COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore DOMENICO BONACCORSI DI PATTI

Seduta del 07/10/2024

FATTO

Il ricorrente rappresenta nel ricorso di aver ricevuto in data 20.07.2023 un sms con il quale gli veniva anticipata la chiamata di un operatore dell'intermediario, apparentemente necessaria ad aggiornare l'home banking. Poco dopo veniva contattato da un sedicente operatore del servizio clienti della banca, il quale si dimostrava a conoscenza delle sue credenziali bancarie e gli "dettava" la procedura necessaria all'aggiornamento. Riceveva quindi un ulteriore messaggio, contenente un link, al quale il ricorrente accedeva. Al termine della procedura il ricorrente si accorgeva tuttavia che erano stati effettuati tre bonifici istantanei per complessivi 20.000,00 euro. Il ricorrente contesta alla banca di non aver trasmesso alcun alert in relazione alle operazioni. Sostiene che esse operazioni erano anomale rispetto alla operatività ordinaria del conto, avuto riguardo al loro importo e alla loro rapida successione. Il ricorrente chiede, dunque, il rimborso delle somme sottratte. La banca nelle proprie controdeduzioni premette di aver tentato, senza esito, il recall dei bonifici oggetto del contendere. Con riferimento ai propri sistemi di autenticazione afferma che per accedere al servizio di home banking sono necessari codice utente, pin, OTP generata da Pass code o token e che nel caso in esame il cliente ha scelto, quale strumento di autenticazione, proprio il pass code, ossia un software capace di generare codici temporanei usa e getta. L'intermediario rileva che le operazioni

controverse sono state correttamente autenticate, registrate e contabilizzate, senza che fossero rilevate anomalie e che le transazioni sono – conseguentemente – state ritualmente autenticate attraverso un sistema di SCA. Quanto alla asserita mancata trasmissione degli alert, la banca afferma che il prodotto "ALERTSMS" non è mai stato opzionato dal cliente per ricevere SMS informativi in merito all' "accesso" al conto corrente, nonostante tale opportunità sia stata concessa dalla banca in fase contrattuale. L'intermediario chiede il rigetto del ricorso.
Nella riunione del 04.07.2024 il Collegio ha deliberato di chiedere all'intermediario "la produzione di copia della documentazione atta a comprovare l'installazione dell'app. sul nuovo dispositivo e i relativi fattori di autenticazione". In data 18.07.2024 l'intermediario ha prodotto la documentazione richiesta. Da essa si trae conferma del fatto che le operazioni controverse sono state disposte e autenticate tramite l'App installata su un nuovo dispositivo S*****, in possesso dei frodatori.

DIRITTO

Il ricorrente disconosce n. 3 operazioni di bonifico istantaneo online, di importo complessivamente pari a euro 20.000,00, effettuate il 20.07.2023, chiedendone la restituzione in quanto da lui non autorizzate. Le operazioni contestate sono state effettuate il 20.07.2023 sotto la vigenza del d.lgs. 11/2010, così come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2).
Il ricorrente produce in atti gli sms civetta. I messaggi risultano essersi inseriti in una chat intestata all'intermediario, contenente anche messaggi genuini. Il link presente nel secondo messaggio contiene il riferimento al nome della banca. Dalla denuncia, inoltre, si rileva che su indicazione del truffatore, il ricorrente ha cliccato sul link ed ha inserito le credenziali di accesso al conto e un codice che ha ricevuto via email da indirizzo riconducibile alla banca.
L'intermediario afferma che le operazioni sono state correttamente autenticate, registrate e contabilizzate, senza anomalie, tramite un sistema di autenticazione forte che ha previsto l'utilizzo di username, password (elementi di conoscenza) e OTP (elemento di possesso) in fase di accesso e l'impiego di OTP generata dal software Pass code (elemento di possesso) in fase di autorizzazione dei singoli pagamenti.
La modalità autorizzativa descritta dall'intermediario utilizza dunque una token app per la generazione di una OTP non visibile all'utente (sistema O*** S****).
Orbene, con riferimento alla procedura di autenticazione essa può dirsi rispondere ai requisiti previsti dalla normativa vigente per potersi qualificare come di autenticazione forte (Strong Customer Authentication), possedendo almeno (i necessari) due dei tre elementi previsti in materia, secondo quanto specificato dalla "Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2", che considera il codice statico scelto dall'utente integrare un fattore di conoscenza, e l'utilizzo di una App previamente associata ad uno specifico dispositivo come un fattore del possesso.
Nel contempo, il Collegio osserva che, nel caso di specie, la parte ricorrente non ha descritto né allegato alcuna circostanza che possa spiegare come una tale appropriazione delle sue credenziali riservata possa essere avvenuta senza la sua collaborazione o comunque senza una sua negligenza, intervenuta, presumibilmente, nell'ambito della telefonata con il frodatore, inducendo a ritenere provata, pur in via presuntiva, una violazione ad opera della parte ricorrente dei suoi obblighi di diligente custodia delle credenziali riservate, secondo una condotta che può ritenersi connotata da colpa grave.

Il Collegio, tuttavia, osserva che la schermata dell'sms civetta ricevuto dalla parte ricorrente appare inviato dallo stesso contatto dell'intermediario, dal quale riceve generalmente le comunicazioni per autorizzare le operazioni ed accodato a precedenti comunicazioni genuine provenienti dall'istituto.
Ebbene, secondo la più recente posizione condivisa da tutti i Collegi territoriali, nelle fattispecie di spoofing non è generalmente ravvisabile la colpa grave del ricorrente, a meno che non si rinvengano indici di inattendibilità o anomalia del messaggio: in tale caso, potrà essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario.
Il Collegio, nel caso di specie, riconosce un concorso di colpa tra le parti e, nell'applicare l'art. 1227 c.c., riconosce dovuta al ricorrete la somma di € 15.000,00 determinata in via equitativa

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 15.000,00, determinata in via equitativa.
Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA