Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) STELLA	Membro designato dalla Banca d'Italia
(MI) MINNECI	Membro designato dalla Banca d'Italia
(MI) BENINCASA	Membro di designazione rappresentativa degli intermediari
(MI) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore MINNECI UGO

Seduta del 06/02/2020

FATTO

Premettendo di avere ricevuto in data 10 giugno 2019 un Sms Alert relativo a un bonifico estero di Euro 1.600,00 e di averlo tempestivamente revocato (non avendolo autorizzato), parte ricorrente riferisce di avere scoperto – in esito a un controllo effettuato proprio in conseguenza di quanto accaduto – l'esistenza sul proprio conto di un addebito di Euro 25.650,00 datato 6 giugno 2019 relativo a una operazione mai richiesta. Aggiungendo di non avere ricevuto alcun Sms Alert in ordine alla suddetta operazione, insiste per la retrocessione dell'importo addebitato.
In sede di controdeduzioni, l'intermediario convenuto premette che il servizio di home banking offerto è a due fattori di sicurezza e che per le operazioni dispositive è necessario digitare, oltre alle credenziali di accesso, anche il codice OTP. Riferisce che l'operazione contestata sarebbe stata regolarmente impostata mediante utilizzo delle credenziali corrette e inserimento del codice OTP. Aggiunge di avere inviato per entrambe le operazioni un Sms Alert, precisando altresì che la mancata ricezione del primo sarebbe con ogni probabilità da ascriversi a un blocco della carta SIM del cliente avvenuto tra il 6 e 7 giugno 2019. Sottolinea inoltre che proprio l'invio del codice OTP varrebbe a dimostrare l'avvenuta attivazione del c.d. mobile token. Contestando alla parte ricorrente una negligente custodia dei dispositivi di sicurezza, insiste per il rigetto del ricorso.

DIRITTO

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.
Tale tipo di truffa è stato così descritto dalla Polizia di Stato tramite comunicato stampa diffuso il 02.07.2018: «*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 […]*».
Ora, anche nel caso odiernamente sottoposto all'attenzione del Collegio, la frode commessa risulta avere 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.
L'inadeguatezza del sistema appare anche da un altro punto di vista. La logica della cosiddetta strong customer authentication (SCA) è quella di consentire l'accesso al sistema del soggetto che effettua la transazione tramite l'inserimento non di uno, ma di almeno due elementi identificativi (password e OTP, nel caso che occupa), per aumentare

la sicurezza del servizio di pagamento. Ora, dalla narrativa di entrambe le parti, emerge che agli autori della sottrazione è stato sufficiente ottenere le credenziali statiche per poter sia accedere al portale titolari, sia di venire a conoscenza del numero di utenza cui vengono inviati i codici alfanumerici, che intervenire sulla relativa sim e appropriarsi di questi ultimi.
In buona sostanza, la violazione di una singola misura di sicurezza ha compromesso anche l'affidabilità dell'altra, quando, al contrario, la piena operatività del sistema di autenticazione multifattore si fonda sull'indipendenza tra le singole misure di sicurezza (cfr. Collegio di Milano, decisione n. 1066/2019). L'esistenza di una relazione funzionale tra di esse consente di eludere il doppio controllo delle credenziali, e rendere, nei fatti, il sistema di autenticazione (non più forte ma) debole.
La portata dirimente del suddetto requisito di indipendenza tra misure di sicurezza è del resto riconosciuta anche dalla Direttiva 2015/2366/UE (cosiddetta Direttiva PSD2 che, a partire dal 13 gennaio 2018, sostituirà la Direttiva 2007/64/CE, cosiddetta Direttiva PSD1), la quale lo prescrive come caratteristica obbligatoria (art. 4, par. 1, lett. 30) che deve improntare il rapporto tra singole misure di sicurezza di un sistema di autenticazione forte (ora da predisporre obbligatoriamente: art. 97, par.1).
D'altro canto, almeno da quanto risulta agli atti, non è dato evincere un contributo di parte ricorrente alla realizzazione della truffa.
Il ricorso merita pertanto accoglimento nella sua interezza.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 25.650,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA