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

Relatore MARCO MARINARO

Seduta del 17/04/2026

FATTO

La parte ricorrente espone quanto segue.
i) Il 27/09/2024, alle ore 20.13, riceveva un messaggio dal proprio gestore telefonico nel quale veniva riferito che se fosse entrata nel link inserito nel messaggio avrebbe avuto la possibilità di vincere dei premi.
ii) La ricorrente entrava nel link e veniva reindirizzata in una pagina simile ad un catalogo premi. Sceglieva quindi il suo premio e la pagina richiedeva i dati della spedizione oltre ai dati della carta per effettuare un piccolo pagamento come saldo per ricevere il regalo.
iii) Inseriti i dati bancari riceveva dall'app della banca la richiesta di autorizzazione di un pagamento pari all'importo di 0,00 UAH (moneta ucraina), autorizzava quindi il pagamento e immediatamente dopo riceveva un'altra richiesta di autorizzazione, stavolta dell'importo di 21.080,00 UAH (459,98 euro).
iv) Tentava invano di non autorizzare il pagamento ma l'importo veniva scalato dal conto a favore di un e-commerce.
v) Specifica quindi di non aver autorizzato il pagamento di tale somma in quanto non ha avuto possibilità di poter cliccare di no quando la banca chiedeva l'autorizzazione al pagamento.
vi) Successivamente bloccava la sua carta di pagamento e sporgeva denuncia.
vii) La transazione fraudolenta è stata in attesa di essere contabilizzata per settimane. La banca avrebbe dovuto occuparsi di impugnare la transazione ed annullarla, poiché immediatamente dopo il prelievo fraudolento si è premurata di bloccare la carta e denunciare il fatto.

La parte ricorrente chiede il rimborso dell'importo sottratto pari a 459,98 euro.
L'intermediario resiste al ricorso ed eccepisce quanto segue.
i) La ricorrente è stata vittima di una frode online, come da lei stessa riferito, mentre nessuna evidenza è stata allegata al ricorso rispetto al messaggio ricevuto, all'indirizzo URL di cui al Link ricevuto e al dominio del sito a cui avrebbe avuto accesso la ricorrente. Inoltre, non si produce evidenza dell'operazione di pagamento, eventuali SMS e messaggi ricevuti, e nemmeno del sito al cui interno sarebbero state inserito le credenziali della carta.
ii) L'onere di verificare l'attendibilità di un sito prima di acquistare un bene e/o un servizio ricade sul ricorrente che sta eseguendo la transazione.
iii) La ricorrente ha in autonomia scelto di accedere al sito e inserire i propri dati, autorizzando la transazione con strong authentication. Avrebbe dovuto riconoscere la frode dal momento che ogni notifica ricevuta ed autorizzata riepilogava i dati dell'operazione in corso: l'esercente indicato in ciascuna transazione non era mai il suo operatore telefonico. Per giunta, l'operazione si è svolta in moneta estera Ucraina. Non è neanche riferito nel ricorso se la ricorrente abbia mai contattato il servizio clienti del merchant per riferire l'accaduto.
iv) Dall'analisi della pratica di frode ed a seguito di quanto dichiarato nella denuncia è evidente che la ricorrente è rimasta vittima di phishing, pur non avendo ricevuto messaggi SMS provenienti o riconducibili alla banca. A seguito di un messaggio apparentemente proveniente da un operatore telefonico, ha consapevolmente disposto un'operazione di pagamento a favore di un operatore economico, che si è successivamente rivelato diverso da quello creduto dalla ricorrente stessa, autorizzando personalmente il pagamento della somma addebitata sul proprio conto corrente.
v) Considerato che l'operazione è stata correttamente autenticata con 3DS non era possibile effettuare un tentativo di recupero e, pertanto, in seguito agli accertamenti disposti dalla funzione antifrode della banca, il rimborso è stato stornato.
vi) La transazione è stata autorizzata con strong authentication (ricezione notifica push + riconoscimento biometrico) e non è stata rilevata alcuna anomalia, come risulta dalle evidenze all'interno dei sistemi informatici della banca.
vii) Le transazioni effettuate con una carta di pagamento non possono essere né annullate né sospese ma, eventualmente, contestate. Il pagamento è stato contabilizzato in data 29/09/2024 e in pari data la somma è stata riconosciuto al beneficiario, ma, a causa del blocco della carta, l'addebito è rimasto fra i sospesi di Filiale ed è stato poi addebitato sul conto collegato alla carta solamente in data 28/10/2024.
viii) La banca ritiene di aver messo a disposizione del ricorrente tutti i possibili mezzi per riconoscere e di conseguenza evitare il raggiro, nonché di aver attivato tutti i necessari presidi a protezione delle transazioni. Nessun accorgimento antifrode può però essere efficace se le operazioni a carattere fraudolento vengono realizzate mediante la collaborazione del titolare del conto.
ix) La banca, attraverso il costante aggiornamento del proprio sito e proprio per cercare di prevenire il fenomeno del phishing, fornisce tutte le raccomandazioni e le informazioni sulla sicurezza online, indicando chiaramente che è opportuno:
• non inserire in nessun sito web password o numeri di carte di credito/debito, senza aver prima verificato che la trasmissione dati risulti "sicura" e che il sito web sia autentico.
• imparare a riconoscere le comunicazioni false.
Alla luce di quanto precede la banca chiede di respingere il ricorso perché infondato siccome costruito su una pretesa ed inesistente responsabilità della banca.
Nelle repliche la parte ricorrente ricapitola i fatti e aggiunge quanto segue.
i) È stata tratta in inganno da un messaggio SMS che appariva inserito nella stessa conversazione di precedenti messaggi legittimi provenienti dal proprio operatore telefonico che proponeva un'offerta promozionale del tutto simile ad altre offerte reperibili online.

ii) Non ha mai comunicato a terzi né le proprie credenziali bancarie né codici OTP, né ha mai autorizzato consapevolmente un'operazione fraudolenta.
iii) Riguardo all'assenza di screenshot del messaggio o del sito, in una situazione di forte agitazione e timore per ulteriori danni, la reazione è stata quella di chiudere il sito e cancellare il messaggio, dedicandosi esclusivamente al blocco della carta ed alla segnalazione dell'accaduto.
Nelle controrepliche la banca si riporta a quanto dedotto nelle controdeduzioni.

DIRITTO

1.- L'operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita in data 27 settembre 2024. 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 parte ricorrente chiede il rimborso della somma di 459,98 euro, corrispondente all'importo distratto con l'operazione disconosciuta.

L'intermediario afferma che la transazione contestata dalla ricorrente è stata autorizzata con strong authentication (ricezione notifica push + riconoscimento biometrico) e che non è stata rilevata alcuna anomalia.

Viene prodotta evidenza della documentazione tecnica attestante l'avvenuta autenticazione tramite notifica push (fattore di possesso) e riconoscimento biometrico (fattore di inerenza).

Schermate analoghe a quelle in esame sono state considerate da questo Collegio idonee a provare l'autenticazione forte (Collegio di Roma, decisione n. 8856 del 26/07/2024.).

5.- La ricorrente dichiara di aver ricevuto un messaggio dal proprio gestore telefonico nel quale veniva riferito che se fosse entrata nel link inserito nel messaggio avrebbe avuto la possibilità di vincere dei premi.

La ricorrente afferma di aver inserito i propri dati bancari e di aver ricevuto dall'app della banca la richiesta di autorizzazione di un pagamento pari all'importo di 0,00 UAH (moneta ucraina), che provvedeva ad autorizzare. Immediatamente dopo riceveva un'altra richiesta di autorizzazione, stavolta dell'importo di 21.080,00 UAH (459,98 euro).

Tentava invano di non autorizzare il pagamento ma l'importo veniva scalato dal conto a favore di un e-commerce.

6.- La parte ricorrente riferisce che la truffa ha avuto origine da un sms del proprio gestore telefonico nel quale veniva riferito che se fosse entrata nel link inserito nel messaggio avrebbe avuto la possibilità di vincere dei premi.

La ricorrente afferma di aver cancellato il messaggio in questione. In ogni caso, il mittente, come da lei stessa dichiarato, è un'utenza non riconducibile alla banca.

Il caso in esame è pacificamente un'ipotesi di smishing, che secondo l'orientamento dell'ABF non costituisce un tipo di frode sofisticata (Collegio di Roma, decisione n. 9294/2019).

7.- La ricorrente ammette di aver disposto in prima persona l'operazione in contestazione.

Secondo l'orientamento condiviso tra i 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").

In questi casi, dunque, non è configurabile una responsabilità oggettiva del PSP.

Il Collegio potrà comunque rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode.

Tuttavia, dall'esame istruttorio è emerso che, nel caso di specie, non risultano sms truffaldini provenienti dal canale ufficiale della banca o comunque in qualche modo astrattamente riferibili alla stessa.

Alla luce dei suddetti principi, tenuto conto della estraneità dell'intermediario resistente alla frode perpetrata, non può ravvisarsi alcuna colpa in capo allo stesso, essendo ravvisabile una esclusiva

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

responsabilità della parte ricorrente, per aver dato seguito con ingenuità alla truffa perpetrata (Collegio di Roma, decisione n. 7622 del 1/8/2025).
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