

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore STEFANO DEPLANO

Seduta del 18/02/2026

FATTO

Parte ricorrente rappresenta che: i.) in data 13 marzo 2025, intorno alle ore 16:50, ha ricevuto un SMS recante l'intestazione all'Intermediario; ii.) il messaggio la allertava di un'imminente autorizzazione al trasferimento di denaro e la invitava, del pari, a contattare un numero telefonico; iii.) alcuni minuti dopo ha ricevuto una chiamata da parte di un'utenza recante il logo dell'Intermediario convenuto nella quale un sedicente operatore la informava della necessità di svolgere alcune operazioni di "prova" che presupponevano la comunicazione dei codici OTP; iv.) prestando fede all'interlocutore, ha dato séguito alla richiesta; v.) insospettita dalla petulanza del chiamante, si è avveduta della natura truffaldina dell'operazione; vi.) pur avendo immediatamente posto fine alla chiamata, ha riscontrato un ammanco pari a 989,40 (novecentoottantanove/quaranta) euro; vii.) ha provveduto a bloccare la carta e a disconoscere le transazioni effettuate.

Parte resistente riferisce che: i.) l'operazione di pagamento in contestazione risulta correttamente approvata tramite un sistema di autenticazione forte e senza alcuna anomalia, nel rispetto dei requisiti SCA; ii.) la ricorrente è stata vittima di *phishing* e *vishing*.

In sede di repliche si ventila la possibilità che i truffatori fossero in possesso delle credenziali riservate. In sede di controrepliche l'Intermediario si riporta integralmente alle controdeduzioni.

Parte ricorrente chiede la restituzione della somma di 989,40 (novecentoottantanove/quaranta) euro (oltre interessi e rivalutazione) corrispondente all'importo di una operazione di rimessa denaro.

Parte resistente insiste per il rigetto del ricorso.

DIRITTO

1. – La controversia ha ad oggetto il disconoscimento di un'operazione di pagamento disposta *online* in data 13 marzo 2025 con carta collegata a un libretto di risparmio intestato alla ricorrente. Si chiede il rimborso di una somma pari a 989,40 euro, in particolare 970,00 euro a titolo di pagamento e 19,40 euro a titolo di commissioni.
2. – Mette conto evidenziare nel dettaglio l'operazione realizzatasi.
 - 2.1. – Tramite i sistemi informatici dell'Intermediario è stato effettuato un bonifico verso un soggetto giuridico estraneo al presente giudizio che ha successivamente trasferito la somma oggetto dell'atto di disposizione per cui è controversia. In tal modo si è costituita la provvista attraverso una transazione in addebito su un libretto di risparmio intestato alla ricorrente.
 - 2.2. – L'intera operazione si può suddividere nelle seguenti quattro fasi: creazione di provvista con trasferimento dei fondi da libretto di risparmio verso una carta prepagata; *enrollment* della carta di pagamento intestata alla ricorrente nel sistema autorizzativo di tipo dinamico tramite *password* inviata con SMS; *login* in APP; fase dispositiva *stricto sensu* dell'operazione oggetto del ricorso.
3. – Con riferimento alla prima fase, l'operazione è stata autorizzata con un codice OTP inviato sul numero di telefono certificato.
4. – Quanto all'*enrollment* l'Intermediario afferma che è stata seguita una procedura che prevede l'impiego di credenziali statiche (*username* e *password*, elementi di conoscenza) e una *password* dinamica OTP trasmessa via SMS al cellulare certificato (elemento di possesso). L'Intermediario ha rilevato che il numero securizzato sulla carta di pagamento della ricorrente è il medesimo evidenziato nel modulo di contestazione di addebito. Si rappresenta, inoltre, che la carta della ricorrente, nella data in cui si è verificata l'operazione contestata, è stata associata su un nuovo dispositivo. Tale operazione è stata possibile a séguito dell'inserimento del codice OTP ricevuto sul numero di telefono certificato della cliente.
5. – L'operazione è stata posta in essere, previo accesso alla piattaforma di *home banking*/APP dell'Intermediario, il quale descrive nel dettaglio l'infrastruttura tecnologica utilizzata. L'utente risulta essersi autenticato mediante digitazione delle credenziali e successivo inserimento del codice necessario per accedere alla propria area personale.
6. – Le operazioni contestate sono state effettuate sotto la vigenza del d.lgs. n. 11 del 2010, così come modificato dal d.lgs. n. 218 del 2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). In base a tali disposizioni, come applicate da questo Arbitro (cfr. Coll. Coord., dec. n. 22745 del 2019), occorre volgere l'attenzione a due dirimenti profili disciplinari. In primo luogo, è l'Intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni, dovendo in particolare fornire evidenza che le operazioni disconosciute siano state autenticate con un c.d. "Sistema di autenticazione forte" (SCA), posto che ai sensi del comma 2 *bis*, art. 12, d.lgs. n. 11 del 2010, come inserito dal d.lgs. n. 218 del 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 accertano l'autenticazione forte del cliente». In secondo luogo, è sempre l'Intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.
7. – Con riferimento al primo profilo, visto quanto versato in atti, l'Intermediario ha dato prova che la modalità autorizzativa è avvenuta secondo procedura SCA, in particolare mediante *notification* in APP e inserimento del codice riservato. L'operazione è stata dunque eseguita tramite il fattore di conoscenza e il fattore di possesso.

7.1. – Alla luce di quanto esposto l'Intermediario ha dimostrato di essersi dotato di un sistema di autenticazione forte in linea con la normativa di settore sopra richiamata (cfr. Coll. Roma, dec. n. 15522 del 2022).

8. – Con riferimento al secondo profilo innanzi richiamato, la ricorrente afferma di essere stata contattata da un sedicente operatore dell'Intermediario in relazione ad alcuni movimenti sospetti. La fattispecie – come posto in luce dal convenuto – appare assimilabile ad una ipotesi non particolarmente sofisticata di *phishing* e *vishing*, nella quale codesto Arbitro è solito riconoscere la colpa grave ed esclusiva del cliente (cfr. Coll. Roma, dec. n. 1479 del 2024).

9. – La condotta della ricorrente risulta caratterizzata da colpa grave anche per aver prestato fede a messaggi SMS e chiamate recanti l'intestazione dell'Intermediario ma non provenienti da utenze ad esso riconducibili.

10. – Si nota, per completezza, che l'Intermediario produce evidenza dell'invio di notifiche in APP in relazione all'operazione contestata.

11. – Tanto premesso, il ricorso non è fondato e non può essere accolto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE