

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

Relatore MASSIMO CARATELLI

Seduta del 22/12/2025

FATTO

La controversia verte sulla contestazione di alcuni addebiti operati attraverso il servizio di home banking a valere su di un conto corrente intrattenuto dal proponente presso la convenuta.

In particolare, in base alla dinamica riferita da parte attrice, l'istante – in data 15 dicembre 2024, alle ore 17.00 – riceveva sul proprio *device* un messaggio proveniente da un'utenza cellulare con il quale la banca avvisava la ricorrente dell'esecuzione di un prelievo di euro 3.000,00 esortandola a contattare l'utenza telefonica indicata nel messaggio stesso in caso di disconoscimento. L'SMS citato veniva visualizzato solo l'indomani dall'interessata che provvedeva a chiamare il numero indicato. Nel corso dell'interlocuzione telefonica un sedicente operatore dell'istituto di credito, dopo averla ricontattata da un altro numero, le comunicava che il conto a lei intestato *“era stato letteralmente prosciugato”*, invitandola a seguire le istruzioni impartite al fine di recuperare gli importi sottratti. Il sedicente operatore la guidava, quindi, nella creazione di due strumenti di pagamento virtuali associati alla carta di debito e alla prepagata di sua titolarità indicandole l'importo che avrebbe dovuto trasferire sulle carte in corso di attivazione; le comunicava, infine, che nel giro di 48 ore il conto sarebbe stato reintegrato

delle somme indebitamente sottratte. A questo punto, parte attrice contattava il servizio clienti e apprendeva di essere rimasta vittima di una truffa. L'operatore della banca la rassicurava circa il blocco tempestivo delle carte ma, ciononostante, continuavano le operazioni per le quali l'istante riceveva anche dei messaggi di *alert*. I malviventi provvedevano, inoltre, ad attivare un'altra carta che perveniva fisicamente l'indomani all'indirizzo di residenza di parte attrice che la riconsegnava quello stesso giorno alla filiale. Tale carta, tuttavia, veniva materialmente attivata prima della consegna fisica e, in quel lasso di tempo, i malviventi le causavano un ammanco di ulteriori euro 118,31. Tanto ricostruito, l'istante rileva che il numero dal quale perveniva il messaggio veniva segnalato come truffaldino già in epoca antecedente alla truffa subita, senza che nessuna autorità si attivasse per sventare l'operatività fraudolenta. Ritiene la proponente che chi ha agito dietro quel numero sapeva che il conto era intestato ad una signora di 84 anni verosimilmente *"in condizione di minorata difesa dinanzi alle minacce con strumenti di telecomunicazione avanzata"*. Ciò posto, l'ammanco complessivo sofferto di cui la ricorrente chiede la restituzione ammonta ad euro 14.625,37.

Con le controdeduzioni parte convenuta chiarisce che la ricorrente era titolare della carta prepagata n.***074 e della carta di debito n.***425, attualmente estinte, abilitate al servizio di home banking, in relazione alle quali – in data 16 dicembre 2024 – sono state eseguite operazioni per un totale disconosciuto di euro 10.235,11. Tale ammontare si discosta dal *petitum* del ricorso che dovrà quindi essere deciso nei limiti dell'importo delle operazioni effettivamente disconosciute in sede prodromica al ricorso stesso. Aggiunge la convenuta che, come dichiarato anche in sede di denuncia, le operazioni oggetto di contestazione sono state disposte dalla stessa ricorrente con il *device* usualmente utilizzato per l'operatività on line, previa creazione delle carte virtuali a valere sulle carte di pagamento ad essa intestate. Le operazioni, dunque, devono qualificarsi come autorizzate ai sensi dell'art. 5, commi 1 e 2, d.lgs. 11/2010, e non risultano sottoposte al regime di speciale protezione previsto dal d.lgs. medesimo. Ciò premesso, la resistente ricostruisce le modalità di funzionamento del servizio di home banking, chiarendo che le operazioni contestate sono state realizzate in modalità SCA, nello specifico, rispettando i requisiti della conoscenza (il codice OTP dinamico è stato generato a seguito di digitazione del PIN noto solo alla cliente) e del possesso (tale codice è stato generato tramite l'App installata sul *device* della ricorrente). In conclusione, secondo l'intermediario, la cliente è rimasta vittima di una truffa telematica, che esula dalla responsabilità della banca e, anzi, è stata resa possibile da comportamenti della ricorrente atti ad integrare una fattispecie di negligenza grave.

Nelle repliche, oltre a ribadire quanto già allegato, l'istante sostiene – in merito all'ammontare della somma richiesta – che l'intermediario omette di dedurre che, in data 25 maggio 2025, veniva proposta

un'altra denuncia nella quale, all'esito dei conteggi nelle more effettuati, risultava che la somma sottratta ammontava ad euro 14.625,37.

Con le controrepliche, la resistente richiama quanto già affermato nelle precedenti difese rinnovando la richiesta di accoglimento delle conclusioni ivi rassegnate. Rileva, inoltre, la banca che la truffa non è durata pochi minuti ma quasi un'ora, nel corso della quale la ricorrente ha disposto le operazioni contestate, non prestando attenzione né alle notifiche push né agli SMS ricevuti sul suo cellulare. Evidenzia, altresì, l'istituto di credito che tra il primo SMS ricevuto, alle ore 18.48.39, e la seconda operazione, eseguita alle ore 19.23.34, sono intercorsi 35 minuti, nel corso dei quali parte attrice avrebbe potuto contattare il numero verde della banca interrompendo la truffa ai suoi danni. Ribadisce, inoltre, la resistente che il *petitum* del ricorso – da limitare ad euro 10.235,11 euro – non può essere imposto dal legale di controparte sulla scorta di documentazione del tutto slegata dalla procedura di disconoscimento che è l'unica a fare fede.

DIRITTO

Osserva preliminarmente questo Arbitro che la ricorrente chiede la restituzione dell'importo complessivo di euro 14.625,37, asseritamente sottrattole all'esito di una truffa ordita ai suoi danni. L'intermediario eccepisce la parziale inammissibilità della richiesta per la parte non contemplata in sede di interlocuzione preliminare al ricorso e, segnatamente, nel modulo di disconoscimento del 19 dicembre 2024. In tale occasione venivano disconosciute quattro operazioni per un totale di euro 10.235,11, al quale – secondo l'istituto di credito – dovrebbe essere limitato il *petitum*. Tuttavia, in atti risulta che, in data 25 maggio 2025, la cliente proponeva un'ulteriore denuncia nella quale, all'esito dei conteggi nelle more effettuati, quantificava la somma sottratta in un maggiore importo rispetto a quanto segnalato a dicembre 2024, da imputare al disconoscimento di 17 operazioni, che parte attrice dettaglia nel documento di contestazione. In data 29 luglio 2025, l'intermediario ha riscontrato la comunicazione contenente questa seconda denuncia. Ne segue che l'eccezione della resistente non coglie nel segno e non può, dunque, essere accolta.

Ciò posto, secondo l'orientamento consolidato dei diversi Collegi territoriali, quando le operazioni contestate sono state interamente eseguite dal pagatore con inserimento delle disposizioni di pagamento e di tutti i fattori di autenticazione, le stesse operazioni devono considerarsi autorizzate e non sono quindi soggette alla speciale disciplina di cui al d.lgs. n. 11 del 2010. In questa fattispecie rientrano anche le operazioni c.d. sotto dettatura, come nel caso in esame.

Ebbene, per un corretto inquadramento della vicenda, è necessario sottolineare che la ricorrente riceveva – in data 15 dicembre 2024 – un SMS che l'avvisava dell'intervenuta esecuzione di un

prelievo, esortandola a contattare l'utenza telefonica indicata in caso di disconoscimento dell'operazione. È versata in atti evidenza dell'SMS da cui è partita la frode. Da tale evidenza emerge che il messaggio risulta provenire da un numero privato, non riconducibile alla banca, che reca la denominazione della convenuta solo nel corpo. Al contempo, l'SMS non pare inserito in coda a precedenti messaggi genuini ed è carente nella punteggiatura.

Ne segue che la ricostruzione dei fatti è tale da far emergere che parte attrice sia verosimilmente rimasta vittima di *phishing* telefonico (o *vishing*). Il carattere anomalo delle richieste avanzate avrebbe dovuto indurre la proponente a non seguire le indicazioni del falso operatore, rivelando a terzi ignoti i propri codici dispositivi. Ne deriva questo Arbitro, nel caso in esame, un contegno gravemente colposo della cliente nel proteggere le credenziali di sicurezza personalizzate (cfr., tra le altre, Collegio di Roma, decisione n. 6036/2022). Nella fattispecie in esame, peraltro, non risulta alcun contributo causale dell'intermediario alla frode.

In relazione a quanto precede, il ricorso non può, pertanto, essere accolto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE