## COLLEGIO DI ROMA

composto dai signori:

| | |
|---|---|
| (RM) GRECO | Presidente |
| (RM) POZZOLO | Membro designato dalla Banca d'Italia |
| (RM) PATTI | Membro designato dalla Banca d'Italia |
| (RM) CAPPIELLO | Membro di designazione rappresentativa degli intermediari |
| (RM) CESARO | Membro di designazione rappresentativa dei clienti |

Relatore POZZOLO ALBERTO FRANCO

Seduta del 07/05/2020

## FATTO

Il ricorso ha per oggetto la richiesta di rimborso di € 24.750,00, corrispondente all'importo di un bonifico disconosciuto effettuato a valere sul conto corrente della ricorrente.
In base alle dichiarazioni della ricorrente e alla documentazione presentata dall'intermediario resistente nelle controdeduzioni, è possibile ricostruire i seguenti fatti, utili alla decisione del ricorso.

- La ricorrente è intestataria, insieme al marito, di un rapporto di conto corrente con l'intermediario resistente, su cui risulta attivato il servizio di home banking.
- Il giorno 24/07/19, mentre la ricorrente si trovava a Gerusalemme, la sua carta SIM (Subscriber Identity Module), che aveva prestato alla propria figlia, rimasta in Italia, cessava di funzionare.
- La figlia della ricorrente si recava presso un negozio della compagnia telefonica che aveva emesso la SIM e apprendeva che alla medesima SIM era stato attribuito il nominativo di un altro soggetto. Veniva per questo invitata ad attendere la correzione oppure ad acquistare una nuova SIM. Verificato che la SIM continuava a non funzionare, ne acquistava una nuova.
- Alle ore 16:51 del 24/07/2019 veniva effettuato un accesso con PIN (personal identification number) statico al servizio di home banking della ricorrente e alle ore 16:53 veniva attivato il servizio di mobile token, il cui codice OTP (One Time Pasword)

veniva inviato al numero di telefono della ricorrente (la cui SIM originale apparentemente aveva smesso di funzionare). Le operazioni venivano effettuate da un telefono di marca Samsung, diverso da quello identificato dal sistema informatico dell'intermediario resistente come il telefono della ricorrente, che è di marca Apple.

- Alle ore 16:56 del 24/07/2019 veniva disposto un bonifico dell'importo di € 24.750,00, con corretta autenticazione tramite sistema a due fattori: il PIN e l'OTP. L'operazione, che in quel momento veniva prenotata e posta in esecuzione il giorno successivo, viene notificata con messaggio tramite l'applicazione installata sul telefono della ricorrente e tramite SMS-alert inviato alla sua utenza telefonica.
- Nelle ore successive venivano effettuati numerosi accessi al servizio di home banking della ricorrente, sempre da un telefono di marca Samsung.
- Alle ore 12:46 alle ore 22:38 del 25/07/2019 venivano effettuati due accessi al servizio di home banking della ricorrente dal telefono di marca Apple della ricorrente.
- Alle ore 15:24, 15:25, 15:36, 16:55, 18:49 e 19:04 del 25/07/2019, dal telefono cellulare di marca Samsung, venivano disposti sei nuovi bonifici dell'importo di € 24.750,00 ciascuno a favore del medesimo beneficiario del bonifico delle 16:56 del giorno precedente, tutti autenticati con PIN e OTP, nessuno dei quali andava però a buon fine.
- Alle ore 8:26 del 26/07/2019, sempre con il telefono di marca Samsung, veniva disposto un bonifico dell'importo di € 4.980,00 a favore di un nuovo beneficiario, con corretta autenticazione tramite PIN e OTP, che veniva prenotato e posto in esecuzione il giorno successivo. L'operazione veniva notificata con messaggio tramite l'applicazione installata sul telefono della ricorrente e tramite SMS-alert inviato alla sua utenza telefonica.
- La ricorrente, affermando di aver ricevuto la notifica con messaggio tramite l'applicazione installata sul proprio telefono relativa all'operazione delle 8:26 di € 4.980,00 e di essersi contestualmente avveduta del bonifico di € 24.750,00, tentava di mettersi in contatto con la propria agenzia di riferimento dell'intermediario resistente, senza successo, e inviava un messaggio di posta elettronica al direttore dell'agenzia nella quale informava di disconoscere le operazioni.
- Alle ore 08:45 riusciva a mettersi in contatto telefonico con il direttore dell'agenzia, che la informava che il bonifico di € 24.750,00 era stato disposto il giorno precedente verso la Romania ed era pertanto complicato bloccarne l'accredito, e che era invece possibile bloccare il bonifico di € 4.980,00.

La ricorrente afferma di essere stata vittima del fenomeno della frode nota come SIM SWAP FRAUD. Lamenta che l'operazione fraudolenta è stata possibile anche perché la procedura applicata per la sostituzione del token fisico con quello virtuale non prevede né la firma del correntista, né l'invio di una comunicazione che tale dispositivo è stato attivato. Rimarca inoltre il comportamento negligente dell'intermediario resistente, che non ha verificato la natura di un bonifico anomalo rispetto alla sua normale operatività e ordinata da un telefono e da indirizzi IP diversi da quelli precedentemente utilizzati, e non si è dotata di un sistema di sicurezza che consenta di individuare operazioni anomale e chiederne conferma al titolare del conto. La ricorrente afferma infine che, dopo aver subito la frode, è stata costretta a chiedere un finanziamento che le veniva concesso nella misura di € 31.796,50 con un TAEG del 6,26%. La ricorrente chiede pertanto la restituzione dell'importo relativo all'operazione fraudolenta, oltre agli interessi moratori sulla somma sottratta o, in subordine, agli interessi dovuti per l'erogazione del finanziamento.

L'intermediario resistente, nelle controdeduzioni, rileva che l'operazione contestata è stata disposta con le credenziali fornite per il servizio di home banking collegato al conto corrente intestato alla ricorrente, che richiedono un sistema di autenticazione a due fattori, il PIN ed l'OTP. Precisa che l'attivazione del *mobile token* al posto del *token* fisico è

possibile esclusivamente attraverso la medesima procedura di autenticazione a due fattori. Osserva che la ricorrente avrebbe potuto notare il bonifico contestato di € 24.750,00 contabilizzato il giorno 25/07/2019 in occasione degli accessi effettuati da Gerusalemme lo stesso giorno. Rimarca di essersi attivato per bloccare li secondo bonifico e di aver recuperato dalla controparte estera l'importo di € 1.029,99. Ribadisce di aver posto in essere tutte le misure di sicurezza e prevenzione idonee a tutelare il cliente e che la frode è stata resa possibile esclusivamente dalla conoscenza da parte dei frodatori delle credenziali di accesso al servizio di home banking.
Nelle repliche alle controdeduzioni, la ricorrente ha richiamato quanto affermato nel ricorso introduttivo, rimarcando inoltre che: a) la ricorrente ha acquistato una nuova SIM soltanto il giorno seguente alla scoperta del malfunzionamento della SIM originale; b) l'attivazione del servizio di *mobile token* è avvenuto in data 24.07.2019 alle ore 16:52 e alle ore 16:55 risulta disposto il bonifico contestato, a dimostrazione che l'attivazione del *mobile token* è avvenuta senza disattivare il *token* fisico.
L'intermediario resistente, nelle controrepliche, ha rimarcato che: a) il ritardo con cui la ricorrente ha provveduto alla sostituzione della SIM configura un comportamento caratterizzato da colpa grave; b) l'attivazione del *mobile token* avviene mediante la digitazione delle credenziali di sicurezza assegnate al cliente nella fase contrattuale di attivazione del servizio, che sostituisce la firma olografa del cliente; c) fino al 14.09.2019 era consentita la possibilità che coesistessero il *token* virtuale e il *token* fisico e, in ogni caso, la disattivazione del *token* fisico non avrebbe impedito la frode. Chiede pertanto il rigetto del ricorso.

## DIRITTO

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 (nota come PSD 2).
Il Collegio osserva che il ricorso in esame si configura come un caso di SIM swap fraud, ovvero di sostituzione della carta SIM del titolare di in conto bancario, resa possibile dal fatto che è possibile accedere alla pagina contenente le informazioni anagrafiche dei titolari di un conto corrente online utilizzando unicamente un PIN statico. La non riconducibilità delle operazioni al dispositivo in uso alla ricorrente si desume chiaramente dalle informazioni fornite dell'intermediario resistente, che evidenziano numerosissimi accessi tramite un dispositivo di marca Samsung, e un numero ridotto di accessi tramite il dispositivo di marca Apple della ricorrente. Appare quindi plausibile che i truffatori abbiano raccolto informazioni riservate relative al ricorrente, incluso il codice cliente e la password per i servizi bancari online, attraverso mezzi diversi dall'accesso al suo conto bancario. Non appare tuttavia evidente una responsabilità tale da configurarsi come dolo o colpa grave della ricorrente, che sarebbe stato onere dell'intermediario resistente provare in modo più circostanziato che con la semplice presunzione, ossia attraverso l'operazione logica che consente di risalire da un fatto noto, la conoscenza del PIN da parte dei frodatori, a uno ignoto, le modalità con le quali hanno acquisito l'informazione. La stessa Corte di Cassazione, a tale specifico riguardo, ritiene ammissibile la prova indiziaria della sussistenza della colpa grave (si veda, Cassazione civile, Sezione II, 18 gennaio 2010, n. 654). Si deve allora ricorrere ai fatti noti, ovvero ai cosiddetti indizi, che, per assurgere al rango di prova presuntiva, debbono però essere gravi, precisi e concordanti, come previsto dall'articolo 2729 del Codice civile.

Il Collegio osserva al contempo che l'intermediario resistente ha basato il proprio sistema di autenticazione dinamico sull'utilizzo di una carta SIM, il cui possesso non può essere univocamente attribuito al titolare del conto corrente. Come dimostra il caso del presente ricorso, è infatti possibile che ignoti truffatori si sostituiscano al titolare del contratto telefonico e si approprino della carta SIM e dell'utenza utilizzata per l'autenticazione dinamica. La responsabilità di simili eventi non può essere attribuita al cliente dei servizi bancari, ma rientra nel rischio d'impresa di un intermediario finanziario, che può prevedere meccanismi aggiuntivi di verifica dell'identità del cliente nel caso di richiesta della sostituzione della carta SIM utilizzata per l'autenticazione dinamica dei clienti.
In sintesi, il Collegio ritiene che la responsabilità dei fatti oggetto del presente ricorso sia da attribuirsi all'intermediario resistente, che ha omesso di cautelarsi di fronte alla possibilità che la carta SIM utilizzata per l'autenticazione dinamica possa essere sostituita fraudolentemente, così vanificando i presidi di sicurezza predisposti a tutela della clientela. Anche in questa ipotesi, come in altre già esaminate da questo Collegio, la violazione di una singola misura di sicurezza ha compromesso anche l'affidabilità delle altre, "quando, al contrario, la piena operatività del sistema di autenticazione multifattore si fonda sull'indipendenza tra le singole misure di sicurezza" (così Collegio di Roma, decisione n. 11777/2019). Il Collegio accoglie pertanto la domanda di risarcimento della ricorrente.
Non possono invece essere accolte la domanda risarcitoria e quella di refusione delle spese di assistenza professionale. La prima perché non è fornita sufficiente evidenza per identificare un legame diretto tra la frode subita e la necessità di richiedere un finanziamento. La seconda perché non vi è prova delle spese sostenute dalla ricorrente per l'assistenza professionale.

**PER QUESTI MOTIVI**

**Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 24.750,00 oltre interessi dal reclamo al saldo. 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
FERNANDO GRECO