Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	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 MARCO MARINARO

Seduta del 04/12/2025

FATTO

La parte ricorrente riferisce che in data 12/6/2025 aveva tentato un pagamento online di € 2,17 con la propria carta di debito al fine di “sbloccare un pacco” sul sito dello spedizioniere. Il pagamento in discorso non andava a buon fine.
In data 14/6/2025 veniva contattata da un numero di telefono riconducibile al servizio antifrode dell’intermediario per bloccare un pagamento sospetto di € 1.000,00. Provvedeva in tal sede a richiedere il blocco della carta.
In tali circostanze, si avvedeva che il giorno 12/6 era stato effettuato un pagamento di € 418,57, che nega di aver mai autorizzato.
Ha presentato reclamo all’intermediario e sostiene di non aver sporto denuncia querela alle autorità in quanto era riuscita a bloccare prontamente la carta e auspicava nel buon esito delle richieste bonarie formulate alla banca.
Chiede la restituzione dell’importo di € 418,57.
L’intermediario chiede che il ricorso venga respinto, sulla base delle seguenti argomentazioni:
- risulta documentalmente provato che:

(i) l’operazione di pagamento e-commerce di 418,57 euro si è perfezionata attraverso il servizio 3D Secure;
(ii) i sistemi informatici della Banca hanno correttamente performato, contabilizzando e registrando le operazioni regolarmente autorizzate dall’utente;
(iii) la banca è assolutamente estranea nella causazione degli eventi che hanno determinato il danno lamentato da parte ricorrente, risultando esonerata da qualsiasi responsabilità;

- parte ricorrente non ha offerto alcuna prova del fatto che l’episodio lamentato sia da ricondursi a colpa della banca;

- inoltre, l'operazione di pagamento contestata non presentava indici di anomalia tali da impedirne ex lege il perfezionamento;
- l'evento criminoso, pertanto, si è perfezionato grazie al consenso di parte ricorrente in quanto ha necessariamente comunicato al truffatore – in violazione del dovere di custodia – i dati funzionali all'utilizzo della carta di credito per l'esecuzione dell'operazione ecommerce, quali: a) dati statici della carta (numero di PAN; nome e cognome; scadenza; CVV); b) codice Key6 (fattore di conoscenza); c) codice OTP trasmesso a mezzo SMS all'utenza telefonica certificata (fattore di possesso).

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita il 12 giugno 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 tale operazione è altresì successiva 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.- Nel caso in esame, l'unica operazione contestata consiste in un pagamento online dell'importo di € 418,57, disposta alle ore 11:37 del 12/6/2025.

L'intermediario deduce che l'operazione è stata autenticata tramite tecnologia multifattoriale, tramite il sistema 3Ds e precisamente utilizzando (i) il fattore di possesso, consistente nella ricezione del codice OTP e (ii) il fattore di conoscenza, vale a dire l'inserimento del codice Key6, precedentemente scelto dal titolare e di sua esclusiva conoscenza.

Produce all'uopo le relative evidenze informatiche. Dai LOG informatici vi è conferma del fatto che l'operazione è stata autenticata tramite il sistema 3Ds 2.0.

Dai Log informatici prodotti dall'intermediario, emerge, pertanto, che l'autenticazione delle operazioni è avvenuta per mezzo di password dinamica (risulta infatti valorizzato 2nd factor Authentication Code il valore 02 – OTP via SMS method) e inserimento del codice K***6.

L'intermediario produce, inoltre, evidenza dell'SMS OTP trasmesso al numero certificato in uso alla ricorrente.

Il messaggio SMS OTP contiene altresì i dettagli dell'operazione da confermare ("Per confermare l'acquisto di 418.57 EUR con la carta ***, digita il codice").

La ricezione di tale SMS non è contestata dalla cliente, che non ha prodotto repliche alle controdeduzioni.

I Collegi ABF hanno affermato in più occasioni che il sistema di autenticazione 3dS 2.0 utilizzato dall'intermediario risulta essere compliant rispetto alla SCA (ex multiis, Collegio di Roma, decisione n. 723/2023).

5.- La ricorrente sostiene di non aver mai autorizzato l'operazione disconosciuta e di non aver comunicato i propri codici identificativi.

Dalla memoria difensiva allegata al ricorso emerge che, il giorno in cui risulta disposto il pagamento disconosciuto, aveva tentato un pagamento di € 2,17 sul sito dello spedizioniere al fine di "sbloccare un pacco".

La ricorrente dichiara di non aver sporto denuncia querela auspicando nella risoluzione bonaria della controversia. Non sembrerebbero emergere ulteriori elementi dai quali poter ricostruire più dettagliatamente la dinamica della frode.

Ciò considerato, unitamente alle allegazioni della banca circa le modalità di autenticazione, sembrerebbe plausibile ritenere che i codici autorizzativi siano stati digitati direttamente dalla cliente sul sito web apparentemente riconducibile allo spedizioniere, nell'erronea convinzione di "sbloccare un pacco".

In assenza di allegazioni in ordine alle modalità di "adescamento" della ricorrente, non è possibile ricondurre la frode a uno schema "sofisticato" in occasione del quale il Collegio di norma esclude (parzialmente o totalmente) la sussistenza di una colpa grave in capo al cliente.

Si richiama sul punto la consolidata giurisprudenza ABF che fa gravare sul ricorrente la scarsa contestualizzazione dei fatti di cui al ricorso, riconoscendone la colpa grave e rigettando pertanto i ricorsi (Collegio di Roma, n. 7046 del 11.07.2023).

6.- Invero, ferma restando l'allocazione dell'onere della prova a carico dell'intermediario, questo Collegio ritiene che sussista in capo al ricorrente un onere di allegazione delle circostanze che possano, al minimo, offrire una attendibile ipotesi alternativa rispetto a quella, altrimenti residuale (ed

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

anzi unica), dell'utilizzo imputabile (direttamente o per colpa grave) al titolare (Coll. Roma, dec. n. 10723/19).

7.- Per cui il Collegio osserva che, ai sensi dell'art. 10 del D. Lgs. 27 gennaio 2010, n. 11, come in vigore dal 13 gennaio 2018, grava sul prestatore di servizi l'onere di dimostrare che l'operazione di pagamento sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

Nel caso di specie, l'intermediario ha prodotto evidenza della corretta autorizzazione dell'operazione contestata.

Come già ritenuto in diverse occasioni da questo Collegio, il ricorso ad un sistema di autenticazione a doppio fattore, in assenza di malfunzionamento del sistema, consente di ritenere che l'intermediario abbia assolto all'onere della prova che la legge gli impone in caso di disconoscimento di una operazione di pagamento.

Infatti, a fronte di una allegazione generica di disconoscimento dell'operazione della parte ricorrente, l'intermediario ha documentato che l'operazione contestata è stata correttamente autenticata, registrata e contabilizzata.

Non si ravvisano, d'altro canto, elementi idonei ad imputare una qualche responsabilità in capo all'intermediario resistente.

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