FOJA: 37 .- .-

NOMENCLATURA : 1. [40]Sentencia
JUZGADO : 26º Juzgado Civil de Santiago
CAUSA ROL : C-38045-2018
CARATULADO : LEITAO/BANCO DE CHILE

Santiago, veintisiete de Marzo de dos mil veinte

VISTOS.
Con fecha 28 de noviembre de 2018, don CRISTIÁN JOSÉ SANTOS LEITAO FUENZALIDA, administrador de edificios, domiciliado en avenida Providencia N° 1930, departamento 61, comuna de Providencia, deduce demanda en juicio ordinario de indemnización de perjuicios, en contra del BANCO DE CHILE, sociedad del giro de su denominación, representado por su gerente general don Eduardo Ebensperger Orrego, ingeniero, ambos domiciliados en Ahumada N° 251, comuna de Santiago, fundada en que mantiene la cuenta corriente N° 160-10907-08 en el Banco de Chile, y el miércoles 8 de agosto de 2018, siendo las 10:57, ingresó a su cuenta corriente vía internet y se abrió una ventana del Banco de Chile obligándole a contratar el Sistema Trusteer Report que maneja el mismo Banco de Chile, sin permitirle realizar operación alguna mientras no enviara la clave dinámica que recibió con el N° 21405 en su teléfono celular 99 8795558. Sin embargo, todo ello resultó ser falso y le cargaron en la cuenta corriente la cantidad de $750.000.- que fueron transferidos a la cuenta corriente 67130283 Banco BCI, del señor Ramón Alberto Pérez, R.U.T. 17.479.039-6, persona a quien no conoce. Señala, que el mismo 8 de agosto, al confirmar lo sucedido y de acuerdo con la instrucción recibida del Sr. Luis Medina Canario, de Banca Telefónica, bloqueó sus claves de inmediato y después completó un formulario con la denuncia formal al Banco de Chile a través de una carta "Objeción de cargo en cuenta corriente" y una "Carta explicativa", todo en plazo y forma. Además, llenó y envió al banco el formulario "Desconocimiento de transferencias por Internet" con todas sus respuestas negativas, salvo la última que era positiva porque sí tenía sistemas anti virus, phishing, troyanos, etc. en su computador. Agrega, que el mismo 8 de agosto, siguiendo las instrucciones del Sr. Luis Medina C. antes mencionado, denunció en Carabineros de Chile, 19a. Comisaría de Providencia de la Prefectura Santiago Oriente, el uso fraudulento de cuenta bancaria (evento 10099376, Parte s/n). Que el 17 de agosto, a solicitud de la Fiscalía Local Ñuñoa, y con la Causa RUC 1800776105-4, narró lo ocurrido informando el cargo indebido en su cuenta corriente. La Fiscalía estampó el delito "Código 12151: Uso fraudulento de tarjeta de crédito y débito Ley 20009 sobre uso de Tarjeta de crédito." quedando pendiente una citación posterior. Añade, que solicitó al Banco de Chile la devolución del importe sustraído, con el Requerimiento 1-22901492846, y el Depto. Línea de Servicio a Clientes, con fecha 10 de septiembre de 2018, no acogió su solicitud de devolución del monto reclamado, argumentando que la operación fue realizada por él, desde su línea privada de internet, para lo que se requiere de su RUT y clave secreta, cuyo "conocimiento, resguardo y confidencialidad son de exclusiva responsabilidad del cliente", para posteriormente ingresar una clave de alta seguridad generada por el dispositivo Digipass. Que respondió el mismo día 10 de septiembre a Línea de Servicio a Clientes indicando que todas sus operaciones del día 8 de agosto habían sido bloqueadas y que, para destrabarlas, fue obligado a digitar una clave dinámica, lo que demuestra que el sistema de seguridad del Banco de Chile fue vulnerado, al permitir bloqueos. Por otra parte, consultó en el Banco BCI por el N° de Rut y cuenta corriente del destinatario de los fondos, a lo cual recibió la respuesta de

que sólo el Banco de Chile podía hacer la reversión de los fondos. Que ello no sucedió, es decir, el área encargada del Banco de Chile en el caso no fue diligente para atender sus intereses. Que dicha falta de interés mostrada por el personal del Banco de Chile no es la respuesta que esperaba de una entidad bancaria en la cual toda su familia actual y pasada tenía confianza por ser clientes directos con cuentas corrientes vigentes. Manifiesta, que el Depto. Línea de Servicio a Clientes, del Banco de Chile, respondió a tal apelación señalando: "Al respecto podemos señalar que la cuenta antes individualizada no fue bloqueada por nuestra institución durante el día de la transacción. Además, es necesario precisar que el Banco no realiza este tipo de procedimientos en los productos de nuestros clientes. […] Por lo tanto, no existen nuevos antecedentes que permitan acceder a la devolución del monto reclamado."

En cuanto al derecho cita jurisprudencia al efecto, solicitando una indemnización por concepto de daño moral de $1.000.000.-, por los perjuicios sufridos por él y su familia, los que persisten ante la falta de respuesta del banco, la tramitación sufrida, el tiempo perdido y la inquietud ante el hecho de tener que recurrir a los tribunales buscando justicia.

En la conclusión, previas citas legales y demás normas pertinentes, solicita tener por interpuesta demanda en juicio ordinario de indemnización de perjuicios en contra del demandado, ya individualizado, acogerla a tramitación y, en definitiva, sea condenado a restituirle la suma de $750.000.- más los intereses devengados desde la fecha de ocurrido el siniestro y más $1.000.000 por concepto de daño moral o la suma que el Tribunal estime, con costas.

Con fecha 26 de diciembre de 2018, se notificó al demandado, de la acción dirigida en su contra.

Con fecha 4 de enero de 2019, el demandado contestó la demanda, solicitando su rechazo, con costas, señalando como primera cuestión, que del relato de los hechos contenido en la demanda, se puede advertir desde ya, que el actor no ingresó a la página web del Banco, cuestión que es imposible que sea verídica, porque jamás éste exige a sus clientes descargar el software Trusteer de Rapport, ni exige para su descarga el ingreso de una clave dinámica enviada al teléfono celular del cliente, cuestión ésta última que es advertida constantemente, mediante diversas comunicaciones que el Banco envía a sus clientes e incluso se trata de un hecho que todos los bancos advierten públicamente. Por lo anterior, afirma que el demandante no ingresó a la página web del Banco de Chile. Que en segundo lugar, la transacción impugnada por el actor fue ejecutada desde la sesión privada en internet del demandante, a través del sitio web que el Banco ha establecido, ingresando en línea, en el sitio privado de Internet del actor, al que sólo se puede ingresar: 1) digitando su número de rut, 2) luego ingresando la clave secreta del actor, la que es creada por él mismo y, 3) además, adicionalmente, de la utilización de una "clave dinámica" que es generada por el mecanismo denominado "digipass" o la aplicación para teléfonos móviles denominada "MiPass". Todos estos elementos son de conocimiento y uso exclusivo del demandante, los que se encuentran además bajo su custodia personal. Agrega, que la transferencia objetada por el demandante fue realizada desde su sesión web privada, a la que se accede ingresando su número de cédula de identidad y además su clave secreta, que es creada por él. Luego, para autorizar la transferencia objetada, se utilizó la clave generada por la aplicación para teléfonos móviles denominada "MiPass", que fue instalada utilizando las claves secretas del demandante, que para su instalación requiere además el uso de la clave que genera su digipass y, adicionalmente, una tercera clave secreta que es enviada a su teléfono celular, para así tener plena certeza que quien instala la aplicación es el propio cliente, respecto de quien se verifica su identidad mediante el envío de esta tercera clave enviada a su teléfono celular. En síntesis, para instalar la aplicación "MiPass" se requieren tres claves secretas que sólo el actor conoce, la primera es la que habitualmente utiliza en internet, la segunda es una clave dinámica generada por su dispositivo digipass y que es válida solo por unos segundos y, la tercera, es otra clave dinámica que es enviada a su teléfono celular, que también es válida por un corto período de tiempo. Así con este sistema de triple clave, el Banco cumple con todas las normativas de seguridad, que aseguran que quien descarga la aplicación es el propio cliente, para autorizar sus transacciones con ella. Que en tercer lugar, resulta relevante también para la resolución del juicio, indicar que la dirección IP desde la que se realizó la transferencia objetada es la misma que se

utilizó para las transacciones anteriores del propio demandante, a partir del mes de junio del año 2018 y que se siguió utilizando después de ejecutar tal transacción. Esto es especialmente relevante, porque la dirección IP identifica un determinado dispositivo, que puede ser un computador, una Tablet, un teléfono, etc.; en la red, por lo que con ese dato, se puede determinar que el dispositivo que se utilizó para efectuar la transferencia objetada es el mismo que había sido utilizado anteriormente para las transacciones del actor y que se siguió utilizando después. Expresa, que tal hecho, unido a la utilización de todas las claves secretas del demandante, incluso la que fue enviada a su teléfono celular, permite descartar cualquier irregularidad en la realización de la transferencia que desconoce en este juicio. Que por lo demás el demandante confiesa espontáneamente en su libelo, que recibió una clave dinámica en su teléfono celular y que la ingresó en la página web a la que había accedido -que como se dijo no era la del Banco de Chile-. Que en dicho punto, aclara que la tercera clave dinámica, necesaria para la descarga de la aplicación "MiPass" fue enviada al teléfono celular que el propio actor registró personalmente en el Banco de Chile, habiendo presentado su cédula de identidad vigente y además autentificando su identidad mediante la lectura de su huella digital en el sistema biométrico del Banco. Que mediante la aplicación de tales sistemas -triple clave- no cabe sino concluir que el Banco cumplió lo pactado con su cliente y, además, que proveyó a éste de todos los mecanismos de seguridad que la Superintendencia de Bancos e Instituciones Financieras y la lógica prevén para la realización de este tipo de transacciones; mismos que todo Banco a nivel mundial entrega a sus clientes; es decir, (1) dispuso de un sistema de claves y mecanismos de acceso al sistema y tipo de operación que impidan que el originador y/o el destinatario desconozcan la autoría de las transacciones; (2) contó con metodología que comprende una encriptación sólida; (3) dispuso a lo menos tres factores de autentificación distintos para cada transacción, debiendo ser a lo menos uno de ellos de generación o asignación dinámica y (4) proveyó de perfiles que permitan identificar, evaluar, monitorear y detectar aquellas operaciones con patrones de fraude. Por consiguiente, niega que el actor haya sido víctima de un delito y, por ende, que terceros ajenos hayan vulnerado las redes del Banco en su perjuicio, pues la transferencia fue efectuada con las claves y password del demandante, según consta de los registros computacionales, de modo que conforme a los contratos se configuró la firma electrónica del cliente, razón por la cual no puede desconocer tales operaciones, cumpliéndose así los requisitos necesarios para que contractualmente puedan atribuírsele. Además, reitera que se efectuó desde la dirección IP utilizada habitualmente por el actor. Todo lo anterior, según lo previsto en los contratos suscritos al efecto, normativa aplicable a esta especie de transacciones y prueba que se rendirá al efecto (logo registro de transacciones). Indica, que dicha normativa previene en la materia, en síntesis, dos cuestiones completamente diversas: la primera, consiste en la intervención directa y por parte de terceros de la página web del Banco y, la segunda, la intervención de terceros, ya no de la página web del Banco, sino del computador o pantalla del cliente o usuario, bajo la modalidad denominada "phishing" u otra similar. Para evitar lo primero -intervención por terceros de la página web del Banco y, por ende, suplantación a través de ella del cliente- el Organismo Supervisor dispone que "el sistema debe proveer un perfil de seguridad que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, además, la privacidad o confidencialidad de la información transmitida o procesada por ese medio". Que la finalidad de lo anterior es que los procedimientos empleados "impidan que tanto el originador como el destinatario, en su caso, desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse claves y mecanismos de acceso al sistema y al tipo de operación, que permitan asegurar su autenticidad e integridad"; esto es, que no haya intervención alguna de terceros en la comunicación entre el banco y el cliente, este último obrando con sus claves. Afirma, que en el caso, la página del Banco no ha sido vulnerada, sino que es el cliente quien ha proporcionado a terceros los medios dados por el Banco -secretos, personales intransferibles y bajo su exclusiva custodia- para su autentificación, existiendo por tanto una comunicación íntegra y "auténtica" para estos efectos entre el Banco y el cliente, con la salvedad de que quien opera las claves no es el titular sino un tercero a quien éste se las proporcionó. Por lo anterior solicita el rechazo de la demanda o en subsidio la rebaja del monto solicitado.

Con fecha 5 de febrero de 2019, se verificó la audiencia de conciliación, con la sola asistencia del apoderado de la parte demandante, instancia que no prosperó
Con fecha 1 de marzo de 2019, se recibió la causa a prueba, interlocutolria que se modificó con fecha 7 de mayo de 2019.
Con fecha 3 de febrero de 2020, se citó a las partes a oír sentencia.

CONSIDERANDO.
PRIMERO. Que, en orden a acreditar los daños y perjuicios cuyo resarcimiento pretende, el demandante se hizo valer de la DOCUMENTAL consistente en:
1. Respuesta del Banco al reclamo telefónico inicial.
2. Formulario Objeción, Mandato y Declaración Jurada.
3. Primera respuesta del Banco a las objeciones.
4. Réplica del demandante al Banco.
5. Dúplica del Banco al demandante.
6. Registros de la Cuenta Corriente (del día cuando se sustrajeron los fondos).
7. Denuncia a Carabineros de Chile.
8. Carta de la Fiscalía del Sr. Pablo Álvarez Gómez.
9. Respuesta a la Fiscalía Oriente

SEGUNDO. Que, el demandado a fin de desvirtuar la pretensión de contrario, se hizo valer de la siguiente prueba, consistente en:
A) INSTRUMENTAL:
1. Hoja de firma del contrato Unificado de Productos de Personas Versión 8.
2. Texto del Contrato Unificado de Productos de Personas Versión 8.
3. Certificado de la empresa Symantec sobre la inviolabilidad de las redes del Banco de Chile.
4. Certificado emitido por la empresa Neosecure, que da cuenta que el demandante no había descargado el software que el Banco pone gratuitamente a disposición de sus clientes, para ayudarlos a evitar ser víctimas de phishing.
5. Log o registro computacional de la transferencia objetada en autos.
6. Registro de las IP utilizadas por el actor, durante los meses de mayo a agosto de 2018.
7. Respuesta de Servicios Interactivos Móviles Limitada, tras no asistir a la audiencia de exhibición de documentos de fecha 9 de septiembre de 2019.

B) CONFESIONAL del actor, quien el 7 de agosto de 2019, respondió a las preguntas contenidas en el pliego de posiciones acompañado por el demandado, señalando que es efectivo el número de celular 998795558 allí indicado; que tiene registrado en el banco su teléfono fijo, además de su celular; que no es efectivo que las claves para operar su cuenta corriente sean conocidas por terceros; que el 8 de agosto de 2018 recibió en su celular un mensaje de texto con una clave dinámica que le fue enviada por el Banco de Chile; que no es efectivo que dicho día instaló las aplicaciones del banco en su celular; que no había descargado el sistema Rapport de Trusteer que el banco puso gratuitamente a su disposición.
TERCERO. Que, apreciada en su conjunto la documental aportada por el actor, se concluye que el día 8 de agosto de 2018, a las 10:57, al tratar éste de ingresar vía internet a su cuenta corriente N° 160-10907-08 en el Banco de Chile, se abrió una ventana obligándolo a contratar el sistema Rapport de Trusteer, con el que el banco demandado opera, bloqueando cualquier tipo de operación que éste deseara realizar, mientras no enviara la clave dinámica que recibió en su teléfono celular. Que el actor confiando en la seguridad de dicha operación, entregó la información referida, la que terminó siendo utilizada por terceros, quienes tras vulnerar el sitio web del Banco de Chile, evadiendo las medidas de seguridad de éste, transfirieron electrónicamente dinero de la cuenta corriente del actor a la de un tercero desconocido, hecho que no implica exposición imprudente al daño por el demandante, pues el buscaba acceder al sitio web del banco y fue dicho sitio el vulnerado, afectando al actor.
CUARTO. Que, habiendo el demandado incumplido sus obligaciones contractuales y legales para con el demandante, por no otorgar el resguardo debido en las operaciones que se realizan por medio de sus plataformas digitales, como las transacciones electrónicas de dinero, se concluye que el actor sufrió perjuicios como consecuencia del

incumplimiento del banco, los que deben ser reparados, por lo que se acogerá la demanda deducida, solo respecto de la pretensión de restitución del monto defraudado y se rechazará en el monto solicitado por concepto de daño moral, por no haberse rendido prueba alguna para ello.
QUINTO. Que, la prueba acompañada por el demandado, no logra desvirtuar lo ya establecido.
SEXTO. Que, incumbe probar la existencia de las obligaciones o su extinción a quien alega aquéllas o ésta.
Por estas consideraciones y visto además, lo dispuesto en los artículos 1, 144, 160, 154, 170, 254 y siguientes, 342, 346 y 385 y siguientes y 698 del Código de Procedimiento Civil; 1437, 1545, 1546, 1547, 1548, 1551, 1556 y 1689 del Código Civil; y Ley 19.496, se declara:
I. Que se acoge parcialmente la demanda deducida y, en consecuencia se condena al demandado a pagar al actor la suma por indemnización de perjuicios de $750.000.- por concepto de daño emergente, con intereses corrientes a contar de la ejecutoria, hasta el pago efectivo; y se rechaza la demanda en la pretensión de pago de un monto por concepto de daño moral.
II. Que no se condena en costas al demandado, por no haber sido totalmente vencido.
Regístrese y notifíquese.

PRONUNCIADA POR DON HUMBERTO PROVOSTE BACHMANN, JUEZ TITULAR.

AUTORIZA DOÑA LORETO GREZ BECKER, SECRETARIA SUBROGANTE.

Se deja constancia que se dio cumplimiento a lo dispuesto en el inciso final del art. 162 del C.P.C. en **Santiago**, **veintisiete de Marzo de dos mil veinte**

PZZPPXTMLX

DOMINGO HUMBERTO PROVOSTE BACHMANN
Fecha: 27/03/2020 14:48:06