Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 14/01/2026

FATTO

In data 10.04.2025 la parte ricorrente riceveva un sms contenente l'invito a cliccare sul link https://b********es.top/it per sbloccare un pacco del quale era effettivamente in attesa.
Pertanto, procedeva a cliccare sul link sopra citato e veniva reindirizzato all'indirizzo internet di una società di trasporti e servizi di spedizione ove gli veniva chiesto di procedere al pagamento della somma di euro 0,27 per "…la riconsegna…" del pacco.
Dopo aver autorizzato il pagamento, però, veniva indebitamente addebitata sul conto corrente della società la somma di euro 817,50 per un'operazione mai autorizzata.
Il ricorrente si avvedeva di ciò solo in un secondo momento, in quanto nell'app non compariva, prima dell'autorizzazione, l'importo dell'operazione e il beneficiario.
Con l'odierno ricorso, agisce per ottenere il rimborso dell'importo dell'operazione (euro 817,50) e della commissione applicata (euro 14,31), per un totale di euro 831,81, lamentando altresì una negligente e ritardata gestione del reclamo.
Nelle controdeduzioni la banca eccepisce quanto segue.

- La parte ricorrente ha ammesso di aver autorizzato la transazione, seppur pensando di autorizzare una cifra diversa.

La transazione è stata autorizzata ed autenticata esattamente dal device del ricorrente, mediante fattore biometrico (FINGERPRINT_FACEID) evidentemente non accorgendosi che l'importo di 15.000.000,00 IDR corrispondesse a 817,50 euro e non a 0,27 euro.

- Il pagamento è stato preceduto dal messaggio autorizzativo della transazione inviato e ricevuto sul device del ricorrente, come confermato dai LOG di autorizzazione depositati (doc.ti 1, 5 e 6) di cui appresso se ne riporta lo stralcio, dove era espressamente indicato, come avviene sempre, sia l'importo che il beneficiario.
- Il ricorrente per sua ammissione ha infine bloccato la carta solo successivamente alla transazione, alle ore 11:51.
- Quanto alla responsabilità per colpa grave di parte ricorrente, evidenzia che nel caso di specie è occorsa un'ipotesi di phishing, in cui peraltro nessuno dei contatti coinvolti è riconducibile alla banca.
- Non ricorrono elementi di anomalia o indici di rischio ex DM 112/2007, essendosi trattato di una sola transazione che non ha esaurito il plafond della carta.

Con le repliche il ricorrente conferma di aver autorizzato l'operazione, ma evidenzia altresì come il consenso prestato non si è formato correttamente, non avendo avuto contezza dei dati dell'operazione prima di autorizzarla.
Deduce di non aver ricevuto l'SMS riepilogativo de dati del pagamento prima dell'autorizzazione, messaggio della cui ricezione la banca non ha dato prova.
Nelle controrepliche la resistente ribadisce che il messaggio autorizzativo è stato generato dall'APP del ricorrente (come dallo stesso ammesso esser installata e scelta come metodo di autenticazione delle transazioni on line) e dal ricorrente autenticato mediante inserimento del fattore biometrico (FINGERPRINT_FACEID ovvero impronta digitale/riconoscimento facciale).
Quanto alla gestione della pratica di disconoscimento, ne deduce l'irrilevanza ai fini della richiesta di rimborso, giacché riguarda il metodo di comunicazione successivo alla trasmissione del modulo di disconoscimento.
Ad ogni modo deduce che il modulo di disconoscimento indica espressamente di inserire un indirizzo email, poiché tale è il canale tecnicamente predisposto. Il ricorrente ha invece voluto indicare un indirizzo PEC che non è utilizzabile dalla resistente come metodo di comunicazione. In ogni caso la resistente (come documentato dallo stesso ricorrente) ha puntualmente (dopo due giorni) risposto il 28.05.2025 al reclamo del ricorrente del 26.05.2025 evidenziando, relativamente alla gestione del disconoscimento, esattamente quanto segue: "in primis le segnaliamo che la Sua richiesta di disconoscimento è stata ricevuta in data 05/05/2025 e che la stessa è stata regolarmente evasa entro i termini previsti dalla normativa, fornendo riscontro alla Sua Banca in data 06/05/2025, poiché, contrariamente a quanto riportato nel modulo, Lei ha inserito un indirizzo pec di contatto e pertanto non gestibile dai nostri sistemi. In secundis, con la presente, confermiamo l'avvenuta ricezione della richiesta, in data 26/05/2025 e di averla presa in carico. Informiamo inoltre che, dopo aver espletato la necessaria istruttoria, daremo riscontro entro i termini previsti dalla normativa (15gg lavorativi), così come indicati nella specifica sezione reclami del sito della Banca."

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita in data 10 aprile 2025. Risulta pertanto effettuata dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.
Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-*ter*, 5-*quater* e 10-*bis* del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) 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. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.
Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.
2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis*, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-*bis* dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "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. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".
3.- Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-*bis*), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "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".
Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, *dall'Opinion of the European Banking Authority on the elements of strong customer authentication under* PSD2 del 21 giugno 2019.
L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".
4.- La transazione disconosciuta consiste in un'operazione on line, avvenuta il 10.04.2025 (come riportato anche nell'estratto conto) dell'importo di 15.000.000,00 IDR (Rupie Indonesiane), pari ad Euro 831,81 (somma comprensiva della conversione valutaria).
La banca eccepisce che tale pagamento debba considerarsi alla stregua di operazione autorizzata dallo stesso ricorrente e, in quanto tale, estranea all'applicazione degli art. 9 e ss. del d.lgs. 11/2010.
Evidenzia infatti che lo stesso sia stato autorizzato dall'app installata sul device della cliente, a seguito della push autorizzativa ricevuta.
Secondo l'orientamento consolidato dei Collegi, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2.
Rientrano in questa fattispecie le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni "sotto dettatura").

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Nel caso di specie, dalle dichiarazioni fornite dal ricorrente, emerge che l'intenzione di quest'ultimo era quella di autorizzare il pagamento della somma di euro 0,27 per la riconsegna di un pacco del quale era in attesa.
Tale circostanza consente di ritenere ragionevolmente che l'importo della disposizione di pagamento sia stato inserito dal truffatore e non dalla cliente, la quale avrebbe poi validato con fattore biometrico la push autorizzativa.
Pertanto, alla stregua dell'orientamento appena richiamato, l'operazione deve ritenersi non autorizzata dalla ricorrente.
5.- L'app non ha subito enrollment su altri dispositivi: è stato infatti lo stesso Titolare tramite l'APP Relax Banking installata sul proprio dispositivo con DeviceId= 9D86A2DF974B4950B42F920501E4733A sin dal giorno 22/12/2024 e già utilizzata per autorizzare accessi e operazioni, ad aver utilizzato la medesima APP ed il medesimo device per autorizzare ed autenticare la transazione contestata.
L'intermediario versa in atti i log relativi alla sua autenticazione, dai quali si evince l'utilizzo dell'app della ricorrente (push autorizzativa come fattore di possesso) installata sul device e del fattore biometrico (fattore di inerenza).
6.- In data 10.4.2025, parte ricorrente riceveva sul suo cellulare un sms proveniente da un'utenza privata, con il quale, per sbloccare la consegna di un pacco messo "in attesa", veniva invitato a cliccare su uno sconosciuto link.
Il ricorrente ha ammesso di avervi cliccato sopra e di esser stato quindi indirizzato su un sito apparentemente identico a quello dell'intermediario, dove ha inserito i dati della sua carta per autorizzare il pagamento della somma di euro 0,27, accorgendosi solo successivamente che l'addebito della transazione effettuata con la sua carta di pagamento ammontava all'importo di 15.000.000,00 IDR.
A riguardo si osserva che il mittente è riconducibile ad un'utenza privata e il link non contiene alcun riferimento alla banca.
Laddove il ricorrente ammetta di aver dato seguito a una comunicazione di phishing (via email, sms o chiamata vocale, peraltro non proveniente dall'intermediario), i Collegi, in linea con la decisione n. 3498/2012 del Collegio di Coordinamento, ritengono che il cliente sia vittima di colpevole credulità, risultando "tali forme di accalappiamento" "ormai note al pur non espertissimo navigatore di internet" (Collegio di Roma, decisione n. 5554/23; Collegio di Bologna, decisione n. 8419/24).
Quanto alla colpa grave, l'intermediario evidenzia altresì che la parte ricorrente ha ignorato sia la push autorizzativa relativa all'operazione, sia il messaggio di alert.
Parte ricorrente evidenzia che le comunicazioni ricevute in app non contengono il controvalore dell'importo in euro.
Deduce che tale circostanza le avrebbe impedito di avvedersi della reale somma che stava per utilizzare.
Sul punto si rileva che l'art. 5 Reg. UE 2018/389 dispone che:
a) il pagatore è informato dell'importo dell'operazione di pagamento e del beneficiario;
b) il codice di autenticazione generato è specifico per l'importo dell'operazione di pagamento e il beneficiario concordato dal pagatore al momento di disporre l'operazione;
c) il codice di autenticazione accettato dal prestatore di servizi di pagamento corrisponde all'importo specifico originario dell'operazione di pagamento e all'identità del beneficiario approvato dal pagatore;
d) qualsiasi modifica dell'importo o del beneficiario comporta l'invalidamento del codice di autenticazione generato.
Non è espressamente previsto che debba essere indicato al pagatore il controvalore in euro delle operazioni in valuta.
7.- Infine, la parte ricorrente si duole della gestione della pratica di disconoscimento, presentato il 5 maggio 2025, al quale sarebbe stata dato riscontro oltre il termine di 15 giorni.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Al riguardo si osserva che, a seguito di un sollecito del ricorrente del 26.05.2025, in data 28.05.2025 la banca faceva presente di avere riscontrato il disconoscimento già il 6.05.2025 ma di avere indirizzato la risposta alla banca del ricorrente, in quanto questi nel modulo di disconoscimento aveva indicato quale canale di contatto un indirizzo PEC anziché un indirizzo e-mail ordinario, e l'utilizzo della PEC non sarebbe gestibile dai sistemi dell'intermediario.
Acquisita la richiesta di rimborso del 26 maggio 2025, la banca ha poi fornito riscontro negativo il 16 giugno 2025, ossia entro i 15 giorni lavorativi previsti dalle Disposizioni di trasparenza.
8.- Alla luce di quanto esposto, il Collegio ritiene che la domanda non possa trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE