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

Relatore FRANCESCO PAOLO PATTI

Seduta del 16/12/2022

FATTO

In data 31.03.2022, alle ore 14:00 circa, la ricorrente riceveva sul suo telefono cellulare una chiamata proveniente dal numero del servizio clienti della banca convenuta. L'interlocutore si qualificava come tecnico della banca e spiegava alla ricorrente di averla contattata per risolvere un problema tecnico sul suo conto, spiegandole che di lì a poco le sarebbe arrivato un SMS contenente un *link* da seguire per dare avvio alla procedura manutentiva; al termine della conversazione la ricorrente, diffidando, provava a richiamare il numero dal quale la telefonata proveniva e otteneva effettivamente risposta dal centralino dell'intermediario; ciò tranquillizzava la ricorrente della genuinità della chiamata ricevuta; poco dopo, la ricorrente riceveva l'SMS che le era stato preannunciato, seguito da una telefonata dal medesimo numero; la ricorrente, seguendo le indicazioni fornitele al telefono, cliccava sul *link* e inseriva il proprio numero cliente e la *password* di accesso all'*home banking*, su una schermata del tutto uguale a quella della banca; sempre nel corso della chiamata, la ricorrente riceveva un ulteriore SMS contenente un *link* da seguire per scaricare una nuova applicazione, denominata "App sms Sicura", cosa che la cliente, seguendo le indicazioni dell'interlocutore, faceva; al termine della chiamata, l'interlocutore

chiedeva alla ricorrente di disinstallare tutte le *app* precedentemente installate nel corso della chiamata, dichiarando che la sua pratica era stata presa in carico e che lui stesso l'avrebbe ricontattata il giorno successivo. Il giorno successivo la ricorrente, non essendo stata ricontattata, provvedeva a chiamare il servizio clienti dell'intermediario, apprendendo che a sua insaputa erano stati effettuati n. 2 bonifici istantanei, rispettivamente di € 27.568,32 e di € 21.536,23; per tali operazioni la ricorrente non riceveva nemmeno i consueti SMS alert. Sostiene che i sistemi informatici dell'intermediario siano stati *hackerati*, e chiede il rimborso delle operazioni disconosciute per l'importo complessivo di € 49.104,55, oltre ad € 1.500,00 a titolo di rimborso delle spese legali.

L'intermediario resiste al ricorso, osservando che la ricorrente è titolare di un conto corrente, al quale è collegato il servizio di *home banking*, e ha attivato sin dal 2014 il servizio di SMS *alert* sul proprio numero di cellulare; l'intermediario afferma che l'accesso alle funzioni di *inquiry* e dispositive tramite *home banking* avviene attraverso un sistema di autenticazione forte. L'intermediario descrive nel dettaglio il sistema di autenticazione adottato. Osserva che, nel caso specifico, il giorno 31.03.22 alle ore 14:35:42 ha inviato al cellulare della ricorrente l'SMS e la relativa notifica push contenente il codice OTP necessario per l'attivazione del *Mobile Token*, avente il seguente contenuto: "Stai attivando il Mobile Token. Ricordati che il personale […] non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato: ******** Info ******". Sostiene che, a fronte di tale SMS, la ricorrente avrebbe dovuto insospettirsi, e in ogni caso non avrebbe dovuto comunicare a nessuno il codice ricevuto; la ricostruzione dei fatti contenuta nel ricorso mostra invece una condotta gravemente colposa della ricorrente, che ha seguito le istruzioni di uno sconosciuto interlocutore divulgando le credenziali di sicurezza del proprio *home banking*; osserva che i *link* contenuti negli SMS ricevuti non erano neppure contraddistinti dal protocollo di sicurezza "https"; segnala che non si deve riporre troppa fiducia nel "*caller ID*" che appare su telefono fisso o mobile, in quanto è risaputo che esso non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display; ritiene che la frode subita dalla ricorrente sia un classico caso di *phishing*; fa presente che dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei propri sistemi, e che le operazioni risultano correttamente autenticate, registrate e contabilizzate come emerge dai log in atti; in particolare, dai *log* si evince che le operazioni sono state validate correttamente con un sistema di autenticazione "forte", nel rispetto dei canoni stabiliti dalla normativa PSD2, c.d. anche "a due fattori", uno statico (PIN - fattore di conoscenza) e uno dinamico (OTP – fattore di possesso); a fronte di ciascuna operazione, inoltre, la banca ha inviato al cellulare della ricorrente la relativa notifica *push* e l'SMS *alert*; eccepisce l'infondatezza della domanda di rimborso delle spese di assistenza professionale, in quanto il ricorso di fronte all'ABF non richiede l'assistenza di un difensore; conclude quindi chiedendo il rigetto del ricorso.

In sede di repliche, la ricorrente ribadisce la ricostruzione dei fatti già enunciata nel ricorso, e afferma che la frode subita rientra nella categoria particolarmente insidiosa dello *spoofing*; afferma di non avere ricevuto gli *alert* relativi alle operazioni disconosciute; insiste quindi per l'accoglimento del ricorso, oltre al pagamento di € 2.500,00 per l'intervento dei propri legali.

Nelle ulteriori repliche, l'intermediario precisa che le operazioni disconosciute non sono state eseguite con modalità "bonifico istantaneo", ma si tratta di bonifici ordinari che avrebbero potuto essere revocati entro le 17:29 del giorno di inserimento; ribadisce l'avvenuta consegna alla ricorrente degli *alert* (SMS e notifiche *push*), come attestato dai *log* allegati alle controdeduzioni; insiste quindi per il rigetto del ricorso.

DIRITTO

1. La ricorrente chiede la restituzione della somma di € 49.104,55, corrispondente all'importo di n. 2 operazioni disconosciute eseguite fraudolentemente da terzi, a seguito di *vishing* e SMS *spoofing*. L'intermediario chiede il rigetto del ricorso, affermando che le operazioni fraudolente sarebbero riconducibili a una condotta gravemente colposa della parte ricorrente.
2. Il ricorso merita accoglimento nei limiti di seguito indicati.
3. Le operazioni contestate sono state effettuate sotto la vigenza del d.lgs. 218/2017, che ha recepito la Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2), e del Regolamento (UE) 2018/389 in tema di autenticazione forte.
4. La ricorrente dichiara che in data 31.03.2022, alle ore 14:00 circa, veniva contattata telefonicamente da un soggetto che appariva chiamare dal numero del servizio clienti dell'intermediario, il quale le spiegava di averla contattata per risolvere un problema tecnico sul suo conto. Produce uno *screenshot* del registro chiamate, che tuttavia mostra una chiamata in uscita alle ore 14:50:
5. La ricorrente, durante la telefonata, riceveva un SMS apparentemente proveniente dall'intermediario, che si accodava a precedenti messaggi legittimi, contenente un *link* che l'interlocutore le chiedeva di seguire. La ricorrente dichiara di avere seguito le indicazioni e di avere inserito le proprie credenziali di accesso all'*home banking* (numero cliente e *password*) su una pagina *web* del tutto identica a quella della banca. La ricorrente riceveva poi un secondo SMS, contenente un *link* a un'*app* "sms Sicura" che l'interlocutore le chiedeva di scaricare. Anche in questo caso la ricorrente seguiva le indicazioni. Gli *screenshot* allegati alla denuncia documentano tali SMS:
6. Al termine della telefonata, l'interlocutore chiedeva alla ricorrente di disinstallare l'*app* scaricata e affermava che avrebbe provveduto a ricontattarla il giorno successivo alle 17:00, facendole pervenire anche un SMS in tal senso. Il giorno successivo, non essendo stata ricontattata, la ricorrente chiamava il servizio clienti della banca, venendo a conoscenza del fatto che il giorno precedente, alle ore 14:39 e alle 14:44,

erano stati effettuati dal suo conto due bonifici, rispettivamente di € 27.568,32 e di € 21.536,23.

7. D'altra parte, l'intermediario produce i *log* relativi alle operazioni, precisando che esse sono state autorizzate, mediante inserimento del PIN + codice OTP (*One Time Password*), generato da *Mobile Token* a seguito di *tap* su notifica *push*. Rileva che le operazioni sono state eseguite previa attivazione del *Mobile Token* sul dispositivo dei frodatori. Precisa che l'attivazione del *Mobile Token* è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS. Produce evidenza dell'invio e della consegna dell'SMS contenente l'OTP.
8. 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.
9. 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 € 20.000,00 determinata in via equitativa. Non può invece essere accolta la domanda di refusione delle spese di assistenza professionale. La relativa domanda era presente nel reclamo per € 1.500,00, ma non è stata prodotta la parcella del professionista.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 20.000,00, determinata in via equitativa. Respinge nel resto.
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