

NOMENCLATURA : 1. [40]Sentencia  
JUZGADO : 30º Juzgado Civil de Santiago  
CAUSA ROL : C-7112-2018  
CARATULADO : CORTÉS/BANCO DE CHILE

Santiago, treinta de Abril de dos mil veintiuno

**VISTOS:**

Con fecha 9 de marzo de 2018, comparece el abogado don Luis Masferrer Farías, con domicilio en calle Rosario Norte N° 615, piso 22, comuna de Las Condes, en representación de don **Manuel Joaquín Fernando Cortés Fravega**, con domicilio en 1 Poniente N° 3305, Lonco Oriente, comuna de Chiguayante, Región del BíoBío, quien deduce demanda de indemnización de perjuicios por responsabilidad contractual en contra de **Banco de Chile**, representado legalmente por su Gerente General don Eduardo Ebensperger Orrego, ambos con domicilio en Ahumada N° 251, comuna de Santiago.

**I. ANTECEDENTES DE HECHO**

Funda la demanda en que don Manuel Cortés es cliente del Banco de Chile, a través del Banco Edwards Citi, con el cual contrató la cuenta corriente N° 743714-00-8, y dos tarjetas de crédito: una tarjeta VISA del Banco Edwards Citi, N° 4349 5605 7210 7204; y otra VISA Entel N° 4697 7220 0379 3725, que también administra el Banco.

Indica que si bien la cuenta corriente no solía tener muchos movimientos, manteniendo usualmente un saldo promedio inferior a los \$500.000; el día 27 de julio de 2017, su representado transfirió a dicha cuenta la suma de \$5.000.000, con objeto de facilitar una futura compra de acciones vía Banchile.

Relata que, en ese contexto, con fecha 31 de julio de 2017, a las 13:42 horas, el demandante recibió una llamada telefónica de una persona que se presentó como ejecutivo del Banco demandado. Ante las consultas que le formuló su representado sobre su personería, ya



que no se trataba de su ejecutiva de cuenta, dicha persona, para corroborar su identidad, le proporcionó una serie de antecedentes personales, como su RUT, número de cuenta corriente, número de ambas tarjetas de crédito, nombre de su ejecutiva, e incluso el número de serie del *digipass*.

Hace presente que, como puede apreciarse, la persona en cuestión poseía una gran cantidad de información que le fue dada a su representado, para acreditar que se trataba de una llamada de parte del Banco de Chile, en el cual mantenía la cuenta a la que se hacía referencia. Con todo esto, don Manuel Cortés no podía más que confiar, pues la información fue proporcionada por la persona que lo llamaba a él, sin que el demandante entregara sus datos personales.

Continúa señalando que la persona que se contactó con el demandante le informó que, por instrucciones de la Superintendencia de Bancos e Instituciones Financieras, el Banco debía devolver ciertos dineros, de escaso monto, alrededor de \$5.000, que habían sido cobrados de más. Esta información, si bien no resultaba usual, sí podía ser plausible y creíble, por lo que, nuevamente, no existían razones para desconfiar de lo que el actor estaba escuchando.

Explica que, para realizar dicha operación, se le pidió a don Manuel Cortés activar el *digipass* e informar el número que aparecía en el mismo, lo que el actor hizo, confiando que hablaba con un ejecutivo del Banco demandado, por todos los datos que le habían sido entregados.

Sostiene que, tras la llamada telefónica, a don Manuel le llamó la atención el procedimiento efectuado, por lo que acudió a la sucursal del Banco que tenía más cerca. Al no obtener mayor información sobre la operación en cuestión, y como la ejecutiva del Banco le informó que no tenía ningún antecedente, el señor Cortés procedió a desactivar el *digipass*, lo que realizó a las 14:17 horas, como precaución.

Denota que el demandante no tenía absolutamente ningún indicio razonable para pensar que estaba siendo víctima de una estafa



telefónica, toda vez que la persona que se comunicó con él tenía todos los datos de sus productos, datos que el Banco demandado debía resguardar, como parte de sus obligaciones.

Señala que, de manera paralela y casi simultáneamente a los hechos recién descritos, a las 13:48 y 13:50 horas, alguien incorporó dos nuevos números de teléfono (N° 29481900 y 981363199) como si fueran del señor Cortés, en el archivo del Banco en que se registran estos datos; gestión que jamás fue realizada por su representado.

Advierte que el trámite de agregar números telefónicos de contacto para cada cliente debe hacerse personalmente en el mesón del Banco, registrando además la huella digital. Sin embargo, en este caso, ninguno de esos requisitos se cumplió, incorporándose dos números telefónicos de respaldo sin que don Manuel Cortés lo solicitara, ni registrado su huella digital.

Agrega que un tiempo después, ante una consulta hecha por el actor a un funcionario del Banco respecto de la incorporación de estos dos teléfonos, se le indicó que los números ya no constaban en el archivo del Banco, eliminación que se dio sin que su representado haya hecho gestión alguna para que se llevara a cabo. En otras palabras, estos números de teléfono de respaldo, tal como fueron incorporados sin cumplir con ningún protocolo de seguridad, también fueron eliminados sin ningún tipo de respaldo o gestión por parte del titular de la cuenta corriente.

Asegura que la incorporación de estos números telefónicos resulta de vital importancia toda vez que, para realizar transferencias electrónicas de dinero, se requiere cumplir con dos requisitos: primero, contar con la combinación de números que arroja el *digipass*; y segundo, con la clave dinámica que es enviada por el Banco al número telefónico que el cliente tenga registrado.

Indica que, en este caso, aun cuando su representado pudo haber entregado una combinación de números del *digipass*, por no existir razones para dudar de que se encontraba hablando con un ejecutivo del Banco; al cambiarse fraudulentamente los números



telefónicos de registro, el señor Cortés no tuvo posibilidad de rechazar las transferencias que se realizaron desde su cuenta, pues se hicieron informando la clave dinámica respectiva a estos números telefónicos que no eran los que el señor Cortés tenía registrados en el Banco.

Relata que, así, el mismo día 31 de julio de 2017, sin autorización del demandante, se traspasaron desde sus tarjetas de crédito Visa, que administra el Banco, hacia la cuenta corriente, dos avances por un monto total de \$2.797.000, que correspondía al máximo que de cada tarjeta se podía girar. Luego, una vez ingresados los dineros de los avances a la cuenta corriente, se registraron trece egresos a diversos destinos, por un monto de \$8.190.650, transferencias que, nuevamente, no contaban con la autorización del señor Cortés.

Precisa que en la cartola del Banco, estos movimientos quedaron registrados el día 1 de agosto de 2017, presumiblemente porque fueron realizados después de las 14:00 horas del 31 de julio. Así, es probable que dichas transacciones se hayan efectuado después de que su representado desactivó el *digipass*, a las 14.17 horas.

Asevera que este fraude solo se pudo concretar porque se registraron dos números de teléfono en el archivo del Banco correspondiente a los antecedentes personales del señor Cortés, lo cual no fue autorizado por él. Como se dijo, una vez ingresada la clave del *digipass*, la clave dinámica debió ser enviada a uno de esos teléfonos, los que jamás debieron estar en el registro del señor Cortés, puesto que él no realizó gestión alguna para su incorporación.

Afirma que, a pesar de haber tomado todos los resguardos posibles y previsibles, procediendo a desactivar el *digipass* en caso de que existiera alguna mínima sospecha de que la persona que había efectuado el llamado no fuera funcionario del Banco, aun cuando contaba con todos los datos de su representado y los productos que había contratado, el actor fue víctima de un fraude bancario que podría haberse prevenido si el Banco demandado hubiera ejecutado los



protocolos de seguridad a los que está obligado para resguardar los dineros de sus clientes y las operaciones que realizan.

Concluye que, desde el momento en que ocurrieron los hechos, el 31 de julio de 2017, y a pesar de múltiples gestiones durante seis meses, su representado no ha tenido ninguna solución, lo que le ha provocado graves problemas, no solo por haber perdido una importante cantidad de dinero, sino que además le ha generado mucha angustia y estrés, por haber tenido que realizar un sinnúmero de trámites para dar aviso del fraude, intentando hacer entender al Banco y a cada uno de los ejecutivos con los que ha tenido que hablar, que no es posible que se hayan registrado números telefónicos de respaldo sin ningún tipo de gestión por parte de él, y que es necesario que responda por los daños ocasionados.

## **II. ANTECEDENTES DE DERECHO**

A) Vulneraciones a la normativa de protección de los derechos de los consumidores

Se refiere a las definiciones que la Ley N° 19.496, sobre Protección de los Derechos de los Consumidores, entrega sobre los conceptos de “consumidores” y “proveedores”, en su primer artículo; y sostiene que el demandado puede considerarse un proveedor, al prestar servicios financieros cobrando una tarifa por ello, mientras que su representado, como cliente del Banco, utiliza estos servicios como destinatario final, pagando el precio que el demandado establece.

Afirma que, en este contexto, el demandado ha vulnerado lo dispuesto por el artículo 3, letra d), de la misma ley, que indica: “*Son derechos y deberes básicos del consumidor: d) La seguridad en el consumo de bienes o servicios, la protección de la salud y el medio ambiente y el deber de evitar los riesgos que puedan afectarles*”.

Explica que el Banco vulneró el derecho a la seguridad en el consumo de bienes y servicios que asiste a su representado, como consumidor de servicios financieros: el señor Cortés tenía el derecho de hacer uso de su cuenta corriente confiando en que el Banco estaba adoptando los protocolos necesarios que permitirían identificar de



manera oportuna y adecuada los intentos de estafa, como la que fue víctima el actor, sin que nada de eso estuviera realmente ocurriendo.

Señala que, por otra parte, de acuerdo al artículo 12 de la misma ley, el proveedor está obligado a respetar los términos, condiciones y modalidades conforme a los cuales se hubiere ofrecido o convenido con el consumidor la entrega del bien o prestación del servicio; y que, en este sentido, es lógico que dentro de los términos y condiciones del contrato de cuenta corriente esté incluido el deber del Banco de prestar un mínimo de condiciones de seguridad en el cuidado de los dineros que se le confían.

Indica que, por último, el artículo 23 de la ley en comento, establece: *“Comete infracción a las disposiciones de la presente ley el proveedor que, en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o de deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio”*.

Sostiene que en el presente caso, el Banco actuó con negligencia en la seguridad de los servicios que estaba ofreciendo, siendo incapaz de cumplir mínimos protocolos de seguridad para la mantención y resguardo de los datos personales del demandante, así como el registro de números telefónicos de respaldo a los que se envía la clave dinámica, antecedentes fundamentales en los cuales se soportan las transferencias de dinero.

Añade que de conformidad al artículo 50, inciso segundo, de la misma ley, su representado se encuentra habilitado para solicitar la indemnización de perjuicios ante la infracción de las normas referidas; y cita jurisprudencia y doctrina sobre la obligación de los Bancos de tomar medidas tendientes a evitar la materialización de fraudes que afecten a los consumidores.

Concluye sobre este punto que su representado tenía una confianza legítima en que el Banco cumpliría sus obligaciones y resguardaría su dinero y su información personal, así como que



aplicaría los protocolos de seguridad establecidos para el registro de nuevos números telefónicos en sus bases de datos, para efectos del envío de las claves de seguridad a ser utilizadas en las transferencias. Sin embargo, el demandado no cumplió y un tercero, que se hizo pasar por su funcionario, contaba con toda la información del actor y de los productos que tenía contratados y fue capaz de registrar dos números telefónicos de respaldo, a los cuales se envió la clave dinámica que lo habilitó para hacer trece egresos y sacar de la cuenta corriente un total de \$8.190.650.

#### B) Responsabilidad contractual

Señala que el Banco incumplió el contrato de cuenta corriente y tarjeta de crédito que mantenía con su representado, en el que se entienden incorporadas las obligaciones de seguridad que tiene el demandado.

Invoca los artículos 1545, 1546 y 1553 N° 3 del Código Civil, e indica que el contrato de cuenta corriente, por disposición de la Ley N° 19.496, contiene el derecho de su representado para exigir seguridad en los bienes o servicios que consume, lo que importa para el Banco la obligación correlativa de entregar productos seguros que no generen ningún daño o perjuicio para sus clientes, lo que no fue cumplido.

Afirma que las infracciones ya mencionadas en la sección anterior, constituyen incumplimiento a obligaciones de hacer expresamente contempladas en el contrato, lo cual ha generado daños a su representado. Por ello, por la presente acción, se solicita que se declare la responsabilidad contractual en que ha incurrido el demandado y su obligación de indemnizar los perjuicios sufridos por su representado, al concurrir todos los requisitos necesarios, que corresponden a: (i) el incumplimiento de la obligación; (ii) la existencia de perjuicios; (iii) la relación de causalidad entre el incumplimiento y los perjuicios; (iv) la imputabilidad, esto es, la culpa o dolo del deudor; y (v), la mora del deudor.



En cuanto al incumplimiento, reitera que el demandado no adoptó los protocolos de seguridad necesarios para la protección de los datos de sus clientes y para el registro de nuevos números de teléfono, de tal manera de asegurarse que era realmente el titular quien estaba procediendo a dicho nuevo registro, y no un tercero ajeno a las partes.

Respecto de los perjuicios, indica que el daño emergente consiste precisamente en el dinero que fue sustraído de la cuenta de su representado, sin su autorización, el cual asciende a la cantidad de \$8.190.650; y que el daño moral, avaluado en \$7.500.000, se ha generado desde que su representado ha debido someterse a un gran estrés, para tratar de hacer que el Banco demandado responda de su omisión de seguridad, lo que le ha provocado gran angustia, por ver que el tiempo pasa y no puede obtener la restitución de los dineros que perdió.

En cuanto a la causalidad, señala que la causa directa del daño que su representado ha sufrido radica en el incumplimiento del demandado, pues de haber adoptado los protocolos correspondientes, las personas que efectuaron el fraude no habrían tenido acceso a toda la información del señor Cortés, ni de todos sus productos contratados (como la existencia de dos tarjetas de crédito y los montos máximos de avance de cada una), ni habrían podido registrar un nuevo número telefónico y, por lo tanto, no podrían haber tenido acceso a la clave dinámica para realizar las transferencias.

En lo relativo a la culpa, invoca el artículo 1547 del Código Civil y hace presente que es el deudor quien deberá probar la diligencia en el cumplimiento de su obligación, dado que la culpa se presume en los contratos bilaterales, como el de autos.

Y, por último, respecto de la mora, señala que se desprende de la sola lectura de los antecedentes expuestos, ya que el incumplimiento del Banco sigue vigente, a pesar que los hechos ocurrieron hace más de seis meses.





Finaliza solicitando que se tenga por interpuesta demanda de indemnización de perjuicios contra el Banco de Chile, someterla a tramitación y, en definitiva, acogerla en todas sus partes, declarando:

1. Que la demandada vulneró los derechos del consumidor de don Manuel Joaquín Fernando Cortés Fravega.

2. Que la demandada incumplió el contrato de cuenta corriente y de tarjeta de crédito que unía a las partes, ocasionando perjuicios.

3. Que, por lo tanto, se condena a la demandada a indemnizar los perjuicios derivados de su incumplimiento, consistentes en la suma de \$8.190.650, en concepto de daño emergente; más la suma de \$7.500.000, en concepto de daño moral, o en subsidio, condenarla a pagar las sumas que el tribunal estime conforme a derecho de acuerdo al mérito del proceso.

4. Que las cifras anteriores deberán ser pagadas por la demandada más reajustes, según la variación que experimente el índice de Precios al Consumidor entre el día 27 de julio de 2017, fecha en que se causaron los daños, y la fecha del pago efectivo, más los intereses corrientes, según la variación que experimente el señalado índice entre la fecha de notificación de la demanda y hasta la fecha del pago efectivo, o bien con reajustes e intereses desde las fechas posteriores que el tribunal estime conforme a derecho.

5. Que se condena en costas al demandado.

Con fecha 18 de abril de 2018, se notificó la demanda.

Con fecha 7 de mayo de 2018, comparece el abogado don Benjamín Jordán Astaburuaga, quien **contesta la demanda** en representación del Banco de Chile, solicitando su rechazo, con costas.

## **I. ANTECEDENTES DE HECHO**

Hace presente que el propio actor confiesa que entregó su clave intransferible generada por el dispositivo *digipass* a un tercero, que se hizo pasar ante él como ejecutivo del Banco de Chile, cuestión que es imposible, porque jamás un ejecutivo solicitará claves secretas a un cliente, menos la generada por el dispositivo *digipass*, cuestión 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.

Explica que las transacciones impugnadas por el actor fueron ejecutadas desde su sesión privada en la página web del Banco, a la que solo puede ingresarse digitando el número de cédula de identidad y la clave secreta, que es creada por el mismo cliente. Luego, para autorizar las transferencias objetadas, se utilizó la clave generada por la aplicación para teléfonos móviles denominada “MiPass”, que para su instalación requiere tres claves secretas que solo el demandante conoce: (i) la que habitualmente utiliza en internet; (ii) una clave dinámica generada por su dispositivo *digipass* y que es válida solo por unos segundos; y (iii) otra clave dinámica que es enviada a su teléfono celular, que también es válida por un corto periodo de tiempo.

Agrega que, con este sistema de triple clave, el Banco cumple con todas las normativas de seguridad, para cerciorarse de que quien descarga la aplicación es el propio cliente.

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, habiendo presentado su cédula de identidad vigente y autenticado su identidad por medio de la huella digital. Por ello, su parte niega que no se haya ajustado al procedimiento establecido para el cambio de número telefónico.

Sostiene que mediante la aplicación del sistema de triple clave, el Banco cumplió lo pactado con su cliente y, además, proveyó a éste de todos los mecanismos de seguridad que la Superintendencia de Bancos e Instituciones Financieras, en su Circular N° 3444, prevé para la realización de este tipo de transacciones: (i) 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; (ii) contó con metodología que comprende una encriptación sólida; (iii) dispuso a lo menos tres factores de autenticación distintos para cada transacción, debiendo ser a lo



menos uno de ellos de generación o asignación dinámica; y (iv) proveyó de perfiles que permitan identificar, evaluar, monitorear y detectar aquellas operaciones con patrones de fraude.

Explica que esta normativa previene, en síntesis, dos cuestiones completamente diversas: primero, la intervención directa y por parte de terceros de la página web del Banco; y, segundo, la intervención de terceros, ya no de la página web del Banco, sino del computador o pantalla del cliente, bajo la modalidad denominada “phishing” u otra similar, por la cual el delincuente le hace creer al cliente, mediante una página similar a la del Banco o a través de llamados telefónicos, que es éste quien le requiere información, y aquel le da a conocer sus claves y todos los demás antecedentes necesarios para operar en la página oficial, la que efectivamente es utilizada con esa información por los terceros.

Afirma que en el presente caso, los sistemas electrónicos del Banco no fueron intervenidos por terceros, por consiguiente, las transferencias no ocurrieron por debilidad del sistema o por negligencia de su parte; sino que fue el cliente quien proporcionó a terceros los medios dados por el Banco para su autenticación, 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, a pesar de las advertencias expresas del Banco sobre el tema.

Denota que consta de los registros o log que todas las operaciones cuestionadas se hicieron con las claves personales del cliente, por lo cual, conforme a la normativa y contratos aplicables, la comunicación fue “auténtica”: se configuró la firma electrónica del cliente, compuesta por su número de RUT y la clave secreta que solo conoce él mismo, y necesaria para el acceso vía internet a la página del Banco. Así, el actor no puede desconocer tales operaciones, pues se cumplieron los requisitos para que contractualmente puedan atribuírseles.



Indica que los contratos entre el actor y su parte regulan este tema, en el sentido que para el acceso vía internet a la página del Banco se requiere el número de rut del cliente y copulativamente digitar una clave secreta que es de su exclusivo conocimiento. Adicionalmente, para ciertas funcionalidades, entre las que se encuentran las transferencias electrónicas, se solicita una clave dinámica y personal, que es generada por un dispositivo que es de uso exclusivo del cliente.

Añade que las claves son desconocidas para el Banco; al mismo tiempo, son personales del cliente y de su exclusiva responsabilidad, por consiguiente éste se hace responsable de su custodia y del uso que se les dé. La obligación del Banco es tener los sistemas de comunicación que le permitan al cliente, en cualquier momento, ordenar el bloqueo de los sistemas de autoatención.

Manifiesta que, en relación al uso de los sistemas de autoatención, el Banco debe entender que toda transacción electrónica que efectúe alguna persona digitando su número personal, su número de RUT, y además una clave dinámica generada por el digipass o la aplicación “MiPass” (cuya instalación requiere la clave digipass y otra clave adicional que es enviada al teléfono celular), ha sido instruida válida, legítima y auténticamente por el cliente.

Recapitula que, entonces, mediante la sesión electrónica del señor Cortés Fravega, a la que se accedió ingresando sus claves secretas dispuestas al efecto y que constituyen su firma electrónica, se dieron las instrucciones de transferencias, que fueron autorizadas a través del dispositivo o aplicación para teléfono celular denominada “MiPass”, que anteriormente fue instalada en un teléfono celular, autorizando esta descarga con la clave generada por el dispositivo digipass del actor y, adicionalmente, validando su identidad con otra clave secreta que fue enviada al teléfono celular del demandante.

## **II. EXCEPCIONES Y DEFENSAS**

### **1. Incompetencia del tribunal**



Alega la incompetencia del tribunal, basada en que la demanda se funda en el incumplimiento de las normas de la Ley N° 19.496, sobre Protección de los Derechos de los Consumidores.

Indica que, según reconoce el propio demandante, la acción deducida corresponde a la contemplada en el artículo 50 de la mencionada ley; sin embargo, el siguiente artículo de dicha normativa, 50 A, establece que la competencia para conocer de las acciones que emanan de la misma ley, corresponde a los jueces de policía local.

Por lo anterior, concluye que la justicia ordinaria no es competente para conocer la acción deducida en estos autos, la cual corresponde a la competencia de los juzgados de policía local.

## 2. Improcedencia del cúmulo de responsabilidades

Señala que la acción interpuesta se funda primero en la supuesta infracción a las normas de la Ley N° 19.496, para luego basarse en el incumplimiento del contrato celebrado entre las partes.

Hace presente que es un hecho no controvertido en la presente causa, que las partes se encuentran vinculadas en virtud de un contrato de cuenta corriente; y que, los fundamentos de la demanda dicen relación con la ejecución de ese contrato. Por tanto, lo que en definitiva busca el demandante es un análisis de la relación contractual de las partes.

Afirma que, por lo anterior, la demanda debe ser rechazada, toda vez que si bien se basa en un supuesto incumplimiento contractual por parte del Banco, se alega que éste constituye una infracción a las normas de protección a los consumidores, cuestión que resulta inadmisibles desde que nuestra legislación no acepta el denominado “cúmulo u opción de responsabilidades”, es decir, no permite al demandante elegir si acciona en virtud de uno u otro régimen según mejor le parezca.

## 3. No existe obligación contractual incumplida

Refiere que, según el actor, la Ley N° 19.496 le reconoce el derecho para exigir seguridad en los bienes o servicios que consume, de manera que la obligación que el Banco habría incumplido estaría



incorporada al contrato en virtud de lo dispuesto en la normativa de protección a los consumidores.

Sostiene que la obligación que el actor reclama incumplida no existe, pues la única obligación que el contrato de cuenta corriente impone al Banco es aquella establecida en el artículo 1 del DL 707, consistente en cumplir con las órdenes de pago del cuenta correntista, lo cual el Banco ha realizado al materializar las transferencias ordenadas a través del sitio de internet, con la utilización de la firma electrónica del demandante.

4. No existe infracción a la Ley N° 19.496, ni incumplimiento de una obligación contractual

Niega la existencia del fraude telefónico alegado por el actor, porque para ingresar al sistema en internet se utilizaron sus datos personales, además de la clave secreta creada por él y adicionalmente se autorizaron las transferencias con la clave generada por la aplicación “MiPass”; así como que el Banco haya sido negligente en el cuidado de sus datos personales, entregándoselos a un tercero.

Afirma que, incluso si las transferencias se realizaron mediante la comisión de un delito, de todas formas el actor es responsable por ellas, por cuanto, debe entenderse que las operaciones fueron ejecutadas por el propio cuenta correntista, como lo establece tanto el contrato como la Ley de Cuentas Corrientes Bancarias y Cheques.

Indica que la normativa en cuestión, hace responsable al Banco o al titular de la cuenta, del pago de un cheque con firma falsificada dependiendo, según los casos, de si la firma de giro es o no visiblemente disconforme. Así, como se desprende de los artículos 16 y siguientes de la mencionada ley, si la firma es falsificada pero visiblemente conforme con la del titular, el Banco no es responsable del pago del cheque, pese a que de acuerdo a las normas civiles generales no concurre en la especie el consentimiento.

Explica que las razones de lo anterior, son: (i) evitar que los titulares defrauden al Banco, dibujando una firma diversa de la registrada en sus propios cheques, para luego alegar la inexistencia



de su consentimiento; y (ii) permitir la operatoria del sistema bancario sin necesidad de recurrir a una pericia caligráfica cada vez que se paga un cheque, privilegiando así el principio de la apariencia por sobre el de la realidad.

Agrega que lo anterior, encuentra fundamento, a su turno, en que el libro talonario, una vez entregado por el Banco debe ser custodiado por el cuenta correntista, siendo él plenamente responsable si no lo hace y, por ende, si alguien falsifica su firma imitando la que se encuentra registrada ante el librado.

Señala que, de esta forma, se unen la obligación de custodia que recae sobre el cliente y la apariencia, con el único objeto de posibilitar el funcionamiento del sistema, impidiendo que los titulares desconozcan las transacciones ejecutadas por ellos.

Asegura que lo mismo acontece con las transferencias electrónicas, realizadas mediante los canales de auto atención, entre los cuales se encuentra el acceso por internet, cuestión específicamente regulada en el contrato celebrado por el Banco con el demandante. En este sentido, sobre el actor recae la custodia de las claves que constituyen su firma electrónica personal y él es legal y contractualmente responsable de todas aquellas transacciones ejecutadas mediante su uso, “auténticas” para estos efectos.

Denota que no existe ninguna razón lógica ni jurídica para hacer responsable al Banco en el presente caso, si (i) las claves eran de custodia personal del demandante; (ii) no hay constancia previa alguna de su extravío; (iii) fueron efectivamente utilizadas en las transacciones objetadas; y (iv) no hay constancia de errores o defectos en los sistemas de seguridad del Banco.

Añade que, en virtud de lo pactado por las partes, en conformidad a lo dispuesto en el artículo 1545 del Código Civil, el Banco no puede ignorar una instrucción recibida por el sistema de internet y, por su parte, el cliente asume las consecuencias del uso que terceros hagan de sus claves secretas y esta estipulación, insoslayable en el presente caso, es lógica, pues es el cliente el único



quien conoce su clave secreta de acceso, por lo que su custodia es evidentemente de su responsabilidad.

Hace presente que, por lo demás, el Banco cumplió íntegramente con lo ordenado en la Circular N° 3444 de la Superintendencia de Bancos e Instituciones Financieras, en relación con las transferencias electrónicas, mediante la aplicación de los sistemas de autorización ya descritos (doble clave), por lo que no cabe sino concluir que cumplió lo pactado y, además, proveyó al cliente de todos los mecanismos de seguridad que la autoridad y la lógica prevén para la realización de este tipo de transacciones.

Finalmente, en cuanto a la alegación del actor en relación al incumplimiento del protocolo de seguridad para el registro de nuevos números telefónicos, niega su efectividad, pues el teléfono celular al que se le envió una tercera clave dinámica para autorizar la descarga de la aplicación para celulares “MiPass”, fue precisamente el que él mismo registró.

5. Controversia entre la mera declaración del actor y la palabra documentada del Banco

Advierte que la teoría del caso de la parte demandante se funda en la mera palabra del cliente contra la palabra documentada del Banco de Chile, validada la de aquel con una simple denuncia y la del Banco con el certificado de la empresa Symantec, que acredita la inviolabilidad de su sitio web. Es decir, el incumplimiento contractual imputado solo se “comprueba” o “acredita” con la palabra del demandante, quien afirma no haber efectuado las transferencias en cuestión y, por ende, que las redes de comunicación del Banco fueron vulneradas por delincuentes.

6. Inexistencia de los daños demandados

Niega que el actor haya sufrido el daño emergente y moral que reclama, y sobre éste último, indica que el demandante se limita a expresar conceptos generales, sin indicar cómo los confusos hechos mencionados, pudieron haber afectado un derecho de carácter extrapatrimonial que justifique una indemnización.





Agrega que el daño moral debe ser probado por quien lo reclama, toda vez que constituye un presupuesto para el origen de la responsabilidad civil. Así la indemnización del daño moral requiere que el mismo sea cierto, vale decir, que sea real y no hipotético, el que deberá ser demostrado por los medios de prueba legalmente establecidos por nuestro ordenamiento jurídico.

Con fecha 16 de mayo de 2018, el demandante evacúa la **réplica** reiterando los argumentos expuestos en la demanda, y agregando lo siguiente.

En cuanto a los hechos relatados por el demandado en su contestación, aclara que su parte jamás entregó sus datos como cédula de identidad y claves para acceder a la página web del Banco, y que tampoco instaló la aplicación MiPass en su teléfono; y que las personas que realizaron el fraude, debieron descargar y usar la aplicación con la clave del *digipass* que sí fue entregada.

Añade que, como reconoce el demandado, para que la aplicación funcione se necesita la tercera clave enviada al celular, momento en que cobra relevancia la incorporación fraudulenta de dos números en el registro del Banco.

Denota que el demandado también reconoce que el registro de número telefónicos debe hacerse presencialmente, por lo que deberá acreditar el cumplimiento del protocolo.

Indica que no está en discusión la intervención de la página web del Banco, pues el problema no se produjo al momento de realizar las transacciones fraudulentas, sino que a la hora de obtener los datos personales de su parte y, sobre todo, a la hora de registrar un nuevo número telefónico en el que se recibió la clave dinámica que supuestamente autorizó la instalación de la aplicación utilizada.

Sostiene que no se trata de un caso de *phishing*, pues jamás ingresó a ningún vínculo del Banco a través de correos, pantallas u otros dispositivos que estuvieran intervenidos, como intenta hacer ver el demandado.



En cuanto a las excepciones y defensas del demandado, indica sobre la incompetencia alegada que si bien el artículo 50 A de la Ley 19.496 establece que las acciones emanadas de dicha ley son de competencia de los jueces de policía local, el artículo 50 B hace aplicable la Ley 18.287, que establece procedimiento ante los juzgados de policía local, la cual, en su artículo 9, permite que la acción de indemnización de perjuicios sea conocida por los tribunales ordinarios, cuando no es ejercida dentro de un procedimiento infraccional.

Acerca de la improcedencia del cúmulo de responsabilidades, señala que en estos autos no se ha alegado en caso alguno la responsabilidad infraccional del Banco, nunca se ha solicitado la procedencia o aplicación de una multa. Se ha reclamado, claramente, la indemnización de los perjuicios por los incumplimientos en que ha incurrido el demandado, en el marco de la responsabilidad contractual del proveedor.

Añade que, como se hizo presente en la demanda, entre las partes existe un contrato de cuenta corriente, así como contratos de tarjetas de créditos. Dichos contratos, como actos de consumo, entienden incorporadas las normas establecidas por la Ley de Protección a los Derechos de los Consumidores, inclusive aquellas que obligan al proveedor a la seguridad en el consumo de bienes o servicios.

En relación a la alegación del Banco consistente en que no existe la obligación contractual incumplida, reitera que los contratos suscritos entre las partes entienden incorporadas las reglas establecidas en la Ley de Protección de los Derechos de los Consumidores, en particular aquellas relativas al derecho del consumidor de exigir la seguridad en los bienes y servicios que adquiere, por lo que la obligación existe.

Respecto a que no existe infracción a la Ley de Protección de los Derechos de los Consumidores ni a alguna obligación contractual, reitera que su parte jamás entregó su información personal, no dio a



conocer su RUT ni su clave secreta de acceso al Banco a ninguna persona. Tampoco descargó la aplicación MiPass, ni recibió mensaje de texto alguno con la tercera clave dinámica que autorizaría la instalación de dicha aplicación. Por lo tanto, no existió ninguna falencia en la custodia de sus claves.

Hace presente que en autos no se cuestiona la autenticidad de la firma electrónica puesta en las transferencias, sino que se alega una falla de seguridad en una etapa anterior, pues se cuestiona el cumplimiento de los protocolos por parte del Banco para la protección de los datos de sus clientes, y para el registro de nuevos números telefónicos, que fue lo que posibilitó la realización de las transacciones.

En cuanto a lo indicado por el demandado sobre la controversia entre la mera declaración del actor y la palabra documentada del Banco, señala que el demandado traslada la discusión de autos a otros temas, que no son materia del juicio.

Aclara que su parte ni debe acreditar la existencia de un delito, puesto que no se trata de un juicio penal, ni debe acreditar que existió una vulneración del sitio web del Banco. Únicamente, debe acreditar que el Banco incumplió con los protocolos de seguridad que establece para el registro de nuevos números telefónicos y que ello generó los daños que se alegan.

Respecto de la supuesta inexistencia de los daños reclamados, sostiene que el daño emergente ciertamente existe y está constituido por las transferencias que se realizaron desde la cuenta corriente. Asimismo, el daño moral también es efectivo, pues la angustia experimentada al ser víctima de una estafa telefónica y no ser creído ni tomado en cuenta por la institución bancaria, es un sentimiento de pesar real.

Añade que el demandado en ningún momento expresa algún sentimiento de empatía, misericordia ni comprensión con su cliente, como se desprende de la contestación de la demanda. Más aun, se encuentra cobrando el monto utilizado de las tarjetas de crédito,



descontando saldos mínimos desde la cuenta corriente y a través de una empresa de cobranza, quienes llaman de forma reiterada al demandante.

Con fecha 25 de mayo de 2018, el demandado evacúa la **dúplica** reiterando todas las alegaciones, defensas y excepciones que se explicaron y opusieron al contestar la demanda, y además agrega lo siguiente.

Indica que la teoría del caso del demandante se funda en un evidente desconocimiento del sistema de transferencias de fondos electrónicas y del sistema bancario.

En cuanto a la excepción de incompetencia y lo señalado en la réplica, señala que el planteamiento del demandante es erróneo, porque si bien la ley que regula el procedimiento ante los juzgados de policía local contiene la disposición invocada, ella se refiere esencialmente a los accidentes de tránsito y por eso, aunque no se haya ejercido la acción civil dentro del procedimiento infraccional, puede deducirse posteriormente en un juicio ordinario, a través de una demanda por responsabilidad extracontractual, de acuerdo a las normas generales. Pero el caso de autos es muy diverso, pues el demandante pretende que se aplique una ley especial, que tiene sus propias reglas de competencia.

Denota que la Ley 19.496 establece cinco acciones distintas: 1) Una acción para perseguir la responsabilidad infraccional del proveedor; 2) Una acción de nulidad de cláusulas abusivas; 3) Una acción para exigir el cumplimiento de la prestación; 4) Una acción para hacer cesar un acto que afecta los derechos de los consumidores y; 5) Una acción indemnizatoria. Precisamente esta última es la acción que ha ejercido el demandante, porque intenta obtener la indemnización de los supuestos perjuicios que habría sufrido. Luego, el artículo 50 A de la ley, contempla que la competencia para conocer de las acciones que emanan de ella, incluida la ejercida por el demandante, es de los juzgados de policía local.



Señala que, de acuerdo al artículo 50 B de la misma ley, la demanda de indemnización de perjuicios no puede interponerse solamente dentro del procedimiento infraccional, sino que también puede ejercerse en forma independiente, pero siempre ante el tribunal competente, en este caso el de policía local.

En cuanto a lo indicado por el demandante en su réplica, respecto a que no se discute la intervención de la página web del Banco, hace presente que allí el actor deja perfectamente acotada la controversia de autos, dejando en claro que no imputa responsabilidad por el funcionamiento del sistema informático. Los únicos incumplimientos que se alegan son: 1) una supuesta falta de seguridad en el manejo de los datos personales del actor y; 2) no haber seguido los protocolos para el registro de su número telefónico.

Sostiene que su parte no ha incurrido en una negligencia en el manejo de los datos personales del demandante, pues las claves personales se encontraban bajo su custodia; y que el teléfono al cual se envió la tercera clave de seguridad para descargar la aplicación “MiPass” fue debidamente registrado en forma personal por el propio demandante.

Con fecha 13 de junio de 2018, se celebró la audiencia de conciliación con la asistencia de la parte demandante, y en rebeldía del demandado, sin producirse acuerdo.

Con fecha 10 de julio de 2018, se recibió la causa a prueba.

Con fecha 2 de julio de 2020, se citó a las partes para oír sentencia.

### **CONSIDERANDO:**

#### **I. EN CUANTO A LAS TACHAS:**

**PRIMERO:** Que en la audiencia de folio 54, el demandado tachó al testigo don Felipe Cuadra Campos, por la causal contemplada en el artículo 358 N° 7 del Código de Procedimiento Civil, en base a la relación de parentesco del testigo con el demandante, que da cuenta de una íntima amistad con la persona que lo presenta, la cual se manifiesta en hechos graves reconocidos por el deponente, quien



señala compartir en ocasiones familiares con el actor por lo menos una vez al mes; y que en su calidad de abogado, lo orientó en el área legal respecto de los hechos sobre los que se presenta a declarar, en forma gratuita, lo que evidencia una amistad íntima, pues lo normal es que un profesional abogado cobre honorarios por sus asesorías.

**SEGUNDO:** Que la parte demandante solicita el rechazo de la tacha, argumentando que el testigo no ha señalado tener una amistad íntima con el demandante, ni se desprende de su declaración la existencia de hechos graves que la configuren.

Agrega que el demandado mezcla diferentes causales de inhabilidad, pues se refiere al parentesco, lo cual se contempla en el artículo 358 N° 1 del Código de Procedimiento Civil, y luego alude a una cierta imparcialidad, lo cual se encuentra en el numeral sexto del mismo artículo.

Por último, indica que el testigo ha sido claro en declarar que ve al actor solo ocasionalmente en la casa de su padre debido a que éste, por su profesión de médico, lo atiende; y que una orientación legal gratuita no implica necesariamente la existencia de una íntima amistad, pues no es cierto que los abogados cobren siempre por una conversación informal.

**TERCERO:** Que la causal de inhabilidad consagrada en el artículo 358 N° 7 del Código de Procedimiento Civil comprende a los testigos que tengan íntima amistad con la persona que los presenta, de manera que, de acuerdo a la norma legal, para que se configure no basta con una mera amistad, sino que con una amistad “íntima”, la que debe manifestarse, además, por “hechos graves”.

Así las cosas, el concepto de amistad íntima que se exige para legitimar la tacha, es más amplio que el de simple amistad, debiendo justificarse por hechos externos de gravedad. Y, de lo expresado por el testigo no surgen estos elementos para configurar la tacha, pues si bien señala que se visitan una vez al mes aproximadamente, luego precisa que los encuentros se dan debido a que coinciden en la casa de un tercero, relatando que el actor visita a su padre por temas



médicos, pero en ningún momento señala, ni tampoco se le pregunta, si se visitan mutuamente en sus propios hogares o si mantienen algún tipo de comunicación fuera de esos encuentros casuales, cuestiones que sí serían indicios de una relación de amistad estrecha; sin embargo, de lo relatado por el testigo se advierte simplemente una conexión de parentesco lejana.

Luego, en cuanto a que la orientación legal gratuita evidenciaría una amistad íntima, ello tampoco puede considerarse como un hecho grave que permita configurar la tacha. De lo dicho anteriormente, la relación del testigo con el actor se muestra como una de dos parientes que coinciden en la casa de un familiar en algunas ocasiones, por lo cual, podría generarse una conversación en relación al problema legal del demandante, dentro de un contexto familiar e informal, lo cual no conlleva necesariamente una amistad íntima.

De esta manera, de lo declarado por el testigo no se advierte la existencia de hechos graves que permitan configurar la causal de inhabilidad, en la forma requerida por la norma invocada, por lo cual será rechazada.

**CUARTO:** Que en la audiencia de folio 75, el demandado tachó al testigo don Fernando Galaz Sbarbaro, en base a la causal establecida en el artículo 358 N° 6 del Código de Procedimiento Civil, la que fundamenta en que el testigo ha declarado que fue consultado en su calidad de abogado por el demandante, manifestándole su apoyo, lo que implica falta de imparcialidad.

**QUINTO:** Que el actor solicita el rechazo de la tacha, señalando que para su procedencia requiere la existencia de un interés pecuniario, que el testigo no tiene.

**SEXTO:** Que para configurar la causal del numeral 6, es necesario que el interés que posea el testigo sea de un carácter pecuniario o económico en el resultado del juicio, situación que atendido lo depuesto por él mismo, no se contempla, considerando que además ni siquiera fue consultado por la existencia de un interés



de ese tipo, lo que tampoco se advierte de las preguntas realizadas, motivo por el cual la tachá será rechazada.

**SÉPTIMO:** Que en la audiencia de folio 82, el demandado tachó al testigo don Mariano Campos Ramírez, por la causal del artículo 358 N° 7 del Código de Procedimiento Civil, en base a que tendría una amistad íntima con el demandante, pues como ha señalado en su declaración, fueron compañeros de colegio, se conocen desde hace más de 40 años, incluso fueron socios de negocios y se ven a lo menos dos veces al mes en el estadio, todo lo cual constituyen hechos graves que configuran el vínculo de amistad.

**OCTAVO:** Que el demandante solicita el rechazo de la tachá, desde que el conocerse por más de 40 años no implica una amistad íntima; que el testigo indicó haber trabajado con el actor en una sociedad, no que fueran socios, como señala el demandado; y que tampoco es un hecho grave que demuestre amistad el verse dos veces al mes en el estadio, pues ello sucede debido a que el testigo es Presidente del Club Deportivo Universidad de Concepción, por lo cual debe acudir al estadio.

**NOVENO:** Que, para proceder a la inhabilidad del testigo, se requiere la existencia de una amistad íntima con la persona que lo presenta, manifestada por hechos graves, no bastando una simple amistad como vínculo.

Al respecto, el mero hecho de que dos personas se conozcan por un largo periodo de tiempo, no puede constituir un hecho grave que permita configurar la íntima amistad, debiendo acompañarse por otros antecedentes que den cuenta de la relación y sus características, lo cual no se evidencia de lo declarado por el testigo.

Así, el deponente indica haber trabajado con el demandante en una sociedad inmobiliaria, lo que implica solo un vínculo profesional, pero nada aporta sobre la existencia de una amistad íntima; y además, que se ven dos veces al mes en el estadio, pero aclara que es Presidente de un club deportivo, por lo cual dichos encuentros bien





pueden responder al compartir un pasatiempo, más que a una amistad.

En este sentido, las preguntas de tacha debieron apuntar a encontrar hechos graves que manifiesten amistad íntima, como por ejemplo, si el testigo y el demandante se reúnen fuera del estadio, si se visitan en sus domicilios, o comparten socialmente en forma habitual, en un ámbito distinto a la afición deportiva en que coinciden, cuestiones sobre las cuales el demandado no indagó.

Por lo anterior, al no evidenciarse hechos graves que manifiesten una amistad íntima, la tacha será rechazada.

## **II. EN CUANTO AL FONDO:**

**DÉCIMO:** Que don Manuel Joaquín Fernando Cortés Fravega deduce demanda de indemnización de perjuicios por incumplimiento de contrato en contra de Banco de Chile, ya individualizados, en atención a los antecedentes de hecho y fundamentos de derecho señalados en lo expositivo de la presente sentencia.

**UNDÉCIMO:** Que el demandado contestó la demanda solicitando su rechazo, en los términos señalados también en lo expositivo de la presente sentencia.

**DUODÉCIMO:** Que se recibió la causa a prueba, fijándose como hechos sustanciales, pertinentes y controvertidos, sobre los que debía recaer, los siguientes:

1. Procedimiento y plataforma utilizada para efectuar las transferencias de dinero desde la cuenta corriente del actor. Época, cuentas involucradas y montos de los traspasos.

2. Efectividad que el actor proporcionó a un tercero sus claves personales, secretas y necesarias para realizar las transferencias bancarias. Razones que motivaron su actuar.

3. Efectividad de haber sido el actor víctima de un fraude bancario.

4. Existencia de Protocolo de Seguridad del Banco demandado para el registro de números telefónicos de sus clientes. En su caso, si dicho Protocolo de Seguridad se cumplió en este caso.



5. Efectividad de que fueron incorporados dos números telefónicos en el Banco demandado como pertenecientes al actor. Época y procedimiento por el que se realizó dicha incorporación.

6. En su caso, si la clave dinámica fue enviada al teléfono celular que el actor registró personalmente en el Banco.

7. Obligaciones supuestamente incumplidas por el Banco demandado con ocasión de las transferencias bancarias.

8. Efectividad de haberse generado perjuicios a la persona del actor. Naturaleza y monto de los perjuicios reclamados.

9. En la afirmativa del punto anterior, relación de causalidad entre los perjuicios sufridos por el actor y el actuar del banco demandado.

**DÉCIMO TERCERO:** Que la parte demandante, a fin de acreditar los fundamentos de su libelo, acompañó la siguiente prueba documental en el folio 56:

1. Dos correos electrónicos enviados por Banco de Chile (casilla serviciotransferencias@bancochile.cl), el día 31 de julio de 2017 a las 14:56 horas, a don Manuel Cortés (casilla joaquin cortés45@gmail.com), con el asunto “Avance tarjeta de crédito”.

2. Estado de cuenta corriente de don Manuel Cortés Fravega, emitido por Banco Edwards Citi del Banco de Chile, para el periodo desde el 30 de junio de 2017 al 29 de marzo de 2018.

3. Dos cupones de pago emitidos por Banco Edwards del Banco de Chile, a nombre de don Manuel Cortés Fravega, de fecha 20 de julio de 2018.

4. Estado de cuenta de tarjeta de crédito Visa (terminada en 3725) emitido por Banco de Chile, a nombre de don Manuel Cortés, de fecha 17 de agosto de 2017.

5. Estado de cuenta de tarjeta de crédito Visa (terminada en 7204) emitido por Banco Edwards Citi del Banco de Chile, a nombre de don Manuel Cortés, de fecha 3 de agosto de 2017.



6. Correos intercambiados entre don Joaquín Cortés (casilla jcortes74@hotmail.com) y don Fernando Fuentealba, ejecutivo de Banco de Chile (casilla fjfuatealbac@bancochile.cl), el día 28 de septiembre de 2018, bajo el asunto “Consulta actualización de datos”.

7. Solicitud de actualización de clave de seguridad de fecha 11 de diciembre de 2017, realizada por una persona de nombre Jorge, primer apellido ilegible, al Banco de Chile.

8. Captura de pantalla de sistema Siebel Financial Services, respecto de los datos de don Manuel Cortés Fravega.

9. Captura de pantalla sobre dispositivos a nombre de cliente Manuel Cortés Fravega, en que aparece que no posee digipass activo, y como fecha de eliminación el 31 de julio de 2017 a las 14:17 horas.

10. Boletín comercial emitido por la Cámara de Comercio de Santiago, respecto de don Manuel Cortés Fravega, de fecha 1 de junio de 2018.

11. Demanda ejecutiva presentada por Banco de Chile en contra de don Manuel Cortés Fravega, y escrito de excepciones opuestas por éste, en causa Rol C-5128-2018 del Primer Juzgado Civil de Concepción.

12. Carpeta investigativa llevada por el Ministerio Público, de la causa RUC 1700710230-5, Fiscalía Local de Concepción.

13. Epicrisis del demandante, hospitalizado con fecha 22 de enero de 2018 (no aparece institución de salud).

14. Certificado emitido por doctor Ervin Schumacher, respecto del demandante, de fecha 17 de enero de 2018.

**DÉCIMO CUARTO:** Que, además, el demandante rindió prueba testimonial consistente en las declaraciones de don Felipe Cuadra Campos, don Fernando Galaz Sbarbaro y don Mariano Campos Ramírez, quienes comparecieron a las audiencias de folios 54, 75 y 82, respectivamente.

**DÉCIMO QUINTO:** Que, de acuerdo a lo solicitado por el demandante en el tercer otrosí de folio 56, el perito ingeniero en



informática don Esteban Gallardo Álvarez emitió su informe en el folio 134.

**DÉCIMO SEXTO:** Que, por su parte, el demandado acompañó la siguiente prueba instrumental en el folio 55:

1. Contrato de cuenta corriente bancaria, celebrado con fecha 10 de mayo de 1995, entre Citibank y don Joaquín Cortés Fravega.

2. Solicitud de actualización de clave de seguridad, realizada por don Manuel Joaquín Cortés Fravega al Banco de Chile, con fecha 11 de julio de 2016.

3. Correos electrónicos intercambiados entre don Camilo Martínez de Mobile Ideas, y doña Bárbara Valenzuela de Banco de Chile, el día 4 de mayo de 2018.

4. Mensaje enviado al número 56981363456, el día 31 de julio de 2017.

5. Documento titulado “Nuevo flujo de biometría para mesón”, elaborado por Banco de Chile.

6. Certificado notarial de fecha 5 de marzo de 2018, emitido por el Notario Público Suplente de Santiago don Jorge Lobos Díaz.

7. Certificado emitido por Neosecure, de fecha 20 de abril de 2018.

8. Impresión de página web de resultados de búsqueda en Google, sobre el número 81363156.

9. Certificado de inscripción y anotaciones vigentes emitido por el Registro Civil, respecto del automóvil placa patente ZJ.5702-8.

10. Certificado de nacimiento de doña María Florencia Cortés Campos, emitido por el Registro Civil.

Que, además, por solicitarlo el demandado en el segundo otrosí de la presentación de folio 55, se recibieron los siguientes oficios:

1. Desde Servicios Interactivos Móviles Limitada, indicando que el día 31 de julio de 2017, por encargo de Banco de Chile, se envió al teléfono móvil +56981363156 el mensaje “Banco de Chile. Ingrese código de registro 414992 en Banca Movil”, agregado en el folio 86.



2. Desde Telefónica Móviles Chile S.A., informando que el servicio telefónico +569 81363156 no corresponde a la empresa, agregado en el folio 88.

**DÉCIMO SÉPTIMO:** Que asimismo la parte demandada citó a absolver posiciones al actor don Manuel Cortés Fravega, diligencia que se llevó a efecto el día 1° de julio de 2019, según consta en cuaderno de medida precautoria.

**DÉCIMO OCTAVO:** Que, de conformidad a lo reconocido por las partes durante la etapa de discusión, y encontrándose además corroborado en documentos acompañados al juicio y que no fueron objetados, son hechos indubitados de la causa:

1. Que entre las partes se celebró un contrato de cuenta corriente bancaria con fecha 10 de mayo de 1995 (contrato del folio 55).

2. Que los productos que el demandante mantenía contratados con el Banco de Chile, al menos durante julio de 2017, consistían en la mencionada cuenta corriente, además de dos tarjetas de crédito.

3. Que el día 31 de julio de 2017, se verificaron dos avances de dinero desde las tarjetas de crédito, abonándose a la cuenta corriente la suma de \$1.770.000, desde la tarjeta Visa terminada en 7204; más \$1.027.000, desde la tarjeta Visa terminada en 3725 (cartola de cuenta corriente y estado de cuenta de tarjetas agregadas en el folio 56).

4. Que, más tarde ese mismo día, y además al día siguiente, se efectuaron trece cargos en la cuenta corriente del demandante, por la suma total de \$8.190.650; dinero que salió de la cuenta por distintos métodos, como transferencias a terceros, recargas de celular, pagos por Servipag y sistema Redgiro.

**DÉCIMO NOVENO:** Que, para entrar en el fondo, es necesario resolver antes sobre las dos primeras defensas opuestas por el demandado consistentes en la incompetencia del tribunal y la



improcedencia del cúmulo de responsabilidades, atendido que ambas apuntan a que el demandante habría deducido una acción especial contemplada en la Ley N° 19.496, sobre protección de los derechos de los consumidores.

De esta manera, resulta imprescindible primero delimitar cuál es la acción interpuesta, para luego analizar –en base a la prueba rendida– si se verifican los requisitos que permitan acoger la demanda.

**VIGÉSIMO:** Que en cuanto a la excepción de incompetencia, el demandado la sustenta en que la acción incoada es de aquellas reconocidas por el artículo 50 de la Ley 19.946, por lo cual su conocimiento corresponde a los juzgados de policía local, de conformidad al artículo 50 A de la misma ley.

Respecto de la improcedencia del cúmulo de responsabilidades, el demandado indica que el actor primero alega una especie de responsabilidad infraccional por vulneración de la Ley 19.946, para luego fundamentar la acción en el incumplimiento del contrato de cuenta corriente, lo cual resulta inadmisibile, al mezclarse dos estatutos de responsabilidad diferentes.

**VIGÉSIMO PRIMERO:** Que de la lectura de la demanda, se advierte que efectivamente el demandante incluye como fundamento la vulneración del deber de seguridad en el consumo que pesaría sobre el Banco, como proveedor de servicios financieros, contemplado en la Ley 19.946.

Sin embargo, también el actor explica que esta obligación de seguridad se entiende incorporada en el contrato de cuenta corriente, y al efecto invoca el artículo 1546 del Código Civil, el cual precisamente contempla que los contratos “*obligan no sólo a lo que en ellos se expresa, sino a todas las cosas que emanan precisamente de la naturaleza de la obligación, o que por la ley o la costumbre pertenecen a ella*”.

A su vez, y como señala el actor en la réplica, en estos autos no se ha solicitado la aplicación de una multa, es decir, no se ha



perseguido la responsabilidad infraccional del demandado, sino que su objeto es obtener la indemnización de los perjuicios producidos por el incumplimiento del contrato de cuenta corriente, al que deben entenderse incorporadas las normas sobre protección de los consumidores.

De esta manera, es posible concluir que la normativa especial aparece citada para dar una mayor fundamentación jurídica a la pretensión ventilada, pero que se trata en definitiva, de una acción de indemnización por incumplimiento contractual, razón por la que este tribunal resulta competente para su conocimiento y resolución, descartándose además el cúmulo de responsabilidades, debiendo desestimarse las dos primeras defensas del Banco de Chile.

**VIGÉSIMO SEGUNDO:** Que, precisado lo anterior, toca decir que los elementos que deben concurrir para acoger una acción de indemnización de perjuicios por responsabilidad contractual, consisten en: (i) que las partes hayan celebrado un contrato que las vincule recíprocamente; (ii) que exista un incumplimiento negligente de dicho contrato por el demandado; (iii) que se hayan ocasionado perjuicios al demandante; (iv) que estos sean una consecuencia directa y necesaria del incumplimiento del contrato; y (v) que el demandado esté constituido en mora si la obligación es positiva.

**VIGÉSIMO TERCERO:** Que, en cuanto al primer requisito, de acuerdo a lo señalado en el considerando décimo octavo, se encuentra reconocido por las partes la existencia de un contrato de cuenta corriente.

Al respecto, fue acompañada una copia del contrato en el folio 55, en el cual, si bien aparece individualizado el Banco como “Citibank”, no cabe duda que se trata del demandado Banco de Chile, pues es la misma parte quien aporta el documento, y nada alega sobre la diferencia en la razón social. Por lo demás, el resto de la documental, agregada tanto por el demandado como por el demandante, da cuenta de las distintas denominaciones del



demandado. Así, aparece como Citibank en el contrato, o como Banco Edwards Citi en la cartola de cuenta corriente del folio 56.

De esta manera, deberá entenderse que tanto las denominaciones Citibank, como Banco Edwards, que aparecen en los diferentes documentos aportados al proceso, corresponden en definitiva al demandado Banco de Chile.

**VIGÉSIMO CUARTO:** Que, el mencionado contrato aparece celebrado el día 10 de mayo de 1995, y contempla la provisión de la cuenta corriente, además de regular el uso de servicios automatizados (cajero automático y sistema telefónico), mediante un contrato anexo denominado “Contrato de prestación y utilización de servicios bancarios automatizados de consulta y transacción”.

Luego, en cuanto a las tarjetas de crédito, si bien no se encuentra en autos el contrato respectivo, no hay controversia al respecto, en el sentido que el demandante mantenía además de la cuenta corriente, las dos tarjetas Visa, y que estas eran gestionadas por el Banco de Chile, conjuntamente con la cuenta. Así también se observa de la cartola del folio 56, en que aparecen los avances de dinero desde las tarjetas, depositados directamente en la cuenta corriente.

Así las cosas, es posible advertir que la relación contractual comenzada en el año 1995, fue cambiando en el tiempo, agregándose nuevos productos, como las tarjetas de crédito, así como el servicio automatizado a través de internet. Sobre lo último, deberá tenerse en cuenta que el contrato regulaba el uso del sistema telefónico para operar a distancia, sin embargo, considerándose la época de suscripción, puede concluirse que con el paso del tiempo, el Banco habilitó las plataformas de atención a través de internet, extendiéndose así el contrato también a dicho servicio, cuestión que resulta relevante para lo que se analizará en los considerandos cuadragésimo cuarto y cuadragésimo quinto.

**VIGÉSIMO QUINTO:** Que, encontrándose acreditada la existencia de la relación contractual, toca referirse al segundo





elemento de la responsabilidad, esto es, que exista un incumplimiento negligente por el demandado.

Al respecto, la obligación que el actor reclama incumplida por parte del demandado, consiste en el deber de seguridad que pesaría sobre el Banco en la prestación de sus servicios. Así, se indica en la página sexta del libelo, que *“el sr. Cortés tenía el derecho de hacer uso de su cuenta corriente confiando en que el Banco estaba adoptando los protocolos necesarios que permitirían identificar de manera oportuna y adecuada los intentos de estafa...”*; y que *“el Banco demandado actuó con negligencia en la seguridad de los servicios que estaba ofreciendo, siendo incapaz de cumplir mínimos protocolos de seguridad para la mantención y resguardo de los datos personales del demandante, así como el registro de números telefónicos de respaldo a los que se envía la clave dinámica”*.

**VIGÉSIMO SEXTO:** Que este incumplimiento habría permitido la materialización de un fraude bancario, por el cual terceros retiraron de la cuenta corriente del actor, sin su autorización, la suma de \$8.190.650, generándose un daño en su patrimonio.

Por lo anterior, previo a determinar si el Banco incumplió el contrato de cuenta corriente, es necesario verificar la existencia de las transacciones objetadas, y si estas fueron realizadas por terceros; es decir, que el demandante efectivamente fue víctima de un fraude.

**VIGÉSIMO SÉPTIMO:** Que, como se dijo en el considerando décimo octavo, el día 31 de julio de 2017, se verificaron dos depósitos en la cuenta corriente del demandante, originados por avances de dinero desde sus tarjetas de crédito; y posteriormente, se realizaron trece egresos a distintos destinos.

Sobre esta situación, el demandante relata que el 31 de julio de 2017, a las 13:42 horas, recibió un llamado de una persona que se presentó como ejecutivo del Banco de Chile, lo cual creyó debido a la información que éste manejaba; que fue convencido por el supuesto ejecutivo para entregarle el número que aparecía en su dispositivo *digipass*; y que, una vez terminada la llamada telefónica, le pareció



extraño el procedimiento, por lo cual, acudió a una sucursal del Banco y desactivó el *digipass*, a las 14:17 horas.

Luego, alega que las transacciones constituyen un fraude, pues fueron realizadas sin su consentimiento, por terceros que poseían sus datos personales.

**VIGÉSIMO OCTAVO:** Que el informe del perito ingeniero en informática, agregado en el folio 134, detalla cuáles fueron las operaciones que se verificaron en la cuenta del demandante, relativas a este juicio. Así, elabora una tabla de las transacciones a partir de los registros (log) del Banco a los que tuvo acceso, como se observa en la página 12 del informe, en la cual, si bien aparece como fecha el 31 de julio de 2019, deberá entenderse que se trata de un error de copia, pues son los movimientos registrados el 31 de julio de 2017, como puede verificarse en la copia del log proporcionada por el demandado, anexada en la página 43 del mismo informe.

Con esta información, y teniendo en cuenta también los documentos aportados por el actor en el folio 56, especialmente los correos recibidos desde el Banco con la notificación de los avances de dinero desde las tarjetas, y el estado de cuenta corriente, puede tenerse por acreditado que las operaciones objetadas por el demandante, por haber sido realizadas sin su consentimiento, fueron las siguientes:

Nº	Fecha	Hora	Detalle	Monto (\$)
Abonos				
1	31/7/2017	13:55	Avance tarjeta (Visa terminada en 3725)	1.027.000
2	31/7/2017	13:56	Avance tarjeta (Visa terminada en 7204)	1.770.000
Cargos				
1	31/7/2017	14:01	Transferencia a Bairon Arias	1.700.000
2	31/7/2017	14:03	Transferencia a Carla Urzúa	1.700.000
3	31/7/2017	14:05	Transferencia a Pedro Pino	1.600.000
4	31/7/2017	14:06	Redgiro	200.000
5	31/7/2017	14:16	Pago por Servipag	2.244.344
6	31/7/2017	14:21	Pago por Servipag	440.306
7	31/7/2017	14:28		2.000



8	31/7/2017	14:31	Recarga celular	2.000
9	31/7/2017	14:33	Recarga celular	2.000
10	31/7/2017	18:21	Recarga celular	15.000
11	31/7/2017	18:22	Recarga celular	5.000
12	31/7/2017	19:39	Pago por Servipag	80.000
13	1/8/2017	9:21	Redgiro	200.000
Total cargos				8.190.650

**VIGÉSIMO NOVENO:** Que, entre los antecedentes aportados por el demandante, también se encuentra una captura de pantalla de lo que parece ser el sistema informático del Banco, en que se evidencia el bloqueo del dispositivo *digipass*, el cual, según explica el demandado en su contestación, se utiliza para la generación de una clave dinámica que permite autorizar transacciones.

Este documento da cuenta que la eliminación del *digipass* se verificó el 31 de julio de 2017, a las 14:17 horas, cuestión que no es controvertida por el demandado. De hecho, el Banco considera dicho momento como el aviso dado por el cliente en relación a las operaciones cuestionadas que se realizaron en su cuenta, según se advierte de la información proporcionada por el demandado al Ministerio Público, como se lee en las páginas 22 y 23 de la carpeta investigativa acompañada en el folio 56.

Allí, se lee que el actor objetó los trece cargos en su cuenta, y que el Banco, luego de analizar el caso, concluyó que siete de ellos por un total de \$306.000 fueron realizados después de la comunicación del cliente, por lo que dicha suma había sido abonada a la cuenta corriente. Así, en el detalle de las transacciones que se consideraron válidas, incluye seis cargos efectuados antes de las 14:17 horas del día 31 de julio de 2017.

De esta manera, el Banco reconoce que el demandante avisó sobre el posible fraude a las 14:17 horas, y que por ello solo haría devolución de los cargos verificados después de esa hora.

**TRIGÉSIMO:** Que, también resulta relevante determinar la forma en cómo las transacciones fueron realizadas, para lo cual se pasará a revisar la versión del Banco.



Al respecto, el demandado explica que las operaciones se hicieron vía internet, utilizándose la sesión web privada del actor, a la cual solo puede accederse ingresando el número de cédula de identidad y la clave secreta creada por el mismo cliente; y que las transacciones fueron luego autorizadas con la clave dinámica generada por la aplicación para teléfonos móviles denominada “MiPass”.

Luego, sobre la utilización de esta aplicación para autorizar las transferencias de dinero, el demandante, en su réplica, indica que jamás la ha instalado en su teléfono móvil.

**TRIGÉSIMO PRIMERO:** Que, sobre este punto es necesario tener en cuenta dos antecedentes. Primero, que –como se explicó en el considerando vigésimo noveno– luego del bloqueo del *digipass* a las 14:17 horas del día de los hechos, solicitado por el demandante en la sucursal bancaria, se siguieron realizando cargos en la cuenta corriente, lo que denota que las transacciones no estaban siendo autorizadas con el dispositivo ya inutilizado, es decir, que debía estarse usando otro método; y segundo, que el perito en su informe, de la revisión del teléfono del demandante, concluye que no encontró evidencias de haberse instalado la aplicación del Banco en el aparato (página 29).

De lo anterior, es posible tener como efectivo lo expuesto por el Banco en su contestación, en el sentido que las operaciones se realizaron desde la sesión web del demandante y se autorizaron con la aplicación MiPass; y al mismo tiempo, permite concluir –junto con lo que se explicará a continuación– que efectivamente las transacciones no fueron realizadas por el actor.

**TRIGÉSIMO SEGUNDO:** Que la investigación del Ministerio Público, según puede observarse de la mencionada carpeta, comenzó por denuncia que realizó don Manuel Cortés Fravega el 31 de julio de 2017, por el delito de estafa, basada en los mismos hechos ventilados en el presente juicio.



Dentro de los antecedentes recopilados por la Policía de Investigaciones, se encuentran las declaraciones de dos imputados por el delito denunciado, y que resultan esclarecedoras sobre los hechos analizados.

**TRIGÉSIMO TERCERO:** Que, una de las transferencias objetadas por el demandante, se realizó a doña Carla Urzúa Molina, quien prestó declaración ante la Policía de Investigaciones como imputada, según consta en la carpeta investigativa (página 17).

En dicha oportunidad, indicó no conocer al afectado por el delito, y explicó sobre el depósito en su cuenta del Banco Estado el 31 de julio de 2017, que mientras caminaba por la calle ese día, se le acercó una persona quien le solicitó prestada su cuenta para recibir un dinero, pues por ser extranjero no tenía él mismo una, a lo que accedió; y que de esta forma, recibió el depósito e inmediatamente giró el dinero, entregándoselo al desconocido.

Por su parte, otro de los imputados que también recibió una de las transferencias objetadas, don Bairon Arias Fuentes, declaró durante la investigación que –al igual que doña Carla Urzúa Molina– no conoce a don Manuel Cortés Fravega, y que ignoraba el depósito de dinero recibido en su cuenta, señalando que dos meses antes había sido víctima de un robo, perdiendo sus pertenencias, entre las cuales estaba su tarjeta de Cuenta Rut, y que desde entonces no había podido acceder a ella.

**TRIGÉSIMO CUARTO:** Que, en definitiva, todos los antecedentes que se han analizado hasta ahora, esto es, que el demandante concurrió al Banco el mismo 31 de julio de 2017, mientras se realizaban las operaciones objetadas, y solicitó el bloqueo del *digipass*; que a pesar de ello, se siguieran efectuando cargos en su cuenta, lo que denota el uso de la aplicación MiPass para autorizarlos, de la que no hay indicios de haber sido instalada por el actor en su celular; que el mismo día, iniciara incluso acciones en sede penal, al realizar la denuncia por el delito de estafa; y que durante la investigación, declararon los imputados señalando no conocer a don



Manuel Cortés y dando cuenta de situaciones irregulares en los depósitos de dinero recibidos en sus cuentas; permiten presumir fundadamente que las transacciones detalladas en el considerando vigésimo octavo, no fueron consentidas por el demandante, sino que se concretaron en el marco de un fraude bancario ejecutado por terceros, quienes utilizaron los datos personales de la víctima para acceder a su sesión privada en la página web del Banco, y desde allí extrajeron dinero de su cuenta corriente.

Así también se apoya esta conclusión, en lo señalado por el perito en su informe, quien habiendo revisado todos los antecedentes del caso, colige que el demandante fue víctima de lo que se conoce como *phishing*, forma de robo de información ampliamente reconocida en la actualidad, utilizada precisamente para conseguir datos personales que permiten a los delincuentes concretar sus estafas.

**TRIGÉSIMO QUINTO:** Que, teniéndose por acreditada la existencia del fraude del cual fue víctima el demandante, corresponde determinar si el Banco incurrió en un incumplimiento contractual en su materialización.

Al respecto, en la demanda se denuncia que el demandado infringió un deber de seguridad en la provisión de su servicio, y se precisan dos situaciones que lo evidenciarían. Primero, se culpa al Banco del no resguardo de los datos personales del demandante como cliente; y segundo, se le imputa el haber permitido el registro de dos números telefónicos en su base de datos, como números de contacto del actor, sin que éste lo hubiera solicitado, y sin seguir el protocolo para ello.

**TRIGÉSIMO SEXTO:** Que, por su parte, el demandado se defiende señalando que la obligación imputada como incumplida por el demandante, no existe; afirmando que el contrato de cuenta corriente le impone solo una obligación, consistente en cumplir las órdenes de pago del cuenta correntista.

**TRIGÉSIMO SÉPTIMO:** Que, efectivamente, el Banco como parte en un contrato de cuenta corriente, se encuentra obligado a



cumplir las órdenes de pago de su cliente, según contempla el artículo 1 del D.F.L. N° 707, que contiene la Ley sobre cuentas corrientes bancarias y cheques, sin embargo sus deberes no se limitan solo a ello.

El contrato acompañado por el demandado, en su primera cláusula, indica que se rige por la Ley sobre cuentas corrientes bancarias y cheques, y por las disposiciones legales y de autoridad que se dicten sobre la materia, las que se entienden incorporadas al mismo.

Luego, es necesario tener en cuenta que los Bancos, debido a la naturaleza de sus funciones, se encuentran bajo la supervigilancia de la autoridad administrativa, que en este caso corresponde a la Superintendencia de Bancos e Instituciones Financieras, entidad que se ha encargado de dictar normas para regular las transferencias electrónicas.

**TRIGÉSIMO OCTAVO:** Que el Capítulo 1-7 sobre transferencia electrónica de información y fondos, de la Circular N° 3444 de la Superintendencia de Bancos e Instituciones Financieras, comienza indicando que las normas allí contempladas *“se refieren a la prestación de servicios bancarios y la realización de operaciones interbancarias que se efectúan mediante transmisiones de mensajes o instrucciones a un computador conectado por redes de comunicación propias o de terceros, efectuadas desde otro computador o mediante el uso de otros dispositivos electrónicos (cajeros automáticos, teléfonos, PINPAD, etc.).*

*Dichos servicios comprenden tanto las transferencias electrónicas de fondos como cualquier otra operación que se realice utilizando documentos o mensajes electrónicos, o dispositivos que permiten a los clientes del banco la ejecución automática de operaciones...”.*

**TRIGÉSIMO NOVENO:** Que, el apartado 4.2 del mismo Capítulo 1-7, se refiere a la prevención de fraudes, indicando:



*“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”.*

De esta manera, las normas dictadas por la autoridad, de acuerdo a lo indicado en el contrato y en conformidad con lo dispuesto por el artículo 1546 del Código Civil, resultan pertinentes para la cuestión aquí discutida, desde que se trata precisamente de un caso en que el cliente imputa una falla en la seguridad del servicio de transferencia de fondos.

**CUADRAGÉSIMO:** Que, entonces, no es efectivo lo alegado por el demandado, en el sentido que su única obligación es cumplir las órdenes de pago del cliente, puesto que los Bancos tienen deberes de seguridad en la provisión de servicios que permiten las operaciones electrónicas, como las transferencias de fondos a través de internet, por mandato de la autoridad.

Aquí cabe tener presente que si bien el demandante fundamenta el incumplimiento del deber de seguridad, en base a lo contemplado en la Ley sobre protección de los derechos de los consumidores; lo cierto es que para la cuestión discutida, existe normativa especial que resulta más acorde, por lo que esta sentenciadora, conforme a la máxima *iura novit curia*, recurrirá a ella por sobre lo expuesto en la demanda.





**CUADRAGÉSIMO PRIMERO:** Que, según se indicó en el considerando trigésimo quinto, el demandante expone dos situaciones que evidenciarían el incumplimiento en el deber de seguridad del Banco.

Así, la primera cuestión consistiría en que el demandado no resguardó los datos de su cliente; señalándose que ello habría permitido a los estafadores acceder a su información personal como el número de cédula de identidad, número de la cuenta corriente, números de las tarjetas de crédito, nombre de la ejecutiva de cuenta, e incluso el número de serie del *digipass*.

**CUADRAGÉSIMO SEGUNDO:** Que sobre lo alegado por el demandante, en autos no hay antecedente alguno que permita siquiera presumir una filtración de datos por parte del Banco. En este punto, cabe tener en cuenta que el demandado, en su contestación, se refiere a la seguridad de sus sistemas, afirmando que estos no han sido vulnerados; cuestión a la que se refiere luego el actor en su réplica (página 3), indicando que dicho tema no es de interés, puesto que no se encuentra en discusión la intervención en la página web del Banco.

Así, el propio demandante descarta que los datos pudieran haberse filtrado por alguna falla en los sistemas del Banco, pero en ningún momento explica cómo entonces los estafadores habrían obtenido su información por parte del demandado, limitándose a imputar el incumplimiento simplemente afirmando que el Banco no protegió sus datos.

**CUADRAGÉSIMO TERCERO:** Que, por el contrario, los antecedentes de la causa permiten inclinarse hacia concluir que los datos personales del actor fueron entregados por él mismo, de forma inadvertida; o bien obtenidas por otros medios.

Como es reconocido por el propio demandante, al recibir el llamado telefónico del supuesto ejecutivo bancario, fue convencido para entregar voluntariamente el número que aparecía en su dispositivo *digipass*.



Además, según ha sido explicado por el demandado, para acceder a la sesión privada en internet, el cliente debe introducir su número de cédula de identidad y una clave secreta, creada por él mismo, y desconocida para el Banco.

**CUADRAGÉSIMO CUARTO:** Que, como se ha señalado en el considerando vigésimo cuarto, el contrato que une a las partes fue celebrado en el año 1995, y regulaba los servicios automatizados de cajero automático y sistema telefónico, más no el acceso a operaciones a través de internet, cuestión que resulta natural considerando que en dicha época aún no se había masificado el uso de internet en el país.

Sin embargo, evidentemente, con el paso del tiempo, el Banco habilitó la plataforma en línea. Al respecto, la mencionada Circular N° 3444 de la Superintendencia de Bancos, señala en su Capítulo 1-7, apartado segundo sobre “Requisitos que deben cumplir los sistemas utilizados”, que *“A) Para la prestación de los servicios deberá celebrarse un contrato entre el banco y el cliente, en el cual queden claramente establecidos los derechos y responsabilidades de cada una de las partes que intervienen en las operaciones”*.

Además, en la letra c) de la misma sección, la norma se refiere a los sistemas que deben ser utilizados en las transferencias electrónicas, señalando que debe *“...utilizarse claves y mecanismos de acceso al sistema y al tipo de operación, que permitan asegurar su autenticidad e integridad”*.

**CUADRAGÉSIMO QUINTO:** Que el contrato contempla la utilización de una clave secreta para el uso de los sistemas automatizados de cajero y telefonía, lo cual puede aplicarse por analogía al servicio de internet, considerando que se trata también de un canal de auto atención dispuesto para que el cliente pueda realizar transacciones a distancia sin necesidad de acudir presencialmente al Banco.

Al respecto, el contrato señala que el Banco proporcionará al cliente que lo solicite, una tarjeta con banda magnética, y que éste



debe registrar una clave de cuatro dígitos solo conocida por él, que constituirá la clave o número secreto personal e intransferible; y que dicha clave podría ser utilizada también para acceder al servicio telefónico (cláusula segunda del contrato de prestación de servicios automatizados).

Luego, el mismo contrato, en su cláusula undécima, señala que la clave registrada por el cliente es confidencial, de su pleno, único y exclusivo conocimiento.

**CUADRAGÉSIMO SEXTO:** Que, así las cosas, para acceder al sitio web del Banco que le permite al cliente realizar transacciones electrónicas, tal como explica el demandado y que además es una cuestión conocida por cualquier cuenta correntista que haya utilizado los servicios en línea que ofrezca la institución bancaria, se requiere introducir la cédula de identidad y una clave secreta.

Dicha clave secreta, como indica el contrato, es creada por el mismo cliente y de su exclusivo conocimiento, pues ni siquiera el Banco tiene acceso a ella.

Luego, debe considerarse que de acuerdo a lo explicado por el perito en su informe, el demandante habría sido víctima de una forma de robo de información conocida como *phishing*, cuyo objeto es obtener los datos que permiten el acceso a las sucursales virtuales de los Bancos (página 10 del informe).

Todo lo anterior, esto es, que el demandante reconoce la entrega voluntaria de la clave generada por el *digipass*, que la clave secreta para acceder al sitio web del Banco es de su exclusivo conocimiento, que habría sido víctima de *phishing*, y teniendo en cuenta que la información que los estafadores habrían tenido no es de custodia exclusiva del Banco, pues el actor también la conoce, permiten concluir que es mucho más factible que la filtración de datos haya sido por el propio actor, en forma inadvertida por él, y no por parte del demandado.

**CUADRAGÉSIMO SÉPTIMO:** Que la segunda situación que evidenciaría la falla de seguridad reclamada, consiste en que se



habrían incorporado sin consentimiento del demandante, dos números telefónicos en su perfil registrado en el Banco; y que por ello, se habrían enviado las claves dinámicas para autorizar las transacciones a un teléfono que no corresponde al del actor.

Al respecto, el demandante acompañó en el folio 56, una captura de pantalla del sistema utilizado por el Banco para administrar los datos del cliente, documento que no fue objetado por el demandado. Allí, se observa que se trata del perfil del actor, y aparecen varios teléfonos de contacto.

El primer teléfono celular corresponde al número (9)81363156, y se indica como fecha de actualización el día 2 de julio de 2009. El segundo número, también es un celular, y corresponde al (9)81363199, actualizado el 31 de julio de 2017, a las 13:50 horas. Asimismo, aparecen dos teléfonos fijos, uno de los cuales, el (41)29481900, fue registrado también el 31 de julio de 2017, a las 13:49 horas.

Son precisamente los dos números incluidos el día 31 de julio de 2017, los cuales el actor desconoce como suyos. Así las cosas, si bien el demandante no aclara en su libelo cuál es el teléfono que sí le pertenece, cabe concluir que se trata del primero, lo que además coincide con la información entregada por el Banco.

**CUADRAGÉSIMO OCTAVO:** Que, el demandado indica que el día de los hechos, 31 de julio de 2017, efectivamente se envió una clave a un teléfono móvil, pero aclara que se hizo al número registrado personalmente por el demandante.

Sobre su afirmación, agrega en el folio 55, una solicitud de actualización de clave de seguridad firmada por el demandante, quien no objetó el documento, y que por haberse tenido por acompañado bajo el apercibimiento del artículo 346 N°3 del Código de Procedimiento Civil, se tendrá por reconocido.

Este documento, da cuenta que con fecha 11 de julio de 2016, el actor autorizó al Banco de Chile para que el envío de la clave de seguridad denominada “tercera clave”, se hiciera al número de celular



81363156; constando además que se realizó una validación de su identidad con la revisión de cédula y huella digital.

**CUADRAGÉSIMO NOVENO:** Que, entonces, coincide que el teléfono móvil 81363156 aparecía en la base de datos del Banco, como número de contacto del demandante, desde el 2 de julio de 2009, según se observa del documento acompañado por el actor; y que desde el 11 de julio de 2016, también se autorizara su uso para el envío de la clave de seguridad denominada “tercera clave”, según el documento agregado por el demandado.

En este punto, es necesario revisar lo explicado por el perito en su informe, acerca de los distintos sistemas utilizados por el Banco, en relación al registro del número de teléfono de un cliente.

**QUINCAGÉSIMO:** Que, como se lee en las páginas 15 y 16 del informe pericial, cuando un cliente realiza un requerimiento de actualización del número para envío de clave de seguridad, este se ingresa en el sistema SIEBEL; y luego, la información pasa al área de Banca Telefónica, ingresándose el número en un sistema distinto, denominado Entrust, en el cual queda registrado el celular para envío de tercera clave, y que soporta solo un número a la vez.

Añade el perito que, en definitiva, se trata de dos sistemas: uno para gestionar todos los requerimientos del cliente, que corresponde a SIEBEL; y otro, Entrust, cuya única función es registrar el número para envío de tercera clave.

Esta duplicidad de sistemas, resulta coherente con la prueba rendida por las partes, en el sentido que, el documento acompañado por el demandante (analizado en el considerando cuadragésimo séptimo), corresponde al sistema SIEBEL, como se observa en la pestaña superior izquierda de la interfaz de uso, donde se lee “Produccion – Siebel Financial Services”. Luego, en dicho sistema aparece el número 81363156 como registrado en el año 2009.

A su vez, el documento acompañado por el demandado (analizado en el considerando cuadragésimo octavo), indica que recién en 2016 se autorizó por el actor, el uso de ese mismo número



ya registrado desde 2009 en SIEBEL, para el envío de clave de seguridad.

**QUINCUAGÉSIMO PRIMERO:** Que, de esta manera, puede concluirse que SIEBEL soporta el registro de varios números de contacto del cliente, y se utiliza para gestionar información de distinta índole, como se observa en la captura de pantalla de la página 19 del informe pericial; mientras que Entrust, es un sistema cuya única función es administrar el número al cual se envía la clave de seguridad necesaria para realizar operaciones en línea por el cliente, y que en este fue registrado el celular del demandante (81363156), como se observa de la imagen de la página 20 del informe, donde se incluyó la captura de pantalla de Entrust.

**QUINCUAGÉSIMO SEGUNDO:** Que, esta aclaración sobre los dos sistemas utilizados por el Banco, resulta relevante para comprender la alegación del demandante, la cual carece de esta información.

Como se ha explicado, el actor imputa una falla de seguridad al Banco, consistente en que al permitir la inclusión de dos números de teléfono sin seguir los protocolos, ha posibilitado el fraude, desde que se habría enviado la clave de seguridad para autorizar las transacciones a un celular que no era suyo.

**QUINCUAGÉSIMO TERCERO:** Que, efectivamente, consta de la prueba rendida por el actor, que el mismo día de los hechos, 31 de julio de 2017, se registraron dos números en su perfil, y que ello ocurrió, por lo demás, justo antes que comenzaron las operaciones objetadas, a las 13:49 y 13:50 horas.

Aquí, resulta relevante lo declarado por uno de los imputados en la causa penal, don Marco Guzmán Tapia, quien fue identificado por la policía gracias a que la compañía Entel (correo de la página 34 de la carpeta investigativa) informó que era el titular del número 81363199, precisamente el teléfono móvil registrado en el Banco el día 31 de julio de 2017, como número de contacto del actor.



Dicha persona declaró ante la Policía de Investigaciones, con fecha 2 de septiembre de 2017 (página 11 de la carpeta), señalando que era usuario del número celular +56981363199, el cual adquirió en el año 2013, y que poseía hasta ese momento; señalando además no conocer a don Manuel Cortés Fravega.

**QUINCUAGÉSIMO CUARTO:** Que, además, cabe tener presente que según el correo electrónico intercambiado con un ejecutivo del Banco el día 28 de septiembre de 2018 (considerando décimo tercero, N° 6), la actualización de teléfono de contacto debe hacerse de manera presencial en el servicio de atención al cliente de alguna sucursal.

Así las cosas, acreditada la inclusión de estos números telefónicos y que ello debía realizarse de manera presencial, el Banco debía probar que siguió el protocolo y que recibió la solicitud de actualización del demandante, cuestión que no hizo.

Por lo anterior, se tendrá por acreditado que se registraron números telefónicos de terceros, como si fueran del demandante, sin previa solicitud o autorización de éste.

**QUINCUAGÉSIMO QUINTO:** Que, ahora bien, corresponde determinar la relevancia sobre los dos sistemas utilizados por el Banco para el manejo de datos de los clientes.

Como se ha explicado, el documento acompañado por el demandante en el cual consta la inclusión de los nuevos números el 31 de julio de 2017, corresponde al sistema SIEBEL. Sin embargo, según aclaró el perito en su informe, el número de contacto para envío de clave de seguridad se registra en Entrust, el cual admite un solo número a la vez, y en el cual aparece el teléfono correcto del demandante, esto es, el celular 81363156, sin constatarse que allí se hubiera introducido el teléfono que correspondía a don Marco Guzmán Tapia, imputado en la causa penal y dueño del celular 81363199, registrado en SIEBEL sin solicitud del actor.

**QUINCUAGÉSIMO SEXTO:** Que, sumado a lo anterior, cabe tener presente lo expuesto en los considerandos trigésimo y trigésimo



primero, acerca de la clave utilizada para autorizar las transacciones objetadas, y lo explicado por el Banco sobre la “tercera clave”.

Como se ha dicho, las operaciones se hicieron a través de internet, desde la sesión del demandante en la página web del Banco, para lo cual es necesario contar con la cédula de identidad y dos claves. Una clave secreta para acceder al sitio, que es creada por el cliente; y una clave dinámica generada por el dispositivo *digipass*, o por la aplicación para teléfonos MiPass, siendo esta última vía la utilizada en las transacciones, desde que el digipass fue bloqueado por el actor el mismo día a las 14:17 horas.

Sobre el sistema de dos claves, esto se encuentra contemplado en la ya mencionada Circular N° 3444, pues en su Capítulo 1-7, apartado 4.1, letra b), señala que los canales electrónicos ofrecidos por los Bancos para realizar transferencias deben “*disponer de a lo menos dos factores de autenticación distintos para cada transacción, debiendo ser uno de ellos de generación o asignación dinámica*”. Así, el Banco cumple con solicitar ambas claves: la clave secreta y la clave dinámica.

Entonces, la denominada “tercera clave” que se envía al teléfono móvil, no sería siempre necesaria para autorizar cada transacción realizada por el cliente.

**QUINCUGÉSIMO SÉPTIMO:** Que el Banco explica que la tercera clave es necesaria para instalar la aplicación MiPass, y que esta fue enviada el 31 de julio de 2017, al celular registrado correctamente por el demandante.

Al respecto, acompaña una serie de correos electrónicos (considerando décimo sexto, N° 3) intercambiados con la empresa Mobile Ideas, encargada de enviar los mensajes de texto de tercera clave a los clientes del Banco, donde se informa que el 31 de julio de 2017 se envió solo un mensaje al número +56981363156, el cual indicaba: “Banco de Chile. Ingrese código de registro 414992 en Banca Movil”.





La misma información fue proporcionada directamente por Mobile Ideas, en el oficio remitido en el folio 86.

**QUINCUAGÉSIMO OCTAVO:** Que, todo lo explicado hasta aquí, lleva a concluir entonces, que las transacciones fueron autorizadas con la clave dinámica generada por MiPass, siendo innecesario el uso de tercera clave, la cual sería utilizada, en todo caso, para instalar dicha aplicación, pero no para cada transacción efectuada.

Luego, el día de los hechos se envió una clave al celular del demandante, registrado por él en el año 2016; mas no hay antecedentes en autos, pues no se rindió prueba al efecto, de si se enviaron claves a alguno de los números registrados sin autorización del actor, lo que resultaba indispensable para verificar su alegación, en el sentido que la inclusión de dichos números permitió el fraude, por haberse enviado claves de seguridad a alguno de ellos.

**QUINCUAGÉSIMO NOVENO:** Que, de esta manera, cabe concluir que efectivamente se agregaron números de teléfono de terceros en el sistema del Banco, como si fueran del demandante, sin su autorización.

Sin embargo, al mismo tiempo, es posible advertir que esta situación no aparece como relevante para la materialización del fraude, primero, porque los números se ingresaron a SIEBEL, y no al sistema Entrust encargado de registrar el teléfono para envío de tercera clave; segundo, porque ese día es cierto que se envió una clave, pero se hizo al celular correcto del actor (81363156); y tercero, porque no hay evidencia en autos que permita a esta sentenciadora saber si se envió alguna clave al celular 81363199, perteneciente a uno de los imputados en la causa penal y registrado en SIEBEL como si fuera del demandante, que hubiera permitido la autorización de alguna transacción.

**SEXAGÉSIMO:** Que, en definitiva, no se evidencia que las dos situaciones descritas por el actor constituyan un incumplimiento en el deber de seguridad del Banco que permitiera las transacciones. Por una parte, no hay evidencia que lleve a concluir que el demandado



filtró los datos personales del demandante. Y por la otra, si bien es efectivo que se incluyeron números telefónicos en el registro del Banco como si fueran del actor, siendo que no lo eran, esta situación no fue relevante para la perpetración del fraude, como alega el demandante.

No obstante, como fue explicado en el considerando vigésimo quinto, el demandante imputa al demandado un incumplimiento contractual, que habría transgredido su *“derecho de hacer uso de su cuenta corriente confiando en que el Banco estaba adoptando los protocolos necesarios que permitirían identificar de manera oportuna y adecuada los intentos de estafa...”*.

Luego, según se dijo en los considerandos trigésimo octavo y trigésimo noveno, los Bancos tienen obligaciones de seguridad cuyo fin es evitar que sus clientes sean víctimas de fraudes en el uso de los servicios de transferencias electrónicas.

Así, el apartado 4.2 del Capítulo 1-7, de la Circular N° 3444 de la Superintendencia de Bancos e Instituciones Financieras, se refiere precisamente a la prevención de fraudes, obligando al Banco a *“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...”*.

**SEXAGÉSIMO PRIMERO:** Que, de acuerdo a lo expuesto en el considerando vigésimo octavo, el día 31 de julio de 2017, se verificaron una serie de movimientos en la cuenta corriente del demandante, que bien pueden calificarse de anormales y sospechosos.

Primero, se realizaron dos abonos desde las tarjetas de crédito, de altas sumas de dinero y con un minuto de diferencia. Así, a las 13:55 horas entraron en la cuenta \$1.027.000; y a las 13:56, \$1.770.000.

Luego, se registraron tres transferencias de fondos de importantes sumas de dinero, entre las 14:01 y las 14:05 horas, las



cuales fueron realizadas a personas recién agregadas en la lista de contactos del demandante.

Sobre este punto, el perito en la página 26 de su informe, indica que entre las 13:58 y las 14:05 horas, se agregaron cuatro nuevos destinatarios de transferencias en la sesión del actor, concretándose transferencias de fondos a tres de ellos: (i) don Bairon Arias fue agregado a las 14:01, efectuándose la transferencia de \$1.700.000; (ii) doña Carla Urzúa fue agregada a las 14:03, realizándose la transferencia de \$1.700.000; y (iii) don Pedro Pino fue agregado a las 14:05, efectuándose la transferencia de \$1.600.000.

**SEXAGÉSIMO SEGUNDO:** Que, durante los minutos posteriores a las transferencias, entre las 14:06 y las 14:33 horas, se ejecutaron seis movimientos más, entre los cuales constan dos pagos por Servipag de \$2.244.344 y \$440.306. Así, se realizaron seis cargos, algunos de altas sumas de dinero, en menos de media hora.

Algunas horas más tarde, entre las 18:21 y las 19:39, se concretaron tres cargos más; y a las 9:21 del día siguiente, 1 de agosto de 2017, otro cargo por \$200.000.

**SEXAGÉSIMO TERCERO:** Que, en este punto, cabe tener en cuenta lo informado por el Banco al Ministerio Público con fecha 20 de septiembre de 2017.

Consta en la página 22 de la carpeta investigativa, que el Banco analizó el caso de don Manuel Cortés, y concluyó que siete de los trece cargos objetados por el actor, habían sido hechos con posterioridad a la comunicación de la situación, por lo que los reintegró en la cuenta, habiéndose abonado la suma de \$306.000.

Luego, en el estado de cuenta acompañado por el actor en el folio 56, aparece efectivamente la devolución de \$306.000, con fecha 13 de septiembre de 2017, bajo el detalle “regularización de cargos”.

Dicha devolución, corresponde a los cargos indicados entre los números 7 y 13 de la tabla de movimientos del considerando vigésimo octavo, registrados entre las 14:28 horas del 31 de julio y las 9:21 horas del 1 de agosto de 2017.



**SEXAGÉSIMO CUARTO:** Que, según se explicó en el considerando vigésimo noveno, el Banco consideró como momento del aviso del bloqueo del *digipass* a las 14:17 horas del 31 de julio de 2017, por lo cual hizo devolución de los cargos realizados con posterioridad a esa hora; manteniendo como válidos, y por ello, no aptos de devolución, los concretados antes de ese momento.

Al respecto, se evidencia el siguiente problema con uno de los cargos considerados por el Banco como válidos, correspondiente al pago por Servipag de \$440.306.

En la información remitida al Ministerio Público, el Banco indica que éste se realizó a las 14:16 horas. Sin embargo, en el informe pericial, aparece el cargo a las 14:21 (página 12), de acuerdo al log o registro que habría entregado el propio demandado.

Así, en la página 43 de informe, el perito anexa una copia del registro de transacciones que el Banco le entregó, en donde aparece la transacción por \$440.306, como realizada a las 14:21:38 horas.

**SEXAGÉSIMO QUINTO:** Que, debido a lo anterior, se ha considerado que el pago por Servipag por la suma de \$440.306, fue hecho a las 14:21, como se ha indicado en la tabla del considerando vigésimo octavo.

Por ello, se dará por acreditado el incumplimiento en el deber de seguridad del Banco en cuanto a este giro, desde que fue realizado y autorizado por el demandado cuando el actor ya había dado aviso de bloqueo del *digipass*.

Lo mismo se aplica, para los otros cargos registrados después de las 14:17 horas, pues si bien el Banco hizo devolución del dinero sustraído desde la cuenta del actor, lo cierto es que existió una falla de seguridad en haber permitido que se siguieran concretando cuando el cliente ya había dado aviso de lo que estaba ocurriendo con su cuenta.

**SEXAGÉSIMO SEXTO:** Que, en cuanto a los cargos efectuados antes del aviso del demandante, como fue explicado en los



considerandos sexagésimo primero y sexagésimo segundo, la forma en que se realizaron fue evidentemente anormal.

A ello, hay que sumar que minutos antes de comenzar la sustracción del dinero, a las 13:49 y 13:50 horas, se registraron nuevos números telefónicos de contacto como si fueran del demandante, lo cual, si bien –como ya ha sido explicado– no permitió directamente las transacciones, desde que no hay constancia que se hubieran utilizado para autorizarlas, constituye también un movimiento que perfectamente pudo haberse calificado de sospechoso, y haber generado automáticamente las alertas para prevenir las operaciones ilícitas.

Es necesario tener en cuenta que en el registro del Banco, al menos en el sistema SIEBEL, el demandante mantenía como número de contacto el mismo desde el año 2009, y de pronto, se registran dos números nuevos sin previa solicitud personal, se realizan dos avances de dinero por sumas millonarias, e inmediatamente comienzan las transferencias de fondos a diferentes destinos, todo ello en cuestión de minutos y por importes significativos. Se advierte, en tal sentido, una insuficiencia en el sistema de detección temprana de fraudes, que es particularmente exigible a una entidad bancaria, por ser blanco habitual de esta especie de ilícitos, y por ser, dada su profesionalidad, recursos y responsabilidad de custodia de los dineros de sus clientes, el contratante llamado a no dejar flancos que propicien el actuar de terceros, tal como ocurrió en la especie.

**SEXAGÉSIMO SÉPTIMO:** Que, así las cosas, la situación descrita debió haber sido identificada, evaluada, monitoreada y detectada en el menor tiempo posible, por el departamento especial de la entidad bancaria, como una operación con patrón de fraude, a fin de abortar rápidamente la actividad, según instruye la Superintendencia de Bancos, lo cual el demandado no hizo, pues incluso permitió que se siguiera sustrayendo dinero de la cuenta después del aviso dado por el actor, cuestión que constituye un incumplimiento contractual.



**SEXAGÉSIMO OCTAVO:** Que, en cuanto al elemento de la culpa en el incumplimiento contractual, ha de señalarse que en esta clase de responsabilidad, ésta se presume, de acuerdo a lo contemplado en el artículo 1547 del Código Civil.

Así, es la ley la que presume que el incumplimiento se provocó porque no se empleó el grado de cuidado al que estaba obligado el demandado, a quien corresponde probar su diligencia, cuestión que no hizo, pues no aportó antecedentes sobre ello, advirtiéndose además, que sus defensas de fondo apuntaron a desconocer su obligación legal en cuanto a la prevención de fraudes y a trasladar la responsabilidad al demandante, por el uso de las claves utilizadas en las transacciones.

De esta manera, se da por acreditado el incumplimiento contractual y que este, además, fue negligente.

**SEXAGÉSIMO NOVENO:** Que, en relación a los daños, el actor solicita la suma de \$8.190.650 por concepto de daño emergente, consistente en la cantidad que fue sustraída desde su cuenta producto del fraude.

Al respecto, como fue detallado en el considerando vigésimo octavo, los trece cargos realizados en la cuenta del demandante, sumaron en total el monto requerido. Sin embargo, es necesario descontar inmediatamente de lo solicitado, la devolución de \$306.000 que el Banco hizo, según quedó establecido en el considerando sexagésimo tercero, y que corresponde a los siete últimos movimientos registrados entre las 14:28 horas del 31 de julio y las 9:21 horas del 1 de agosto de 2017.

**SEPTUAGÉSIMO:** Que, ahora, es necesario realizar otra distinción en relación a lo establecido en el considerando sexagésimo quinto, esto es, al cargo de \$440.306 concretado a las 14:21 horas del día de los hechos, posterior al aviso y que el Banco no consideró en la devolución realizada en septiembre de 2017.

En cuanto a este cobro, una vez dado el aviso de la situación a las 14:17 horas del 31 de julio de 2017, el Banco debió



necesariamente restringir los movimientos de la cuenta del actor, impidiendo la salida de dinero, lo que no hizo.

En este sentido, el demandante tomó los resguardos adecuados ante el fraude del que estaba siendo víctima, acudiendo a la sucursal bancaria y solicitando el bloqueo del *digipass* a fin de impedir la autorización de las transacciones. Sin embargo, el Banco siguió cumpliendo las órdenes de pago a pesar de encontrarse informado que no era el actor quien las estaba dando.

Por esta conducta, que según ya ha quedado establecido, corresponde a un incumplimiento contractual negligente, el actor vio disminuido su patrimonio en la suma de \$440.306, acreditándose el daño emergente, y debiendo acogerse la demanda en este sentido.

**SEPTUAGÉSIMO PRIMERO:** Que, en cuanto al resto de los cargos, consistentes en los que se realizaron antes de las 14:17 horas del día de los hechos, y que suman \$7.444.344, es necesario decir que también corresponden a daño emergente producto del incumplimiento contractual, pues como se ha explicado, el Banco debió identificar el patrón de fraude en el menor tiempo posible y evitar su materialización. No obstante, resulta preciso además tener en cuenta la conducta del propio demandante.

Según ya ha sido establecido, las transacciones se hicieron desde la sesión privada del demandante, a la cual se accede con una clave secreta creada y conocida solo por él mismo. Luego, cada operación fue autorizada con la clave dinámica generada por la aplicación MiPass.

Sobre esta aplicación, el Banco explica que para su funcionamiento es necesario activarla mediante las claves del cliente, requiriéndose la clave dinámica del *digipass*, además de la tercera clave enviada al teléfono, lo cual coincide con lo explicado por el perito en su informe (página 14), por lo que se estará a ello.

**SEPTUAGÉSIMO SEGUNDO:** Que, entonces, quienes ejecutaron las transacciones debieron instalar la aplicación en un



teléfono celular utilizado por ellos, para lo cual necesitaron acceder a las claves del actor.

En cuanto a la tercera clave enviada al teléfono, no hay antecedentes en autos que permitan establecer cómo pudieron tener conocimiento de ella, pues según ya ha sido explicado, no se rindió prueba acerca del envío de claves a algunos de los teléfonos registrados el mismo 31 de julio de 2017; en cambio, sí consta que ese día se envió una clave al número correcto del demandante. En todo caso, este antecedente resulta imposible de determinar con la prueba aportada.

Sin embargo, cuestión distinta sucede con la clave dinámica generada por el *digipass*. En este sentido, es el propio actor quien reconoce haber informado el número que aparecía en el dispositivo al supuesto ejecutivo bancario.

Así las cosas, con los antecedentes del proceso, es posible establecer que al menos una de las variables necesarias para que terceros instalaran y activaran la aplicación que permitió autorizar las transacciones, la entregó el propio demandante.

**SEPTUAGÉSIMO TERCERO:** Que, debido a lo anterior, la indemnización del daño emergente, al menos en relación a las transacciones generadas antes del aviso dado por el demandante y que suman \$7.444.344, será reducida, de conformidad a lo dispuesto en el artículo 2330 del Código Civil, por considerarse que el actor se expuso imprudentemente al daño.

**SEPTUAGÉSIMO CUARTO:** Que, además, el demandante solicita la indemnización del daño moral por la suma de \$7.500.000, el que fundamenta en el estrés y angustia a que ha sido sometido por intentar que el Banco le restituyera el dinero sustraído desde su cuenta, agregando en la réplica que incluso ha sido objeto de cobranza por los montos utilizados desde las tarjetas de crédito.

Al respecto, consta de la prueba rendida que el demandante inició acciones legales en sede penal por el fraude del que fue víctima, y que en el marco de la investigación, el Banco informó al Ministerio





Público que el actor objetó los trece cargos realizados en su cuenta, y que se dio respuesta a ello en septiembre de 2017, haciendo devolución de siete de ellos, y sin dar solución a los otros seis.

**SEPTUAGÉSIMO QUINTO:** Que, además, la documental acompañada por el demandante da cuenta de la afectación en su situación patrimonial, y que ha sido objeto de cobranza por el Banco de Chile, debido a la deuda proveniente de las tarjetas de crédito.

Así, constan los cupones de pago emitidos en julio de 2018, que señalan como operación “crédito tarjetas vencidas consumo”, y que la deuda se encuentra en “cobranza socofin” (considerando décimo tercero, N° 3).

Luego, los mismos montos de los cupones de pago, aparecen como deudas publicadas en el Boletín Comercial por el Banco de Chile, a nombre del demandante (considerando décimo tercero, N° 10).

Asimismo, una de las deudas, la que asciende a \$2.255.399, fue objeto de demanda ejecutiva interpuesta por el Banco de Chile en contra de don Manuel Cortés Fravega, originándose la causa Rol C-5128-2018 del 1° Juzgado Civil de Concepción (considerando décimo tercero, N° 11).

**SEPTUAGÉSIMO SEXTO:** Que, así las cosas, se evidencia que el demandante, al percatarse que podría ser víctima de un fraude, inició una serie de gestiones. Primero, acudió a la sucursal bancaria el mismo día de los hechos, dando aviso de la situación, a pesar de lo cual se siguieron autorizando transacciones por parte del demandado; segundo, el mismo día 31 de julio de 2017, realizó una denuncia ante la Policía de Investigaciones, por el delito de estafa; y tercero, objetó los cargos ante el mismo Banco, quien no entregó una respuesta satisfactoria, negándose a la devolución completa de lo sustraído.

Sumado a lo anterior, el Banco inició gestiones de cobranza, y llegó a interponer una demanda ejecutiva en contra de don Manuel Cortés, debido a las deudas que lo aquejan producto del fraude.



Todo esto, naturalmente conlleva estrés, angustia, molestia y pesar que necesariamente provienen del incumplimiento del demandado en su deber de seguridad en el servicio de transferencias electrónicas y obligación en la prevención de fraudes, por lo que la demanda será acogida en este punto, debiendo estarse a la reducción en el monto de la indemnización de conformidad a lo expuesto en los considerandos septuagésimo segundo y septuagésimo tercero.

**SEPTUAGÉSIMO SÉPTIMO:** Que, entonces, el monto de la indemnización será el que se explicará a continuación.

En relación al daño emergente: (i) deberá descontarse de lo solicitado el monto reintegrado por el Banco en septiembre de 2017, ascendente a \$306.000; (ii) el demandado deberá hacer devolución por completo del cargo de \$440.306 efectuado con posterioridad al aviso dado por el demandante; y (iii) en cuanto a los cargos anteriores al aviso, por haberse expuesto del demandante imprudentemente al daño, el monto de \$7.444.344 será rebajado prudencialmente a la mitad. De esta manera, la indemnización por daño emergente queda en la suma de \$4.162.478.

En cuanto al daño moral, este fue avaluado por el actor en la suma de \$7.500.000, monto que aparece adecuado en atención a la angustia que conlleva la situación descrita, por lo que, encontrándose acreditado y habiéndose acogido la demanda en ese sentido, será también rebajado a la mitad, quedando en \$3.750.000.

**SEPTUAGÉSIMO OCTAVO:** Que en cuanto al elemento de la causalidad, este se encuentra plenamente acreditado, desde que los daños son una consecuencia del incumplimiento del demandado, desde que de haberse identificado y evitado las transferencias como ordena la autoridad, no se habrían generado.

**SEPTUAGÉSIMO NOVENO:** Que, finalmente, entendiéndose que la mora se constituye como el retardo en el cumplimiento de la obligación, imputable al deudor, que persiste después de la interpelación del acreedor, y constando en autos que aquel ha sido reconvenido judicialmente por el acreedor mediante formal demanda,



ha de tenerse por concurrente dicho presupuesto de conformidad a lo dispuesto en el artículo 1551 del Código Civil.

Por estas consideraciones y visto además lo dispuesto por los artículos 1437, 1438, 1545, 1546, 1547, 1551, 1556, 1698 y siguientes del Código Civil; y artículos 144, 160, 170, 254 y siguientes del Código de Procedimiento Civil, se declara:

I. Que **se rechazan las tachas** deducidas por el demandado en las audiencias de folios 54, 75 y 82.

II. Que **se acoge parcialmente la demanda** deducida con fecha 9 de marzo de 2018, y se condena al Banco de Chile a pagar a don Manuel Joaquín Fernando Cortés Fravega, la suma de \$4.162.478 como indemnización del daño emergente, más \$3.750.000 por indemnización del daño moral.

III. Que las sumas indicadas deberán pagarse reajustadas conforme a la variación que experimente el Índice de Precios al Consumidor entre la fecha de la dictación de esta sentencia y su pago efectivo, y con intereses corrientes desde que el fallo quede ejecutoriado.

IV. Que **se condena en costas al demandado**.

Regístrese, notifíquese y archívese en su oportunidad.

**ROL C-7112-2018**

Pronunciada por doña Daniela Royer Faúndez, Juez Titular.



En Santiago, a treinta de Abril de dos mil veintiuno, se notificó por el estado diario, la resolución precedente.

