Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

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

Relatore ESTERNI - FABIO GIROLAMO PORTA

Seduta del 22/01/2026

FATTO

Il ricorrente, titolare di una carta di debito rilasciata da altro istituto bancario, chiede il rimborso del controvalore di cinque operazioni di pagamento eseguite su un sito di commercio elettronico in data 11 aprile 2025, per l'importo complessivo di euro 1.379,34 (al netto degli storni già riconosciuti), dal medesimo asseritamente non autorizzate.
In particolare il ricorrente afferma: di aver ricevuto, in data 11/04/2025, un sms apparentemente riconducibile ad un intermediario diverso dall'IMEL convenuto che segnalava l'imminente blocco della carta di debito a sé intestata; di aver azionato il link contenuto nel messaggio ricevuto e inserito, negli appositi campi della schermata apparsa, le credenziali di accesso all'app dell'emittente; di aver ricevuto un nuovo messaggio in cui gli veniva comunicato che entro cinque minuti sarebbe pervenuto un codice OTP; di essere stato contattato telefonicamente, alle ore 18:00 circa, da un numero sconosciuto, non presente nella sua rubrica, e di aver interloquito con un presunto agente della Polizia Postale, il quale segnalava la presenza di una operazione di prelievo di € 900,00 addebitata sul proprio conto corrente incardinato presso altra banca; di aver seguito le istruzioni ricevute dal chiamante nella convinzione di bloccare l'operazione fraudolenta segnalata; di aver eseguito le istruzioni ricevute dal sedicente agente di Polizia, inserendo nell'app dell'odierna convenuta i codici OTP "*per un certo numero di volte"; di essersi* insospettito e di aver interrotto la telefonata; di essersi infine avveduto della truffa in corso e di aver chiesto il blocco delle disposizioni di pagamento ad un operatore della convenuta, in riscontro al quale gli veniva comunicato che il disconoscimento poteva essere effettuato solo a seguito della contabilizzazione dei movimenti sul conto corrente. Il ricorrente soggiunge che il giorno della truffa l'app

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

della banca presso cui detiene il rapporto di conto corrente non funzionava a causa di un disservizio generale. All'uopo, dichiara di produrre una dichiarazione testimoniale sulla vicenda rappresentata.
Ritenendo di essere rimasto vittima di una truffa sofisticata, il ricorrente ha disposto il blocco dello strumento, sporto denuncia presso gli organi di P.G. e chiesto il rimborso all'intermediario ricevendo riscontro negativo. Sicchè, insoddisfatto dell'esito del reclamo, il ricorrente invoca la tutela dell'Arbitro affinché accerti il proprio diritto alla restituzione del maltolto.
Instaurato il contraddittorio, l'intermediario (IMEL) resiste al ricorso eccependo il proprio difetto di legittimazione passiva, sul rilievo che il ricorrente sarebbe legittimato a far valere le proprie istanze esclusivamente nei confronti dell'intermediario emittente e collocatore della carta, quale titolare del rapporto con il cliente nonché gestore del conto corrente o di altro conto di pagamento sul quale vengono addebitati gli importi relativi alle operazioni di pagamento e di prelievo con l'uso della carta.
Sottolinea che in forza di una convenzione con l'intermediario emittente, il suo ruolo ancillare sarebbe limitato allo svolgimento di specifici servizi finalizzati a garantire la funzionalità delle carte e del relativo circuito di pagamento, tra cui: l'attivazione della carta, l'operatività relativa alle operazioni di pagamento e dei flussi di spesa presso gli esercenti, l'operatività relativa alle operazioni di prelievo di denaro contante, i flussi delle operazioni di pagamento e delle operazioni di prelievo di denaro contante, che consentono la corretta rilevazione contabile relativa alla carta, il controllo delle frodi, il corretto funzionamento del sito internet, il servizio clienti, le contestazioni ma non i reclami e tantomeno i ricorsi.
L'intermediario evidenzia che, in esecuzione delle attività di sua competenza, il riscontro fornito al cliente è circoscritto alla comunicazione degli esiti della lavorazione della pratica di contestazione; di conseguenza assume che il ricorrente avrebbe dovuto rivolgendosi all'ufficio reclami dell'emittente per la formulazione di eventuali rilievi e, se del caso, convenire quest'ultimo dinanzi all'ABF.
In via pregiudiziale, l'intermediario chiede dunque al Collegio di accertare la propria carenza di legittimazione passiva, qualificandosi né emittente né collocatore dello strumento di pagamento adoperato e non rivestendo il ruolo di prestatore di servizi di pagamento nei confronti dell'odierno istante.
Nel merito, l'intermediario eccepisce l'infondatezza del ricorso con il quale il ricorrente avanza richiesta il rimborso del controvalore di cinque operazioni di pagamento on line, quantificate in € 1.379,34, quale differenza tra il totale delle transazioni disconosciute e gli storni disposti direttamente dall'esercente.
Rileva che i pagamenti contestati sono stati convalidati mediante inserimento del codice personale K**6 (conosciuto esclusivamente dal ricorrente e da questi generato in data 03/07/2024), e validazione di apposita OTP SMS inviata sul numero di cellulare certificato. Contesta la colpa grave del ricorrente anche in considerazione del fatto che le notifiche ricevute riportavano chiare indicazioni in ordine all'importo di ciascuna transazione e all'esercente beneficiario del relativo pagamento. Il resistente esclude dunque profili responsabilità ascrivibili al proprio operato in relazione alle procedure adottate nella fattispecie, né una mancata adozione di iniziative concrete volte ad impedire l'uso non autorizzato dello strumento di pagamento in relazione alla vicenda che occupa, sottolineando come, nonostante l'assenza di un rischio di frode normativamente tipizzato, la stessa ha sospeso cautelativamente l'utilizzo della carta inviando apposita mail al cliente. Conclude, pertanto, chiedendo la declaratoria di rigetto del ricorso per difetto di legittimazione passiva, ovvero per infondatezza della domanda in fatto e in diritto.

DIRITTO

Il ricorrente rivendica il rimborso del controvalore di cinque operazioni di pagamento on line - che quantifica in complessivi euro 1.379,34, quale differenza tra il totale delle transazioni disconosciute e gli storni disposti direttamente dall'esercente - eseguite a distanza su un sito di commercio elettronico con l'uso asseritamente non autorizzato della carta di debito al medesimo intestata.

Preliminarmente occorre vagliare l'eccezione di difetto di legittimazione passiva sollevata dall'intermediario resistente, il quale ritiene che legittimato all'azione sia l'istituto emittente e collocatore della carta di debito attraverso cui sono state eseguite le operazioni disconosciute. In proposito, la resistente afferma di svolgere, per conto dell'emittente (controparte del rapporto), specifici servizi ed attività finalizzati a garantire la funzionalità delle carte, secondo i termini e le condizioni stabilite da un'apposita convenzione (di cui non allega alcuna evidenza). Sostiene dunque che la banca emittente lo strumento di pagamento sia responsabile dei reclami pervenuti dal cliente avendone in carico la gestione operativa.
Secondo l'orientamento condiviso dei Collegi, in caso di domanda relativa al rimborso di transazioni effettuate in conseguenza dell'utilizzo fraudolento di uno strumento di pagamento, sussiste la legittimazione passiva dell'intermediario collocatore, onerato della prova sulla corretta autenticazione delle transazioni contestate in ragione del rapporto contrattuale instaurato tra quest'ultimo e l'utente. Fa eccezione l'ipotesi in cui il PSP sia "mero" collocatore della carta. In tal caso, per accertare questo profilo si ha riguardo alla documentazione in atti (a titolo esemplificativo, se la denominazione e il marchio dello strumento sono riconducibili esclusivamente all'emittente, in mancanza di ulteriori elementi, l'intermediario viene considerato "mero" collocatore; viceversa se le previsioni contrattuali affidano al collocatore il ruolo di riscontro all'utenza in caso di reclami, ovvero se il collocatore ha risposto al reclamo dell'utente senza segnalargli l'eventuale difetto di legittimazione passiva, non si tratta di "mero" collocatore).
Nella fattispecie non risulta versata in atti copia della convenzione stipulata tra l'IMEL e la banca, che il resistente afferma essere emittente della carta. Consta unicamente il foglio informativo della carta di debito, da cui si evince che il dispositivo è emesso dalla banca "*in collaborazione con* [la convenuta] *che è il gestore e titolare della licenza del circuito di pagamento internazionale"*. A ciò aggiungasi che nell'interlocuzione preliminare al ricorso, intrattenuta unicamente con la resistente, quest'ultima non ha mai eccepito il proprio difetto di legittimazione passiva, argomentando nel merito. Si osserva inoltre che nella mail con cui la convenuta ha comunicato direttamente al ricorrente l'esito della pratica di contestazione, l'IMEL ha fornito esaustivo riscontro nel merito, specificando che, per formulare un reclamo, il cliente può utilizzare i canali e i riferimenti riportati sul suo sito "*o della sua Banca e sulla copia del Regolamento da lei sottoscritto"*. Di conseguenza, ritiene il Collegio che il comportamento concludente posto in essere dalla resistente abbia indubitabilmente concorso a determinare l'affidamento del ricorrente quanto alla sussistenza della propria legittimazione passiva, al di là di ogni altro rilievo, in forza della regola *nemo contra factum proprio venire potest*, che è espressione del generale principio di buona fede (cfr. ABF Coll. Bari, Dec. nn. 7500/2023, 4870/2023, 134/2023; Coll. Milano, Dec. nn. 6153/2025, 9729/2023; Coll. Torino, Dec. n. 6291/2025; Coll. Bologna, Dec. nn. 7249/2025, 5554/2025, 5376/2025).
Appurata la legittimazione della resistente, il ricorso si palesa non meritevole di tutela per le ragioni di seguito esposte.
La materia oggetto di vertenza trova specifica regolamentazione nelle disposizioni del d.lgs. 27 gennaio 2010, n. 11, di recepimento della direttiva 2007/64/CE, come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno (PSD2). Le operazioni controverse risultano poste in essere anche sotto la vigenza del Regolamento Delegato (UE) n. 2018/389 della Commissione che definisce i requisiti per l'autenticazione forte previsti dalla citata direttiva.
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. 27 gennaio 2010 n. 11, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, a mente dei commi 1 e 2 dell'art. 10 (d.lgs. n. 11/2010, cit.): "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. 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".

Tratteggiato il quadro normativo di riferimento, come evidenziato nella narrativa del ricorso, il ricorrente invoca la restituzione della somma netta (euro 1.379,34) portata da cinque operazioni di pagamento elettroniche compiute a distanza, tra le ore 19:00 e le ore 19:14 dell'11/04/2025, su un sito di commercio elettronico, con l'uso asseritamente non autorizzato della carta di debito al medesimo intestata, prima del blocco operativo apposto alle ore 22:14 dello stesso giorno.

L'intermediario convenuto ha negato il ristoro del controvalore delle transazioni disconosciute, in ragione della riscontrata corretta autenticazione avvenuta con le credenziali fornite al cliente e la conseguente autorizzazione forte mediante inserimento di una password statica (codice K**6) e una chiave dinamica (sms OTP). A tale ultimo riguardo l'intermediario ha evidenziato che il codice K**6 (chiave a 6 cifre che il Titolare deve utilizzare per completare i pagamenti online) viene definito e attivato dall'utente all'interno dell'area personale del portale titolari (cui egli accede con codice utente, password e OTP o riconoscimento biometrico) inserendo, altresì, il codice OTP che riceve via SMS per terminare la messa in funzione.

Ciò precisato, l'intermediario afferma che all'esito delle verifiche effettuate, l'importo richiesto a titolo di rimborso *"corrisponde alla differenza tra il totale delle operazioni correttamente eseguite dal Cliente, pari a euro 1.897,82, e gli storni disposti direttamente dall'esercente, pari a euro 518,48. L'ammontare complessivo risultante è dunque di euro 1.379,34".* All'uopo l'intermediario allega una schermata, corredata di legenda esplicativa, dalla quale si evince, in relazione al primo pagamento online, l'utilizzo della OTP SMS (elemento di possesso) con positiva validazione del codice K**6 (elemento di conoscenza; cfr., colonna "Tipo Autenticazione", stringa "02-SMS OTP). Quanto alle restanti operazioni sembra evincersi l'uso del codice K**6 (elemento di conoscenza) finalizzato a convalidare le notifiche ricevute dal ricorrente in app (elemento di possesso; cfr., colonna "Tipo Autenticazione", stringhe "09-OOB Other" e "*autenticata con K**6 in app"*). In corrispondenza della colonna "K**6Status" è altresì presente il valore "A" che, secondo la legenda ("*Attivo = verifica di K**6")*, confermerebbe l'operatività della password statica. L'intermediario ha inoltre dichiarato, senza essere smentito, che tale codice segreto risulta associato al profilo del ricorrente sin dal 03/07/2024, mentre l'operatività contestata riguarda la giornata dell'11/04/2025. L'intermediario ha prodotto anche evidenza degli sms alert e del codice OTP SMS inviati all'utenza telefonica del ricorrente - coincidente con quella indicata in sede di denuncia - per autorizzare la prima operazione, nonché delle notifiche push convalidate per le restanti operazioni tramite lo stesso dispositivo usato in fase di primo accesso (risalente al 26/03/2025). Le allegazioni dell'intermediario convenuto, in merito ai fattori utilizzati, appaiono corroborate dalle dichiarazioni rilasciate dal ricorrente in sede di denuncia presso le autorità competenti (cui può attribuirsi valore di prova legale ai sensi dell'art. 2730 c.c.; cfr. ABF Coll. Bari, dec. n. 6764/2025), il quale ha ammesso di aver comunicato allo sconosciuto interlocutore i codici dinamici OTP ricevuti tramite sms per finalizzare le operazioni di pagamento.

Sulla scorta delle risultanze in atti può dunque affermarsi che l'intermediario resistente abbia assolto l'onere probatorio sul medesimo gravante (ex art. 10, d.lgs. n. 11/2010, cit.) fornendo adeguata evidenza dell'autenticazione avvenuta in regime di *Strong Customer Authentication* e della formale

regolarità delle operazioni disconosciute con i relativi chiarimenti (cfr. ABF Coll. Roma, Dec. n. 6519/2025; Coll. Bari, Dec. n. 4945/2024).
Tuttavia, come non si è mancato di sottolineare, la norma citata va interpretata nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità delle transazioni 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 di ciascuna operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente (cfr. ABF Coll. Coord. Dec. n. 22745/2019). Sotto questo fronte, nella fattispecie consta che il numero indicato nel campo mittente dello sms civetta non è riconducibile ai contatti dell'intermediario resistente, né il link contenuto nel messaggio esca reca riferimenti al PSP. Tali circostanze inducono il Collegio a ravvisare gli estremi di una condotta gravemente negligente del titolare della carta, nella misura in cui ha intrattenuto una conversazione con un sedicente agente della Polizia Postale, che l'ha contattato da una utenza (numero di cellulare) non riconducibile tanto all'Autorità quanto al PSP e, ciò nonostante, ha dato seguito alle istruzioni ricevute dallo sconosciuto interlocutore comunicando i codici OTP dispositivi ricevuti tramite sms. In proposito si rammenta che nei casi di *phishing* tradizionale, l'assenza di cautela dell'utente appare difficilmente scusabile, trattandosi di fenomeni diffusamente noti, che qualunque utilizzatore dotato di normale avvedutezza e prudenza, "deve essere in grado di individuare, non facendosi trarre in inganno" (cfr. ABF Coll. Coord., Dec. nn. 1820/2013, 3498/2012). Quanto innanzi induce a ritenere che il ricorrente abbia disatteso l'obbligo posto a suo carico dall'art. 7, d.lgs. n. 11/2010, di diligente custodia e non divulgazione delle credenziali statiche e dinamiche necessarie per finalizzare i pagamenti on line, in tal modo neutralizzando tutti i presidi di sicurezza approntati dall'intermediario, consentendo, seppure all'esito di un raggiro, la causazione dell'evento delittuoso. A tale conclusione non osta il rilievo del ricorrente sul presunto malfunzionamento del servizio di home banking dell'intermediario emittente la carta, posto che le operazioni contestate sono state autorizzate tramite l'app dell'odierna convenuta.
Per vero, sebbene in linea generale non è configurabile una responsabilità oggettiva del PSP nei casi in cui, come nella specie, l'intermediario abbia dimostrato di avere adottato un sistema di autenticazione rispondente ai requisiti di SCA e sussistano elementi concludenti della colpa grave dell'utilizzatore, a diverso esito può giungersi allorquando, sulla base delle evidenze disponibili e secondo le norme di diritto comune, emerga in concreto un apporto causale dell'intermediario all'evento dannoso tale da comportare una sua colpevolezza (cfr. Coll. Bari, Dec. n. 9279/2024; Coll. Bologna, Dec. n. 9454/2024). Ciò può accadere, tra l'altro, nei casi di fallace monitoraggio, ovvero di mancato rilievo di indici sintomatici di un illecito rispetto a operazioni inusuali, secondo le "indicazioni contenute nel d.m. 30 aprile 2007, n. 112, adottato in attuazione della legge 17 agosto 2005, n. 166 (recante 'Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento')". In particolare, ai sensi dell'art. 8, 1° comma, lett. b), n. 1) del citato d.m., si configura un rischio di frode quando si verificano, tra l'altro, "tre o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento, presso un medesimo punto vendita".
Nel caso in esame il ricorrente ha disconosciuto cinque pagamenti online, tre dei quali eseguiti presso uno stesso esercente.
Ebbene, all'esito di un attento monitoraggio, risulta che l'intermediario opportunamente ha sospeso, a tutela del cliente, l'operatività della carta inviando apposita comunicazione via mail (alle ore 19:17:49 dell'11/04/2025) al fine di verificare direttamente con il titolare la paternità dell'attività registrata, evidentemente ritenuta sospetta. Inoltre, dai log in atti sembra evincersi la presenza di un'operazione inibita automaticamente dai sistemi di monitoraggio antifrode dell'intermediario (alle ore 19:14) e lo storno delle tre operazioni successive (eseguite alle ore 19:29, 19:46, 20:06) attestato dalla dicitura "STO" riportata nella colonna "flusso" della schermata principale prodotta dalla resistente. Di conseguenza, in relazione agli ulteriori aspetti di natura organizzativa considerati, nel caso sottoposto all'esame del Collegio, alcun rilievo può muoversi all'intermediario avendo questi adottato misure di

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

carattere tecnico idonee a conferire un maggiore grado di sicurezza ai servizi offerti, in linea con l'art. 2 del Reg. EBA n. 2018/389.
Il ricorso non può pertanto trovare accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE