

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 NICOLA CIPRIANI

Seduta del 23/02/2026

FATTO

A. La ricorrente si rivolge all'Arbitro riferendo di essere stata vittima di una truffa su un portale di annunci per compravendite e di avere subito un danno di € 294,76. In particolare, ella illustra di aver messo in vendita un bene e di essere stata contattata da persona interessata all'acquisto che, per effettuare il pagamento, le ha inviato un link a una pagina che imitava l'home page dell'intermediario; poco dopo, la ricorrente ha riscontrato che, anziché ricevere un accredito, le era stato addebitato l'importo di € 294,76, del quale oggi chiede il rimborso.

B. Si è costituito nel procedimento un IMEL, in luogo dell'intermediario convenuto. L'IMEL chiarisce che la ricorrente era titolare di carta collegata a un conto corrente, e che la stessa reclama il rimborso della somma di € 294,76 relativa un'operazione di pagamento e-commerce, autorizzata da APP. Sul punto, l'intermediario fa presente che la ricorrente ha presumibilmente autorizzato l'operazione in app ed evidenzia che l'operazione è stata correttamente autenticata, registrata e contabilizzata, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi, dei quali illustra dettagliatamente il funzionamento. Pertanto, l'IMEL costituito ritiene che l'operazione disconosciuta - tenuto conto della modalità con la quale è stata autorizzata - possa essere stata eseguita soltanto dal titolare dello strumento di pagamento. Quanto alla valutazione della condotta della ricorrente, l'intermediario fa presente che quest'ultima non allega evidenza del link fraudolento ricevuto. In ultimo, il resistente rappresenta che, alla ricezione del reclamo, ha provveduto a inoltrare verso i circuiti internazionali la richiesta di chargeback relativamente alla operazione in questione, ma che la stessa ha ricevuto esito negativo da parte del merchant di riferimento. Pertanto, l'intermediario conclude per il rigetto del ricorso.

DIRITTO

1. La controversia concerne una vicenda di utilizzo non autorizzato di uno strumento di pagamento (artt. 9 ss. d.lgs. 27 gennaio 2010, n. 11), nella specie consistente in un pagamento online dell'importo di € 294,76 eseguito con carta il 09/10/2025 alle ore 14:26.

2. Preliminarmente, il Collegio osserva che l'operazione contestata non può tecnicamente essere considerata quale operazione autorizzata dal cliente. Infatti, nella specie, sebbene l'operazione risulti autorizzata con digitazione del codice ***ID sull'app installata sul device già in uso alla ricorrente - l'inserimento della disposizione di pagamento sembrerebbe essere avvenuto ad opera dei truffatori. Orbene, conformemente all'orientamento consolidato dell'Arbitro, deve ribadirsi che, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale, la transazione non può intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 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.

3. Ciò premesso, il Collegio rileva che l'operazione contestata è stata eseguita sotto il vigore del d.lgs. 27.1.2010, 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 13.1.2018. Inoltre, l'operazione contestata è stata eseguita successivamente all'entrata in vigore delle nuove 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).

4. La disciplina appena 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 (artt. 7 e 12, co. 4, d.lgs. n. 11/2010).

In particolare, "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" (ai sensi dell'art. 10, d.lgs. n. 11/2010). Inoltre, ove l'utente 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'utente 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" (art. 10 comma 2, d.lgs. cit.).

Ai sensi del successivo art. 12, co. 2 bis, d.lgs. cit., "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).

I prestatori di servizi di pagamento sono tenuti a utilizzare l'autenticazione forte "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” (art. 97, comma 1, direttiva UE 2015/2366; art. 10-bis, comma 1, d.lgs. 11/2010).

In relazione alla disciplina richiamata, 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 non superiore a 150 euro). 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. Coord., decisione n. 3947 del 24.6.2014. Più di recente, cfr. Coll. Coord., decisione 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, co. 2, d. lgs. n. 11/2010).

5. Fatte queste premesse, venendo al caso di specie, il Collegio ritiene che il ricorso non possa trovare accoglimento, in quanto da un lato l'intermediario ha fornito adeguata prova del corretto svolgimento delle procedure di autenticazione, registrazione e contabilizzazione; dall'altro deve ritenersi sussistente la colpa grave della ricorrente, la quale ha fornito una decisiva cooperazione affinché le operazioni fraudolente potessero compiersi.

In particolare, l'intermediario eccepisce che l'operazione contestata è stata eseguita con autenticazione dell'utente in modalità SCA. A riguardo, l'intermediario sostiene che le procedure di autenticazione forte adottate sono due, ovvero la procedura “primaria” (push notification in app e codice ***ID) e la procedura “secondaria” (One Time Password (OTP) via SMS e password). Nel caso in esame, la ricorrente ha utilizzato la prima delle due modalità, che garantisce 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). Sul punto, l'intermediario 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 (cfr. controdeduzioni e allegato 7 “La Soluzione *****ID In Ottica Strong Customer Authentication”). Inoltre, il resistente attesta che, ai fini dell'utilizzo del *****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 codice “*****ID” tramite l'inserimento dei seguenti fattori:

- 1) credenziali di accesso ai servizi di internet banking (username e password);
- 2) dati dello strumento di pagamento utilizzato per effettuare i pagamenti online (nel caso della carta PAN, CVV2 e data di scadenza);
- 3) 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.

A sostegno di quanto affermato, l'intermediario produce in atti alcune schermate dalle quali emerge che la transazione è stata effettivamente autorizzata dallo stesso dispositivo in uso alla ricorrente nonché il canale utilizzato per autorizzare le operazioni oggetto di ricorso (app^{***}) e il device id (^{***}D95). Inoltre, l'intermediario afferma che la transazione risulta correttamente eseguita ed autorizzata attraverso l'inserimento del codice ^{*****}ID al ricevimento della notifica in APP e, a riprova, allega in atti:

- 1) estratto indicante il metodo dispositivo della operazione in oggetto, da cui emerge l'utilizzo del Protocollo 3DSecure (sigla 3DS nel campo MOD DISP);
- 2) estratto, con relativa legenda, nel quale risultano presenti il codice 07 (che fa riferimento all'autenticazione dell'operazione tramite riconoscimento biometrico del titolare), il valore "CHALLENGE" all'interno del campo "METODO AUTENTICAZIONE" (che indica con certezza che è stata richiesta una SCA all'utente) nonché il codice "Y" della voce "esito" (che fa riferimento all'autenticazione del titolare della carta, "cardholder authenticated").

Per di più, l'intermediario produce gli estratti informatici dell'operazione contestata, con il dettaglio delle fasi delle transazioni e le tracciatore relative alla firma digitale applicata con il codice ^{*****}ID dalla cliente, dai quali si evince l'utilizzo del medesimo deviceID ^{*****}D95, su cui vi è stato "l'enrollment native app" nell'ottobre 2024. Unitamente a tali tracciatore, il resistente riporta una legenda dei codici utilizzati, dove è specificato che il "deviceID" rappresenta l'identificativo del telefono utilizzato per apporre la firma con il codice ^{*****}ID, che la voce "appID" corrisponde all'identificativo dell'app utilizzata per apporre la firma con il codice ^{*****}ID e che 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.

Ciò premesso, il Collegio ritiene che il sistema di sicurezza adottato dall'intermediario sia conforme alla SCA e che la documentazione tecnica allegata alle controdeduzioni, corredata da legenda esplicativa, sia idonea a dimostrare la corretta autenticazione e la regolarità formale dell'operazione disconosciuta (cfr. Collegio di Bari, decisione n. 9055/2025; decisione n. 4839/2025; decisione n. 10993/2024).

6. In ordine alla colpa grave, deve rilevarsi che la ricorrente non allega, neanche nelle repliche e dopo specifica contestazione dell'intermediario, alcuna evidenza delle interlocuzioni intercorse con i truffatori né del link sul quale assume di essere stata dagli stessi indirizzata. Ebbene, secondo il consolidato orientamento dell'Arbitro (cfr. Collegio di Bari, decisione n. 7120/2024; decisione n. 2663/23; Collegio di Milano, decisione n. 5431/2024), la mancata allegazione del messaggio civetta e/o degli eventuali messaggi scambiati con i truffatori costituisce elemento rilevante ai fini della valutazione della gravità della colpa del cliente, in quanto non consente ai Collegi di valutare se risultino o meno integrati gli estremi di un legittimo affidamento dell'utente circa la genuinità dell'interlocuzione con l'intermediario. Pertanto, alla luce delle considerazioni svolte, il Collegio ritiene che la domanda della ricorrente non sia meritevole di accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE