

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 ESTERNI - FABIO GIROLAMO PORTA

Seduta del 13/04/2026

FATTO

Il ricorrente rivendica il proprio diritto al rimborso del controvalore di quattro operazioni di pagamento eseguite fraudolentemente da terzi, con l'uso illecito della carta prepagata a sé intestata, rilasciata dall'istituto di moneta elettronica partecipato dall'intermediario convenuto. In particolare, in sede di denuncia sporta in data 02/10/2025 presso le autorità competenti, il ricorrente rappresenta: di aver riscontrato, a seguito del controllo effettuato sull'app dell'intermediario installata sul proprio device, taluni addebiti derivanti da operazioni non autorizzate, per un totale di € 198,00; di aver provveduto al blocco della carta associata al proprio conto, denunciato la vicenda e presentato reclamo alla convenuta, ricevendo riscontro parziale. L'intermediario ha infatti riconosciuto solo la somma di € 55,00, negando il rimborso delle operazioni asseritamente autorizzate in regime autenticazione forte con la collaborazione attiva del titolare della carta. Il ricorrente sostiene, invece, di non aver autorizzato nessuna delle operazioni contestate e di non aver comunicato ad altri le credenziali segrete necessarie per l'accesso al conto e l'uso della carta. Saggiunge che tra le operazioni sconosciute, effettuate a poca distanza di tempo le une dalle altre, sono presenti anche due bonifici effettuati all'estero in orario notturno. Afferma di aver contattato immediatamente il numero verde della convenuta per bloccare la carta, rimasta in suo esclusivo uso e possesso.

Insoddisfatto dell'esito del reclamo, il ricorrente invoca la tutela dell'Arbitro affinché disponga, a carico della convenuta, il rimborso della somma sottratta, pari a € 149,00, oltre agli interessi legali e alla refusione delle spese di assistenza difensiva.

Instaurato il contraddittorio, l'intermediario convenuto si oppone alla richiesta del ricorrente evidenziando, preliminarmente, che sebbene il ricorso risulti indirizzato nei propri confronti, il

deducente rassegna le controdeduzioni per conto del collegato istituto di moneta elettronica (appartenente al medesimo gruppo societario) che ha rilasciato lo strumento in questione.

Ciò premesso, la resistente eccepisce l'infondatezza del ricorso precisando che il ricorrente chiede il rimborso della somma di € 149,00 relativa a n. 3 operazioni di pagamento online disposte da APP – di cui n. 2 bonifici istantanei di € 50,00 e 35,00 e n. 1 transazione di ricarica P2P di € 55,00 – eseguite in data 27/09/2025. Evidenzia che rispetto al totale delle operazioni disconosciute, complessivamente pari a € 198,00, la medesima ha riconosciuto un parziale rimborso (€ 55,00), sicchè il petitum ammonterebbe ad € 143,00.

Nel merito, l'intermediario specifica che il sistema di autenticazione adottato nella vicenda rimessa alla cognizione dell'Arbitro prevede l'invio in App (fattore di possesso) di una notifica push che il titolare convalida inserendo il codice alfanumerico segreto "*****ID" (fattore di conoscenza). Osserva che dalle proprie evidenze può evincersi, in primo luogo, l'avvenuto enrollment della carta di pagamento del ricorrente al sistema autorizzativo di tipo dinamico funzionante mediante invio con SMS della OTP sul numero di cellulare certificato. Sottolinea 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, PAN, CVV2 e data di scadenza); della password dinamica "usa e getta" (OTP) inviata tramite SMS sul numero di cellulare certificato fornito dal cliente e associato allo strumento di pagamento in modo sicuro. Sostiene che tale sistema sia conforme ai requisiti previsti dalla normativa vigente in tema di SCA, in quanto basata su un fattore di conoscenza (il codice statico scelto dall'utente) e un fattore di possesso (l'utilizzo di una *app* previamente associata ad uno specifico dispositivo). Saggiunge che è possibile utilizzare il fattore di conoscenza solo sul *device* sul quale è stato abilitato precedentemente il prodotto finanziario e, in caso di possesso del *device* ma non del codice e di errato inserimento di quest'ultimo per più di 5 volte, è prevista una procedura di blocco del codice stesso.

Sulla scorta degli elementi acquisiti, la resistente ritiene che le operazioni contestate sono state eseguite con il descritto sistema di autenticazione forte, attraverso l'inserimento del codice ***ID al ricevimento dell'apposita notifica in APP. Produce, tra l'altro, apposita evidenza da cui risulta che le operazioni oggetto di ricorso sono state autorizzate tutte dal medesimo device (n. ***7BC) associato alla carta, senza soluzione di continuità, dal 14/04/2025 (circa cinque mesi prima delle operazioni disconosciute). Sul punto fa presente che nel periodo intercorso dall'enrollment della carta sino alla sua estinzione non vi è stato alcun cambio di utenza né di device. Ritiene, dunque, la circostanza indicativa del fatto che le operazioni disconosciute siano state eseguite integralmente dal cliente (e non tramite un dispositivo terzo). All'uopo, l'intermediario allega i log estratti dai propri sistemi che valorizzano i fattori di autenticazione forte utilizzati in corrispondenza di ciascuna attività di accesso all'app e dispositiva.

L'intermediario deduce pertanto la colpa grave del cliente, il quale, del resto, non ha fornito alcun elemento utile a chiarire la dinamica della frode denunciata, evidentemente agevolata dal suo comportamento oltremodo negligente. Rappresenta che il cliente ha provveduto a bloccare la carta alle ore 14:19 del 27/09/2025, successivamente alle operazioni controverse. Alla stregua dei superiori argomenti, la resistente esclude profili di censurabilità ascrivibili al proprio operato, sottolineando di mettere a disposizione dei clienti il servizio di SMS alert gratuito, che offre la possibilità di mantenere sotto controllo i movimenti della carta. Precisa che tale servizio è attivo di default all'interno dell'App di internet banking. Afferma di condurre da tempo campagne informative antifrode e iniziative di sensibilizzazione della clientela tramite il proprio sito web, anche trasmettendo avvisi relativi a possibili comportamenti anomali che l'intermediario non è solito tenere. Conclude chiedendo al Collegio di dichiarare il rigetto del ricorso in quanto infondato in fatto e in diritto.

Le parti hanno depositato memorie di replica e di controreplica insistendo per le rispettive conclusioni.

DIRITTO

Preliminarmente si osserva che il presente ricorso è stato azionato nei confronti dell'intermediario che esercita il controllo sull'istituto di moneta elettronica emittente la carta prepagata utilizzata nella fattispecie; l'IMEL si è costituito volontariamente nel procedimento ABF, rassegnando le proprie controdeduzioni a mezzo delle quali asserisce di essere l'effettivo titolare del rapporto giuridico oggetto di vertenza. Sia l'intermediario destinatario del ricorso, sia il ricorrente hanno implicitamente accettato il nuovo contraddittore non avendo contestato la costituzione del diverso soggetto.

La circostanza non osta al valido svolgimento del procedimento; tuttavia, in ossequio ai principi processuali civilistici, la pronuncia viene resa nei confronti dell'intermediario convenuto, destinatario del reclamo e del successivo ricorso (cfr. ABF Coll. Bari, Dec. nn. 3841/2025, 10162/2024).

Chiarito quanto sopra, il ricorrente invoca il diritto al rimborso del controvalore di quattro operazioni di pagamento asseritamente eseguite da terzi in data 27/09/2025, in difetto di autorizzazione, prima del blocco della carta intervenuto alle ore 14:10. Trattasi in particolare di due bonifici istantanei (€ 35,00 ed € 50,00, oltre € 2,00 per commissioni), una operazione di pagamento P2P (€ 55,00, oltre € 1,00 per commissione) e una operazione di e-commerce (€ 55,00). Appurato che l'intermediario ha restituito il controvalore (€ 55,00) della transazione di e-commerce, il petitum del ricorso va circoscritto all'importo di € 143,00 (al lordo delle commissioni) corrispondente alle restanti (tre) operazioni disconosciute e non rimborsate.

Dette operazioni risultano poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, di recepimento della direttiva 2007/64/CE, come modificato dal d.lgs. 218/2017, che ha attuato la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno, e il Regolamento Delegato (UE) n. 2018/389 della Commissione che definisce i requisiti per l'autenticazione forte previsti dalla citata normativa.

Tale disciplina prevede che il rischio di utilizzazione illecita degli strumenti di pagamento ricada in prima battuta sull'intermediario (tenuto a garantire l'affidabilità e la sicurezza complessiva del servizio offerto, in relazione al sistema informatico, organizzativo e di controllo all'uopo adottati) il quale può sottrarsi all'obbligo di rimborso delle transazioni impugnate fornendo la prova del dolo o della colpa grave dell'utilizzatore (tenuto alla diligente custodia dello strumento e alla segretezza delle credenziali necessarie per l'autenticazione) ai sensi del combinato disposto degli artt. 7, 10 e 12, comma 4, d. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, l'art. 10 del citato decreto legislativo n. 11/2010 stabilisce: "1. Qualora l'utente 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". Inoltre "2. Quando l'utente di servizi di pagamento neghi di aver 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. 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".

Nel caso in esame, l'intermediario afferma che le transazioni controverse sono state eseguite con un sistema di autenticazione forte, conforme alla normativa in materia, attraverso l'inserimento del codice ***ID (fattore di conoscenza) al ricevimento della notifica in APP, previamente associata allo specifico dispositivo in uso al ricorrente (fattore di possesso). In proposito svolge alcune considerazioni tecniche volte a descrivere 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. Con specifico riferimento alla fase di configurazione dell’APP sul dispositivo abbinato allo strumento di pagamento, l’intermediario afferma 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 della chiave “***ID” tramite 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 (nel caso della carta PAN, CVV2 e data di scadenza); la password dinamica “usa e getta” (c.d. “OTP”) inviata via SMS sul numero di cellulare certificato fornito dal cliente e associato allo strumento di pagamento. All’uopo, la resistente produce specifica evidenza attestante l’avvenuto enrollment della carta di pagamento di titolarità del ricorrente al sistema autorizzativo di tipo dinamico funzionante mediante invio dello SMS OTP sul numero di cellulare certificato indicato nella denuncia in atti.

In ordine alla fase dispositiva, l’intermediario afferma che le operazioni disconosciute, tenuto conto della modalità con cui sono state autorizzate, potevano essere eseguite soltanto dal titolare dello strumento di pagamento, in possesso del device su cui sono state inviate le notifiche in App per l’inserimento del codice di sicurezza ****ID. Allega evidenza del processo di configurazione dell’App sul device (n. ***7BC) in uso al ricorrente (alle ore 11:33 del 14/04/2025), dal quale risultano disposte le transazioni disconosciute tramite inserimento del codice “***ID” in App. La circostanza sembra trovare conferma nei Log (stringa “PID” valorizzata nel campo “MOD DISP”) relativi agli accessi in App, operati tramite il device n. ***7BC con codice ***ID.

In ordine alla fase di autenticazione delle operazioni contestate, gli estratti informatici prodotti, unitamente alla legenda esplicativa e alle traccature della firma digitale applicata con il codice ****ID, documentano parimenti che le transazioni sono state compiute attraverso l’inserimento del codice “***ID” in App. Depongono in questo senso le stringhe presenti nei log in atti dove: il codice associato alla voce “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; la descrizione “transaction-challenge” rappresenta la richiesta di autorizzazione disposta sul canale e firmata in formato jwt dal canale stesso nonché autorizzata con il codice ****ID.

Sulla scorta della documentazione esaminata può dunque affermarsi che il sistema adottato dall’intermediario soddisfa i requisiti di autenticazione forte dell’utente, secondo gli standard di sicurezza indicati dall’EBA attraverso gli orientamenti del 21 giugno 2019 elaborati in tema di SCA (cfr. ABF Coll. Bari, Dec. n. 5813/2024); ciò consente di ritenere raggiunta la prova in ordine alla corretta esecuzione delle operazioni in esame (ex art. 10, comma 1, del d.lgs. n. 11/2010), ovvero che le stesse non siano il frutto di malfunzionamenti delle procedure esecutive (cfr. ABF Coll. Bari, Dec. n. 224/2025; id. Dec. n. 10993/2024, Dec. n. 7434/2024).

Pur tuttavia, alla stregua della normativa sopra richiamata, la dimostrazione della regolarità formale di un’operazione contestata non è di per sé sufficiente ad attribuirne le conseguenze patrimoniali in capo al titolare dello strumento quando non consti il dolo o la colpa grave dell’utilizzatore. In questa prospettiva, il Collegio deve quindi valutare gli elementi ulteriori acquisiti agli atti del procedimento che consentano una plausibile ricostruzione su base indiziaria delle caratteristiche della truffa denunciata dal ricorrente, onde formare il proprio convincimento in ordine alla sussistenza o meno di profili di negligenza inescusabile ascrivibili alla condotta del cliente nell’uso del dispositivo.

Nel caso esaminato assumono rilievo le succinte allegazioni del ricorrente, il quale non ricostruisce le modalità della truffa subita né allega elementi utili a ricondurre il fatto ad una determinata fattispecie, limitandosi ad affermare di essere venuto a conoscenza degli addebiti fraudolenti solo a seguito di un controllo dei movimenti.

Alla luce del quadro probatorio, queste circostanze integrano, in applicazione degli artt. 7, comma 1, lett. a), e 12, co. 4, d.lgs. n. 11/2010, una tipica ipotesi di colpa grave dell’utilizzatore nella custodia

delle credenziali segrete in suo possesso, necessarie per l'uso degli strumenti di pagamento (cfr. ABF Coll. Coord., Dec. n. 897/2014; Dec. n. 5304/2013).

Nondimeno, è stato chiarito come l'obbligo a carico dell'utente dello strumento di pagamento di tempestiva segnalazione del suo utilizzo indebito (previsto dall'art. 7, lett. *b*, d.lgs. 11/2010, cit.) sia strettamente correlato all'obbligo in capo all'intermediario di assicurare che siano sempre disponibili strumenti adeguati affinché il cliente possa eseguire tale comunicazione (ex art. 8, lett. *c*). In particolare, 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 (cfr. ABF Coll. Coord., Dec. n. 24366/2019); per cui "la mancata prova dell'attivazione del servizio di sms alert da parte dell'intermediario rappresenta una violazione al corretto adempimento degli obblighi posti a suo carico" (cfr. ABF Coll. Coord., Dec. n. 8672/2024).

Nella fattispecie in esame, la seconda operazione (€ 50,00) è avvenuta a distanza di 15 minuti dalla prima e la terza (€ 55,00) a distanza di 47 minuti dalla seconda. Ora, considerata la tempistica, con riferimento alle operazioni successive alla prima è ragionevole ritenere che, ove fosse stato attivo il servizio di sms alert, il congegno avrebbe verosimilmente consentito al ricorrente di avere contezza più immediata dei movimenti, offrendo al medesimo la possibilità di attenuare il pregiudizio patrimoniale risentito (cfr. ABF Coll. Bari, Dec. n. 10735/2023; Coll. Napoli, Dec. n. 8838/2022). Pertanto, in relazione ad esse (al netto del rimborso già effettuato) l'intermediario non può andare esente da responsabilità ed è tenuto alla restituzione del corrispondente importo, pari a € 107,00 al lordo delle commissioni (cfr. ABF Coll. Bari, Dec. nn. 416/2024, 10010/2023, 15207/2022).

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 107,00, oltre gli interessi legali dalla data del reclamo al saldo.

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