

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) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) NASO	Membro di designazione rappresentativa dei clienti

Relatore DOMENICO NASO

Seduta del 22/01/2026

FATTO

Con ricorso introduttivo del presente giudizio preceduto da reclamo del 07/08/2025, parte ricorrente chiedeva all'Arbitro Bancario Finanziario il riconoscimento del diritto alla restituzione dell'importo di euro 359,98, corrispondente a due operazioni di pagamento online non autorizzate, eseguite in data 01/08/2025 tramite la sua carta prepagata, nell'ambito di una frode.

Nelle proprie controdeduzioni l'Intermediario resistente contestava preliminarmente la genericità del ricorso e, nel merito, specificava che le operazioni di pagamento veniva correttamente autorizzate dalla ricorrente tramite la digitazione della password (elemento di conoscenza) della ricorrente nell'app *token* dalla medesima installata sul proprio smartphone (elemento di possesso), a seguito della ricezione della notifica *push*.

La Banca insisteva pertanto per il rigetto del ricorso, dovendo l'operazione di pagamento considerarsi autorizzata.

Nelle proprie repliche, la ricorrente sosteneva che l'autenticazione delle operazioni tramite il suo smartphone non escludeva la possibilità che un terzo frodatore si fosse insinuato, senza sua diretta cooperazione.

La Banca, nelle proprie controrepliche, precisava che le operazioni contestate erano state eseguite a distanza di 20 minuti una dall'altra e che la medesima ricorrente, all'interno della querela presentata, asseriva di aver ricevuto una notifica *push*, che avrebbe dovuto allertarla ai fini del blocco precauzionale della carta.

DIRITTO

Parte ricorrente chiede la restituzione della somma complessiva di euro 358,98 relativa a due operazioni di pagamento online disconosciute, eseguite in data 01/08/2025.

Le operazioni contestate sono state effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (cosiddetta 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.

Le suddette operazioni sono altresì successive all'entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Ai fini della verifica del rispetto della Strong Customer Authentication (c.d. SCA), affinché l'Intermediario possa andare esente da responsabilità dovrà fornire prova, oltre che dell'insussistenza di malfunzionamenti, dell'adozione di un sistema di sicurezza adeguato e della corretta registrazione, autenticazione e contabilizzazione delle operazioni contestate.

La previsione dell'art. 10, comma 1, d.lgs. n. 11/2010 [così come introdotto dall'art. 2, comma 10, lettera c) d.lgs. n. 218/2017], in relazione alla prova di autenticazione ed esecuzione delle operazioni di pagamento: *“Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già 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”*.

Il comma secondo della medesima norma precisa che: *“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, compreso, se del caso, il prestatore di servizi di disposizione di ordine 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
”.

Come sancito dal Collegio di Coordinamento con la decisione n. 22745/19: *<<...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>>*.

Secondo l'orientamento condiviso dai Collegi, quando l'operazione è eseguita per intero dal pagatore, deve considerarsi autorizzata e pertanto non soggetta al regime di responsabilità di cui alla PSD2.

Nella fattispecie per cui è causa, la ricorrente contesta il mancato blocco preventivo da parte dell'Intermediario, a fronte della natura anomala rispetto al profilo di spesa.

Il Regolamento Delegato (UE) n. 2018/389 della Commissione, in tema di monitoraggio preventivo delle operazioni di pagamento, sancisce all'art. 2 la possibilità in capo agli Intermediari di attivare meccanismi di monitoraggio in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente, anche laddove le predette *<<...per frequenza oltre che per consistenza appaiano ictu oculi assolutamente non in linea con un'operatività fisiologica>>* e dunque anomale (Cfr. Collegio di Roma, decisione n. 8019 del 28/07/2023).

Pur tuttavia, le due operazioni oggetto della presente controversia, non risultano anomale, trattandosi di un importo complessivo relativamente modesto, tale da non ingenerare alcun onere di monitoraggio preventivo in capo alla Banca resistente.

Le operazioni contestate sono state autorizzate tramite la digitazione della password (elemento di conoscenza) della ricorrente all'interno dell'app token installata sul suo smartphone (elemento di possesso), a seguito della ricezione di una notifica *push*.

Dai *log* depositati in atti, risulta l'utilizzo del *token* in uso alla ricorrente (elemento di possesso) in fase di autenticazione delle operazioni.

Le operazioni risultano pertanto correttamente autorizzate dalla ricorrente, circostanza la quale deve essere valutata unitamente alla mancata contestualizzazione dei fatti da parte della predetta, la quale non ha ricostruito le modalità della truffa, limitandosi ad affermare la ricezione delle due notifiche relative all'autenticazione delle operazioni online.

Secondo il condiviso orientamento dei Collegi, ai fini dell'applicazione della PSD2, è necessario e sufficiente che il cliente neghi di aver autorizzato la transazione; in ogni caso, dopo aver verificato la sussistenza della SCA, il Collegio può valutare la mancata allegazione dei fatti quale elemento ulteriore ai fini della formazione del proprio convincimento in ordine alla colpa grave del ricorrente (cfr. Collegio di Roma, decisione n. 13177/2024; in senso conforme, Collegio di Roma, decisione n. 8058/2022).

Nella fattispecie per cui è causa, ulteriore elemento rilevante attiene alla scarsa contestualizzazione dei fatti, che ingenera in capo al Collegio il proprio convincimento circa la colpa grave della ricorrente.

Alla luce dei suddetti principi, non può ravvisarsi alcuna colpa in capo all'Intermediario, essendo ravvisabile una esclusiva responsabilità in capo alla ricorrente, la quale ha autorizzato ed autenticato le operazioni di pagamento online contestate.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE