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) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 09/01/2026

FATTO

Nel ricorso, l'istante espone quanto segue:
- in data 15/07/25, ha messo in vendita un bene su una nota piattaforma e al momento della vendita ha cliccato il tasto conferma vendita, si è dunque aperta una pagina in cui le è stato chiesto di ricevere i soldi sul conto e ha inserito il codice dell'app; da quel momento ha subito due operazioni di addebito rispettivamente di € 199,00 e di € 99,00;
- a quel punto un operatore della banca resistente l'ha contattata e gli ha chiesto se le operazioni fossero genuine e dunque ha bloccato l'ultima operazione per la somma di € 200,00;
- si è recata presso la banca resistente e ha bloccato la carta; nonostante ciò, le operazioni sono state contabilizzate in data 17.07.2025.

Chiede la restituzione di € 298,00.
Nelle controdeduzioni, l'intermediario eccepisce quanto segue:
- la parte ricorrente è titolare della carta di debito n. *480 sulla quale sono state eseguite, tramite app bancaria, due operazioni fraudolente per complessivi € 298,01 in data 15.05.2025;
- la frode perpetrata ai danni della cliente sembrerebbe essere riconducibile allo schema del "phishing" classico, nel quale il malcapitato, comunicati i propri codici, consente al frodatore di predisporre operazioni dispositive, che vengono poi inconsapevolmente autorizzate sul proprio dispositivo dal soggetto frodato;

• in ogni caso, le operazioni disconosciute sono state correttamente autenticate senza alcuna compromissione dei sistemi di sicurezza del resistente; i frodatori sono infatti riusciti ad aggirare il processo di enrollment in SCA attraverso la necessaria partecipazione della cliente per carpire i dati personali ed i codici di sicurezza, ovvero attraverso le tecniche comuni di Social Engineering;
• più precisamente risulta regolarmente avvenuta: la fase di enrollment della carta di pagamento n. *480 della parte ricorrente al sistema autorizzativo di tipo dinamico; la fase di Log-in nella quale la ricorrente risulta essersi autenticata nella data indicata alla propria Home Banking mediante digitazione delle credenziali (userid e password) e successivo inserimento del codice P**ID necessario per accedere alla propria area personale ed infine la fase dispositiva delle operazioni oggetto di ricorso, avvenuta con inserimento del codice P**ID del ricorrente;
• in relazione alle operazioni in oggetto l'utenza telefonica collegata alla posizione del ricorrente non sembra aver ricevuto alcuna modifica e anche il device utilizzato non sembra aver subito modifiche;
• è presumibile che la ricorrente dopo aver concluso la vendita abbia comunicato i dati dello strumento di pagamento al falso acquirente e, successivamente, abbia autorizzato sul proprio dispositivo le operazioni oggetto della materia del contendere;
• la ricorrente, infatti, nel modulo di ricorso ammette e afferma di aver digitato nella APP il codice autorizzativo;
• il blocco/estinzione della carta in questione è avvenuto alle ore 15:17, del giorno 15/07/2025 pertanto successivamente alle operazioni per cui è controversia;
• peraltro, era attivo di default il servizio di SMS alert e push notification.

Chiede il rigetto del ricorso.

Nelle repliche, la parte ricorrente:

• conferma di aver autenticato di persona le operazioni fraudolente in quanto è stata raggirata dai frodatori;
• quanto all'obbligo di monitoraggio, ella si è accorta della frode grazie ad un operatore della banca che l'ha chiamata ed avvisata dei movimenti sospetti ed è riuscita così a bloccare il bancomat.

Nelle controrepliche l'intermediario si riporta alle precedenti difese.

DIRITTO

Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite in data 15 luglio 2025. Risultano pertanto effettuate 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.

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".
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)*".
La controversia ha ad oggetto due operazioni fraudolente eseguita in data 15.07.2025, tramite app bancaria. Si tratta in particolare di: un pagamento di € 199,00; un pagamento di € 99,01; per complessivi € 298,01.
L'intermediario afferma che le operazioni di pagamento risultano correttamente autenticate, registrate e contabilizzate e che non è emerso alcun malfunzionamento o compromissione dei sistemi.
L'intermediario produce il LOG relativo all'enrollment dello strumento di pagamento da cui risulta che l'app era stata installata a giugno 2021 sul device in uso alla ricorrente.
Pertanto, il frodatore non sembra aver installato l'app sul suo dispositivo. Ciò significa che l'operazione dispositiva è avvenuta sul device della ricorrente.
L'intermediario produce altresì i LOG da cui si evince che l'accesso all'app bancaria, propedeutico alle operazioni dispositive, è avvenuto mediante il codice P**ID (fattore di conoscenza).
Dai LOG emerge che le operazioni dispositive sono state effettuate sull'app bancaria installata sul device della ricorrente (fattore di possesso).
Inoltre, vi è stato inserimento del fattore biometrico o di conoscenza (cfr. il codice 07 sotto la voce "tipo di autenticazione").
In particolare, l'intermediario fa presente che dalle schermate dei LOG, si evince che parte ricorrente ha utilizzato la modalità primaria, con inserimento del codice P**Id all'interno dell'app in seguito a ricezione della notifica push.
Tale modalità è evidenziata all'interno delle schermate dal codice 07 presente nel campo TIPO AUTENTICAZIONE.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Secondo la legenda esplicativa, il codice 07 fa riferimento all'autenticazione dell'operazione tramite riconoscimento biometrico del titolare, il quale è possibile solo qualora il cliente stesso sia titolare di certificato P**Id.
Tale modalità può infatti essere scelta come alternativa all'inserimento del codice P** Id, qualora il device sia abilitato.
Per utilizzare il codice identificativo alfanumerico in App il cliente può seguire una delle seguenti modalità: inserire manualmente il codice alfanumerico; apporre una delle impronte digitali (modalità Fingerprint) registrate sul sistema operativo del dispositivo mobile; utilizzare altre modalità biometriche eventualmente rese disponibili tramite il sistema operativo del device.
Si osserva altresì che la presenza del valore CHALLENGE all'interno del campo METODO AUTENTICAZIONE indica con certezza che è stata richiesta una SCA all'utente.
Tale sistema è stato ritenuto conforme a SCA dal Collegio (Collegio di Roma, decisione n. 15522/2022).
In base a quanto emerge dalla denuncia:

- in data 15.07.2025, la ricorrente stava effettuando una vendita su un noto portale quando è rimasta vittima di phishing;
- in particolare, al momento di finalizzare la vendita ha cliccato il tasto di conferma vendita e si è aperta una pagina in cui gli è stato chiesto di ricevere i soldi sul conto; ha inserito il codice dell'app e da quel momento ha subito due operazioni di addebito rispettivamente di € 199,00 e di € 99,00;
- a quel punto un operatore della banca resistente l'ha contattata e le ha chiesto se le operazioni erano genuine e dunque ha bloccato l'ultima operazione per la somma di € 200,00;
- la parte ricorrente ha prodotto il registro chiamate da cui risulta una telefonata in entrata presumibilmente riferibile al numero dell'intermediario resistente, sembrerebbe però trattarsi della chiamata con la quale un operatore del resistente l'ha avvisata delle operazioni fraudolente; Infatti, la chiamata è delle ore 13:20 e le operazioni fraudolente sono state eseguite alle ore 11:50 e alle ore 11:57.

Nel caso di specie, il ricorrente ha instaurato le trattative per la vendita di un bene su un sito internet non riconducibile al resistente.
È possibile che i frodatori abbiano reindirizzato la ricorrente su un sito clone dell'e-commerce dove ella ha inserito i codici segreti dell'app bancaria.
In tali ipotesi, i Collegi tendono ad escludere la responsabilità della banca non essendovi stata compromissione dei suoi sistemi di sicurezza (Collegio di Roma, decisione n. 6534 del 4 giugno 2024; Collegio di Milano, decisione n. 12607 del 5 dicembre 2024).
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