COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) GENOVESE	Membro di designazione rappresentativa degli intermediari
(RM) SARZANA DI S. IPPOLITO	Membro di designazione rappresentativa dei clienti

Relatore SALVATORE FULVIO SARZANA DI S. IPPOLITO

Seduta del 07/12/2022

FATTO

La ricorrente si rivolge all'ABF, dopo aver invano proposto reclamo, per chiedere la restituzione della somma di euro € 51.995,00, corrispondente all'importo di 3 operazioni di bonifico online disconosciute in quanto eseguite fraudolentemente da terzi non autorizzati a seguito di truffa perpetrata nelle forme dello *smishing/spoofing* e *vishing*.

In particolare, il ricorrente dichiara di aver ricevuto, il 31.03.2022, alle ore 13.38, un sms dall'intermediario resistente, con il quale veniva informato del fatto che il suo conto online era stato "limitato". Afferma di esser stato contattato da un operatore della banca, il quale la invitata a "*installare il protocollo di sicurezza web*".

Parte ricorrente riferisce che tale procedura si attivava attraverso un link che la banca le trasmetteva contestualmente via sms.

La ricorrente seguiva le indicazioni ricevute. Non le veniva richiesto di comunicare password e codice cliente. Riceveva quindi un messaggio di conferma dell'avvenuta aggiornamento.

La ricorrente veniva invitata a cancellare l'app e attendere 3 giorni lavorativi.

Nei giorni successivi (1,4,5,6 aprile) la ricorrente veniva contattata dall'operatore, il quale la invitava a non accedere all'app "*fino all'attivazione della sicurezza web*". Non riuscendo ad accedere all'App la ricorrente confidava che la procedura fosse ancora in corso.

Il 7 aprile contattava infine il servizio clienti dell'intermediario ed apprendeva di aver subito una truffa all'esito della quale erano stati effettuati 3 bonifici fraudolenti (di importo pari a € 24.997,00, 24.997,00, 2.001,00).

Parte ricorrente sostiene che le operazioni siano imputabili a disfunzioni organizzative della banca.

Sostiene di non aver comunicato a terzi le credenziali riservate.

Nelle controdeduzioni la banca precisa che i ricorrenti sono cointestatari di conto corrente e usufruiscono del servizio di *home banking*.

Afferma che le operazioni controverse sono state poste in essere previa attivazione del mobile token su dispositivo in possesso del frodatore.

Precisa che parte ricorrente ha ricevuto sul proprio cellulare il messaggio contenente il codice OTP di attivazione del mobile token su nuovo dispositivo, in data 01.04.2022 alle ore 15.08.

Parte ricorrente avrebbe comunicato al frodatore il codice OTP contenuto nel messaggio, via telefono o attraverso i link truffaldini ricevuti via sms. Attraverso tale OTP il frodatore ha potuto installare il mobile token su dispositivo in suo possesso.

Le operazioni controverse sono state poste in essere attraverso un sistema di autenticazione forte, senza che fossero rilevate anomalie.

La banca è venuta a conoscenza della truffa solo 12 giorni dopo l'ultima operazione e non è riuscita a bloccare o richiamare i bonifici.

In definitiva le operazioni fraudolente sono imputabili alla negligenza del ricorrente nella custodia del dispositivo di pagamento e relative credenziali.

Nelle repliche parte ricorrente ribadisce di aver confidato nella genuinità dei messaggi e delle telefonate ricevute.

La truffa è stata posta in essere a seguito del furto dei dati personali del cliente; furto la cui responsabilità va imputata alla banca.

La banca ribadisce nelle controrepliche, che tutte le operazioni sono state autorizzate mediante OTP, cliccando sulle notifiche o aprendo l'app di BNL e confermando l'autorizzazione nella lista delle notifiche, come si puo' vedere nei Log (allegato 1 delle controdeduzioni), e da dove si puo' evincere che la banca ha inviato al cellulare del cliente una notifica push per ogni operazione effettuata.

La ricorrente è rimasta colpevolmente vittima di "smishing- vishing", comunicando le proprie credenziali ai frodatori.

Insiste per il rigetto del ricorso.

DIRITTO

Il ricorso è parzialmente fondato.

Le operazioni contestate sono state effettuate tra il 01 e il 05 aprile 2022 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).

Parte ricorrente afferma di aver ricevuto, il 31.03.2022, un messaggio civetta che la informava del blocco della carta e/o del conto.

Il messaggio si inserisce in una chat intestata alla banca resistente, in cui è presente almeno un precedente messaggio genuino dell'intermediario; il link civetta non contiene riferimenti alla banca resistente.

La ricorrente afferma di aver "*provato a vedere di cosa si trattava*", ma non fidandosi avrebbe provato a contattare il servizio clienti della banca. La linea sarebbe caduta e sarebbe stata ricontattata dal sedicente operatore "8704" dell'intermediario, il quale la informava del blocco del conto e la invitava a "*installare il protocollo di sicurezza web*" cliccando sul link presente in altro messaggio che le faceva pervenire sul cellulare.

Parte ricorrente allega lo screenshot del registro chiamate, dal quale risultano, nelle giornate in cui si è articolata la frode, una serie di chiamate in entrata apparentemente provenienti dall'intermediario.

Concluse le operazioni di presunto aggiornamento, la ricorrente riceveva un messaggio di conferma.

Nei giorni successivi la ricorrente veniva contattata dal sedicente operatore, che le diceva di attendere il completamento delle operazioni di aggiornamento e di non accedere al conto.

Solo il 07.04.2022 la ricorrente, insospettita, chiamava il servizio clienti e apprendeva di essere stata truffata.

Parte ricorrente contesta tre operazioni di bonifico online poste in essere rispettivamente in data 01 – 04 e 05 aprile 2022 di importo complessivamente pari a € 51.995,00 (due bonifici di € 24.997,00 e uno di € 2.001,00).

La banca afferma che le operazioni sono state poste in essere attraverso un sistema di autenticazione forte, senza che fossero registrate anomalie e previa attivazione del mobile token su dispositivo del frodatore.

Il mobile token è stato attivato il 01.04.2022 alle 15:09.05.

Per l'attivazione è stato necessario effettuare l'accesso al portale con id utente e Pin (fattori di conoscenza) e inserire il codice OTP di attivazione del token, trasmesso via sms al ricorrente (fattore di possesso).

È stata poi effettuata una ulteriore verifica a due fattori con OTP generato proprio dal mobile token (fattore di possesso.

Dopo aver attivato il token il frodatore ha inserito il primo bonifico di € 24.997,00, alle ore 15:10. Il bonifico è stato autorizzato con Pin (fattore di conoscenza) e OTP generata da mobile token (fattore di possesso).

Il 04.04.2022, previo accesso al conto con Pin e OTP generata dal mobile token, il frodatore ha inserito il secondo bonifico, sempre di € 24.997,00, validato con Pin (fattore di conoscenza) e OTP generata da mobile token (fattore di possesso).

Il 05.04.2022, previo accesso al conto con Pin e OTP generata dal mobile token, il frodatore ha inserito il terzo bonifico, di € 2.001,00, autorizzato con Pin (fattore di conoscenza) e OTP generata da mobile token (fattore di possesso).

La banca produce un allegato contenente il dettaglio degli sms e delle notifiche push trasmesse in relazione alle diverse fasi dell'operazione truffaldina sopra descritta.

Ciò detto, il Collegio rammenta la più recente posizione condivisa da tutti i Collegi territoriali, secondo cui 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".

In applicazione dell'orientamento condiviso dei Collegi, il Collegio di Roma, in presenza di indici di inattendibilità o anomalia del messaggio, ha di recente ravvisato un concorso di colpa (Collegio di Roma, decisione n. 1625 del 25/01/2022: "*(…) In data 15.05.2021, il ricorrente, titolare di un conto corrente presso l'intermediario convenuto, riceveva un sms che lo invitava ad accedere al link allegato al messaggio stesso, per aggiornare le proprie utenze. Una volta cliccato il link, il ricorrente inseriva i codici successivamente ricevuti via sms, autorizzando due operazioni, per l'importo complessivo di € 945,99.*

*[…] È notorio che il sistema delineato dal legislatore comunitario in materia di strumenti di pagamento è di particolare favore per il cliente soprattutto per quel che concerne l'onere probatorio. Ciò in quanto, per un verso limita la responsabilità del cliente alle sole ipotesi di dolo e colpa grave e, per altro verso, pone in capo all'intermediario l'onere di provare che l'operazione di pagamento sia stata eseguita correttamente e non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti. L'intermediario afferma che le operazioni sono state correttamente autenticate e autorizzate senza anomalie con un sistema di autenticazione forte a due fattori, precisamente le operazioni sono state autenticate mediante il sistema P****ID, per la cui configurazione sul dispositivo dei frodatori è stato necessario l'utilizzo delle credenziali statiche di accesso all'home banking e di un OTP trasmesso via SMS alla parte ricorrente. L'intermediario allega evidenza dell'invio, sul numero di cellulare del ricorrente, del codice OTP necessario alla configurazione del P****ID. Secondo tale evidenza, l'OTP è stato trasmesso al ricorrente il 15.05.2021 allo stesso numero di telefono indicato nella denuncia. Orbene, una tale procedura di autenticazione può dirsi rispondere i 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. Pertanto, nel caso di specie, il Collegio osserva che le circostanze che il terzo malfattore, per abilitare il codice di "P**** Id" sul suo dispositivo come se fosse quello della parte ricorrente, abbia necessariamente potuto procurarsi prima i dati relativi alle credenziali statiche di accesso della parte ricorrente, e poi la password dinamica (cd. "usa e getta") comunicatale tramite OTP e che la parte ricorrente non abbia 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, inducono a ritenere provata, pur in*

via presuntiva, una violazione da parte 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 € 350,00 determinata in via equitativa (…)".

Il Collegio intende confermare l'orientamento condiviso dei Collegi territoriali riconoscendo nel caso di specie un concorso di colpa tra le Parti e determinando l'entità del rimborso 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 26.000,00, 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