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 FRANCESCO PAOLO PATTI

Seduta del 07/12/2022

FATTO

La ricorrente riferisce che, in data 14.4.2022, ha ricevuto un sms che si inseriva nel canale di comunicazione ufficiale con l'intermediario; il messaggio con un pretesto la invitava a cliccare su un *link*. A questo sms sono succeduti altri messaggi nei quali si comunicava un appuntamento telefonico con un operatore per la soluzione del problema. Precisa che, come emerge dagli *screenshot* allegati, i messaggi contenenti le richieste di eseguire le verifiche di sicurezza provenivano da un'utenza della banca e sono in continuità con operazioni effettivamente effettuate dalla correntista. Seguivano, dunque, successivi contatti telefonici tramite i quali la cliente veniva invitata ad eseguire accesso Internet tramite *link* di aggiornamento volta per volta inviati al fine di rimuovere la problematica evidenziata. In data 26.4.2022, non riuscendo ad accedere all'*home banking*, provvedeva a contattare il servizio clienti e apprendeva di essere rimasta vittima di frode informatica. Contesta l'esecuzione di venti bonifici eseguiti il 14 e il 15.4.2022. In particolare, 17 bonifici (tutti di € 2.999,00 tranne uno di € 1.970,00) sono stati effettuati il 14 aprile 2022 a beneficio della stessa persona e con la stessa causale; in data 15.4.2022, vengono disposti altri due bonifici: il primo di € 2.999,00 e il secondo di € 1.500,00; lamenta la mancata ricezione di sms di conferma dell'esecuzione delle operazioni; ravvisa un negligente comportamento del servizio antifrode della banca per non aver rilevato le operazioni fraudolente, che appaiono del tutto incompatibili con l'operatività media della

ricorrente. In particolare, l'anomalia consiste nella predisposizione di venti (*rectius* diciannove) operazioni nei confronti del medesimo soggetto nell'arco di meno di 24 ore; ravvisa responsabilità della banca per non aver vigilato sulla modifica dei numeri di telefono su cui indirizzare gli sms di conferma di esecuzione dell'operazione richiesta. Chiede il rimborso delle somme illecitamente prelevate per complessivi € 54.444,00.
L'intermediario resiste al ricorso, rilevando che l'accesso alle funzioni *inquiry* e dispositive avviene tramite un sistema con autenticazione forte; in particolare, l'accesso alla HB da *App* prevede: per effettuare il *login* e le operazioni di *inquiry*, l'inserimento del numero cliente + PIN e il codice OTP, codice dinamico generato da *mobile token*; per disporre le operazioni, l'inserimento del PIN e della OTP generata da *mobile token*. L'attivazione del *mobile token* è possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare certificato; la cliente, infatti, ha ricevuto alle ore 14:43 del 14.4.2022 un SMS al cellulare certificato n. ***866 dal seguente tenore "*Stai attivando Mobile Token. Ricordati che il personale *** non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato: ****Info***". Presume che tale codice sia stato comunicato dalla cliente al frodatore, consentendogli di scaricare l'*App* e operare in autonomia sulla HB. Afferma di aver adottato un sistema di autenticazione forte. Dai LOG risulta che il 14.4.2022 alle 14:43 è stato attivato il *mobile token* mediante inserimento del PIN e del codice OTP ricevuto via sms; il 14.4.2022 tra le 14:46 e le 14:52 sono stati inseriti i bonifici autorizzati con PIN e OTP generato da *mobile token*; il 15.4.2022 alle 14:28 è stato effettuato il *login* mediante inserimento del PIN e OTP generato da *mobile token*; sono stati disposti gli altri bonifici disconosciuti, autorizzati con PIN e OTP generato da *mobile token*. Inoltre, la cliente avrebbe ricevuto tutti gli sms di avviso dell'inserimento dei bonifici, denunciando l'accaduto solo 12 giorni dopo. La banca ha tentato la procedura di *recall* con esito negativo. Presume, pertanto, una colpa grave del cliente nella custodia delle credenziali, in presenza di un sistema di autenticazione forte. Ritiene che la cliente sia rimasta vittima di uno schema di frode classica. L'intermediario informa la propria clientela sui rischi di frodi informatiche. Chiede, pertanto, il rigetto del ricorso.
In sede di repliche, il ricorrente contesta le controdeduzioni e aggiunge quanto segue: il sistema adottato dall'intermediario che, consiste nell'invio di sms, è vulnerabile ai rischi di frode; ribadisce l'assenza di adeguati presidi a tutela della clientela. Inoltre, come appare dalla lettura dei LOG, ben 18 delle 20 operazioni contestate sono state effettuate nell'arco di meno di dieci minuti, ovverosia dalle 14.43 alle 14.52 (ci sono addirittura cinque differenti operazioni di bonifico eseguite nello stesso minuto, alle 14:50), mentre i successivi due bonifici rimanenti sono stati effettuati alle 17:17 ed alle 17:33 del medesimo giorno, anche se contabilizzati il giorno successivo. Richiama l'art. 8 D.M. n. 112 del 2017 sul rischio frode. Nessun sms di conferma esecuzione del bonifico è stato inviato al numero di cellulare della cliente.

DIRITTO

1. La ricorrente chiede il rimborso di € 54.444,00, corrispondenti all'importo di diciannove bonifici disconosciuti. L'intermediario chiede il rigetto del ricorso, affermando che le utilizzazioni fraudolente sono riconducibili a una condotta gravemente negligente della ricorrente.
2. Il ricorso merita accoglimento nei limiti di seguito indicati.
3. Anzitutto non può essere accolta l'eccezione preliminare dell'intermediario. Nel caso di specie non sussiste litispendenza con il procedimento avviato in sede penale (Collegio di Roma, decisione n. 8610/19).

4. Le operazioni contestate sono state effettuate sotto la vigenza del d.lgs. 11/2010, così come modificato dal 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).
5. Dalla documentazione in atti risulta che la ricorrente è stata vittima di un disegno criminoso riconducibile al fenomeno dello *spoofing* e del *vishing*. L'sms civetta si è inserito nel canale di comunicazione ufficiale. Il messaggio non sembra contenere errori grammaticali. La ricorrente disconosce diciannove bonifici per un totale di euro 54.444,00 eseguiti tra il 14.4.2022 e il 15.4.2022. Nelle repliche, parte ricorrente invoca la violazione dell'art. 8 del DM 112/2007 (Regolamento di attuazione della legge 17 agosto 2005, n. 166, recante "*Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento*").
6. L'intermediario afferma che le operazioni disconosciute risultano regolarmente autenticate, registrate e contabilizzate. L'accesso alle funzioni *inquiry* e dispositive avviene tramite un sistema con autenticazione forte. In particolare, l'accesso alla HB da *App* prevede, per effettuare il login e le operazioni di *inquiry*, l'inserimento del numero cliente + PIN e il codice OTP, codice dinamico generato da *mobile token*; per disporre le operazioni, le stesse devono essere confermate con l'inserimento del PIN e della OTP generata da *mobile token*.
7. L'intermediario presume che il *mobile token* sia stato attivato dal frodatore sul proprio device, in modo da operare in autonomia sulla HB. Nel caso di specie, l'intermediario afferma che l'attivazione del mobile token è possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare certificato.
8. L'intermediario adotta, per le operazioni di internet banking, un sistema di autenticazione basato sull'utilizzo del *mobile token* integrato nell'*app*, che genera una OTP (fattore di possesso), in seguito all'inserimento di un PIN. Questo Collegio di Roma ha ritenuto *compliant* alla SCA tale modalità autorizzativa adottata dall'intermediario.
9. Ebbene, secondo la più recente posizione condivisa da tutti i Collegi territoriali (v. Collegio di Roma, decisione n. 1625 del 25/01/2022), 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. Con riguardo alle operazioni contestate, si rileva altresì che il numero e la tipologia delle dedotte operazioni è decisamente anomalo in quanto difforme da quelle usualmente poste in essere dai titolari del rapporto (per la valorizzazione di questo elemento, v. spec. Collegio di Milano, decisione n. 5346 del 31 marzo 2022).
10. Alla luce di quanto esposto, 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 € 35.000,00 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 35.000,00, 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