il codice *****ID, come nel caso in esame.

Evidenzia quindi che per questo tipo di operazioni non è necessario effettuare *login* né in *app* né sul sito dell'intermediario.

Rappresenta altresì che non vi è stato alcun cambio di utenza ovvero di dispositivo dall'*enrollment* del rapporto.

Aggiunge che la previsione di obblighi generali di monitoraggio in capo all'intermediario non è correlata ad "*un dovere di intervento preventivo*".

Quanto alla valutazione della condotta del ricorrente contesta "*l'ingenuità*" dello stesso, che ha eseguito gli ordini impartiti da uno sconosciuto interlocutore, consentendo di fatto la consumazione della truffa ai suoi danni.

Ravvisa inoltre la violazione degli obblighi di condotta richiesti al fine di non condividere, in alcun modo, con terzi le proprie credenziali o qualsiasi altro codice personale.

Fa presente di mettere a disposizione dei clienti il servizio di SMS-*alert*, attivo di *default* all'interno dell'*app*.

Precisa di condurre da tempo campagne informative antifrode informando i propri clienti tramite il proprio sito *web*, trasmettendo avvisi relativi a possibili comportamenti anomali che l'intermediario non è solito tenere, svolgendo azioni di sensibilizzazione della clientela.

Chiede, pertanto, il rigetto del ricorso.

In sede di repliche il ricorrente contesta la qualificazione delle operazioni come "autorizzate" sostenuta dall'intermediario, in quanto non intendeva disporre alcun pagamento, essendo *"convinto di porre in essere attività necessarie a ricevere un accredito connesso a una compravendita online"*.

Sostiene, inoltre, che l'autorizzazione carpita per il tramite di artifici o raggiri non può essere equiparata a una valida autorizzazione dell'operazione di pagamento.

Sul punto precisa che la mera dimostrazione dell'avvenuto utilizzo della *Strong Customer Authentication* non è di per sé sufficiente ad escludere la responsabilità dell'intermediario ove l'operazione risulti frutto di una frode e presenti elementi di anomalia.

Infatti, ritiene che le operazioni siano state *"ravvicinate temporalmente; l'importo complessivo è significativo rispetto alla normale operatività del ricorrente; i destinatari erano estranei alla sua sfera economica"*.

Aggiunge, altresì, che la condotta, *"seppur imprudente, non integra colpa grave, ma al più una colpa lieve, che non esclude il diritto al rimborso"*.

Sostiene, in sintesi, di essere stato vittima di una truffa sofisticata e contesta la genericità della prova circa la colpa grave fornita dall'intermediario.

Chiede, pertanto, il rimborso di € 801,00.

L'intermediario nelle controrepliche si riporta a quanto già eccepito in sede di controdeduzioni e insiste per il rigetto del ricorso.

DIRITTO

Preliminarmente, si rappresenta che si è costituito volontariamente nel presente giudizio, tramite il rituale deposito delle controdeduzioni, un istituto di moneta elettronica (intermediario "B", soggetto al controllo dell'intermediario "A" convenuto in giudizio dal ricorrente), asserendo di essere l'effettivo titolare del rapporto giuridico oggetto della presente materia del contendere, ossia una carta prepagata. La ricorrente, che ha ricevuto regolarmente le controdeduzioni, non ha replicato sul punto.

Effettivamente, dalla disamina del sito internet dell'intermediario convenuto dal ricorrente (intermediario "A"), si evince che al conto corrente da quest'ultimo offerto possa essere associata la carta prepagata emessa dal diverso intermediario/IMEL che si è costituito nel presente giudizio (intermediario "B").

Tanto ricostruito, si aderisce al più recente orientamento di questo Collegio secondo il quale la decisione deve essere comunque resa nei confronti dell'intermediario originariamente convenuto e (intermediario "A"), in quanto gestore del rapporto principale e sostanziale dedotto in lite sul quale l'operazione controversa risulta addebitata (cfr. Collegio di Bari, decisione n. 5753/23).

Premesso che le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27/01/2010, n. 11, come modificato dal d.lgs. 15/12/2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/01/2018, il ricorrente ricostruisce la modalità della truffa nella denuncia in atti, al quale integralmente rinvia nell'atto introduttivo dell'odierno giudizio.

Nel modulo di reclamo, dichiara di non aver rivelato credenziali di sicurezza né fornito a terzi codici OTP, e di aver provveduto al blocco della carta lo stesso giorno della frode (15/12/2025); tuttavia, non constano evidenze documentali sul punto.

La carta risulta comunque essere estinta.

Le operazioni contestate consistono in due pagamenti *online* eseguiti con carta prepagata il 15/12/2025:

- per il pagamento di € 424,00, sebbene dalla denuncia e dall'*inquiry* risultino le ore 11:34, dai *log* si evince quale orario le 12:34;
- per il pagamento di € 377,00 risulta pacifico come orario le ore 12:37.

L'intermediario sostiene che le suddette operazioni risultano interamente autorizzate dal ricorrente, con conseguente inapplicabilità della richiamata disciplina in materia di utilizzi fraudolenti.

Ebbene, secondo la costante giurisprudenza arbitrale:

- l'operazione deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD 2, se eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione);
- se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad esempio, con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD 2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP; resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 d.lgs. n. 11/2010 (ex multis, Collegio di Milano, decisioni nn. 319/2025 e 8295/2024).

Nel caso di specie il ricorrente, in sede di denuncia, non dichiara di avere inserito e autorizzato le operazioni, limitandosi ad affermare di aver fornito al truffatore i dati della carta e di aver successivamente "accettato" le due operazioni.

Pertanto l'apporto causale del ricorrente è stato solo parziale, avendo quest'ultimo autorizzato le disposizioni di pagamento presumibilmente inserite dal truffatore.

Ne consegue che la disamina del ricorso può proseguire, ritenendosi applicabile al caso di specie la disciplina di tutela prevista dal d.lgs. n.11/2010.

Con riferimento all'autenticazione delle operazioni, l'intermediario sostiene che sarebbero state eseguite in ossequio alla SCA.

Premette che le procedure di autenticazione forte adottate sono due:

- procedura "primaria": *push notification* in *app* e codice *****ID;
- procedura "secondaria": *One Time Password* (OTP) via SMS e *password*.

Descrive quindi tecnicamente il processo autorizzativo di una transazione tramite *****ID, il quale prevede – in sintesi – la firma della transazione "*mediante certificato presente sul Back-End*", l'inserimento di un PIN e la generazione di OTP.

Afferma che il ricorrente ha utilizzato la prima delle due modalità, che garantirebbe la *compliance* con la normativa in materia di SCA in virtù dell'inserimento del codice alfanumerico *****ID (elemento di conoscenza) nell'*app* installata sul *device* associato (elemento di possesso).

Precisa che, ai fini dell'utilizzo del codice *****ID, è necessario preliminarmente installare l'*app* sul *device*, per poi procedere con l'associazione dello strumento di pagamento (carta di pagamento o conto corrente) e con la configurazione del medesimo codice *****ID tramite l'inserimento dei seguenti fattori:

- le credenziali di accesso ai servizi di internet banking (username e password);
- i dati dello strumento di pagamento utilizzato per effettuare i pagamenti online (nel caso della carta PAN, CVV2 e data di scadenza);
- la password dinamica “usa e getta” (OTP) inviata via SMS sul numero di cellulare certificato fornito dal cliente e associato allo strumento di pagamento.

Deduce, pertanto, che *“l’operazione sconosciuta, tenuto conto della modalità con cui è stata autorizzata, poteva essere eseguita soltanto dal titolare dello strumento di pagamento, che è in possesso del device su cui è inviata la notifica in APP per l’inserimento del codice di sicurezza *****ID”*.

A sostegno, versa in atti alcune schermate che dimostrerebbero che la transazione è stata autorizzata dallo stesso dispositivo in uso al ricorrente.

In particolare, dall’analisi della suddetta documentazione si evincono – tra gli altri – *device id* (n. AB**19) e l’*app* utilizzata per autorizzare le operazioni oggetto di ricorso (cfr. colonna *“App con *****ID”*).

L’intermediario allega inoltre le schermate relative all’*enrollment* sul dispositivo in questione (n. AB**19) avvenuto il 03/12/2025.

Dalla documentazione analizzata e dalle dichiarazioni dello stesso ricorrente non sembra dunque che vi sia stata la configurazione dispositiva dell’*app* sul *device* del truffatore.

L’intermediario afferma quindi che le transazioni risultano correttamente eseguite ed autorizzate attraverso l’inserimento del codice *****ID al ricevimento della notifica in *app*.

Produce in atti le seguenti evidenze:

- estratto indicante il metodo dispositivo della operazione in oggetto, da cui emerge l’utilizzo del Protocollo 3DSecure (sigla “3DS” nel campo “MOD DISP”);
- estratto attestante l’autorizzazione con codice *****ID, tramite riconoscimento biometrico, con la relativa legenda; dalla stessa legenda si evince che il codice “Y” della voce “esito” fa riferimento all’autenticazione del titolare della carta (*“cardholder authenticated”*).

Produce altresì le schermate di dettaglio dei pagamenti delle operazioni sconosciute, corredate dalla legenda dei codici utilizzati, dove è specificato che il “*deviceID*” rappresenta l’identificativo del telefono utilizzato per apporre la firma con il codice *****ID; la voce “*appID*” corrisponde all’identificativo dell’*app* utilizzata per apporre la firma con il codice *****ID e la descrizione “*transaction-challenge*” rappresenta la richiesta di autorizzazione disposta sul canale e firmata in formato jwt dal canale stesso e autorizzata con il codice *****ID.

In ogni caso, è lo stesso cliente ad ammettere, in denuncia, di aver “*accettato*” le operazioni.

Tanto complessivamente ricostruito, questo Collegio non intende discostarsi dal proprio orientamento che, pronunciandosi sul sistema di sicurezza adottato dall’odierno intermediario, lo considera conforme alla SCA (*ex multis*, Collegio di Bari, decisioni nn. 224/2025, 10993/2024, 7434/2024 e 6494/2024), e ritiene che la documentazione tecnica allegata alle controdeduzioni (assimilabile a quella prodotta in questa sede) sia idonea a dimostrare la corretta autenticazione e la regolarità formale delle operazioni sconosciute ex art. 10, co. 1 d.lgs. n. 11/2010, nell’ipotesi di esecuzione delle stesse con l’utilizzo dell’*app* installata sul *device* del ricorrente e l’inserimento del codice *****ID (così Collegio di Bari, decisione n. 9055/2025 e 4839/2025).

A ciò si aggiunga che, secondo la costante giurisprudenza arbitrale, 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.

Inoltre, anche eventuali dichiarazioni confessorie del cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c. (così Collegio di Bari, decisione n. 13216/2024; Collegio di Torino, decisione n. 11213/2024; Collegio di Milano, decisione n. 12404/2024).

Senonchè, *“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”* (Collegio di Coordinamento, decisione n. 22745/2019).

Difatti, la mancanza della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente, atteso che rappresenta, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.

Sul punto, si deve evidenziare che il ricorrente non allega evidenza delle interlocuzioni intercorse con i truffatori, e pertanto non si può non richiamare la consolidata giurisprudenza arbitrale secondo la quale la mancata allegazione del messaggio civetta (o della telefonata ricevuta) non consente ai Collegi di accertare se risultino o meno integrati gli estremi di un legittimo affidamento dell'utente circa la genuinità dell'interlocuzione con l'intermediario (cfr. Collegio di Bari, decisioni nn. 7120/2024 e 2663/2023; Collegio di Milano, decisione n. 5431/2024).

Per ragioni di completezza, si deve rammentare che l'art. 8 d.m. n. 112/2007 identifica i casi di frode che, ai fini della normativa stessa, vanno segnalati all'Ufficio Centrale Antifrode dei Mezzi di Pagamento del Ministero dell'Economia e delle Finanze (UCAMP) per consentire un monitoraggio del mercato delle carte di pagamento.

Secondo le posizioni condivise dai Collegi, le previsioni di cui all'art. 8 (sinora mai modificate anche a fronte della significativa evoluzione degli strumenti di pagamento) non hanno un valore precettivo diretto sulla materia in esame, ma rappresentano utili indicatori per identificare anomalie e scenari di frode anche ai sensi dell'art. 2 del regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente.

Conseguentemente, ad avviso dei Collegi, una volta accertata la colpa grave del cliente, qualora sussista uno dei seguenti indici di frode:

- 7 o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento, prevista al punto 1 della lett. b) del menzionato art. 8;
- tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita, di cui al punto 2 della lett. a) del citato art. 8;
- due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti, di cui al punto 3 della lett. b) del medesimo art. 8,

la ripartizione della responsabilità con il prestatore dei servizi di pagamento (PSP) deve essere determinata caso per caso, in quanto le previsioni del D.M. rappresentano un parametro per la formulazione di un giudizio in concreto della negligenza tecnica dell'intermediario (Collegio di Bari, decisione n. 7126/2024).

Nel caso di specie non risulta riscontrato alcuno dei suddetti indici.

Tuttavia i Collegi hanno ritenuto possibile valorizzare anche indici di frode ulteriori rispetto a quelli del d.m. n. 112/2007 in presenza di un'operatività anomala rispetto alle movimentazioni storiche del

ricorrente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario), ove vi sia un'evidenza delle stesse (così Collegio di Bari, decisioni nn. 7228/2025, 9732/2024 e 4110/2024; Collegio di Milano, decisione n. 6578/2024)

Nel caso in esame, il ricorrente – in sede di repliche – ravvisa l'anomalia delle operazioni nei seguenti indici: *“le operazioni sono state ravvicinate temporalmente; l'importo complessivo è significativo rispetto alla normale operatività del ricorrente; i destinatari erano estranei alla sua sfera economica”*. Senonché dalla lista movimenti in atti (relativa al periodo 24/09/2025-15/12/2025) risultano altri addebiti con la stessa descrizione di quelli oggetto di ricorso (*“pagamenti POS”*), di importo massimo di € 58,84, nonché due bonifici dell'importo di € 1.000,00 e di € 4.000,00.

In tema di sistemi di *alert*, secondo l'autorevole insegnamento del Collegio di Coordinamento *“fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto”* (Collegio di Coordinamento, decisione n. 24366/2019).

Il medesimo Collegio di Coordinamento ha precisato che *“la mancata attivazione del servizio sms – alert costituisce in ogni caso una carenza organizzativa imputabile all'intermediario che, oltre a produrre l'effetto giustificativo solo a fronte della specifica dichiarazione liberatoria di rifiuto del cliente ad avvalersene (già affermata dal precedente “coordinamento”), non può non essere rilevata anche d'ufficio”* (Collegio di Coordinamento, decisione n. 8672/2024).

Nel caso di specie, non constano alcuna allegazione o evidenze in ordine al funzionamento del sistema di *alert*, che l'intermediario dichiara attivo di *default* in *app*.

Tuttavia, secondo la condivisibile giurisprudenza arbitrale, la mancata attivazione ovvero il mancato funzionamento di tale servizio (o di servizio assimilabile) sono ritenuti irrilevanti nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta, ovvero 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 (*ex multis*, Collegio di Bari, decisione n. 11254/2024 e 3835/2022)

Nel caso in esame, la seconda operazione – secondo gli orari evincibili dai *log* – è stata eseguita a distanza di circa 3 minuti dalla prima, con la conseguenza che, anche qualora fosse stato attivo un sistema di allerta, sarebbe stata ugualmente inevitabile.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE