Santiago, catorce de agosto de dos mil diecinueve.

Vistos:

Se reproduce sólo lo expositivo de la sentencia en alzada, suprimiéndose lo demás.

Y se tiene en su lugar y además presente:

Primero: Que, en los presentes autos, don Francisco Iván Alviña Sánchez interpone recurso de protección en contra del Banco de Chile, señalando como acto arbitrario e ilegal la negativa de la recurrida a realizar la devolución del dinero sustraído fraudulentamente desde su cuenta corriente que asciende a 1.500 dólares de los Estados Unidos.

Precisa que el día 28 de septiembre del año 2018, ingresó a la página web de la recurrida, desplegándose un aviso en la pantalla que indicaba que debía instalar un programa llamado Trustter Rapport, solicitándole la digitación de su clave, la que ingresó y tras lo cual, aparece en su estado de cuenta una transacción por 1.500 dólares, cuyo origen se sitúa en la ciudad de Chipre, en circunstancias que al verificarse la referida operación se encontraba en Chile.

Conforme a lo señalado precedentemente, el actuar de la recurrida configura una palmaria vulneración a la garantía constitucional establecida en el artículo 19 n° 24 de la Constitución Política.

Segundo: Que, informando la recurrida, solicita el rechazo del recurso y señala que la materia en controversia excede el ámbito del recurso porque la supuesta vulnerabilidad sólo se puede comprobar en definitiva en un proceso ordinario que permita resolver con propiedad acerca de las pretensiones de las partes.

Afirma que la operación objetada por el actor cumplió con el ingreso de su rut, clave personal, y finalmente con el ingreso de clave otorgada por el dispositivo digipass, por lo tanto no existe antecedentes que evidencien la vulneración de la infraestructura y/o equipos perteneciente al banco. Agrega que todo indica que el actor fue víctima de un delito de phishing o pharming, puesto que la instalación del software Trustter Rapport no exige el ingreso de la clave digipass, concluye señalando que probablemente la intervención en su equipo se ha producido en su equipo personal para luego hacerse de las claves en el sitio real y auténtico del banco.

Tercero: Que, como lo ha sostenido esta Corte, el contrato de cuenta corriente bancaria constituye una especie de depósito respecto de un bien eminentemente fungible, y que es de cargo del depositario el riesgo de pérdida de la cosa depositada durante la vigencia de la convención (SCS de 20/06/18, rol N° 2.196-2018); y que, para cada caso, resulta relevante analizar si los eventos que originaron las transferencias cuestionadas no han

tenido como única causa la voluntad del depositante o cuentacorrentista, o han ocurrido otros que llevan a sostener que se han incumplido las obligaciones de resguardo y seguridad que recaen en la institución bancaria respectiva.

Cuarto: Que, en efecto, la variedad de las formas como se intenta vulnerar los sistemas de seguridad y la dificultad probatoria inmediata obligan a realizar un juicio acerca de indicios sobre la ocurrencia de los hechos y confrontar aquellos con las diversas normas que determinan las obligaciones de seguridad de las instituciones bancarias.

Así, para el caso de transferencias electrónicas, el Capítulo 1-7, punto 4.2, de la Recopilación de normas de la Superintendencia de Bancos indica que: "*Los bancos deberán contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible aquellas operaciones con patrones de fraude, de modo de marcar o abortar actividades u operaciones potencialmente fraudulentas, para lo cual deberán establecer y mantener, de acuerdo a la dinámica de los fraudes, patrones conocidos de estos y comportamientos que no estén asociados al cliente.*

Estos sistemas o mecanismos deberán permitir tener una vista integral y oportuna de las operaciones del cliente, del no cliente (por ejemplo en los intentos de acceso), de

los puntos de acceso (por ejemplo direcciones IP, Cajero Automático u otros), hacer el seguimiento y correlacionar eventos y/o fraudes a objeto de detectar otros fraudes, puntos en que estos se cometen, modus operandi, y puntos de compromisos, entre otros."

Quinto: Que, de lo expuesto, se concluye que la recurrida se limitó a señalar en su informe que las transferencias se realizaron utilizando las claves del cliente, planteando como hipótesis la intervención por parte de terceros del equipo del actor a efectos de obtener sus claves. Sin embargo no acreditó de modo alguno que la operación objetada se haya realizado desde el computador de éste; por consiguiente, el banco recurrido no ha podido excepcionarse de cubrir las pérdidas sufridas por el recurrente, dado que no acreditó, estando en posición de hacerlo, que el siniestro haya ocurrido con ocasión de la sustracción de las claves por parte de terceros por una vía distinta a la obtención de las mismas a través de su página web oficial.

Sexto: Que, teniendo presente los hechos asentados resulta que se advierte que la operación cuestionada se realizó a través de la página web oficial del banco recurrido y fuera del espacio habitual de operaciones del cliente, lo que permite descartar que los hechos se han debido única e inequívocamente a una actividad dolosa o negligente de su parte.

Además, las obligaciones de monitoreo y control de fraudes recaen expresamente en la institución recurrida, donde los patrones de conducta del cliente son elementos de juicio para la determinación de una operación engañosa, cuestión que no fue informada en detalle por el Banco recurrido. Sobre la institución bancaria recae la obligación de vigilancia y el análisis de la correlación de eventos y seguridad de las operaciones, por lo que, una vista general de las operaciones del cliente en la cuenta corriente respectiva otorgan verosimilitud a la intervención de terceros en los sistemas de seguridad que otorgó la recurrida.

Séptimo: Que asentado lo anterior, no queda más que calificar el actuar de la recurrida como ilegal y arbitrario, puesto que al no asumir el perjuicio económico trasladando los efectos del fraude bancario al actor, afecta directamente el patrimonio de éste, vulnerando así el artículo 19 N° 24 de la Constitución Política.

Por estas consideraciones y de conformidad con lo que dispone el artículo 20 de la Constitución Política de la República y el Auto Acordado de esta Corte sobre la materia, **se revoca** la sentencia en alzada de fecha cinco de marzo de dos mil diecinueve y en su lugar se declara que **se acoge** el recurso de protección debiendo la recurrida Banco de Chile restituir a don Francisco Iván Alviña Sánchez la suma de 1.500 dólares de los Estados Unidos.

Acordada con el voto en contra del Ministro Sr. Arturo Prado Puga, quien atendido a las circunstancia que no existe claridad acerca del origen que causó el incidente que permitió que terceros accedieran a los datos del cliente reclamante, facilitando la sustracción de fondos de su cuenta, fue del parecer que la garantía involucrada y su vulneración debían ser objeto de un juicio de largo conocimiento, no siendo esta la vía.

Regístrese y devuélvase.

Redacción a cargo de la Ministra Sra. Vivanco y el voto de su autor.

Rol N° 7155-2019.

Pronunciado por la Tercera Sala de esta Corte Suprema integrada por los Ministros Sr. Sergio Muñoz G., Sra. María Eugenia Sandoval G., Sr. Carlos Aránguiz Z., Sr. Arturo Prado P. y Sra. Ángela Vivanco M. Santiago, 14 de agosto de 2019.

SERGIO MANUEL MUÑOZ GAJARDO
MINISTRO
Fecha: 14/08/2019 10:49:11

MARIA EUGENIA SANDOVAL GOUET
MINISTRA
Fecha: 14/08/2019 10:51:07

CARLOS RAMON ARANGUIZ ZUÑIGA
MINISTRO
Fecha: 14/08/2019 10:51:08

ARTURO JOSE PRADO PUGA
MINISTRO
Fecha: 14/08/2019 13:54:34

ANGELA FRANCISCA VIVANCO
MARTINEZ
MINISTRA
Fecha: 14/08/2019 10:51:08

KJXKMBHNVX

En Santiago, a catorce de agosto de dos mil diecinueve, se incluyó en el Estado Diario la resolución precedente.