Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) GRECO	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) NERVI	Membro di designazione rappresentativa degli intermediari
(RM) CHERTI	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - CHERTI STEFANO

Seduta del 10/04/2020

FATTO

1) La ricorrente si ritiene vittima di una “truffa bancaria” e disconosce un’operazione di euro 4.492,00; afferma di non aver mai ceduto, comunicato o condiviso le credenziali di accesso ai servizi di home banking e di non aver risposto a comunicazioni di richiesta delle medesime credenziali. Precisa che l’accesso all’home banking è sempre avvenuto su sito web o mediante app ufficiale dell’intermediario “e con inserimento delle credenziali ad ogni singolo accesso”.
2) Dal verbale di denuncia che allega evidenzia che in data 25.07.2019, intorno alle ore 17:00 il telefono cellulare diveniva inattivo, credendo si trattasse di un disservizio del gestore telefonico, attendeva il ripristino della funzionalità ma, persistendo il problema, contattava il servizio clienti del gestore e apprendeva che la sua sim card era stata disabilitata su richiesta per avvenuto smarrimento (tuttavia, non avendo smarrito la sim, chiedeva la riattivazione immediata, che avveniva poco dopo).
3) Appena ripristinata la sim, le pervenivano degli sms da parte dell’intermediario resistente, collocati alle ore 17:31 e 19:30 del 25.07.2019, aventi ad oggetto l’attivazione del servizio mobile token, nonché un messaggio di alert. Controllava la lista movimenti e rilevava un prelievo da lei non autorizzato, per l’importo di euro 4.992,00.
4) L’intermediario, costituendosi, ha dichiarato che la transazione è stata effettuata utilizzando l’opzione “prelievo extra”, modalità di prelievo che può essere effettuata presso

gli ATM (fino a un importo di € 4.990,00) anche senza l'utilizzo della carta bancomat, tramite l'inserimento in un primo momento delle credenziali di sicurezza previste per l'accesso all'home banking (numero cliente e codice segreto PIN) ed il successivo inserimento all'atto della conferma dell'operazione, del codice OTP "dinamico" (valido solamente per una singola operazione dispositiva) in analogia a quanto previsto per l'esecuzione di operazioni sui canali diretti".
5) Nel caso di specie, è configurabile la colpa grave della ricorrente per non aver diligentemente custodito le sue credenziali di sicurezza, tuttavia, in conformità all'orientamento dell'ABF, "senza alcun riconoscimento di responsabilità da parte della banca per i fatti accaduti e per merito spirito conciliativo", ha offerto alla ricorrente una restituzione parziale, corrispondente al 50% del petitum, pari a euro 2.469,00, oltre al rimborso della somma di euro 20,00 sostenuta per la presentazione del ricorso.

DIRITTO

Dalla documentazione in atti questo Collegio rileva che l'intermediario ha fornito la prova di autenticazione, corretta registrazione e contabilizzazione delle operazioni di pagamento ed ha descritto i profili delle operazioni fraudolente; tuttavia, la prova diretta del dolo o della colpa grave della cliente nella custodia dello strumento di pagamento.
È orientamento pacifico che l'onere della prova che incombe sull'intermediario possa essere assolto anche attraverso la c.d. presunzione, ossia attraverso l'operazione logica che consente di risalire da un fatto noto ad uno ignoto. La stessa Corte di Cassazione, a tale specifico riguardo, ritiene ammissibile la prova indiziaria della sussistenza della colpa grave (v. Cass. civ., Sez. II, 18 gennaio 2010, n. 654). Si deve allora ricorrere ai fatti noti, ovvero ai c.d. indizi, che, per assurgere al rango di prova presuntiva, debbono però essere gravi, precisi e concordanti, come previsto dall'art. 2729 c.c.
Il Collegio evidenzia che la ricorrente abbia dichiarato: i) di non aver mai perso il possesso dello strumento di pagamento; ii) di non aver rivelato a terzi estranei le credenziali per la funzionalità del sistema di home banking; iii) di non aver richiesto la sostituzione e/o blocco della SIM per furto/smarrimento.
Sulla base di quanto emerge dalla documentazione prodotta, il Collegio osserva come la pluralità di elementi addotti dalle parti induca a pensare che la ricorrente sia stata vittima di una frode nota come "*Sim swap fraud*", diffusasi in tempi relativamente recenti, al fine di vanificare i presidi di sicurezza basati su autenticazione con OTP inviato tramite SMS.
Si consideri al riguardo che, con comunicato stampa diffuso dalla Polizia di Stato il 02.07.2018, la truffa perpetrata ai danni dei clienti delle banche sia stata così descritta: "*La SIM SWAP è una avanzata tipologia di frode informatica articolata in vari passaggi. Una volta individuata la vittima si procede alla acquisizione dei suoi dati e delle credenziali di home banking tramite tecniche di hacking ovvero di ingegneria sociale e, successivamente, utilizzando documenti falsificati ad hoc, si sostituisce la sim card della vittima e, attraverso lo stesso numero telefonico, si ottengono dalla banca le credenziali per operare sul conto corrente on-line. Nel caso specifico, carpiti i dati anagrafici e il numero di telefono della vittima, nonché i dati dei conti correnti e le relative credenziali di accesso, gli indagati, utilizzando un falso documento di identità intestato alla vittima, si recavano presso un dealer al fine di chiedere la sostituzione della SIM in uso alla persona offesa. La scheda SIM del titolare veniva allora disabilitata in quanto sostituita da quella attivata fraudolentemente. La vittima rilevava il mancato funzionamento della sua SIM ma, generalmente, non associava immediatamente l'evento ad una frode in corso. Sostituita la SIM, gli autori del reato penetravano nel sistema informatico dell'istituto di credito presso*

cui la vittima aveva acceso il conto corrente, riuscendo il più delle volte a reimpostare le credenziali di accesso attraverso una telefonata all'assistenza clienti, presentandosi come il titolare del conto e rispondendo alle varie domande di sicurezza. Una volta effettuato l'accesso, gli indagati erano abilitati ad operare sul conto corrente on-line della vittima, disponendo bonifici e/o ricariche di carte prepagate in favore di altri conti correnti e/o carte prepagate nella loro disponibilità, in quanto appositamente accesi da complici e prestanome, così ostacolando l'identificazione della provenienza delittuosa delle somme e l'individuazione degli effettivi beneficiari dei proventi del reato attraverso il tracciamento dei flussi finanziari generati dall'operazione dispositiva indebita. La serrata successione temporale delle varie sequenze attraverso le quali si snoda la frode informatica in esame non consentiva alla vittima di attivare tempestivamente i dispositivi di sicurezza; la vittima acquisiva dunque consapevolezza del prelievo indebito solo al momento della lettura dell'estratto del conto corrente […]".

Infatti, anche nel caso odiernamente sottoposto all'attenzione del Collegio la frode ha avuto luogo tramite un intervento sul numero di cellulare, sul quale si fonda il sistema di autenticazione delle operazioni tramite home banking.

Posto che la OTP è un sistema di controllo dell'identità dinamico e monouso, essa consiste generalmente in un codice alfanumerico - generato da un algoritmo - trasmesso all'utente su un canale fuori banda (nella specie, messaggistica SMS), per cui è sempre necessaria, ai fini della sua utilizzazione, una tecnologia supplementare (ITC mobile - come in questo caso -, o token ecc.).

Dalla descritta logica di autenticazione, consegue che l'operazione di modifica dell'utenza telefonica sulla quale ricevere la OTP o la semplice possibilità di venire a conoscenza del numero di telefono, può rischiare di svuotare la password dinamica della propria funzione protettiva di verificare la genuinità dell'operazione, e dunque costituisce di per sé un'operazione o una situazione anomala. In buona sostanza, la violazione di una singola misura di sicurezza ha compromesso anche l'affidabilità delle altre poste a presidio dall'intermediario per prevenire utilizzi fraudolenti a danno dei clienti (come già prescritto invece a livello comunitario dalla Direttiva 2015/2366/UE, cosiddetta Direttiva PSD2).

Nel caso di specie, pur non potendosi escludere la presenza di un'autenticazione forte dell'operazione, si deve tuttavia escludere che la stessa sia dipesa dalla volontà e/o da comportamenti coscienti della ricorrente, alla quale dunque, deve essere restituito l'importo fraudolentemente sottratto.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 4.992,00.

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