Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) PATTI	Membro designato dalla Banca d'Italia
(RM) BARTOLINI	Membro designato dalla Banca d'Italia
(RM) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore DILETTA FULCHERI

Seduta del 22/04/2024

FATTO

Con ricorso del 3.10.2023, la ricorrente precisa di essere intestataria di conto presso l'odierna resistente. Il 14.06.2023, alle ore 13:09, riceveva un sms apparentemente inviato dalla banca, che la informava "che aveva limitato la Carta/Conto per la mancata verifica della sicurezza Web" e la invitava a "selezionare" un link, che cliccava e che portava ad una pagina web con intestazione della banca e con richiesta di inserimento delle credenziali per accedere al conto che, tuttavia, non inseriva. Riceveva un ulteriore sms che la preavvisava di una comunicazione da parte di "personale" della banca che, puntualmente, alle ore 15:40 riceveva. L'interlocutore la informava che era necessario bloccare l'applicazione collegata al conto corrente "per effettuare l'operazione di reset per la sicurezza web". Riceveva ulteriore sms che la informava che l'operatore con il quale stava parlando "aveva il codice 4896". A quel punto, forniva le credenziali per accedere al conto corrente e l'applicazione di bloccava. Veniva informata, prima verbalmente, poi

tramite sms, che sarebbe stata ricontattata nella giornata seguente per il ripristino dell'applicazione. Riceveva quindi l'ulteriore chiamata e veniva messa a conoscenza che qualcuno aveva tentato di effettuare "diversi bonifici" e che tali operazioni "intasavano l'applicazione": pertanto doveva attendere "un altro giorno per ritornarne in possesso". Contattava la banca si rendeva conto che era stato effettuato il 14.06.2023 un bonifico di euro 46.186,26 e nella giornata successiva un bonifico di euro 12.376,00. Importi di cui chiede la restituzione per complessivi euro 58.563,26.

Con le controdeduzioni, l'intermediario assume che le operazioni disconosciute risultano eseguite da app il 14 e il 15 giugno 2023, inserite e autorizzate con le credenziali della cliente. Precisa che la stessa ha aderito al servizio sms alert collegato al medesimo telefono cellulare dichiarato nella denuncia/querela e produce evidenza degli sms e delle notifiche push inviati al cellulare della cliente il 14 e il 15 giugno 2023. Descrive la modalità di funzionamento del servizio di home banking che prevede l'accesso alle funzioni di inquiry e dispositive mediante un sistema di autenticazione forte, in linea con la PSD2, come pure per l'attivazione del TOKEN. Osserva come il 14.06.2023 alle ore 15:30:29 e alle ore 15:46:18 la ricorrente avesse ricevuto dalla banca al suo indirizzo di posta elettronica due mail aventi il medesimo contenuto ed alle ore 15:40:53 e alle ore 15:46:17 due sms (e notifica push), contenenti il codice OTP necessario per l'attivazione del mobile token, indispensabile per completare l'attivazione dell'app. Ritiene, pertanto, che a fronte della ricezione di tali email e degli sms "parlanti" e sapendo di non aver richiesto una nuova attivazione dell'app e del relativo mobile token, avrebbe dovuto interrompere la telefonata in corso e soprattutto non avrebbe dovuto comunicare i codici OTP ricevuti, né inserirli in un eventuale link o pagina web, come da raccomandazioni contenute nella e-mail e negli sms stessi.

Precisa che dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi così che le operazioni risultano correttamente autenticate, registrate e contabilizzate, con le credenziali di sicurezza della ricorrente e in conformità con quanto previsto dall'art. 10 del d.lgs. 11/2010. Evidenzia di essere venuta a conoscenza del disconoscimento delle operazioni solo il 16 giugno, tardivamente per bloccare i bonifici inseriti e autorizzati nei giorni precedenti e pur avviando l'azione di recall verso la banca corrispondente, questa aveva avuto esito negativo. Conclude per il rigetto del ricorso.

DIRITTO

La controversia ha ad oggetto il disconoscimento di due bonifici di importo complessivo pari a euro 58.563,26 effettuati tra il 14.06.2023 e il 15.06.2023.

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 nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2).

Si precisa che nella riunione del 15.03.2024, il Collegio aveva disposto una richiesta documentale alla ricorrente riguardante la copia delle schermate con l'sms civetta ed il registro delle chiamate relativi alla vicenda. Tale documentazione è stata in effetti poi prodotta e viene dunque esaminata ai fini della decisione.

La ricostruzione della questione operata dalla ricorrente sembra poter ricondurre alla fattispecie ai casi di c.d. spoofing.
Ed infatti, la ricorrente ha affermato, in sede di denuncia, che il 14.06.2023, alle ore 13:09, riceveva un sms apparentemente inviato dalla banca, che la informava "*che aveva limitato la Carta/Conto per la mancata verifica della sicurezza Web*" e la invitava a "*selezionare*" un link che cliccava sul link e che apriva una pagina web "*con intestazione*" della banca e con richiesta di inserimento delle credenziali di accesso al conto, che tuttavia non fornica. Riceveva poi un ulteriore messaggio che preannunciava una chiamata dal personale della banca.
In effetti seguiva la chiamata e – confortata dalla ricezione di ulteriori messaggi – confidava nelle istruzioni fornite dal sedicente operatore.
Ai fini della decisione occorre accertare in via preliminare la corretta autenticazione delle operazioni.
L'intermediario innanzitutto fornisce sia i log relativi alla fase di attivazione dell'app, sia i log relativi alla fase di esecuzione dei bonifici.
Per l'attivazione del mobile token documenta che questa è stata possibile attraverso la digitazione delle credenziali di sicurezza (IdUtente + PIN) [fattore di conoscenza] e del codice OTP inviato al cliente via mail e via SMS (al numero alla stessa riferibile) al cellulare collegato all'home banking [fattore di possesso].
Per l'accesso al conto, dai log, emerge l'inserimento del PIN [fattore di conoscenza] e l'utilizzo del mobile token per la generazione dell'OTP [fattore di possesso], sul device come sopra installato.
Le operazioni di bonifico risultano poi autorizzate con PIN [fattore di conoscenza] e utilizzo dell'OTP generato da mobile token [fattore di possesso].
Sul punto si richiama l'Opinion dell'EBA del 21 giugno 2019 che ritiene integrante valido fattore di possesso un meccanismo che preveda l'utilizzo di una OTP generata (da un device) o ricevuta (su un device).
Questo Collegio ha ritenuto più volte compliant alla SCA una modalità autorizzativa che preveda la generazione di una OTP da mobile app (Coll. Roma, dec. n. 9649/2023).
Sulla base di questi fatti si ritiene che l'intermediario abbia fornito la prova della formale regolarità dell'autenticazione del *device* del truffatore e delle operazioni contestate.
Va a questo punto analizzata la condotta del ricorrente in relazione alla dinamica della truffa.
La ricorrente ha affermato, in sede di denuncia, che il 14.06.2023, alle ore 13:09, riceveva un sms apparentemente inviato dalla banca, che la informava "*che aveva limitato la Carta/Conto per la mancata verifica della sicurezza Web*" e la invitava a "*selezionare*" un link che cliccava sul link e che apriva una pagina web "*con intestazione*" della banca e con richiesta di inserimento delle credenziali di accesso al conto, che tuttavia non fornica. Riceveva poi un ulteriore messaggio che preannunciava una chiamata dal personale della banca. In effetti seguiva la chiamata e – confortata dalla ricezione di ulteriori messaggi – confidava nelle istruzioni fornite dal sedicente operatore.

Dalla documentazione fornita in sede di integrazione, emerge come la ricorrente abbia ricevuto svariate chiamate da un numero (06**60) che in effetti, da una mera ricerca internet, appare riconducibile all'intermediario.
Analogamente, si apprende dalle schermate degli sms la ricezione di numerosi messaggi sul canale genuino della banca che – ancorchè contenti lievi errori grammaticali – sono formulati in maniera tale dall'aver ingenerato nella ricorrente la fiduciosa convinzione di stare operando nell'interesse della tutela del proprio account.
Secondo l'orientamento condiviso dei Collegi, quando il cliente è vittima di spoofing non può essere in genere ravvisata una sua colpa grave, salvo che il messaggio civetta presenti indici di evidente inattendibilità o anomalia che dovrebbero allertare l'utente avveduto; in quest'ultimo caso può essere riconosciuto un concorso di colpa per l'utente a causa della sua grave negligenza che agevola la truffa.
Il Collegio, nel caso di specie, valutata complessivamente la vicenda e gli elementi probatori piò ravvisarsi un concorso di colpa tra le parti e, nell'applicare l'art. 1227 c.c., riconosce dovuta al ricorrete la somma 45.000,00.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 45.000,00 a titolo di risarcimento del danno determinato 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