NOMENCLATURA : 1. [40]Sentencia
JUZGADO : 8º Juzgado Civil de Santiago
CAUSA ROL : C-6558-2018
CARATULADO : Vegetalia SPA/BANCO DE CHILE

Santiago, veinticuatro de Febrero de dos mil veinte .-

VISTOS:

Al folio 1, rectificada a folio 7, comparece Vegetalia Spa., sociedad del giro de actividades silvícolas, representada legalmente por don Mariano Díaz Campusano, paisajista, y por don Alex Acuña Vargas, ingeniero forestal, todos domiciliados en calle Profesora Amanda Laborea N° 96, oficina N° 65, Santiago, interponiendo demanda de indemnización de perjuicios por responsabilidad contractual en contra de Banco de Chile, sociedad del giro de su denominación, representada legalmente por don Eduardo Ebensperger Orrego, ignora profesión u oficio, domiciliados en Ahumada N°251, Santiago.

Funda su demanda en un contrato de cuenta corriente y demás productos asociados, celebrado con la demandada, quien, según señaló, desde el comienzo estuvo en conocimiento de la administración conjunta de ambos socios y de la necesidad de doble firma para efectos bancarios.

Indica que con este propósito, con fecha 13 de julio de 2016 las partes firmaron contrato de cuenta corriente suscribiendo conjuntamente un contrato de apertura de crédito, anexos relativos a mandatos especiales, constitución de garantías personales, y un contrato de autoservicio bancario denominado "Banconexion web", haciéndose entrega de una clave secreta y de un dispositivo de seguridad denominado digipass, ofreciéndolo como un sistema mucho más seguro que aquellos ofrecidos para personas naturales, con más controles para realizar transferencias electrónicas, aspectos los que llevaron a Vegetalia a contratarlo, lógicamente sujeto al pago de una comisión por la prestación del servicio, constituyéndose cada socio como administrador y usuario de la sesión que la demandada creó para la empresa, los que para realizar transferencias electrónicas debían acceder a la sesión ingresando el Rut y la clave secreta para luego crear al destinatario indicando Rut y nombre, creación que debía ser confirmada ingresándose la clave numérica contenida en el digipass.

Acusa que el día 3 de septiembre de 2017, el socio señor Díaz quiso ingresar a la sesión de Vegetalia pero apareció un mensaje en el que se solicitaba a ambos socios cambiar la clave de seguridad, requerimiento que se

cumplió dado que el mensaje apareció en la página de internet que el Banco de Chile dispuso para sus clientes, no teniendo razones para sospechar, intentando nuevamente el 8 de septiembre de 2017, ingresar a la sesión web de Vegetalia, apareciendo un mensaje de idénticas características que el anterior informando del bloqueo del digipass y que sería contactado telefónicamente por personal del Banco para solucionar el problema, recibiendo un llamado telefónico a su celular privado de una mujer la cual se presentó como la persona que el Banco había designado para encargarse del desbloqueo del dispositivo, quien señaló correctamente el número de serie del digipass entregado por el Banco a Vegetalia, información que supuestamente es confidencial y que sólo conocía el Banco y el cliente, por lo que presumiéndose que tal nivel de información solo pudo tenerlo alguien que trabaja en el Banco, a requerimiento de dicha persona se prendió el digipass y la clave numérica generada se insertó en la página del Banco de Chile tal como cuando se realiza una transferencia, haciendo hincapié en que la clave numérica se insertó en la página web de la demandada, sin que se le haya informado de la misma a la persona que estaba al otro lado del teléfono.

Expone que ese mismo día, a las 16:00 horas aproximadamente, el socio señor Díaz empezó a recibir correos electrónicos del Banco de Chile informándole la realización de 8 transferencias electrónicas, producto de esto, uno de los socios ingresó a la sesión de Vegetalia constatando que dichas transferencias eran por un total de $40.000.000, a cuentas corrientes del Banco Santander que no estaban registradas como destinatarios de transferencias de Vegetalia, todas ellas en el lapso de menos de dos minutos, cuyos destinatarios eran i) Rut 76.408.465-6, correspondiente a M & L Ingeniería y Construcción, de propiedad de Mauricio Lara; y, ii) 15.441.530-0, correspondiente a Héctor Cid Espina y que ante esto, y revisando por iniciativa propia la cuenta corriente de Vegetalia, los socios comprobaron que además se habían creado de manera fraudulenta otros 3 destinatarios cuyas transferencias no alcanzaron a materializarse, constatándose que era posible crear un nuevo destinatario ingresando únicamente su Rut, no siendo un requisito ingresar su nombre ya que dicho espacio también podía ser llenado reiterando el Rut, lo que evidenciaba que las medidas de seguridad para crear nuevos destinatarios eran deficientes, alegando que estas fallaron de tal manera que no fue el Banco quien detectó el fraude sino que la propia actora, alegando que una vez puesto al Banco en conocimiento de la situación por medio de su ejecutiva de cuentas doña Verónica Valderrama, en vez de tomar todas las medidas urgentes que ameritaba la situación, optó por señalar que ella no era la encargada de conocer y resolver estos asuntos sino que los afectados debían llamar a un callcenter que el Banco había creado para enfrentar este tipo de situaciones, optando por la burocracia en vez de dar solución urgente a un fraude señalando a Vegetalia que había sido víctima de una modalidad de fraude

informático conocido como phishing por medio del cual se intenta obtener de un usuario sus datos, claves, cuentas bancarios, números de tarjeta de crédito, identidades, entre otra información, para luego ser usados de forma fraudulenta, suplantando la imagen de una empresa o entidad pública para de esta manera hacer creer a la víctima que realmente los datos solicitados proceden del sitio oficial.

Señala que tras el fraude, Vegetalia solicitó al Banco el bloqueo de la cuenta corriente y la restitución de los fondos traspasados fraudulentamente, realizando la respectiva denuncia ante la Fiscalía Local de Las Condes, donde en el marco de dicha investigación el señor Lara confesó que su empresa recibió $30.000.000 desde la cuenta que Vegetalia tiene en el Banco, evidenciándose en estos hechos que el traspaso de fondos fue fraudulento y posible porque las medidas de seguridad del Banco fallaron de principio a fin, acusando que en un primer momento, en reunión presencial sostenida con la ejecutiva del Banco doña Daniza Parada y el Jefe de Gestión don Darry Johnnson, informaron que restituirían íntegramente el dinero dolosamente transferido, descartando dicha solución posteriormente pero que para soportar la pérdida podían ofrecer el otorgamiento de un crédito con condiciones más favorables que las del mercado, y finalmente, por carta de 25 de octubre de 2017 firmada por el Gerente de Clientes don Gonzalo del Real, se informó que el Banco no accedería a la solicitud de devolución de fondos basándose en argumentos insuficientes para sustraerse de la responsabilidad civil que les correspondía.

En cuanto a la responsabilidad contractual del Banco, explicó que en la especie concurren todos los presupuestos que la hacen procedente: (i) existencia de un contrato de cuenta corriente bancaria y un contrato accesorio denominado "Banconexion web" para efectos que el cliente pudiese utilizar la página de internet del Banco para realizar diversas operaciones bancarias, reiterando que los socios debían actuar de consuno proporcionando el Banco sólo un digipass en circunstancias que en caso que la administración fuese separada debía entregar dos, una para cada socio; (ii) existencia de un incumplimiento al no garantizar la seguridad de las transacciones y transferencias electrónicas de dinero (iii) existencia de un perjuicio, consistente en el menoscabo patrimonial real y efectivamente sufrido equivalente al monto irregularmente transferido desde la cuenta corriente del actor, por la suma de $40.000.000, sumado a mayores gastos en financiamiento derivado de las trasferencias fraudulentas, debiendo factorizar facturas y abrir cuentas corrientes en otros bancos de la plaza con todas las comisiones y seguros asociados, todo ello para poder cumplir con todas sus obligaciones, costos que ascienden a $2.000.000; (iv) la relación de causalidad entre el incumplimiento de la contraria que posibilitó la ocurrencia del fraude

informático y el daño; (v) sin que concurran ausencia de causales de exención de responsabilidad establecidas en nuestro ordenamiento jurídico.

En mérito de lo expuesto y previa cita de las disposiciones legales pertinentes, solicitó tener por interpuesta demanda de indemnización de perjuicios por responsabilidad contractual en contra de Banco de Chile, y declarar que incumplió con las obligaciones de seguridad que eran de su cargo derivadas del contrato de cuenta corriente y de Banconexion celebrado entre ambas partes, que Vegetalia Spa sufrió perjuicio material, siendo el Banco de Chile el responsable de resarcir todos los perjuicios sufridos producto del incumplimiento, se condene al demandado al pago de $42.000.000, por concepto de indemnización de perjuicios patrimoniales, o la suma que SS. estime pertinente, las cuales deben ser pagadas debidamente reajustadas y con los intereses legales correspondientes, con costas.

Al folio 10, compareció Banco de Chile contestando la demanda, solicitando su total rechazo, con expresa condenación en costas, controvirtiendo los hechos en que se fundó y/o la interpretación que se hizo de los mismos, agregando que no se incurrió en incumplimiento alguno al cursar las transferencias con la sola intervención del socio administrador Sr. Díaz, por cuanto él se encontraba facultado para operar por sí solo en materia de transferencias bancarias, sin que ese hecho en nada haya contradicho los estatutos sociales, puesto que, si bien esos estatutos disponían que ambos socios debían actuar conjuntamente, éstos también autorizaban a delegar sus facultades incluso en terceros, por lo que nada obstaba a que la delegación operara en favor del otro socio, de modo de reunir en éste la plenitud de las facultades sociales, siendo ésta la figura que se utilizó en el contrato de Banconexión en donde el o los representantes del actor confirieron a los administradores del contrato, los socios, facultades amplias, entre otras, para administrar las cuentas del cliente, girar y transferir fondos incluso desde líneas de crédito, efectuar transferencias de fondos, sea entre los productos del cliente o a terceros, acordando asimismo que la designación de usuarios también puede realizarse a través del sistema Banconexión, en forma electrónica, dejándose constancia que los administradores tendrán la atribución de designarse a sí mismos como usuarios, quedando además, en el anexo del contrato, establecido que los administradores del sistema, señores Mariano Díaz Campusano y Alex Vicuña Vargas, podían actuar en él en forma separada, desconociendo en su demanda las transferencias efectuadas por el Sr. Díaz, lo que contraviene la doctrina de los actos propios, pues son innumerables las transferencias ejecutadas con anterioridad por ese socio de la misma manera que las ahora cuestionadas. VER PRUEBA AL RESPECTO

En relación a las transferencias precisó, en primer lugar, que Vegetalia confesó que cuando recibió el llamado de la persona supuestamente encargada

de desbloquear el digipass digitó el número, por tanto, estampó su firma electrónica; de modo tal que, cualquiera que hayan sido las circunstancias del caso, firmó electrónicamente las transacciones que estaban en curso, haciendo presente que el Banco jamás solicita la firma electrónica, salvo para cursar transferencias de fondos. Asimismo negó que desde el interior del Banco haya habido fuga de información y, especialmente que Vegetalia haya sido víctima de un delito y, por ende, que terceros ajenos hayan vulnerado las redes del Banco en su perjuicio, pues las transferencias fueron efectuadas con las claves, password y digipass de la demandante.

Indicó que los contratos disponen que para acceder a los servicios, el cliente deberá proporcionar su Rut seguido de la clave secreta de acceso, siendo ambas condiciones copulativas, habilitando y poniendo a disposición del cliente dicha clave secreta de acceso, la que deberá ser inmediatamente modificada por éste a través de los sistemas automatizados del Banco.

Adicionalmente, el cliente deberá identificarse con una clave de carácter dinámica y personal que es generada y asignada por un dispositivo de seguridad, declarando que las claves de acceso suministradas son secretas, personales e intransferibles, siendo responsabilidad del cliente mantener la debida diligencia y cuidado en su mantención, asumiendo éste las consecuencias tanto de su divulgación a terceros, como por el uso que éstos hagan.

Añadió que el cliente lo instruye para que éste acepte y entienda que todo llamado telefónico, operación o transacción electrónica que efectúe alguna persona dando o digitando su clave secreta de acceso y, además, cuando corresponda, de su número de Rut y su clave dinámica, deberá entenderse hecho por el propio cliente, por tanto el Banco considerará que tal instrucción emanó válida, legítima y auténticamente del cliente, sin necesidad de efectuar, realizar o tomar otro resguardo, es decir el uso de las claves, particularmente aquella que genera el digipass o clave dinámica constituye la firma electrónica del cliente, circunstancia que permite indefectiblemente atribuir al mismo el acto o contrato celebrado a distancia con dicha clave, porque así se encuentra pactado, sin que importe el hecho que voluntariamente entregó el digipass a un tercero para su operatoria o que terceros hayan accedido a la información que provee el mismo, por mal uso o descuido del titular, cuestión que evidentemente no es responsabilidad del Banco.

Señaló que mediante la aplicación de esos sistemas el Banco cumplió lo pactado y previsto y, además, proveyó al cliente de todos los mecanismos de seguridad que la Superintendencia de Bancos e Instituciones Financieras y la lógica prevén; indicando que la normativa previene dos cuestiones completamente diversas: la primera, consiste en la intervención directa y por

parte de terceros de la página web del Banco y, la segunda, la intervención de terceros, ya no de la página web del Banco, sino del computador, teléfono o pantalla del cliente o usuario, bajo la modalidad del "fishing", de esta forma, y para evitar lo primero, el Organismo Supervisor dispone que los procedimientos empleados impidan que tanto el originador como el destinatario, desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse claves y mecanismos de acceso al sistema y al tipo de operación, que permitan asegurar su autenticidad e integridad; esto es, que no haya intervención alguna de terceros en la comunicación entre el banco y el cliente, este último obrando con sus claves.

Manifestó que respecto de la segunda cuestión prevista por la normativa, esto es la intervención de terceros, ya no de la página web del Banco sino del computador, pantalla o sistema empleado por el cliente, bajo la modalidad del "fishing", en la cual el delincuente hace creer mediante una página similar a la del Banco que es éste quien le requiere información, y aquél 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, añadiendo que en este caso, la página del Banco no ha fue vulnerada, sino que fue el cliente quien proporcionó a terceros los medios dados por el Banco para su autentificación, existiendo por tanto una comunicación integra y "autentica" para estos efectos entre el Banco y el cliente, con la salvedad de que quien operó las claves no fue el titular sino un tercero a quien éste se las proporcionó, por lo tanto, no es un problema de autenticidad de la comunicación o de violación de la página del Banco o de la encriptación, sino simplemente el mal uso que terceros hacen de las claves confidenciales del cliente, quienes pese a las advertencias expresas de los Bancos, se las dan a conocer, añadiendo que no les consta que la actora haya sido víctima de la acción delictual de terceros, por lo que debe acreditar esta circunstancia, cuestión que es de toda lógica, porque se ha de descartar que el propio titular desconozca sus transacciones. En caso contrario el sistema no podría funcionar.

Explicó que los sistemas de seguridad del Banco no fueron vulnerados en modo alguno, encontrándose además sus portales certificados en cuanto a su integridad por Symantec, empresa que es autoridad en estas materias y líder a nivel mundial; dejando constancia que en todas las operaciones cuestionadas concurrieron las claves personales del cliente, es decir, las transferencias se efectuaron con las claves personales e intransferibles del cliente, todas de su creación y bajo su custodia, no existiendo incumplimiento alguno del Banco al cursar las transferencias de autos, causa por la cual debe rechazarse la demanda de autos.

Indicó que recae sobre el cliente la custodia de sus claves y él es legal y contractualmente responsable de todas las transacciones ejecutadas mediante su uso, "auténticas" o con firma electrónica para estos efectos, sin poder ser de otro modo, pues de lo contrario el sistema no funcionaría si se permite el desconocimiento de la autoría de las transacciones.

Manifestó que no existe ninguna razón lógica ni jurídica para que la responsabilidad recaiga sobre el Banco, de modo que las cláusulas contractuales no son contrarias a la buena fe ni a la finalidad del contrato ni al principio que le rige, el de la apariencia jurídica, tomado de la propia Ley de Cuentas Corrientes Bancarias y Cheques, tendientes todas a posibilitar el funcionamiento del sistema y a evitar que los cuentacorrentistas desconozcan la autoría de sus propias transacciones, añadiendo que nada tiene de particular que en menos de dos minutos se hayan cursado ocho transferencias, porque el sistema Banconexión opera sobre la base de inscribir previamente las transferencias que se van a ejecutar, pudiendo ser una o muchas, y luego, sobre la opción de autorizar las ya inscritas, autorización que sirve conjuntamente para todas las previamente inscritas; de modo tal que en segundos o minutos se cursan la totalidad de las mismas.

Justificó que el Banco Santander, a Septiembre de 2017, tenía retenidos $ 10.000.000 del total que fueron transferidos desde la cuenta de Vegetalia SpA a cuentas de esa entidad, la cual no ha sido restituida a la actora exclusivamente por negligencia de ésta, causa por la cual cualquier eventual condena que se aplique al Banco de Chile debe ser con exclusión de esa suma.

Del mismo modo y por aplicación del artículo 2.330 del Código Civil, debe reducirse la indemnización, ya que fue la actora quien entregó imprudentemente a desconocidos sus claves, password y N° de digipass, esto es, su firma electrónica, negando la existencia de los gastos de financiamiento que la actora señalo haber incurrido por no haber contado con el dinero de las transferencias.

Por tanto, solicitó tener por contestada la demanda de autos y, en definitiva, rechazarlas en todas sus partes, con expresa condenación en costas.

Al folio 13, el actor evacuó el trámite de la réplica, indicando previamente que el demandado reconoció hechos que son básicos para configurar la responsabilidad reclamada, como es que los estatutos sociales de Vegetalia disponen que los socios deben actuar conjuntamente, que el 20 de Julio de 2017 se celebró entre las partes el contrato de autoservicio denominado "Banconexion web", que el 9 de septiembre de 2018 se realizaron transferencias a terceros desde la cuenta corriente por la suma de $40.000.000, indicando respecto de lo señalado por la demandada que efectivamente los

estatutos sociales indican que ambos socios deben actuar conjuntamente, lo cual fue reafirmado en una Junta realizada a instancias del Banco, el cual solicitó tal formalidad para que no hubiera duda respecto a la Administración social, negando la existencia de la delegación de poderes de parte del socio don Alex Acuña en el otro socio don Mariano Díaz, y en caso de ser cierto esta delegación, el Banco no habría exigido doble firma para todos los productos que ofrecía, por lo tanto, más allá del error de la ejecutiva, los socios siempre utilizaron el producto Banconexion de consuno, por lo que si la doctrina de los actos propios tiene aplicación, debería aplicarse en favor de su representada.

Añade que el Banco omitió señalar que la clave dinámica contenida en el digipass fue entregada luego de ser engañado, ya que en la página web se abrió una ventana el que informaba del bloqueo del digipass, agregando que sería contactado por una ejecutiva, siendo contactado posteriormente, y acertando éste en señalar el número de serie del digipass, información la cual es confidencial, por tanto, sólo la pudo obtener del propio Banco, reflejando la deficiente seguridad de la página web del demandado.

Señaló que el Sr. Díaz le indicó a quien dijo ser ejecutiva sólo una clave dinámica generada por el digipass, y no 8 claves dinámicas, como tampoco autorizó la creación de nuevos destinatarios ni las 8 transferencias fraudulentas, lo cual evidenció la negligencia de la demandada ya que quienes cometieron el fraude con sólo una clave dinámica pudieron inscribir a varios destinatarios y autorizar dichas transferencias, siendo que cada operación requiere una clave dinámica distinta.

Manifestó que aunque la contraria intentó relativizar la denuncia, en la actualidad existe un procedimiento penal ante el 4° Juzgado de Garantía de Santiago donde Mauricio Lara, dueño que la sociedad que facilitó su cuenta corriente para recibir $30.000.000, se encuentra formalizado por el delito de estafa, por su parte, Héctor Cid, quien facilitó su cuenta corriente para recibir $10.000.000, no ha sido formalizado únicamente porque no se ha pudo encontrar su domicilio, agregando que insulta a la lógica sugerir que el actor realizó de manera voluntaria tales transferencias a terceros con quienes no tenía obligación alguna, teniéndolo al borde de la insolvencia al tener que pagar intereses por préstamos que debió solicitar a otras entidades financieras para seguir realizando sus operaciones habituales.

Indicó que el Banco al sostener que bajo la modalidad del fishing sigue existiendo con el cliente una comunicación íntegra y auténtica, sin que haya existido una vulneración de su seguridad, ya que fue el cliente quien entregó la información al tercero, no hace sino que desconocer las normas que dictó la Superintendencia del ramo, las normas que rigen el depósito, el DFL 707 y la

jurisprudencia reciente, enfatizando que no funcionaron los mecanismos de detección de fraude ya que las transferencias se efectuaron en menos de 2 minutos a destinatarios no habituales, debiendo el Banco no permitir tales transferencias y contactarse con su titular para corroborar.

Respecto de la aplicación del principio de la apariencia, esta ha sido descartada en casos de fraude por nuestra jurisprudencia de manera reiterada y uniforme, por lo que insistir en su preeminencia citando para ello ejemplos que no pueden homologarse a transacciones electrónicas, carece de todo sustento jurídico, concluyendo que la demandada no pudo desvirtuar la configuración de la responsabilidad contractual que se le imputó, y por esto su primera reacción ante el fraude fue restituir inmediatamente el monto transferido.

Por tanto, solicitó tener por cumplido el trámite de la réplica.

Al folio 15, el demandado evacuó el trámite de la dúplica, reiterando todas las alegaciones, defensas y excepciones que se opusieron, indicando que la teoría del caso de la actora se fundó en un evidente desconocimiento del sistema de trasferencias de fondos electrónicas y del sistema bancario, ya que respecto del contrato denominado Banconexion ambos socios de la empresa delegaron poder recíprocamente en el otro, para que cualquiera pudiera actuar en forma individual, en materia de consultas y operaciones mediante internet, siendo precisamente como la empresa demandante utilizó dicho sistema, a través de su apoderado Mariano Díaz, disponiendo un solo digipass para operar la cuenta corriente, porque cada uno de los socios podía por sí sólo autorizar las transferencias electrónicas, lo cual nunca objetaron, excepto al presentar esta demanda, exponiendo que el contrato Banconexion rige solo la relación entre las partes respecto de su uso para efectuar operaciones por internet, por tanto, la delegación de poder es válida sólo para su utilización, y no para otras operaciones bancarias, como para la solicitud de vale vistas y giros de cheque que la actora mencionó en su réplica.

Aclaró que la supuesta ventana en la que se informó el bloqueo del digipass no se abrió de la página del Banco, ya que su sitio web es inviolable, por tanto, la única explicación es que el demandante se encontró en una página web que no era la del Banco, sino que sólo pareció serlo, a la que debió haber ingresado a través de un link u otro método que le fue enviado por un tercero, luego aclaró que el sistema de seguridad del Banco no permitió la creación de una página espejo, sino que lo que pudo haber ocurrido es que el demandante ingresó a una página web, a través de un medio no autorizado por el Banco, que se parecía a la de éste, correspondiendo a una imitación, funcionando de esta forma el delito de phishing, en que el delincuente hace creer al cliente que ingresó a una página web que corresponde al banco, en la que el cliente

ingresa sus claves pensando que va a acceder a la página oficial, pero en realidad se las entrega a aquél, ocurriendo lo mismo posteriormente cuando entregó directamente la clave de su dispositivo digipass a una persona que lo llamó por teléfono.

Finalizó reiterando que el Banco cumplió con todas las medidas de seguridad establecidas por la Superintendencia de Bancos e Instituciones Financieras para el funcionamiento de las transferencias por internet, especialmente respecto de empresas que realizan gran cantidad de movimientos diarios, por esta razón no se puede poner un límite de $250.000 para una primera transferencia como ilusamente propuso la actora. En efecto, el monto límite para realizar transferencias y quién puede autorizarlas es una cuestión que se definió en el contrato Banconexión, por la propia demandante, quien no obstante estableció montos superiores para que cada uno de sus socios pudiera autorizar, quienes en virtud del mismo contrato fueron designados como usuarios del sistema.

Por tanto, solicitó tener por evacuado el trámite de la dúplica.

Al folio 21, se llevó a efecto audiencia de conciliación, con la asistencia de don Diego Martínez, en representación de la parte demandante, y en rebeldía de la parte demandada; llamadas las partes a conciliación, ésta no se produjo.

Al folio 22, se recibió la causa a prueba.

Al folio 139 se citó a las partes a oír sentencia.

CONSIDERANDO:

PRIMERO*: Que Vegetalia Spa, representada legalmente por don Mariano Díaz y por don Alex Acuña, haN deducido en sede civil demanda de indemnización de perjuicios por responsabilidad contractual en contra de Banco de Chile, representada legalmente por don Eduardo Ebensperger Orrego, a fin de que se declare que Banco de Chile incumplió con las obligaciones de seguridad que eran de su cargo derivadas del contrato de cuenta corriente y de Banconexión celebrado entre ambas partes, que Vegetalia Spa sufrió perjuicio material, siendo el Banco de Chile el responsable de resarcir todos los perjuicios sufridos producto del incumplimiento, se condene al demandado al pago de $42.000.000, por concepto de indemnización de perjuicios patrimoniales, o la suma que SS. estime pertinente, las cuales deben ser pagadas debidamente reajustadas y con los intereses legales correspondientes, con costas.

Baso su demanda y peticiones, en los hechos y fundamentos de derecho que ya fueron reseñados en la primera parte expositiva de esta sentencia, y que se resumen en que al querer ingresar a la sesión de Vegetalia aparecieron mensajes en que se les solicitaba cambiar la clave de seguridad, apareciendo con posterioridad un mensaje de idénticas características que el anterior informando del bloqueo del digipass y que sería contactado telefónicamente por personal del Banco para solucionar el problema, recibiendo un llamado a su celular de una mujer la cual se presentó como la persona que el Banco designó para encargarse del desbloqueo, quien señaló correctamente el número de serie del digipass, prendiéndose éste, y la clave numérica generada se insertó en la página del Banco, recibiendo con posterioridad correos electrónicos que daban cuenta de la realización de 8 transferencias electrónicas, constatando que fueron por un total de $40.000.000, a cuentas corrientes del Banco Santander que no estaban registradas como destinatarios de transferencias, todas ellas en el lapso de menos de dos minutos y creándose de manera fraudulenta otros 3 destinatarios cuyas transferencias no alcanzaron a materializarse.

SEGUNDO*: Que la demandada, válidamente emplazada, contestó la demanda incoada en su contra, solicitando su total rechazo con expresa condena en costas, basado en que fue el propio demandante quien estampó su firma electrónica, firmando las transacciones que estaban en curso, negando, a su vez, que haya habido fuga de información desde el Banco y, especialmente que Vegetalia haya sido víctima de un delito y, por ende, que terceros ajenos hayan vulnerado las redes del Banco en su perjuicio, pues las transferencias fueron efectuadas con las claves, password y digipass de la demandante.

TERCERO*: Que evacuando su réplica, el actor reseñó que el Banco omitió señalar que la clave dinámica contenida en el digipass fue entregada luego de ser engañado, ya que en la página web se abrió una ventana la que informó del bloqueo del digipass, agregando que sería contactado por una ejecutiva, acertando ésta en señalar el número de serie del digipass, información la cual es confidencial, por tanto, sólo la pudo obtener del propio Banco, reflejando la deficiente seguridad de su página web, agregando que quienes cometieron el fraude, lo efectuaron con sólo una clave dinámica pudiendo inscribir a varios destinatarios y autorizar dichas transferencias, siendo que cada operación requiere una clave dinámica distinta, haciendo hincapié en que no funcionaron los mecanismos de detección de fraude ya que las transferencias se efectuaron en menos de 2 minutos a destinatarios no habituales, debiendo el Banco no permitir tales transferencias y contactarse con su titular para corroborar.

CUARTO*: Que la demandada en su dúplica aclaró que la supuesta ventana en la que se informó el bloqueo del digipass no se abrió de la página del Banco, ya que su sitio web es inviolable, por tanto, la única explicación es que el demandante se encontró en una página que no era la del Banco, a la que debió haber ingresado a través de un link u otro método que le fue enviado por un tercero, reiterando que el Banco cumplió con todas las medidas de seguridad establecidas por la Superintendencia de Bancos e Instituciones Financieras para el funcionamiento de las transferencias por internet.

QUINTO*: Que para acreditar sus dichos, el actor acompañó prueba documental no objetada de contrario, y testimonial, consistentes en:

Prueba documental:

a) Al anexo del folio 34:

1.- Copia de expediente virtual de causa Rit 8646-2017, caratulada Ministerio Publico con Mauricio Lara, sustanciada ante el 4° Juzgado de Garantía de Santiago, la que al reseñar lo hechos señaló que el día 8 de Septiembre de 2017, don Mauricio Lara, previamente concertado con terceros, conociendo o no pudiendo menos que conocer el origen fraudulento de los fondos, facilitó la cuenta bancaria de su empresa M y L Ingeniería, recibiendo la suma de $30.000.000 a través de 6 transferencias electrónicas bancarias, provenientes de la cuenta corriente cuyo titular es la empresa Vegetalia Spa, perteneciente a la víctima Mariano Díaz, lo cual se concretó ya que ese mismo día, una mujer se contactó por teléfono con la víctima, a quien engañó señalando ser una ejecutiva del Banco Chile, solicitándole que le entregara el número que figuraba en su digipass, el cual correspondía a un dispositivo que da un código de seguridad que permite realizar transferencias y otras operaciones con el Banco; posteriormente revisó su correo electrónico, percatándose que tenia un total de 8 correos electrónicos correspondientes a comprobantes de transferencias, de los cuales 6 correspondían a la cuenta del requerido, sufriendo la víctima perjuicios por un monto de $30.000.000. Resolviéndose que se condena a Mauricio Lara, a la pena de 41 días de prisión en su grado medio, a pagar una multa equivalente a un tercio de UTM, y a la sanción accesoria de suspensión de cargo u oficio público durante el tiempo de la condena, como cómplice de un delito de estafa residual consumado.

2.- Copia de carpeta investigativa, respecto del delito de estafa y otras defraudaciones contra particulares, del que ya se reseñó en el número anterior, resultando pertinente la declaración efectuada por don Mariano Díaz, quien señaló que los hechos ocurrieron el día 8 de septiembre; tiene una cuenta conjunta con un socio en el Banco de Chile, la cual pertenece a Vegetalia S.A, teniendo la obligatoriedad desde la escritura y contrato con el banco de firma

conjunta y que cualquier acción que se realice, se requiere la autorización de los 2 socios, por lo que cuando contrataron con el Banco, su socio inscribe las transferencias que se deben realizar y él las autoriza ingresando su clave y poniendo los números del digipass; declaró que el 4 de septiembre, al ingresar a su cuenta se le pidió cambiar la clave de seguridad, y lo mismo a su socio, el día viernes, que generalmente pagan las cuentas, su socio inscribió las cuentas para pagar, y al tratar de autorizarlas en la página le decía que su digipass estaba bloqueado, y que se comunicarían con él para desbloquearlo, llamándolo una mujer identificándose como ejecutiva, señalándole que le desbloqueará el digipass, **dándole todos los número de éste,** pidiéndole ingresar un número del digipass para desbloquearlo. Ese mismo día revisó su correo electrónico, apareciéndole 8 transferencias de 5 millones cada una a dos empresas distintas .Agregando que el Banco Santander pudo retener dos transferencias por $10.000.000.

b) Al anexo del folio 35:

1.- Copia de escritura pública de constitución de sociedad por acciones "Vegetalia Spa", de fecha 14 de Marzo de 2016, por medio del cual don Alex Eduardo Acuña Vargas y don **Mariano Rafael Díaz Campusano se declaran accionistas de dicha empresa. En artículo undécimo se señala que la administración y representación de la sociedad les corresponderá a ambos socios de consuno, quienes la ejercerán personalmente, o bien a través de personas especialmente designadas para ello por instrumento privado protocolizado o por escritura pública, con aquellas facultades que expresamente se le otorguen en el instrumento respectivo.**

2.- Copia de acta de junta extraordinaria de Vegetalia Spa, de fecha 26 de Mayo de 2016, los temas en la tabla de junta extraordinaria dicen relación con los requerimientos hechos por el Banco de Chile en orden a que haya claridad respecto de quienes son los administradores de la sociedad, ello con vistas a la apertura de cuenta corriente o a cualquier otro producto bancario, para lo cual los **comparecientes ratifican el pacto de constitución y su consecuencial inscripción en el registro de comercio, conjuntamente con lo anterior ratifican que tanto don Alex Acuña y don Mariano Díaz son ambos tanto representantes legales como administradores de la sociedad de la que son cofundadores, los que para todos los efectos bancarios deberán firmar conjuntamente.**

3.- Copia de contrato de cuenta corriente, de fecha 13 de Julio de 2016. Cliente: Vegetalia Spa. Identificando como cliente/representante legal a don Mariano Díaz y a don Alex Acuña. En su parte pertinente señala que para el uso de tarjetas de crédito y débito la clave secreta es de uso personal y

exclusivo del cliente o usuario, por lo que debe mantenerse en exclusiva reserva.

4.- Copia de contrato de autoservicio bancario Banconexion Web, de fecha 20 de Julio de 2016, entre Banco de Chile y Vegetalia Spa, conviniendo que éste último podrá acceder a un sistema de autoservicio bancario vía internet, en adelante Banconexion, el cual para acceder, el cliente deberá vía internet acceder al portal empresas a través de su dirección www.empresas.bancochile.cl a otros portales del Banco de chile o a nuevos que se establezcan en el futuro; para efectos de la prestación de este servicio el cliente deberá contactarse en dicha página web a Banconexion mediante el ingreso de los Rut y claves o firmas electrónicas correspondientes; las partes acuerdan que los apoderados del cliente que actúen a través de Banconexion podrán ser designados y/o informados, en forma electrónica por medio del mismo sistema Banconexion, de igual modo, las partes acuerdan que las facultades de los apoderados del cliente que actúen a través de Banconexion podrán ser conferidas y/o informadas, en forma electrónica por medio del mismo sistema; para estos efectos se establecen las siguientes definiciones: "Administrador" son aquellas personas designadas por el cliente que tendrán por función designar o informar a los usuarios que operarán en forma electrónica a través del sistema de Banconexion y/o conferir o informar las atribuciones que dichos usuarios podrán ejercer en ese canal. "Usuarios", son aquellas personas que operarán en forma electrónica a través del sistema de Banconexion, las operaciones y transacciones de carácter bancario que se les atribuya en ese canal electrónico; para los servicios o funcionalidades que el Banco determine, los mismos usuarios y/o administradores se deberán identificar con una clave adicional de carácter dinámica y personal que es generada y asignada por un dispositivo de seguridad el cual estará asociado al Rut del mismo usuario. El dispositivo de seguridad de generación o asignación de clave dinámica personal correspondiente, constituye una firma electrónica del usuario que lo identifica en las consultas, transferencias de fondos y operaciones en general que efectúe respecto de los productos del cliente, mediante canales de auto atención remota o a distancia; **atendido que el dispositivo generador de clave dinámica constituye una firma electrónica personal del usuario, el cliente declara y acepta que el usuario también podrá utilizarlo en aquellas consultas, transferencias de fondos y operaciones en general que efectúe el propio usuario en su carácter de titular de uno o más productos en el Banco de chile y/o en su carácter de mandatario y/o representante de otras personas naturales o jurídicas, distintas del cliente,** titulares de uno o más productos en el mismo Banco; los administradores y los usuarios accederán al servicio proporcionando su número de Rut, clave secreta personal y clave dinámica según corresponda; los servicios y/o funcionalidades otorgados por el Banco al clientes en

conformidad al presente contratos están dotados de sistemas de seguridad y de claves de acceso que son con conocidas exclusivamente por el cliente y/o por los administradores y/o usuarios designados **por éste, por lo tanto, el uso y manejo de las mismas son de exclusiva responsabilidad del cliente, asumiendo éste último las consecuencias tanto de su divulgación a terceros, como por el uso que éstos hagan de éstas.** Conforme lo anterior adicionalmente, el Banco no tendrá responsabilidad por la mala utilización que pudiera otorgársele por parte del propio cliente y/ o usuarios, por consiguiente, **el Banco no responderá de modo alguno, por los perjuicios y daños que puedan provocarse al cliente por el mal uso por parte de éste y/o de los usuarios de todas las claves indicadas, en Banconexion o en las funcionalidades a que se pueda acceder a través de dicho canal;** el cliente instruye al Banco que para que éste acepte y entienda que toda consulta, operación o transacción efectuadas a través del sistema Banconexion por alguna persona dando o digitando las claves secretas correspondientes, deba entenderse efectuado por él mismo; **el cliente asume toda responsabilidad que pudiere derivarse de hechos, actos** y contratos que realicen o celebren los administradores y/o usuarios a través del sistema Banconexion, liberando al Banco de toda responsabilidad al respecto; los administradores solo podrán ser designados por el cliente por escrito y a través de anexo al presente contrato, el cual firmado por el cliente, forma parte integrante del mismo; las partes dejan constancia y declaran que las claves y/o dispositivos que estuvieren asociados al certificado digital son secretas, personales e intransferibles, siendo de exclusiva responsabilidad del cliente y/o apoderados mantener la debida diligencia y cuidado en su utilización, por tanto, el cliente asume las consecuencias de su divulgación o entrega a terceros, como por el uso que estos hagan de ellas, quedando liberado el Banco de toda responsabilidad que de ello derive, sea ya de carácter patrimonial, por infracción a las normas de secreto o reserva bancaria y/o por responsabilidades civiles y penales que pudieren derivarse de transferencias de fondos y otras; todos los servicios computacionales o funcionalidades ofrecidos están dotados de sistemas de seguridad y de claves de acceso que son conocidas exclusivamente por el cliente y/o por los usuarios y/ o por los administradores, por lo tanto, el uso y manejo de las mismas son de exclusiva responsabilidad del cliente. **El banco no responderá de modo alguno por los perjuicios y daños que puedan provocar al cliente el mal uso por parte del mismo cliente, de los administradores y/o usuarios de las claves de Banconexion** y de las funcionalidades a que se pueda acceder a través de dicho canal; las partes convienen que los registros (log) de las operaciones efectuadas por el cliente, que se encuentren en los archivos del Banco tendrán, para todos los efectos legales, el carácter de plena prueba. **En anexo contrato de autoservicio bancario Banconexion web, de fecha 20 de Julio de 2016, el cual indica que el cliente designa a los siguientes administradores del**

sistema Banconexion, quienes actuaran individual y separadamente cada uno de ellos, don Mariano Díaz y don Alex Acuña, señalando al reverso que la forma de actuar de los administradores es separada. Se adjunta continuación anexo contrato de autoservicio bancario Banconexion web, el cual indica que el cliente y las sociedades que se indican en el anexo y que firman el presente instrumento, declararon que asumen toda responsabilidad que pudiere derivarse respecto de hechos, actos y contratos que realicen o celebren los administradores y/o usuarios a través del sistema Banconexion, **quedando liberado el banco de toda responsabilidad al respecto, contrato y anexo suscrito por ambos socios.**

5.- Copia de solicitud de cierre, de fecha 21 de Febrero de 2018, por medio del cual se le solicitó al Banco el cierre de la tarjeta de crédito, cuenta corriente, tarjeta de débito o cajera automático, por el motivo de atención o servicio inadecuado, cliente Vegetalia Spa, y sus representantes legales, don Mariano Diaz y don Alex Acuña.

6.-Copia de correo electrónico, de fecha 8 de septiembre de 2017, enviado por doña Verónica Valderrama de Banco de Chile, dirigido a don Alex Acuña y don Mariano Díaz, comentándoles que efectuaron el bloqueo de la cuenta, solicitando el envío de un mail solicitando el bloqueo de la cuenta corriente por transferencias no realizadas por ellos, agregando que deben ir a Investigaciones a realizar la denuncia, así mismo, solicitó ingresar erróneamente la clave de ingreso a la página 3 veces para que se bloquee, quedando a la espera del envío del mail solicitando el desbloqueo.

c) Al anexo del folio 38:

1.- Copia de sentencia de fecha 20 de Junio de 2018, pronunciada por la Tercera sala de la Excelentísima Corte Suprema, rol N° 2196-2018, el cual en su considerando séptimo señaló que aun cuando el fraude informático se ejecutó mediante el uso irregular de los datos y las claves bancarias personales del recurrente, no resulta posible soslayar que lo sustraído es dinero, bien fungible que se confunde con otros de igual poder liberatorio, con lo que resulta no sólo jurídica sino físicamente imposible acreditar la exacta identidad de las especies sustraídas mediante el fraude ejecutado a través de la cuenta bancaria del actor, circunstancia que fuerza a concluir que el único y exclusivo afectado por el engaño es el banco recurrido, dada su calidad de propietario del mismo y al ser en quien recae finalmente el deber de eficaz custodia material de éste, debiendo adoptar, al efecto, todas las medidas de seguridad necesarias para proteger adecuadamente el dinero bajo su resguardo; en el considerando octavo indicó que asentado lo anterior, no queda más que calificar el actuar de la recurrida (banco) como ilegal y arbitrario, puesto que al no asumir el perjuicio económico, trasladando los

efectos del fraude bancario al actor, afectó directamente el patrimonio de éste, vulnerando el articulo 19 n° 24 de la Constitución Política.

2.- Copia de sentencia de fecha 29 de Junio de 2017, pronunciada por la octava sala de la Iltma. Corte de Apelaciones de Santiago, señalando en su considerando séptimo que cada vez que las instituciones bancarias o financieras ofrecen a sus clientes la posibilidad de desarrollar por vía electrónica operaciones de transferencias de fondos u otras, se asume que aquéllas deben asegurar sus fines sustrayendo de cualquier menoscabo a quienes, guiados por los beneficios de rapidez y precisamente mayor reserva y seguridad, deciden utilizar estos métodos. Mismo sentido en el que la autoridad fiscalizadora de dichas entidades oferentes, la Superintendencia de Bancos e Instituciones Financieras ha puntualizado en sus respectivas Circulares, que los bancos están obligados a garantizar la seguridad de las transacciones y transferencias electrónicas de dinero, debiendo asegurar que las operaciones solo puedan ser realizadas por personas autorizadas para ello, debiendo recabar todas las validaciones previas que sean necesarias para resguardar la operación, manteniendo "sistemas y procedimientos" que les posibiliten "identificar, evaluar, monitorear y detectar" movimientos con "patrones de fraude", de manera que puedan abortar actividades u operaciones potencialmente dolosas.

3.- Copia de sentencia, de fecha 29 de Agosto de 2012, pronunciada por la Quinta sala de la Iltma. Corte de Apelaciones de Santiago, el cual declaró que la Superintendencia ha dicho que los bancos deben contar con sistemas que permitan identificar, evaluar, monitorear y detectar en el menor tiempo aquellas operaciones con patrones de fraude, de modo de marcarlas o abortarlas, para lo cual deberán establecer patrones conocidos de éstos y comportamientos que no estén asociados al cliente, añadiendo que habiéndose reconocido que se produjo una operación no deseada y notoriamente inusual, que fue inducida a través de los propios medios que entregó el banco a sus clientes para el desarrollo de sus operaciones electrónicas, sin que operaran los resguardos de control que ella pregona, no es sostenible que la entidad bancaria que fue utilizada para cometer el fraude, posteriormente, se libere de responder ante ese cliente que confió, de buena fe, en sus procedimientos y mecanismos de seguridad, lo que no significa que ésta pueda perseguir por las vías judiciales pertinentes, a quienes hicieron uso de esos medios con el fin de defraudar a otro.

4.- Copia de recurso de protección, interpuesto ante la Iltma. Corte de Apelaciones de Santiago, en contra de Banco de Chile, basado en que con fecha 22 de Agosto de 2018, ingresó a la página web del banco de modo directo, sin haber sido redirigido mediante correo electrónico o pop-up alguno, solicitándole, luego de ingresar sus datos personales, el ingreso de clave

digipass, la cual otorgó; aduce que con posterioridad al revisar su cartola de cuenta corriente, se percató de la existencia de un giro anormal cuyo monto ascendió a $990.000, el cual había sido girado en pago a Servipag.

5.- Copia de recurso de protección, interpuesto ante la Iltma. Corte de Apelaciones de Santiago, en contra de Banco de Chile, basado en que con fecha 12 de septiembre de 2018 la recurrente recibió en su correo electrónico un email desde la casilla contactos@bancochile.cl cuyo asunto se tituló "vigencia aprobación aumento de cupo del 1 al 30 de septiembre 2018", adjuntándose una imagen que se encontraba efectivamente en la página web de la entidad bancaria, pinchando la barra que decía "consulte aquí", desplegándose la página del banco en la cual se le solicitaba clave y digipass, lo cual hizo, percatándose el día 20 de septiembre de 2019 que se hizo una transacción de $990.000 cargados a su línea de crédito y un pago posterior a Servipag; configurándose por tanto, actos ilegales y arbitrarios que deben ser reparados mediante la concesión de una medida de protección respecto de una operación que no fue efectuada ni autorizada de modo alguno por la recurrente, lo cual se hizo por terceros desconocidos a través de la figura llamada phishing.

6.- Copia de recurso de protección, interpuesto ante la Iltma Corte de Apelaciones de Santiago, en contra del Banco de Chile, fundado en que fue víctima de un fraude bancario, ya que la transferencia de $5.000.000 efectuada, fue realizada por un tercero.

7.- Copia de recurso de protección, interpuesto ante la Iltma Corte de Apelaciones de Santiago, en contra del Banco de Chile, basado en que fue víctima de fraude, por medio de llamado telefónico de una persona que señaló ser asistente de ejecutiva de cuentas, por un problema con el digipass, siendo víctima de transferencias electrónicas por un total de $30.000.000, dando cuenta de la vulneración de los sistemas del Banco.

8.- Copia de nota de prensa, publicada en fayerwayer.com, de fecha 8 de agosto de 2018, la cual da cuenta de la creación de una división de ciberseguridad de Banco de Chile.

9.- Copia de nota de prensa, publicada en Economía y negocios online, de fecha 25 de Mayo de 2018, el cual reseña que debido a un problema en el sistema informático del Banco de Chile, obligó a cerrar todas las sucursales que operan en el país.

10.- Copia de nota de prensa, publicada en biobiochile.cl, de fecha 25 de julio de 2018, informando respecto de la masiva filtración de datos de tarjeta de crédito de clientes de bancos chilenos, principalmente al Banco de Chile.

11.- Copia de nota de prensa, publicada por biobiochile.cl, de fecha 21 de septiembre de 2018, la cual informó respecto a hackeo millonario al Banco de chile, el cual se originó a partir de un correo electrónico abierto desde un computador de una sucursal de Valdivia, a través del método de phishing.

12.- Copia de nota de prensa, publicada en emol.cl, de fecha 11 de mayo de 2017, informando respecto que debido a problemas técnicos del Banco de chile, impidieron que contribuyentes reciban devolución.

13.- Copia de nota de prensa, publicada por biobiochile.cl, de fecha 31 de agosto de 2018, el cual indica que Banco de chile confirmó falla en su portal web dirigido a las empresas, señalando que el portal Banconexion se encuentra sin servicio.

d) Al anexo del folio 39:

1.- Carta enviada por don Fernando León, supervisor línea servicio al cliente de Banco de Chile, a don Mariano Díaz, de Vegetalia Spa, de fecha 28 de septiembre de 2017, comunicándole que analizaron los antecedentes del caso, corroborando que de acuerdo a sus registros, con fecha 8 de septiembre de 2017, ingresó una objeción por 8 transferencias electrónicas a terceros, efectuadas desde la cuenta corriente de la sociedad, las cuales indicó desconocer. Señaló que dicha objeción se encuentra actualmente en proceso de investigación.

2.- Carta suscrita por don Gonzalo del Real, gerente de clientes, dirigida a don Mariano Díaz, de Vegetalia Spa, de fecha 25 de octubre de 2017, por medio de la cual informaron que se corroboró que las transferencias fueron realizadas habiendo ingresado previamente el Rut de la empresa, luego el Rut 8.606.091-4 correspondiente a un apoderado de la empresa y su clave personal al sitio seguro de internet (Banconexion), así como también el código digipass perteneciente al apoderado autorizado por la empresa, del mismo modo, no existen indicios que permitan señalar que en la materialización de dichas transacciones se hubiesen vulnerado infraestructura o sistemas informáticos del Banco de Chile, de manera que las transferencias se encuentran correctamente efectuadas, haciendo presente que el agendamiento de los beneficiarios de transferencias electrónicas de fondos, se realiza ingresando a la plataforma de Banconexion, en donde se despliega una lista con beneficiarios ya agendados, permitiendo ingresar nuevos, para lo cual el usuario debe seleccionar el botón agregar beneficiario, así, una vez agendado el beneficiario, y para autorizar la transacción, deben transcurrir 15 minutos desde cada agendamiento. Indicaron respecto a la contratación del servicio Banconexion que la empresa contrató el convenio poder plus 1, en la cual se designó dos administradores, el señor Díaz, Rut 8.606.091-4, y el señor

Acuña, Rut 14.083.038-0, de esta forma, con fecha **30 de agosto de 2016, el apoderado Díaz creó perfiles para ambos administradores, asignando para transferencias de fondos número de firmas 1, lo que significó que basta con una autorización de cualquier apoderado facultado para efectuar transferencia de fondos**, señalando que sólo el Señor Díaz puede autorizar transferencias, sin embargo, éste mismo también puede inscribirlas. Por tanto, no accederán a la solicitud de devolución de fondos en los términos solicitados, no existiendo indicios que para efectuar dichas operaciones se hubiese vulnerado infraestructura o sistemas informáticos del Banco de Chile.

3.- Carta suscrita por don Pedro Vargas, jefe sección reclamos y respuestas formales de Banco de Chile, dirigida a don Alex Villalobos, jefe departamento de atención al público de la Superintendencia de Bancos e Instituciones financieras, de fecha 31 de octubre de 2017, por medio del cual informa las razones que se tuvieron en vista para no proceder a la devolución de fondos solicitada, indicando que las transacciones fueron realizadas desde la cuenta corriente N° 1732126406, previo ingreso del Rut de la empresa y del Rut 8.606.091-4, correspondiente a un apoderado de la empresa más la clave personal que permite acceder al sitio seguro de internet, Banconexion, así como también un código digipass **perteneciente al apoderado autorizado para estos efectos**, además de que el agendamiento de beneficiarios, se realiza ingresando a la plataforma de Banconexion a través del módulo "Agenda de Benef", desplegándose una lista con los beneficiarios ya agendados, y se permite ingresar nuevos, para lo cual se debe seleccionar el botón "Agregar beneficiario", así, una vez agendado y con el fin de autorizar y materializar las transferencias, deben transcurrir 15 minutos desde cada agendamiento, los que se producen: Rut beneficiario 76.468.465-5 con fecha 8 de septiembre de 2017 a las 09:2:23 y Rut N° 15.441.530-0, con misma fecha a las 10:52:18 horas.

4.- Copia de cartola de cuenta corriente N° 1732126406, perteneciente a Vegetalia Spa, de fecha 28 de abril de 2017 hasta 31 de mayo del mismo año, con un saldo disponible de $68.294.788.

5.- Copia de cartola de cuenta corriente N° 1732126406, perteneciente a Vegetalia Spa, de fecha 31 de mayo de 2017 hasta 30 de junio de 2017, con un saldo disponible de $75.509.230.

6.- Copia de cartola de cuenta corriente N° 1732126406, perteneciente a Vegetalia Spa, de fecha 30 de junio de 2017 hasta 31 de Julio del mismo año, señalando un saldo disponible de $87.509.240.

7.- Copia de cartola de cuenta corriente N° 1732126406, perteneciente a Vegetalia Spa, de fecha 31 de julio de 2017 hasta 31 de agosto del mismo año, señalando un saldo disponible de $109.337.124.

8. -Copia de cartola de cuenta corriente N° 1732126406, perteneciente a Vegetalia Spa, de fecha 31 de agosto de 2017 hasta 29 de septiembre del mismo año, el cual da cuenta de 8 transferencias efectuadas el día 8 de septiembre a dos cuentas, cada una por un monto de $5.000.000 dejando un saldo disponible de $61.572.832.

e) Al anexo del folio 40:

1.- Copia de sentencia dictada por la Undécima Sala de la Corte de Apelaciones de Santiago, de fecha 10 de diciembre de 2018, en contra del Banco de Chile, el cual se fundó en el incumplimiento de las medidas de seguridad por parte del Banco para la realización de transacciones por internet, lo que permitió que terceros sustrajeran, mediante 3 transacciones, por la suma de $2.979.000 desde la cuenta corriente de la recurrente.

2.- Copia de correos electrónicos, enviados entre Daniza Paredes de Banco de Chile y Mariano Díaz de Vegetalia Spa, de fecha 12 y 13 de septiembre de 2017, por medio del cual informó el ingreso de dos nuevas solicitudes con información de respaldo relevante a la fiscalía, así mismo, que al revisar la cuenta corriente, su socio Alex Acuña, quien inscribe, detectó en el listado de cuentas inscritas, tres cuentas las cuales no reconocen y no corresponden a sus proveedores, viendo una gran debilidad en esto, ya que no se exige ningún respaldo para inscribir y menos verifica la información, como si sucede en las cuentas personales, es decir, el Rut y el nombre deben coincidir, de lo contrario no es aceptada, y luego debe ser confirmada con el digipass.

3.- Copia de correos electrónicos entre Mariano Díaz de Vegetalia Spa y Daniza Paredes de Banco de chile, con fecha entre 20 y 27 de septiembre de 2017, por miedo del cual solicitó formalmente respuestas al Banco respecto a las transferencias irregulares realizadas, tales como el permiso a efectuar 8 giros consecutivamente, sin aviso y sin una cuenta nueva, sin ninguna clave de respaldo y sin clave de seguridad de ninguno de los socios, de los cuales uno de ellos inscribe y el otro autoriza, así mismo, el no aviso realizado por su ejecutiva de las realización de dichos giros, como el conocimiento de su clave de digipass, número de cuenta corriente y nombre de su ejecutivo, entre otros.

f) Al folio 76 a través de audiencia de exhibición de documentos:

1.- Copia de transacciones o logs efectuados desde la cuenta corriente N° 1732126406 de Vegetalia Spa, efectuados el día 8 de Septiembre de 2017, a las cuentas N° 70845334 de M&L Ingeniería y Construcción, y N° 70188112

perteneciente a Héctor Cid, todas efectuadas por un monto de $5.000.000 realizadas a las 11:21:20, 11:21:23, 11:28:50, 11:26:51, 11:26:55, 11:29:00, 11:21:14, y 11:21:10 respectivamente.

2.- Copia de registro extraído del sistema Banconexion, de fecha 30 de Agosto de 2016, con asunto creación, modificación de contrato firmas empresa, enviado por empresas@bancochile.cl, dirigido a Nomina de pagos, el cual indica como responsable a don Mariano Díaz y como apoderado a don Mariano Díaz.

g) Al folio 77, a través de audiencia de exhibición de documentos:

1.- Copia de registro de transacciones o logs, en la cual da cuenta de 8 transacciones efectuadas con fecha 8 de septiembre de 2017, efectuadas a la cuenta N° 70845334 y N° 70188112 perteneciente a M&L Ingeniería y Construcción y Héctor Cid respectivamente, por un monto de $5.000.000 cada una.

h) Al anexo del folio 95:

1.- Copia de correo electrónico de fecha 5 de Agosto de 2019, enviado por serviciodeempresas@bancochile.cl, dirigido a don Mariano Díaz de Vegetalia Spa, por medio del cual le informan que debe sincronizar su dispositivo digipass, la cual es obligatoria y debe realizarse hasta el día 3 de mayo de 2019, de lo contrario la cuenta será bloqueada.

2.- Copia de correo electrónico de fecha 6 de Agosto de 2019, enviado por serviciosdetransferencia@bancochile.cl, dirigido a don Mariano Díaz de Vegetalia Spa, con el fin de informar que la empresa Metflife le transfirió un total de $5.000.000.

Prueba testimonial:

Al folio 42 y 66, comparecen don Matías Nicolás Moreno Villagra, contador auditor, y don Walter Erich Hombauer Pape, diseñador industrial, quienes legalmente juramentados, sin tachas e interrogados al tenor del auto de prueba expusieron:

Al punto 3, respecto a la efectividad de los hechos que se le imputan al demandado como incumplimiento del contrato, el testigo 1 depuso que le informó el representante legal de lo sucedido, y como es su trabajo el prestar servicios llevando el control de las cuentas del banco, **los montos eran inusuales al promedio de los movimientos de períodos anteriores y también los titulares de las cuentas no eran proveedores o prestadores habituales de Vegetalia,** lo cual es corroborado por el testigo 2, añadiendo que a Mariano lo llamaron supuestamente del Banco y le pidieron ingresar su

clave de Digipass en una ventana en la página del Banco, después recibió mensajes de que se habían realizado varias transferencias, agregando que Mariano tiene un socio y supuestamente firmaban en conjunto las transacciones, lo cual no sucedió en este caso.

Repreguntados el testigo 1, para que diga si sabe quién realizó las 8 transferencias, señalando que desconoce quien realizó las transferencias, conociendo sólo que éstas fueron de cinco millones cada una, totalizando diez millones a la cuenta del señor Héctor Cid, y seis transferencias de cinco millones cada una, totalizando treinta millones, a la cuenta de MyL Ingeniería y Construcción Limitada, efectuadas el mismo día, adicionando que tales transferencias no tienen respaldo contable, y que no es habitual la inexistencia de respaldos contables en Vegetalia; el **testigo 2 señala que las transferencias fueron fraudulentas, ya que no se conocían a las personas que se les efectuó, y que el Señor Díaz ingresó a la página del Banco de Chile desde su computador personal.**

Contrainterrogado, en el sentido como le constan los hechos declarados, el testigo 2 responde que le constan estos hechos debido a que Mariano Díaz le contó lo ocurrido hace un par de días.

SEXTO: Que a su turno, la demandada acompañó prueba documental observada de contrario, confesional y pericial consistente en:

Prueba documental:

a) Al anexo del folio 47:

1.- Copia de hoja de firma de contrato unificado de productos de empresas, de Banco de Chile, versión 12, de fecha 13 de julio de 2016, respecto del cliente Vegetalia Spa, por el cual declaró que la presente hoja constituye constancia fiel y suficiente de la celebración del contrato unificado de productos de empresas, y asimismo, constancia fiel y suficiente de la aceptación de todas y cada una de sus cláusulas, términos y condiciones contenidas en el instrumento protocolizado. Se indica como representante legal 1 a don Mariano Díaz, y como representante legal 2 a don Eduardo Acuña.

2.- Copia de contrato de autoservicio bancario Banconexion Web, de fecha 20 de Julio de 2016, entre Banco de Chile y Vegetalia Spa, ya reseñado en considerando quinto, letra b) N°4.

3.- Copia de certificado notarial, de fecha 5 de marzo de 2018, con el fin de revisar los certificados de seguridad de los sitios de internet de Banco de Chile, lo cual se efectuó en una terminal de computador del jefe de proyectos del departamento de seguridad tecnológica de dicho banco, quien explicó que

los distintos sitios de éste son seguros, porque ellos confían en la entidad certificadora Symantec, pues si se ingresa a cualquier sitio del Banco aparece el sello de seguridad (candado) pudiendo constatarse esto, accediendo al certificado donde se muestra que fue emitido por la empresa certificadora.

4.- Copia de logs de navegación de transacciones efectuadas entre el 7 de marzo de 2017 hasta 31 de agosto del mismo año.

5.- **Copia de tabla, la cual indica 8 transacciones efectuadas el día 8 de septiembre de 2017, desde la cuenta de Vegetalia Spa, a través del dispositivo digipass, por un monto de $5.000.000, con una diferencia de segundos entre una y otra transacción.**

6.- Carta suscrita por don Pedro Vargas, jefe sección reclamos y respuestas formales de Banco de Chile, dirigida a don Alex Villalobos, jefe departamento de atención al público de la Superintendencia de Bancos e Instituciones financieras, de fecha 31 de octubre de 2017, ya acompañada en considerando quinto, letra d) N° 3.

7.- Carta suscrita por don Gonzalo del Real, gerente de clientes, dirigida a don Mariano Díaz, de Vegetalia Spa, de fecha 25 de octubre de 2017, ya reseñada en considerando quinto, letra d) N° 2.

8.- Copia de protocolización de contrato unificado de productos de empresas, Banco de Chile, de fecha 31 de marzo de 2014, por medio del cual se acuerdan las condiciones por las cuales se regirán los contratos de los productos y servicios que éstos han señalado en la correspondiente solicitud de productos y servicios de empresas, en la cual se contiene contrato de cuenta corriente, sobregiros, contrato de cuenta corriente en moneda extranjera, convenio línea de crédito automático en cuenta corriente, entre otros, y contrato de servicios mediante uso de canales de auto atención, los cuales comprenden los servicios de consulta, transacción y/u operación que el banco prestará al cliente en banca telefónica fonobank, servicios automatizados; servicios a través de internet mediante el acceso a la página web www.bancochile.cl y cualquiera otra acción que el banco en el futuro incorpore a su servicio; señala que si el cliente fuera una persona jurídica, el cliente se obliga a operarlos exclusivamente a través de su representante que se indicó al efecto en la solicitud correspondiente, asimismo, que para acceder a los servicios y funcionalidades del contrato, el cliente o representante legal, deberá proporcionar el N° de Rut seguido de la clave secreta de acceso correspondiente, siendo ambas condiciones copulativas para acceder a uno o más de los servicios habilitados por el Banco; adicionalmente para los servicios y funcionalidades que el Banco determine, se requerirá además el ingreso, formulación o digitación de una clave de carácter dinámica y personal

que es generada y asignada por un dispositivo de seguridad que igualmente es proporcionado por el Banco; la totalidad de las claves constituyen una firma electrónica que los identifica en las consultas, transferencias de fondos y operaciones en general que efectúen respecto de los productos del cliente y en las operaciones realizadas al efecto por los medios electrónicos remotos con el Banco; para todos los efectos se entenderá que el uso de estas claves produce iguales efectos que la firma manuscrita; las partes dejan constancia y declaran que las claves secretas de acceso son secretas, personales e intransferibles, siendo de responsabilidad del cliente mantener la debida diligencia y cuidado en su utilización. El cliente asume las consecuencias tanto de su divulgación a terceros como por el uso que éstos hagan de éstas.

9.- Copia de lista de correos electrónicos, enviados a don Mariano Díaz, en diversas fechas, con asuntos como Si te piden tus claves, es un fraude; Si te llaman y piden tus claves, es un fraude; Evita fraudes, jamás entregues tus claves de seguridad.

10.- Copia de correos electrónico enviados por Banco de Chile a clientes, en los cuales se aconseja respecto a no entregar telefónicamente las claves, o bien evitar fraudes por internet con las herramientas del nuevo Banco el línea, otorgando recomendaciones como escribir la dirección del Banco directamente en la barra del navegador, jamás entregar claves, además de recordar que el Banco jamás llamara ni pedirá por mensaje de texto las claves, y nunca bloqueara la cuenta como argumento para solicitar actualización de datos, además de nunca incluir enlaces al sitio web de Banco de chile en sus comunicaciones, como también si se recibe una llamada de un ejecutivo del Banco preguntando claves secretas, es porque se trata de un fraude.

La contraria objetó el documento signado con el N° 5 por falta de autenticidad e integridad, debido a que no consta quien es el autor del referido documento, tanto así que ni siquiera está firmado, además de que contiene información distinta o menor en comparación al documento signado con el N° 4; en razón de que éstas objeciones no constituyen objeción formal, su valor probatorio se determinará en esta sentencia.

b) Al folio 132: Copia de informe de peritaje informático, Vegetalia Spa con Banco de Chile, realizado por doña María Cristina Valdés Arellano, de fecha 22 Enero de 2020, el cual en sus conclusiones indicó que para poder ingresar al sistema Banconexion se debe ingresar obligatoriamente Rut de empresa, Rut de usuario y clave; el sistema Banconexion permite inscribir beneficiarios para transferencias electrónicas, inscribir, autorizar y realizar transferencias electrónicas; por cada operación que se realice en el sistema Banconexion, el sistema genera un log en

forma automática; el sistema Banconexion para empresas pymes no permite realizar transferencias con un monto superior de $5.000.000 para transferencias a terceros y otros bancos por beneficiario; para poder autorizar y realizar una transferencia electrónica en el sistema Banconexion, se debe inscribir primero al beneficiario, una vez inscrito este se debe autorizar y para poder realizar la transferencia el sistema obliga a que el cliente debe ingresar un código de digipass; al ingresar un beneficiario nuevo, el sistema Banconexion no permite realizar una transferencia a este beneficiario nuevo antes de 15 minutos transcurridos; el día 8 de septiembre de 2017, se realizaron ingresos al sistema entre las 09:46 y 16:05 de distintas IP, registradas en las ciudades de Motta Visconti ubicada en Italia y Grays ubicada en Reino Unido; el día 8 de septiembre de 2017, se realizaron 5 intentos de ingreso al sistema, los que fueron rechazados, siendo 2 de éstos desde Italia y 3 desde el Reino Unido; los Rut de usuarios que se registran en los log que lograron ingresar son el Rut 8-606.091-4 con 5 ingresos y 14.083.038-0 con un solo ingreso; se constató por los log que el usuario Rut 8.606.091-4 perteneciente a la cuenta asociada al Rut 76.530.786-4 realizó 10 inscripciones de beneficiarios en el sistema Banconexion el día 8 de septiembre de 2017, para transferencias electrónicas por un monto de $5.000.000 cada una de ellas, siendo un total de 6 inscripciones para la cuenta de destino N° 76468 y 4 inscripciones para la cuenta de destino N° 5441; el Rut usuario N° 8.606.091-4 autorizó 8 transferencias electrónicas en total desde la cuenta perteneciente a la empresa Rut 76.530.786-4 por un monto de $5.000.000 cada una, siendo 6 de ellas a la cuenta de destino N°76468 y 2 de ellas a la cuenta N° 15441; se deja constancia que las cuentas corrientes de destinos reflejados en el log que se le entregó a la perito para su análisis y los log que se encuentran adjuntados por la parte demandada no coinciden en el número de cuentas corrientes de destino; el digipass N° de serie 3556799365 es el que estaba asignado y vigente a don Mariano Díaz el día 8 de septiembre de 2017; la empresa Vegetalia Spa para los servicios de transferencias solamente requiere de un solo autorizador para realizar transferencias electrónicas, independiente a que los dos apoderados estén autorizados a realizar transferencias bancarias; los montos máximos de Vegetalia para transferencias a otro Banco es de $5.000.000 por transferencia para cada autorizador y el monto máximo a transferir para cada uno de ellos diario es de $40.000.000; los montos máximos que tiene Vegetalia para cada

uno de los autorizadores es de $10.000.000 por cada beneficiario y el monto máximo por día para cada uno de ellos es de $20.000.000; el Rut de usuario N° 8.606.091-4 pertenece al usuario Mariano Díaz y el Rut usuario N° 14.083.038-8 pertenece a Alex Acuña; si bien se pudo constatar que los Rut de los usuarios Díaz y Acuña fueron ingresados el día 8 de septiembre de 2017 para acceder al sistema Banconexion, con la finalidad de realizar las 8 transferencias electrónicas que se registran ese día, no se pudo comprobar que quienes ingresaron ese día para realizar las transacciones electrónicas fueran efectivamente don Mariano Díaz y don Alex Acuña.

Prueba confesional:

Al folio 89, compareció don Mariano Rafael Díaz Campusano, quien respondió el pliego de posiciones de la siguiente manera:

Señaló que es efectivo que celebró con la contraria los contratos denominados contrato unificado de productos empresas y Banconexion web, negando el hecho de que él se haya designado como apoderado de Vegetalia Spa en el sistema Banconexion, ya que la escritura de constitución de la sociedad indica que ambos socios son apoderados, agregando que el Banco para abrir la cuenta, les pidió aclarar dicho punto, lo cual efectuaron por medio de escritura pública, señaló que nunca se facultó a sí mismo para realizar, inscribir y autorizar transferencias electrónicas de fondos a destinatarios del Banco y de otros; que cuando ingresó a la página, ésta indicaba su bloqueo, y que después de 10 minutos el Banco lo llamó, debiendo activarla con su digipass digitando el número en la página, y que ese mismo problema le apareció a su otro socio que vive en Talca; Además de que es efectivo que el 8 de septiembre de 2017 al ingresar supuestamente al sitio web del Banco de Chile, nuevamente se le solicitó actualizar sus datos, mediante el ingreso de la clave generada por su digipass, informándole que sería contactado por una persona del Banco, y que además, mientras hablaba por teléfono con la ejecutiva, se digitó su clave digipass para un procedimiento que no era una transferencia electrónica; añadió que es efectivo que la clave para operar en internet, le fue entregada por la contraria, pero que fue modificada por él, eligiendo una de su elección, además de que descargó el sistema Rapport de Trusteer; respondió que no es efectivo que anteriormente había realizado otras transferencias electrónicas, ya que el procedimiento que ellos efectuaban era que su socio Alex Acuña inscribía las cuentas, y el las autorizaba, pensando siempre que ambos debían autorizar las transferencias como lo indicó las escritura de aclaración solicitada por el Banco.

SÉPTIMO*: Que de la prueba rendida y analizada pormenorizadamente, han quedado acreditados los siguientes hechos no controvertidos:

1.- Que entre el Banco de Chile y Vegetalia Spa, existe un contrato unificado de productos de empresas, celebrado con fecha 31 de marzo de 2014, por medio del cual se acordaron las condiciones por las cuales se regirían los contratos de los productos y servicios que éstos han señalado en la correspondiente solicitud de productos y servicios de empresas.

2.- Que Vegetalia Spa y Banco de Chile celebraron con fecha 20 de Julio de 2016, el contrato de autoservicio denominado "Banconexion web", en el cual en su anexo se designó como administrador de dicho sistema a Mariano Díaz Campusano y don Alex Acuña Vargas, **quienes podían actuar en forma individual y separada.**

3.- Que el día 8 de septiembre de 2017, se efectuaron 8 transacciones electrónicas por $5.000.000, cada una, por un monto total de $40.000.000, a cuentas corrientes del Banco Santander todas ellas en el lapso de menos de dos minutos, cuyos destinatarios eran Rut 76.408.465-6, correspondiente a M & L Ingeniería y Construcción, de propiedad de Mauricio Lara; y, 15.441.530-0, correspondiente a Héctor Cid Espina.

OCTAVO*: Que de lo que se lleva razonado, el problema a dilucidar por el Tribunal quedó circunscrito al hecho de si existió un incumplimiento contractual de parte de Banco de Chile, y su subsecuente responsabilidad civil, toda vez que el fundamental reproche que el demandante le imputa es que lo acontecido se debió a que incumplió con las obligaciones de seguridad que eran de su cargo derivadas del contrato de cuenta corriente y de Banconexion celebrado entre ambas partes, lo que conllevó a que digitara su digipass, de acuerdo a lo indicado por la supuesta ejecutiva del Banco, efectuando diversas transacciones por un monto total de $40.000.000, lo que llevó a efectuar una denuncia ante la Fiscalía Local de Las Condes, sustanciada ante el 4° Juzgado de Garantía de Santiago, condenándose a Mauricio Lara, a la pena de 41 días de prisión en su grado medio, a pagar una multa equivalente a un tercio de UTM, y a la sanción accesoria de suspensión de cargo u oficio público durante el tiempo de la condena, como cómplice de un delito de estafa residual consumado.

NOVENO*: Que se hace necesario en este estadio de situaciones, analizar los requisitos copulativos de la responsabilidad civil contractual o necesarios para que se genere la obligación de indemnizar perjuicios contemplada en aquél, aparte de la capacidad, la que no se discutió; el incumplimiento del deudor (derivado de una relación contractual previa); el

perjuicio del acreedor; la relación de causalidad entre el incumplimiento y los perjuicios; la imputabilidad del deudor (dolo o culpa); y la inexistencia de una causal de exención de responsabilidad y la mora del deudor.

DÉCIMO*: Que al respecto, el artículo 1547 inciso tercero del Código Civil, señala que la prueba de la diligencia o cuidado incumbe al que ha debido emplearlo, esto es, el demandado de autos, Banco de Chile, quien deberá demostrar en esta sede que su sistema bancario cuenta con la debida seguridad que le permite al cliente realizar sus gestiones bancarais que ha confiado al Banco, atendida la naturaleza jurídica de este contrato

DÉCIMO PRIMERO*: Que el primer reproche que el demandante alega es que Vegetalia actuaba de consuno entre sus socios, lo que era sabido por el Banco, para evitar problemas.

Sin embargo consta del anexo de contrato suscrito por ambos socios responsables de esta empresa que ellos podían actuar en forma individual y separada, por lo que no resulta ser efectivo lo señalado en la confesional por el propio señor Díaz Campusano, siendo esta alegación del todo improcedente.

DÉCIMO SEGUNDO*: Que por otro lado el demandante señala que fallaron las medidas de seguridad de protección de datos que debía adoptar el Banco causando con ello un traspaso de $40.000.000 fraudulento.

Que al respecto, guarda especial relevancia el contrato Unificado de Producto de empresas, el cual en su capítulo VI, denominado “Convenio de Servicios mediante uso de canales de autoatención, establece que para acceder a los servicios y funcionalidades objeto de este convenio, el Cliente, persona natural, o el representante de cliente, indicado en la solicitud, tratándose de personas jurídicas, deberá proporcionar su número de RUT del cliente, seguido de clave secreta de acceso, siendo ambas condiciones copulativas para que el Cliente pueda acceder a uno o más de los servicios habilitados por el Banco; asimismo se estableció que el banco entregó al cliente o su representante una clave secretan de acceso personal e intransferible

Las claves indicadas constituyen una firma electrónica del Cliente, de su representante y/o de las personas designadas conforme al contrato, que lo identifica en las consultas, transferencias de fondos y operaciones en general que efectúe respecto de sus productos y operaciones realizadas por los medios electrónicos remotos con el Banco”, debiendo la clave proporcionada por el Banco ser inmediatamente modificadas a su vez, la cláusula 4 dispone que **"Las partes dejan constancia y declaran que las claves de acceso suministradas por el Banco al Cliente son secretas, personales e intransferibles, siendo de responsabilidad de este último mantener la debida diligencia y cuidado en su utilización.”; asumiendo el cliente las**

consecuencias de su divulgación a terceros, así como el uso que éstos hagan de ellas.

Asimismo, se instituyó que todo llamado telefónico, operación o transacción electrónica que se efectúe dando o digitando su firma electrónica, su número de RUT deberá entenderse hecha por el cliente, sin ser necesario que el Banco tome otro resguardo.

DÉCIMO TERCERO*: Que en este mismo orden de ideas, las partes suscribieron también el contrato de autoservicio bancario Banconexión web, el que el la parte que nos convoca especialmente, señala que, el dispositivo de seguridad de generación o asignación de clave dinámica personal correspondiente, constituye una firma electrónica del usuario que lo identifica en las consultas, transferencias de fondos y operaciones en general que efectúe respecto de los productos del cliente, mediante canales de auto atención remota o a distancia; **atendido que el dispositivo generador de clave dinámica constituye una firma electrónica personal del usuario, el cliente declara y acepta que el usuario también podrá utilizarlo en aquellas consultas, transferencias de fondos y operaciones en general que efectúe el propio usuario en su carácter de titular de uno o más productos en el Banco de chile y/o en su carácter de mandatario y/o representante de otras personas naturales o jurídicas, distintas del cliente,** titulares de uno o más productos en el mismo Banco; los administradores y los usuarios accederán al servicio proporcionando su número de Rut, clave secreta personal y clave dinámica según corresponda; los servicios y/o funcionalidades otorgados por el Banco al clientes en conformidad al presente contratos están dotados de sistemas de seguridad y de claves de acceso que son con conocidas exclusivamente por el cliente y/o por los administradores y/o usuarios designados **por éste, por lo tanto, el uso y manejo de las mismas son de exclusiva responsabilidad del cliente, asumiendo éste último las consecuencias tanto de su divulgación a terceros, como por el uso que éstos hagan de éstas;** por lo que el Banco no tendrá responsabilidad por la mala utilización que pudiera otorgársele por parte del propio cliente y/ o usuarios, **no respondiendo de modo alguno, por los perjuicios y daños que puedan provocarse al cliente por el mal uso por parte de éste y/o de los usuarios de todas las claves indicadas, en Banconexion o en las funcionalidades a que se pueda acceder a través de dicho canal;** el cliente instruye al Banco que para que éste acepte y entienda que toda consulta, operación o transacción efectuadas a través del sistema Banconexion **por alguna persona dando o digitando las claves secretas correspondientes, deba entenderse efectuado por él mismo**; **el cliente asume toda responsabilidad que pudiere derivarse de hechos, actos** y contratos que realicen o celebren los administradores y/o usuarios a través del sistema

Banconexion, liberando al Banco de toda responsabilidad al respecto; las partes dejan constancia y declaran que las claves y/o dispositivos que estuvieren asociados al certificado digital **son secretas, personales e intransferibles**, **siendo de exclusiva responsabilidad del cliente y/o apoderados mantener la debida diligencia y cuidado en su utilización**, por tanto, el **cliente asume las consecuencias de su divulgación o entrega a terceros,** como por el uso que estos hagan de ellas, quedando liberado el Banco de toda responsabilidad que de ello derive, sea ya de carácter patrimonial, por infracción a las normas de secreto o reserva bancaria y/o por responsabilidades civiles y penales que pudieren derivarse de transferencias de fondos y otras; todos los servicios computacionales o funcionalidades ofrecidos están dotados de sistemas de seguridad y de claves de acceso que son conocidas exclusivamente por el cliente y/o por los usuarios y/ o por los administradores, por lo tanto, el uso y manejo de las mismas son de exclusiva responsabilidad del cliente. **El banco no responderá de modo alguno por los perjuicios y daños que puedan provocar al cliente el mal uso por parte del mismo cliente, de los administradores y/o usuarios de las claves de Banconexion** y de las funcionalidades a que se pueda acceder a través de dicho canal; las partes convienen que los registros (log) de las operaciones efectuadas por el cliente, que se encuentren en los archivos del Banco tendrán, para todos los efectos legales, el carácter de plena prueba.

DÉCIMO CUARTO*: Que en este sentido el representante legal de Vegetalia reconoció frente a un engaño y al haber sido contactado en forma telefónica por una persona que señaló ser el encargado de desbloquear el dispositivo, el cual había sido bloqueado según aparecía de la página web y al indicarle el número de serie, es que prendió el digipass, insertando la clave numérica en la página del banco, tal como cuando se realiza una transferencia, haciendo presente, que ella no se informó a la persona que estaba al teléfono, enterándose ese mismo día y al recibir correos electrónicos del Banco que se había llevado a cabo ocho transferencias por un total de $40.000.000, a destinarios que no eran proveedores habituales y en un lapso de menos de dos minutos.

DÉCIMO QUINTO*: Que el Banco se excepciona en esta materia, señalando, que la demandante confesó judicialmente que digitó el digipass, esto es estampó su firma electrónica en las transacciones que estaban en curso, por lo que deniega que se hayan vulnerado las redes del banco, y por tanto no habría incumplimiento contractual de acuerdo a los términos del mismo.

DÉCIMO SEXTO*: Que lo cierto es que en sede penal se tuvo como hecho acreditado que el actor quien fue víctima del delito de estafa y debido a un engaño hizo entrega del número de clave de seguridad del dispositivo digipass que permite realizar transferencias electrónicas, por lo que y

analizados los contratos ya referidos se entiende que entregó a un tercero datos personales e intransferibles que habría hecho mal uso de ellos, por lo que en principio la responsabilidad de los perjuicios sufridos recaerían sobre él.

DÉCIMO SÉPTIMO*: Que no obstante lo anterior en el caso de marras nos encontramos enfrentados a un tipo de estafa sofisticada y estudiada, en la que primero se procedió a bloquear la clave del cliente y luego mediante engaño se obtuvo la misma realizando en un **período de un minuto y dos segundos** ocho transferencias bancarias por una suma millonaria lo que no constituía de acuerdo al mérito de los antecedentes que esta juez ha tenido a la vista, un comportamiento habitual del cliente, situación que debió haber sido identificada, evaluada, monitoreada y detectada por el departamento especial de la entidad bancaria como movimientos con **"patrones de fraude",** debiendo así en su calidad de custodio de los dineros entregados por un contrato tan especial y de confianza como lo es el de cuenta corriente, abortar rápidamente, estas operaciones potencialmente dolosas, lo que no hizo, no siendo excusa aquello indicado por la entidad bancaria en cuanto a **que en general las empresas efectúan múltiples transferencias** para pagar a sus proveedores ya que en el caso particular de este cliente y conforme a las cartolas allegadas al Tribunal, sus movimientos eran por sumas inferiores, y en el caso de ser ellas superiores a $1.000.000, no se efectuaban más de dos diarias, siendo por montos distintos entre sí.

DÉCIMO OCTAVO*: Que por otro lado y en cuanto a los $10.000.000 que fueron retenidos por el Banco Santander, y no restituidos a la actora, cabe señalar que ello se trata de una entidad bancaria ajena a este juicio, que no ha sido emplazada y por lo demás el contrato de cuenta corriente fue suscrito con el Banco de Chile, sin perjuicio de otros derechos.

DÉCIMO NOVENO*: Que asimismo el demandado solicita que se aplique el artículo 2330 del Código Civil, reduciéndose la indemnización, toda vez que la actora fue quien entregó imprudentemente a desconocidos sus claves, password y digipass.

VIGÉSIMO*: Que en este escenario, cabe pronunciarse sobre la entrega de las claves secretas y al respecto, cabe distinguir en las siguientes situaciones: a) El resultado nocivo obedece exclusivamente a culpa del autor del hecho, caso en el que éste debe asumir la reparación total del daño; b) la producción del daño se debe a la culpa propia y privativa de la víctima, situación en que el autor del hecho se haya exonerado por completo de la obligación de indemnizar, pues no se advierte en este evento la relación casual entres u conducta y el efecto nocivo y c) el daño se genera por la conducta culpable del autor a la que se suma la concausa culpa de la víctima, lo que

repercute en una atenuación de la responsabilidad indemnizatoria que empece al primero, reduciéndose el monto a indemnizar.

VIGÉSIMO PRIMERO*: Que lo señalado precedentemente se encuentra en estricta relación con los requisitos copulativos de la responsabilidad contractual señalados en otro considerando de este fallo y en el caso que nos convoca la situación prevista se configura por la conducta culpable del autor a la que se suma la concausa culpa de la víctima, precisado en el punto c) precedente, toda vez que éste confeso en su libelo que entregó sus claves secretas, incluyendo la del Digipass, en una creencia errada de que quién lo llamaba era un ejecutivo de su Banco, **sin embargo el proceder de los terceros debió haber sido advertido con un mínimo de diligencia por el departamento de fraude del banco,** al menos desde la tercera de las transferencia electrónica al ser ésta del mismo monto y realizadas con segundos de diferencias, lo que hace procedente acoger esta excepción y rebajar la indemnización solicitada a la suma de $30.000.000.

VIGÉSIMO SEGUNDO*: Que por otro lado Vegetalia solicita la suma de $2.000.000 por los mayores gastos en financiamiento en que debió incurrir, ya que tuvo que factorizar facturas, abrir cuentas corrientes con gastos en comisiones y seguros asociados; lo que desconoce la entidad bancaria, recayendo sobre el primero el onus probandi, no acreditando su ocurrencia, lo que basta para rechazarlo.

VIGÉSIMO TERCERO*: Que también el actor solicita sean pagadas las sumas con reajustes e intereses legales; a lo que se hará lugar, pero sólo respecto a los intereses corrientes para operaciones no reajustables, de conformidad al artículo 1559 del código Civil, esto es, desde que el demandado es constituido en mora, lo que sólo ocurre desde que esta sentencia se encuentra ejecutoriada, atendido la naturaleza declarativa del juicio incoado.

VIGÉSIMO CUARTO*: Que la demás prueba no analizada pormenorizadamente en nada altera a lo que se lleva razonado, por lo que se omite su análisis.

Y vistos y además lo dispuesto en los artículos 1437, 1545, 1546, 1547, 1698, 2215 y siguientes, 2330 del Código Civil; artículos 144, 160, 170, 254, 341, 342, 346, 384 y 385 y siguientes, del Código de Procedimiento Civil, y demás normas pertinentes, se resuelve:

I. Que se acoge la demanda de indemnización de perjuicios por responsabilidad contractual, sólo en cuanto se declara que los perjuicios económicos sufridos por Vegetalia SPA, deben ser resarcidos por el Banco de Chile pero sólo hasta el monto de

$30.000.000 (treinta millones de pesos), por efecto de lo dispuesto en el artículo 2330 del Código Civil, condenándosele a pagar esta suma , más intereses establecido en el considerando vigésimo tercero de este fallo.

II. Que cada parte pagará sus costas.

Regístrese, notifíquese y archívese en su oportunidad.

Rol: C-6.558-2018.-

DICTADA POR DOÑA SYLVIA PAPA BELETTI, JUEZ TITULAR.-

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

JFLDXPGEFC

SYLVIA JOSEFINA PAPA BELETTI
Fecha: 24/02/2020 15:18:45