COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) PIRAINO	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) ASTONE	Membro di designazione rappresentativa degli intermediari
(PA) CLEMENTE RUIZ	Membro di designazione rappresentativa dei clienti

Relatore MARIA ANNUNZIATA ASTONE

Seduta del 26/02/2025

FATTO

Parte ricorrente, dopo aver regolarmente eseguito il reclamo, si rivolge all'Abf per chiedere la restituzione della somma di euro 3.665,90 per operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati. Parte ricorrente riferisce che in data 16/10/2024 riceveva un sms dal numero ***444, che la informava di un accesso su un nuovo dispositivo e la invitava a cliccare su un link allegato. Nel link inseriva il proprio nome e cognome e veniva in seguito contattata telefonicamente da un presunto operatore della banca dal n. ***200, il quale le riferiva di un pagamento in uscita di € 1.480,00. Per bloccarlo, la invitava ad effettuare una operazione inversa tramite bonifico istantaneo. L'operatore comunicava che nel frattempo era stata effettuata un'altra operazione di € 1.470,00 e la invitava ad eseguirne un'altra inversa tramite bonifico istantaneo di pari importo in favore dello stesso beneficiario. L'operatore la informava che era stato eseguito anche un pagamento tramite carta di credito avente n. ***235 di € 795,90 e provvedeva ad effettuare analogo bonifico dalla sua carta a favore di una società. Contattato il n. verde della banca, parte ricorrente si rendeva conto di essere stata truffata. Bloccava quindi carta e conto corrente. In sede di repliche rilevava altresì di non aver ricevuto nessun sms o alert da parte della banca. Chiede quindi la restituzione delle somme corrispondenti alle tre operazioni contestate per un importo pari a Euro 3.665,90. Costituitosi l'intermediario eccepisce che il messaggio da cui ha tratto origine la frode, non proviene

dall'Intermediario e presenta evidenti sgrammaticature. Il link in esso contenuto non è riconducibile allo stesso. I log informatici evidenziano, poi, che tutta l'operatività è avvenuta dal device della cliente. Le operazioni disconosciute sono state eseguite dopo essere state "autenticate, correttamente registrate e contabilizzate" e non hanno "subito le conseguenze del malfunzionamento delle procedure necessarie per la loro esecuzione o di altri inconvenienti". Secondo l'intermediario la colpa grave della cliente emerge in maniera evidente da tali circostanze: 1) il messaggio da cui ha tratto origine la frode proviene da un numero non riconducibile alla Banca e presenta evidenti sgrammaticature; 2) il link in esso contenuto non è riconducibile alla Banca; non è stato prodotto il registro delle chiamate, a conferma che la telefonata ricevuta dalla signora cliente appariva provenire da un numero dell'intermediario; 3) anche i messaggi successivi presentano errori; 4) le tracciature informatiche non evidenziano enrollment, ossia una operatività da un cellulare diverso da quello della ricorrente; 5) tutta l' operatività è avvenuta dal suo device, dal quale sono state confermate le otp virtuali, necessarie per accedere al sistema ed autorizzare le transazioni. Chiede il rigetto del ricorso.

DIRITTO

La questione oggetto della controversia in esame riguarda l'accertamento della presunta responsabilità dell'intermediario per non avere adottato le misure di protezione previste per legge nei confronti dell'utente, vittima di un attacco di *spoofing-vishing*. Oggetto del ricorso sono due operazioni di bonifico istantaneo eseguite in data 16/10/2024 alle ore 17.51 e 17.58 di € 1.470,00 e € 1.400,00; una operazione di pagamento eseguita tramite carta di credito in data 16/10/2024 alle ore 18.24 (di € 795,90, per un ammontare complessivo di € 3.665,90. Dalla documentazione versata in atti e prodotta dallo stesso intermediario emerge che i messaggi provenivano da numeri non riconducibili all'Intermediario; che le operazioni di bonifico sono state eseguite volontariamente e consapevolmente da parte ricorrente, con la conseguenza che – conformemente agli orientamenti di questo Collegio – risulta inapplicabile la disciplina di cui al D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II). Infatti, le operazioni sono state eseguite da parte ricorrente, a nulla rilevando il fatto che egli abbia eseguito le istruzioni del truffatore, poiché , usando la richiesta diligenza, avrebbe potuto comprendere la natura fraudolenta dei messaggi, contenenti errori grammaticali e un link non riconducibile all'intermediario resistente
Inoltre con riferimento all'operazione compiuta con carta di credito sono agli atti le prove attestante i fattori di autenticazione per l'autorizzazione dell'operazione di pagamento con carta di credito a doppio fattore (PIN e OTP)
In considerazione di tali circostanze, debitamente provate dall'intermediario, e conformemente agli orientamenti di questo collegio, si può considerare raggiunta la prova dell'effettiva utilizzazione di un sistema di autenticazione forte dell'utente, ai sensi dell'art. 10-bis d. lgs. n. 11/2010, quale strumento idoneo a proteggere adeguatamente il cliente dal rischio di frodi. Per queste ragioni, in conclusione, il Collegio non accoglie il ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARIA ROSARIA MAUGERI