COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore ANDREA TINA

Seduta del 19/12/2023

FATTO

Nel proprio ricorso, il ricorrente riferisce quanto segue:

- in data 12/07/2023, alle ore 11:30, si recava presso la propria filiale, per resettare le credenziali di *HomeBanking*;
- un operatore procedeva al ripristino;
- alle ore 17:12 riceveva una telefonata da un sedicente operatore dell'intermediario che gli riferiva la mancanza di un ultimo passaggio al fine di completare la procedura e gli fissava un appuntamento per il giorno successivo;
- il 13/07/2023, alle ore 13:00, riceveva una telefonata dal medesimo numero riconducibile all'intermediario e, tramite procedura guidata, veniva invitato a certificare la propria mail;
- non forniva alcun codice o password in sede telefonica;
- in data 14/07/2023, alle ore 12:00, un addetto della filiale gli comunicava l'avvenuta truffa, ossia la sottrazione di Euro 10.000,00 dal conto corrente.

Il ricorrente ha, quindi, chiesto il rimborso dell'importo di Euro 10.000,00, corrispondente alle operazioni disconosciute.

Con le proprie controdeduzioni, l'intermediario resistente ha precisato quanto segue:

- i messaggi truffaldini ricevuti dal cliente sono stati apparentemente inviati da un altro intermediario, non dall'intermediario resistente;

- verosimilmente il cliente ha comunicato al terzo frodatore le credenziali personali di accesso all'home banking nonché gli OTP necessari per l'installazione e l'attivazione di una nuova app/licenza "sm**OTP" e ha disinstallato l'app della banca dal proprio dispositivo mobile;
- sussiste, pertanto, la colpa grave del cliente che ha attivamente collaborato con il truffatore;
- la banca ha adottato un sistema di autenticazione forte (provato mediante la produzione dei file di Log);
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali;
- l'intermediario ha attivato apposite campagne informative anti-frode, volte a sensibilizzare la clientela rispetto a forme di truffa analoghe a quella perpetrata nella specie;
- al termine di ogni operazione il sistema della Banca invia all'indirizzo e-mail collegato all'utenza del cliente le relative e-mail di notifica dell'esecuzione delle operazioni, come è avvenuto anche nel caso di specie;
- a seguito della segnalazione del cliente, l'intermediario ha bloccato l'internet banking del cliente e esperito un tentativo di *recall* dei bonifici disconosciuti, che non ha, tuttavia, avuto esito positivo.

DIRITTO

La questione rimessa all'esame del Collegio attiene all'esecuzione di due operazioni di pagamento (bonifici) effettuate con il servizio home banking del ricorrente, per l'importo complessivo di Euro 10.000,00. Il ricorrente riferisce, in sintesi, di essere stato vittima di un caso di spoofing; le operazioni disconosciute risultano essere state effettuate il 12 e il 13 luglio 2022 ottobre 2022 e sono, quindi, assoggettate alle disposizioni del D.lgs. n. 11/2010 nella versione oggi vigente.
Ciò premesso, giova precisare che, per l'ipotesi di disconoscimento di operazioni da parte del cliente, l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.
In relazione al primo profilo, sebbene descriva una procedura conforme ai criteri SCA di autenticazione c.d. "forte", l'intermediario resistente non ha fornito piena prova della corretta autenticazione delle operazioni disconosciute dal ricorrente, in relazione alla registrazione di un nuovo *device*, all'accesso all'app e all'esecuzione delle operazioni disconosciute. Più in particolare, per tutte le fasi ora richiamate non vi è evidenza dell'inserimento delle credenziali di accesso (login e password), né del codice OTP e del PIN dispositivo di volta in volta inviati, il cui inserimento sarebbe confermato, secondo la legenda esplicativa prodotta dall'intermediario, unicamente dai codici "*Esito 000*" e "*Esito OK*".

Di conseguenza, in assenza di una piena e completa evidenza dell'utilizzo del doppio fattore di sicurezza, non può ritenersi provata, secondo i criteri SCA, la corretta autenticazione delle operazioni disconosciute dal ricorrente, che, per tale ragione, ha diritto al rimborso dell'importo complessivo di Euro 10.000,00, corrispondente alle operazioni medesime.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 10.000,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA