Rol: C-314-2018
Carátula: Zelada con Banco de Chile
Materia: Cumplimiento de contrato.

Casablanca, siete de agosto de dos mil veinte.

Visto:

Comparece Emiliano Zelada Silva, empresario, representante legal de Mecagri-Chile E.I.R.L., ambos domiciliados en Punta Arenas N° 90, comuna de Casablanca, quien en virtud de la escritura de constitución de la Sociedad Mecagri Ltda., de la cual es su representante legal, interponiendo demanda de cumplimiento de contrato e indemnización de perjuicios en contra del Banco de Chile, representada por su Agente en la comuna de Casablanca, Jaime Cáceres López, desconoce profesión u oficio, ambos domiciliados en Avenida Portales N°211, Casablanca.

Con fecha 05 de marzo de 2018 (F.5), se notifica legalmente la demanda al demandado.

Con fecha 04 de abril de 2018 (F.11), se contesta la demanda, solicitando su rechazo, con costas.

Con fecha 14 de junio de 2018 (F.24), se lleva a cabo audiencia de conciliación. Llamadas las partes a conciliación, esta no se produce.

Con fecha 27 de junio de 2018 (F.27), se recibe la causa a prueba, rindiéndose la que consta en autos.

Con fecha 16 de abril de 2020 (F.128), se cita a las partes a oír sentencia.

Considerando:

I. En cuanto a las objeciones de documentos:

Primero: Que con fecha 02 de agosto de 2018 (F.38), el demandante objeta los documentos acompañados por la demandada al folio 36, respecto a:

a) Certificados emitidos por la empresa Neosecure, que dan cuenta que ni la empresa demandante, ni su representante legal habían descargado el software Rapport de Trusteer, que el Banco de Chile dispone gratuitamente para sus clientes y que advierte ante la posibilidad de ser víctima de phishing, fundado en las causales legales de impugnación, esto es, falta de autenticidad e integridad, de conformidad con lo establecido en los artículos 17 del Código Civil y 346 del Código de Procedimiento Civil, por tratarse de instrumentos privados emanados de un tercero que no es parte en la presente causa, y que no ha sido reconocido ante el Tribunal. Indica que quien comparece suscribiendo el documento N° 2 es don Alejandro Keulen, representando supuestamente a la empresa Neosecure S.A., quien firma atribuyéndose el cargo de Gerente de Finanzas, no constando en autos quien es Alejandro Keulen, ni menos consta la profesión que tiene para ocupar ese cargo, ni tampoco consta la representación que detenta de Neosecure S.A., por la cual dice comparecer.

b) Certificado emitido por la empresa Symantec, sobre la inviolabilidad del sitio, fundado en las causales legales de impugnación, esto es, falta de autenticidad e integridad, de conformidad con lo establecido en los artículos 17 del Código Civil y 346 del Código de Procedimiento Civil, por tratarse de instrumentos privados emanados de un tercero que no es parte en la presente causa, y que no ha sido reconocido ante el Tribunal. Indica que se presenta un certificado notarial que da cuenta de certificado de seguridad de

los sitios de internet del Banco a petición del abogado del Banco; revisando el Notario Suplente el terminal de don Daniel Castro Reales, el que declara que todos los certificados de seguridad son proporcionados por la Empresa Symantec. El Notario Suplente no tiene la expertise informática para darse cuenta que los demostrado sea real; la información anterior se la entrega un funcionario del banco, el que no es imparcial en este procedimiento y finalmente la certificación proporcionada por Symantec no consta de ningún modo en los autos; ya que no se sabe quién firma los documentos, que profesión tiene y no consta la representación de nadie de esta empresa.

c) Contrato Unificado de Productos de empresas versión 9, que corresponde al suscrito por la empresa demandante, fundado en las causales legales de impugnación esto es falta de autenticidad e integridad, de conformidad con lo establecido en los artículos 17 del Código Civil y 346 del Código de Procedimiento Civil, por tratarse de instrumentos privados emanados por el propio Banco y carecen de autenticidad e integridad. Indica que es una simple copia de un contrato del año 2012, protocolizado el año 2014 y que no tiene ninguna firma de mi representado; Así las , el instrumento privado referido no puede producir ningún efecto en contra de esta de esta parte, mucho menos constituir una presunción judicial, por cuanto, este documento no está vigente y no viene acompañado en original y por lo tanto, no se sabe quién lo firma y que representación detenta quien lo presenta a los autos y no se ha presentado ante el tribunal a reconocer su firma.

d) Cuadro con las facultades del apoderado, Emiliano Zelada Silva, para operar en el sistema Banconexión de la empresa demandante, que acreditan que se encontraba facultado a ejecutar las operaciones por montos muy superiores a los que corresponden a las transferencias objetadas, fundado en las causales legales de impugnación esto es falta de autenticidad e integridad, de conformidad con lo establecido en los artículos 17 del Código Civil y 346 del Código de Procedimiento Civil, por tratarse de instrumentos privados emanados por el propio Banco y carecen de autenticidad e integridad. Señala que Es una simple copia de un correlato de facultades que supuestamente puede realizar mi representado y que tiene data del año 2012; no tiene pie de firma ni ningún timbre que señale que es un documento o instrumento de uso corriente en el Banco. Nada aporta, ya que además de estar con una antigüedad de casi 6 años, nada se señala en forma explícita de las facultades y como se puede inferir que ha sido aceptado por mi representado si no está firmado por éste. Así las cosas el instrumento privado referido no puede producir ningún efecto en contra de esta de esta parte, mucho menos constituir una presunción judicial, por cuanto, este documento no está vigente y no viene acompañado en original y por lo tanto, no se sabe quién lo firma y que representación detenta quien lo presenta a los autos y no se ha presentado ante el tribunal a reconocer su firma.

La parte demandada responde al traslado conferido indicando que la contraria ha objetado una serie de documentos por la causal de falsedad y falta de integridad; más en el desarrollo de lo objeción lo que ha hecho es referirse al mérito probatorio de los mismos documentos, cuestión que le resta todo sustento a la causal invocada, no siendo las observaciones al mismo una verdadera causal de impugnación, procede que se rechacen las objeciones promovidas, con costas.

Estimando que los fundamentos de la impugnación, relativos a la falta de autenticidad o de integridad no constan de los instrumentos ni del resto de los antecedentes de la causa, y que el resto de las alegaciones planteadas

en lo precedente dicen relación con el valor probatorio de cada documento, el que será determinado de forma exclusiva por el tribunal, de modo que la objeción será rechazada.

II. En cuanto al fondo:

Segundo: Que comparece Emiliano Zelada Silva, representante de Mecagri-Chile E.I.R.L., interponiendo demanda de cumplimiento de contrato e indemnización de perjuicios en contra del Banco de Chile, representada por Jaime Cáceres López, por haber permitido que se retirara de la cuenta corriente de la empresa la cantidad de Catorce Millones novecientos noventa y nueve mil pesos ($ 14.999.000) mediante fraude informático denominado actualmente "PHISHING", lo cual infracciona lo que dispone el DFL 707-1982 sobre cuentas corrientes bancarias y cheques, los artículos 3, 12, 23, 46 de la Ley del Consumidor Nº 19.446; artículos 1489, 1545, 1558 del Código Civil y en conformidad del 253 y siguientes del Código de Procedimiento Civil, solicitando que se le condene a la restitución de los dineros defraudados y se les indemnice.

Asevera que el Banco de Chile incurrió efectivamente en infracción a lo dispuesto en el artículo 23 de la Ley N° 19.496, al actuar con negligencia, lo que ha causado menoscabo al patrimonio de su empresa al no emplearse las medidas de seguridad y resguardo necesarios en el uso y manejo de su cuenta corriente, permitiendo concretamente que se retirasen fondos en forma electrónica, sobrepasando todos los controles y protocolos que permitiesen comprobar que la persona que efectuó los giros de dinero realmente haya sido la legítimamente autorizada por este representante legal.

Añade que con fecha 05 de diciembre de 2017, a las 11:30 horas aproximadas, al momento de conectarse al Banco de Chile con el computador de la empresa, Marca ASUS, Modelo / X302L, Serie F4NOCV 2846655168, para saber de la cuenta corriente contratada Nº 421-00073-02, siguiendo el protocolo o procedimiento establecido (Banconexion), esto es, ingresar los datos que le pide la página, sorpresivamente se abre otra página anexa que señalaba que "estamos actualizando el sistema" e indicando el porcentaje de carga de la página; luego de 10 minutos y al no cargar el 100%, se cerró dicha página, por lo tanto, no pudo ingresar a la cuenta corriente. Al día siguiente, la Secretaria de la empresa, Carla Silvana Báez Urzúa, Rut Nº 13.429.356.-8, ingresa a la página del Banco y al revisar el estado de la cuenta corriente de la empresa, se percata que el día 05 de enero de 2017 se habían realizado tres(3) transferencias de dinero entre las 11:33 y 11:36 horas a una cuenta corriente del Banco de Crédito e Inversiones perteneciente don René Javier La Court Salinas, Rut Nº 12.241.878-2, conductor de Buses Pullman Bus, por la cantidad de cuatro millones novecientos noventa y nueve mil novecientos noventa y nueve pesos ($4.999.999) cada vez, totalizando la suma de catorce millones novecientos noventa y nueve mil novecientos noventa y nueve pesos($14.999.999). Hecho que se puede comprobar en el estado de Cuenta de la Cuenta Corriente de fecha 30 de noviembre de 2017 a 29 de diciembre de 2017 donde figuran los tres (3) traspasos comentados.

Refiere, en otras palabras, que se configuró la denominada estafa informática en contra de su empresa, a saber: "El "phishing" y el "pharming", señalando que en la práctica, el modo como opera, en palabras sencillas como sigue: el o los estafadores consiguen una cuenta corriente de una persona natural o jurídica correntista de un Banco de la Plaza, sin que este lo advierta por medio de HACKEO de su cuenta corriente; a su vez, consiguen

de un tercero (Moneymules) una cuenta corriente de otro Banco (sin que éste tampoco advierta que es una estafa), además de que esas dos personas coludidas o no, obtienen el dinero de la cuenta corriente del estafado, hecho, el Moneymules retira el dinero en efectivo de su propia cuenta bancaria y se lo entrega al estafador, que lo compensa con una determinada cantidad de dinero por el uso de la cuenta corriente.

Relata que al presentar el reclamo correspondiente al Banco con fecha 06 de diciembre de 2017 por las transferencia o traspasos de dinero no autorizadas por su parte, el Banco resuelve con fecha 08 de enero de 2018, acompañando resolución en el otrosí, que: " habiendo realizado con particular atención los antecedentes disponibles, se corroboró que las mencionadas transferencias fueron realizadas habiendo ingresado previamente el RUT de la empresa, luego el Rut del apoderado de la empresa Nª 7.255.489-2 (que le pertenece) y la clave personal a Banconexion), así como también el Código Digippass perteneciente al apoderado autorizado de la empresa. Del mismo modo, no existen indicios que permitan señalar que en la materialización de dichas transferencias se hubieren vulnerado infraestructura o sistemas informáticos del Banco Chile, de manera que las transferencias se encuentran correctamente efectuadas." Cabe hacer notar del documento referido, Uno.- "que las transferencias objetadas se realizaron de acuerdo al siguiente detalle: la hora de las transferencias es de 11:43:25; 11: 43: 29 y 11: 43: 33, es decir, se tardaron la transferencias un total de 8 segundos". Dos.- Agrega que " una vez agendado el beneficiario, y a fin de autorizar la transacción que se efectué, deben transcurrir 15 minutos desde cada agendamiento que se haya materializado exitosamente, los que en este caso se realizaron de acuerdo al siguiente detalle: Rut beneficiario 12.241.878-2, fecha 05/12/2017, hora: 09:53:25 ?????", no entendiendo esta parte, si las transferencias se realizaron a partir de las 11:43: 25 horas ¿¿¿ cómo se puede autorizar a las 09: 53: 25 horas AM. El traspaso de dinero ???. Señala el Banco que cada autorización tarda 15 minutos, entonces la primera tardó una (1) hora; tampoco en la Resolución del Banco señala que paso con las otras dos transferencias.

Acompaña jurisprudencia que establece criterios de la Corte de Apelaciones que establece la responsabilidad del Banco en todos estas Estafas informáticas, citando además, en cuanto al derecho, el numeral 24 del artículo 19 de la Constitución Política de la República, artículo 3, 12 y 23 de la Ley 19.496 sobre protección de los derechos de los consumidores; además del artículo 1 del DFL N° 707 sobre cuentas corrientes bancarias y cheques, artículo 602 del Código de Comercio, artículo 1489 y 1558 del Código Civil, indicando finalmente que el Banco de Chile ha dejado de cumplir con el contrato firmado por las partes y ha actuado negligentemente al no proteger los dineros de su empresa depositado en la cuenta corriente; la pérdida patrimonial producto del fraude permitido por el Banco, perjudican gravemente a su empresa.

Concluye su presentación solicitando en definitiva, condenar al Banco a la restitución de los dineros defraudados por tercero ajeno desde la cuenta corriente de la empresa, con indemnización de perjuicios, más reajustes, intereses y costas.

Tercero: Que con fecha 04 de abril de 2018 (F.11), comparece Benjamín Jordán Astaburuaga, abogado, en representación del Banco de Chile, contestando la demanda y solicitando su total rechazo, con expresa condena en costas.

Indica en primer lugar que se debe dejar establecido que del relato de

los hechos contenido en la demanda, se puede advertir desde ya, que el representante legal de la empresa demandante no se encontraba en la página web que el Banco de Chile pone a disposición de los usuarios que utilizan el sistema Banconexion para empresas, pues al indicar que la página le indicó que se estaba actualizando el sistema, es evidente que se trataba de un sitio web distinto, cuestión que jamás ha aparecido en el sitio web del Banco de Chile, agregando en segundo lugar, que se debe tener presente que en el caso de autos, las tres transacciones impugnadas fueron ejecutadas desde la sesión privada en internet de la empresa demandante, a través del sitio web que el Banco ha establecido para este tipo de clientes, denominado Banconexion, ingresando en línea, en el sitio privado de Internet de la empresa, al que sólo se puede ingresar: 1) digitando el Rut de Mecagri-Chile E.I.R.L., 2) luego el número de la cédula de identidad de su representante legal, don Emiliano Zelada Silva, 3) además con la clave secreta de la empresa, la que es creada por su administrador y, 4) adicionalmente, de la utilización de su "clave dinámica" que es generada por el mecanismo denominado "digipass". Todos estos elementos son de conocimiento y uso exclusivo de la demandante, los que se encuentran además bajo su custodia personal.

Añade que, mediante la aplicación de esos sistemas – doble clave- no cabe sino concluir que el Banco cumplió lo pactado con su cliente y, además, que proveyó a éste de todos los mecanismos de seguridad que la Superintendencia de Bancos e Instituciones Financieras y la lógica prevén para la realización de este tipo de transacciones; mismos que todo Banco a nivel mundial entrega a sus clientes, todo lo anterior, según lo previsto en los contratos suscritos al efecto, normativa aplicable a esta especie de transacciones y prueba que se rendirá al efecto (log o registro de transacciones), debiendo hacer constar aquí que esa normativa previene en la materia, en síntesis, dos cuestiones completamente diversas: la primera, consiste en la intervención directa y por parte de terceros de la página web del Banco y, la segunda, la intervención de terceros, ya no de la página web del Banco, sino del computador o pantalla del cliente o usuario, bajo la modalidad denominada "phishing" u otra similar.

Asevera que para evitar lo primero – intervención por terceros de la página web del Banco y, por ende, suplantación a través de ella del cliente- el Organismo Supervisor dispone que "el sistema debe proveer un perfil de seguridad que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, además, la privacidad o confidencialidad de la información transmitida o procesada por ese medio", siendo la finalidad de lo anterior, que los procedimientos empleados "impidan que tanto el originador como el destinatario, en su caso, desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse claves y mecanismos de acceso al sistema y al tipo de operación, que permitan asegurar su autenticidad e integridad"; esto es, que no haya intervención alguna de terceros en la comunicación entre el banco y el cliente, este último obrando con sus claves. Como se desprende de la norma, de la que derivan los contratos, no se trata de un pacto en beneficio exclusivo del Banco y en perjuicio del cliente, sino de garantizar el funcionamiento del sistema bancario y financiero (1) si concurren la autenticidad de las claves y (2) la integridad en la comunicación entre cliente y banco.

Aclara que los sistemas electrónicos del Banco son inviolables y no han sido intervenidos por terceros, dejando asentado que en el caso que se relata

en la demanda no existió intervención de terceros a la página web del Banco de Chile, por consiguiente la transferencia señalada no ocurrió por debilidad del sistema o por negligencia de su representado.

Relata que la segunda cuestión prevista por la normativa, pero completamente diversa de la anterior es la intervención de terceros, ya no de la página web del Banco y por ende de la comunicación entre ambos, sino del computador, pantalla o sistema empleado por el cliente o usuario, bajo la modalidad del "phishing" antes descrito u otra similar; operación en la que el delincuente le hace creer al cliente, mediante una página similar a la del Banco, que es éste quien le requiere información, y aquel le da a conocer sus claves y todos los demás antecedentes necesarios para operar en la página oficial, la que efectivamente es utilizada con esa información por los terceros, siendo el caso que la página del Banco no ha sido vulnerada, sino que es el cliente quien ha proporcionado a terceros los medios dados por el Banco –secretos, personales intransferibles y bajo su exclusiva custodia – para su autentificación, existiendo por tanto una comunicación íntegra y "auténtica" para estos efectos entre el Banco y el cliente, con la salvedad de que quien opera las claves no es el titular sino un tercero a quien éste se las proporcionó.

Indica que en este caso la página oficial del Banco sigue contando con una plataforma tecnológica que comprende una encriptación sólida, igualmente se aplican a lo menos dos factores de autentificación distintos para cada transacción y siendo uno de ellos de generación o asignación dinámica. Sin embargo, lo que ha ocurrido es que el cliente, custodio de sus claves, se las ha proporcionado – probablemente en forma inadvertida- a un tercero, pudiendo observarse aquí que ya no estamos frente a un problema de autenticidad de la comunicación o de violación de la página del Banco o de la encriptación, sino simplemente ante el mal uso que terceros hacen de las claves confidenciales del cliente, quienes pese a las advertencias expresas de los Bancos, se las han dado a conocer.

Agrega que en el relato de la demanda, se afirma que en contra de la sociedad demandante se configuró la estafa informática de phishing y pharming, lo que se entiende como un hackeo a la cuenta corriente, sin embargo esta no es la concepción de ese tipo de estafa informática, en efecto, a través del phishing, no se produce un hackeo a la cuenta corriente a través de la página web del banco, sino que se realiza un engaño al propio cliente, quien ingresa sus datos personales y claves secretas en un sitio web distinto, entregando entonces esos datos y contraseñas a terceros, quienes ingresan al sitio web oficial del Banco, premunidos de las claves secretas del cliente, por lo que pueden operar en ellas. El banco no es engañado por terceros, sino que esto lo sufre el cliente, quien entrega sus datos personales como número de Rut y sus claves secretas a un tercero, por lo que, pareciera que el representante legal de la demandante se enfrentó a este segundo caso, pues señala haber ingresado al sitio web del Banco y que se le habría advertido que el sistema se estaba actualizando, cuestión que jamás ha acontecido en el sitio oficial, por lo que podemos deducir que ingresó a un sitio distinto, en el que efectivamente escribió sus datos personales y claves secretas. En todo caso esta parte niega que esto haya ocurrido efectivamente, por lo que será cargo de la actora acreditar haber sido víctima del phishing de terceros.

Refiere en todo caso, que para poder autorizar las transferencias electrónicas el Banco debe proveer inmediatamente una "clave dinámica", que en tiempo inmediato es generada por el dispositivo digipass, para que se

digite en la página del Banco y sólo así la transacción sea autorizada. Si el cliente, por obra del phishing o de otro ardid, también la da a conocer al tercero al cual en forma previa dio a conocer sus claves, quien la ocupa, no hay responsabilidad alguna para el Banco, porque en tal caso concurren la integridad y autenticidad de la comunicación conforme a los sistemas empleados y, adicionalmente, cumplió con su obligación de emplear un doble elemento de seguridad, en este caso proporcionar una clave dinámica. Debemos advertir, que sin ingresar esta clave dinámica en la página web del Banco dentro de un determinado lapso de tiempo, falta entonces un elemento para la autenticidad de la operación, por lo que la transacción no es autorizada.

Señala que, en todo caso y para evitar que los clientes del Banco sean víctima de "phishing", se aconseja a todos ellos descargar la aplicación Trusteer Rapport, software número uno en seguridad para la banca online, que el Banco de Chile, preocupado por la seguridad en las operaciones a través de Internet, en el mes de agosto de 2012 puso a disposición, en forma gratuita a todos sus clientes, la cual le permite detectar si el sitio ingresado es efectivamente del bancochile.cl, y protege al equipo computacional desde el cual se descargó la aplicación. Ni la sociedad demandante, ni su represente legal tenían descargado en su computador este sistema. Si lo hubiera instalado anteriormente, este sistema le habría alertado que ingresaba a una página que no correspondía al Banco de Chile. Reiteramos que el Banco ha puesto a disposición de todos sus clientes, en forma gratuita, este sistema.

Enseguida añade que, conviene precisar que al Banco de Chile no consta, en modo alguno, 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, correspondiendo también hacer presente que los sistemas de seguridad del Banco en este caso no han sido 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; de modo tal las transferencias no se ejecutaron vulnerando el sistemas de seguridad del Banco, como lo sostiene la actora. Por consiguiente, en este aspecto, corresponde dejar establecido que ninguna deficiencia, omisión o error administrativo ha presentado el sistema del Banco.

Por último, deja constancia que en todas las operaciones cuestionadas concurrieron las claves personales de la empresa demandante y la clave dinámica generada por su dispositivo digipass, según consta de los registros o log, de modo tal que conforme a la normativa y contratos aplicables la comunicación además fue "auténtica". Es decir, la transferencia se efectuó con las claves personales e intransferibles de la empresa, todas de su creación y bajo su custodia, haciendo presente asimismo, que es importante señalar que es un hecho no controvertido que la empresa demandante es cliente del Banco de Chile y suscribió con éste sendos contratos para la operatoria de la cuenta corriente, mediante los canales de Autoatención, entre los que se encuentran las transferencias electrónicas de fondos. La empresa demandante celebró con el Banco un contrato denominado Contrato Unificado de Productos de Empresas Versión 9 y otro denominado Banconexion Web, los que regulan en forma íntegra las relaciones entre las partes del juicio.

Cita en lo que interesa a objeto de esta litis, el Contrato Unificado estipula en su Capítulo VI.: "Convenio de servicios mediante uso de canales de autoatención.", indicando que se debe tener claro que las claves son conocidas únicamente por el cliente y por el contrario desconocidas para el Banco. La obligación del Banco es tener los sistemas de comunicación que le permitan al cliente, en cualquier momento, ordenar el bloqueo de los sistemas de autoatención, y en la cláusula 5 y que dice relación a los efectos del uso de estos sistemas de autoatención y de las claves secretas, se deja establecido que se equipara a la firma manuscrita y que produce los mismos efectos, debiendo entender el Banco que el uso de ella importa que la transacción ha sido debidamente autorizada por el cliente, añadiendo que por otro lado la empresa demandante suscribió con el Banco, además un contrato denominado Contrato de Autoservicio Bancario Banconexión Web, con fecha 4 de mayo de 2012, citando algunas de sus cláusulas, dentro de las cuales, se regula además, lo que se denomina firma electrónica secreta, necesaria para el acceso vía internet a la página del Banco, cuyos elementos son el número de Rut del cliente, en este caso de Mecagri-Chile E.I.R.L., el Rut del usuario, es decir, de don Emiliano Zelada Silva y una clave secreta que es de conocimiento únicamente del mismo. En este mismo sentido, adicionalmente, para ciertas funcionalidades, entre las que se encuentran las transferencias electrónicas, se solicita una clave dinámica y personal, que es generada por un dispositivo que es de uso exclusivo del cliente, que se conoce como digipass. En estas cláusulas se explicita que la firma electrónica es de uso personal del cliente y de su exclusiva responsabilidad, por consiguiente éste se hace responsable de su custodia y del uso que se le dé, haciendo presente que el propio señor Zelada Silva, se designó como administrador de la cuenta de la empresa en el sistema de Banconexion.

Relata que en su rol como administradora, don Emiliano Zelada Silva se autodefinió como usuario del servicio, con facultades para crear nuevos destinatarios y realizar transferencias de fondos de la cuenta corriente, con los límites que estableció en la misma oportunidad, los que son ampliamente superiores a las transferencias objetadas, es decir, el señor Zelada Silva, fue establecido por el administrador del sistema Banconexion, en este caso él mismo, como un apoderado que podría crear nuevos destinatarios y transferirles sumas de dinero muy superiores a las que son objeto del presente juicio. Para este proceso de configuración el sistema exige la clave que el administrador utiliza en el canal, que es creada por el mismo. Adicionalmente, el señor Zelada Silva, también configuró la opción de agregar nuevos beneficiarios de transferencias.

Reseña que así las cosas, mediante la sesión electrónica del señor Zelada, a la que se accedió a través del sistema Banconexion de Mecagri, ingresando sus claves secretas dispuestas al efecto y que constituyen su firma electrónica, se creó el nuevo destinatario de transferencias electrónicas, funcionalidad para la cual estaba expresamente facultada esta persona, digitando su clave secreta, además, desde esta misma sesión, horas después de haber creado a los destinatarios y, utilizando el digipass de la empresa, que se encontraba bajo su custodia, se autorizaron las transferencias que se objetan en la presente causa, por montos inferiores a los límites que tenía el señor Zelada para operar en la cuenta.

Asevera que otro antecedente importante es que la creación de los destinatarios de las transferencias electrónicas antecedió por horas la realización de ellas, tal como se sostiene en la propia demanda y de acuerdo a los hechos en que se funda la demanda que se contesta y los agregados al

contestarla, la cuestión a dilucidar, entonces, consistente en precisar si existe un incumplimiento contractual y la subsecuente responsabilidad civil del Banco, aun considerando la autenticidad de la comunicación entre éste y su cliente, configurada de la forma dicha, en otras palabras ¿de cargo de quién es la pérdida, cuando concurriendo la "autenticidad contractual y normativa", como ocurre en este caso, ella –presuntamente– no es coincidente con la voluntad del titular, porque las claves habrían sido ocupadas por un tercero?.

Indica que la respuesta, como veremos, es que en tales casos la pérdida monetaria es de cargo del cliente y por una razón muy obvia – superior y ajena al interés particular del Banco – cual es, la de permitir o posibilitar el funcionamiento del sistema bancario y financiero, en algunos de cuyos productos u operaciones, entre los que se cuentan las transacciones a distancia, rige el principio de la apariencia por sobre el de la realidad, lo que significa que prima "la autenticidad" de la firma del titular, dada por el uso de sus claves, por sobre la voluntad real del mismo, en caso de ser esta diversa, principio que emana de la propia Ley de Cuentas Corrientes Bancarias y Cheques y de la Ley de Letras de Cambio y Pagarés, entre otras, cuyo objetivo esencial es permitir el funcionamiento del sistema, debiendo precisar que lo establecido en el contrato precitado, no se trata de un pacto en beneficio exclusivo del Banco y en perjuicio del cliente, sino que para garantizar el funcionamiento del sistema bancario y financiero si concurren la autenticidad de las claves entregadas al cliente.

Añade que teniendo presente los antecedentes expuestos y, considerando que la acción interpuesta en esta causa desconoce por completo la función económica del contrato cuenta corriente y de los principios legales que rigen su operatoria –dados por la Ley de Cuentas Corrientes Bancarias y Cheques y normas impartidas por la Superintendencia de Bancos e Instituciones Financieras– oponen a la demanda de autos las siguientes excepciones y defensas:

a) La demanda no señala cuál sería la obligación infringida, ni cuál contrato la establece

Indica que el actor se limita a efectuar un breve relato de los hechos y citar una serie de normas jurídicas que no tienen conexión entre sí, ni que tampoco sirven de sustento a la acción de responsabilidad contractual que ejerce. Así, ni la norma constitucional invocada, ni aquellas contenidas en la Ley Nº 19.496 sobre protección de los derechos de los consumidores tienen aplicación en la presente causa, por responsabilidad contractual. Por otro lado, el actor se ha limitado a señalar que el contrato de cuenta corriente habría sido infringido por parte del Banco de Chile, pero no se invoca cuál es la obligación específica de este contrato que se habría incumplido, es más, ni siquiera se hace mención alguna a los contratos que hemos relatado anteriormente, que son el Unificado de Productos de Empresas y el Banconexion Web, por lo que debemos entender que el actor dirige su reproche al contrato de cuenta corriente regulado por la ley.

Agrega que, no obstante el contrato de cuenta corriente no impone ninguna obligación de custodia de los dineros por parte del banco, toda vez que estos le son entregados mediante un depósito irregular, título translaticio de dominio, por el cual se hace dueño de los mismos y no pesa sobre él la obligación de restituirlos. En efecto, la única obligación que el contrato de cuenta corriente impone al banco es aquella establecida en el artículo 1º del DL 707, que señala: "La cuenta corriente bancaria es un contrato a virtud del cual un Banco se obliga a cumplir las órdenes de pago

de otra persona hasta concurrencia de las cantidades de dinero que hubiere depositado en ella o del crédito que se haya estipulado.", reiterando que no existe una obligación de custodia sobre los dineros depositados por la empresa demandante, razón por la cual la demanda ha sido mal interpuesta, pues se funda en el incumplimiento de una obligación que no existe, de manera que debe ser rechazada en todas sus partes, con expresa condena en costas.

b) No existe infracción a ninguna obligación de los contratos celebrados

La actora pretende hacer responsable al Banco de Chile de las transacciones ejecutadas mediante claves y dispositivos válidos, entregados al representante legal de la empresa, alegando la supuesta existencia de un fraude, hecho que por cierto no es efectivo ni consta en modo alguno, porque se utilizaron los datos de la empresa y de su representante, además de la clave secreta creada por éste y adicionalmente se autorizaron las transferencias con la clave generada por el dispositivo digipass.

Refiere que en el supuesto incluso que las transferencias se realizaron mediante la comisión de un delito; esto es que terceros utilizaron la firma electrónica personal de la empresa sin su consentimiento, nada tiene de particular que igualmente sea responsable de las transacciones cuestionadas; esto es, que se entienda que la transacción fue ejecutada por la propia cuenta correntista, porque no sólo el contrato así lo establece, sino también la propia Ley de Cuentas Corrientes Bancarias y Cheques. En efecto, esta última hace responsable al Banco o al titular, del pago de un cheque con firma falsificada – no suscrito ni autorizado por el titular – dependiendo, según los casos, de si la firma de giro es o no visiblemente disconforme. Si la firma de giro es falsificada pero visiblemente conforme con la del titular, el Banco no es responsable del pago del cheque, pese a que de acuerdo a las normas civiles generales no concurre en la especie el consentimiento del titular para considerar que existe una orden de pago. Así por lo demás se desprende de los artículos 16 y siguientes de la Ley de Cuentas Corrientes Bancarias y Cheques.

c) Imposibilidad de acoger la demanda porque no tiene peticiones concretas.

La demanda que se contesta no puede ser acogida, toda vez que ella no tiene peticiones concretas, pues se pide que se decrete el cumplimiento forzado de un contrato, pero sin explicar a qué prestaciones deben ser condenadas las partes. Por otro lado se pide que se decrete el cumplimiento con indemnización de perjuicios que se deberá fijar, esta petición es derechamente inadmisible, puesto que era la actora la que debía consignar con toda claridad en el petitorio de la demanda cuál es la suma que reclamaba como indemnización de perjuicios, cuestión que no hizo y que por lo tanto no podrá ser objeto de discusión, sin incurrir en el vicio de ultrapetita.

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

Indica que la teoría del caso de la parte demandante se funda en la mera palabra del cliente contra la palabra documentada del Banco de Chile, validada la de aquel con una simple denuncia y la del Banco con el certificado de la empresa Symantec, tercero ajeno, que se acompañará oportunamente acerca de la inviolabilidad de sus redes, es decir el incumplimiento contractual imputado solo se "comprueba" o "acredita" con la simple palabra del representante de la empresa demandante, quien afirma no haber

efectuado las transferencias en cuestión y, por ende, que las redes de comunicación del Banco fueron vulneradas por delincuentes, según consta de su propio relato en el libelo y, sobre esas única base -mera aserción de haber sufrido una estafa-pretende que por esta vía se condene a su parte al cumplimiento forzado del contrato.

Reitera que lo grave del caso es que fundado en la mera aserción de vulnerabilidad de las redes y en la presunta existencia de un delito, se pretende hacer al Banco responsable de la pérdida del dinero, en circunstancias que el Banco tiene constancia que las transferencias fueron efectuadas con las claves secretas de la empresa demandante y tiene una certificación de la inviolabilidad de su sitio web. Es decir, se pretende hacer responsable a su representado sobre la única premisa de que en la especie habría tenido lugar un delito en perjuicio de la actora, que pretende justificarlo mediante la simple afirmación de la existencia de un delito en su contra.

Cuarto: Que con fecha 14 de junio de 2018 (F.24) se lleva a cabo audiencia de conciliación. Llamadas las partes a conciliación esta no se produce.

Quinto: Que con fecha 27 de junio de 2018 (F.27) se recibe la causa a prueba, fijándose como hechos substanciales, pertinentes y controvertidos los siguientes: 1.- Efectividad de haber sufrido la demandante un acceso no autorizado a su cuenta bancaria, y que producto del mismo, se efectuaron uno o más giros de dinero de su propiedad. Hechos y circunstancias que lo acrediten. 2.- En la afirmativa del punto previo, efectividad de haberse provocado el acceso no autorizado por falencias técnicas de seguridad, en los sistemas informáticos de manejo de cuentas bancarias de la demandada, todo ello, en infracción al contrato de cuenta corriente celebrado entre las partes. Hechos y circunstancias que lo acrediten. 3.- En la negativa del punto previo, efectividad de haberse provocado el acceso no autorizado por el actuar negligente, o bien, imprudente de la actora, ello, en el manejo de los dispositivos de seguridad y claves de acceso de sus cuentas bancarias. Hechos y circunstancias que lo acrediten. 4.-En la afirmativa de los puntos uno y dos, efectividad de haberse causado perjuicios a la actora, en razón de los hechos alegados. Naturaleza y monto de los mismos. 5.- En su caso, efectividad de existir relación de causalidad entre la conducta de la demandada, el resultado acaecido y los perjuicios que se demandan.

Sexto: Que la parte demandante, a fin de acreditar sus pretensiones, incorporó la siguiente prueba:

<u>Documental</u>:

1. Escritura de constitución de la Sociedad MECAGRI LTDA, con citación (Al folio 1);
2. Resolución del Banco del reclamo de la sustracción de dinero de la cuenta corriente de fecha 08 de enero de 2018, bajo apercibimiento del artículo 346 n° 3 del Código de Procedimiento Civil (Al folio 1);
3. Circular N° 3.451 de 2008 de la Superintendencia de Bancos e Instituciones Financieras, con citación (Al folio 1);
4. Contrato Servicios Banco, (Al folio 1);
5. Cartola Cuenta Corriente, (Al folio 1);
6. Jurisprudencia sobre Banco Edwards-Chile, (Al folio 30);
7. Jurisprudencia, Estafas Informáticas, (Al folio 30);
8. Jurisprudencia Banco Chile año 2012, (Al folio 30);
9. Multa aplicada a Banco, (Al folio 30);
10. Oficio N° 60-2009, párrafo 11 donde se informaba a los fiscales de los

delitos informáticos y medidas que debían realizar en las investigaciones, (Al folio 30);

11. Recurso de Protección de doña Stephanie Nannig Tuchie, deduce en contra de Banco de Chile año 2017, (Al folio 30);

Séptimo: Que el demandado, a fin de desvirtuar la pretensión de la actora, incorporó la siguiente prueba:

Documental:

1. Contrato Unificado de Productos de empresas versión 9, que corresponde al suscrito por la empresa demandante, (Al folio 36);
2. Certificados emitidos por la empresa Neosecure, que dan cuenta que ni la empresa demandante, ni su representante legal habían descargado el software Rapport de Trusteer, que el Banco de Chile dispone gratuitamente para sus clientes y que advierte ante la posibilidad de ser víctima de phishing, (Al folio 36);
3. Cuadro con las facultades del apoderado, Emiliano Zelada Silva, para operar en el sistema Banconexión de la empresa demandante, que acreditan que se encontraba facultado a ejecutar las operaciones por montos muy superiores a los que corresponden a las transferencias objetadas, con citación (Al folio 36);
4. Certificado emitido por la empresa Symantec, sobre la inviolabilidad del sitio web del Banco de Chile, con citación (Al folio 36);
5. Hoja de firma del contrato Unificado de Productos de empresas versión 9, debidamente suscrita por el representante legal de la empresa demandante, bajo apercibimiento del artículo 346 n° 3 del Código de Procedimiento Civil (Al folio 36);
6. Contrato Banconexión web suscrito entre las partes del presente juicio, bajo apercibimiento del artículo 346 n° 3 del Código de Procedimiento Civil (Al folio 36);
7. Carta de objeción de cargo en cuenta corriente, debidamente suscrita por el representante legal de la empresa demandante, bajo apercibimiento del artículo 346 n° 3 del Código de Procedimiento Civil (Al folio 36).

Octavo: Que ambas partes solicitaron y rindieron prueba pericial, consistente en el informe de doña Karen Alaluf, perito ingeniero mención computación, agregado al folio N° 110 d con fecha 12 de noviembre de 2019, quien indicó como conclusiones las siguientes:

"Respecto de la pregunta: que ilustre al Tribunal sobre la forma en que se realizaron las transferencias electrónicas de fondos que ha objetado el demandante en el presente juicio, estableciendo especialmente a través de qué medio se efectuaron y cómo fueron autorizadas cada una de ellas: Basado en lo desarrollado en el informe este perito puede informar que las transferencias de fondos objetadas por el demandante en el presente juicio fueron realizadas mediante el medio computacional de Computador Personal ingresando al sitio WEB del Banco de Chile, denominado Banconexion Versión 1.0. La forma en que fueron autorizadas dichas transacciones fue utilizando el Rut de La empresa (76902400-K), el Rut del usuario autorizado (7255489-2) la clave de ese usuario validados para realizar los pasos de Pasos de Inscripción y Autorización. Además para el paso final que libera los fondos y envía dichos dineros a la Cuenta bancaria que los recibe se agregó al empresa (76902400-K), el Rut del usuario autorizado (7255489-2) la clave de ese usuario validada el numero aleatorio de 6 dígitos que entrega el dispositivo DIGIPASS que debe coincidir en ese momento con el proceso de seguridad del banco.

Respecto de la pregunta: Asimismo el perito deberá informar si terceros vulneraron el sistema de seguridad del Banco para realizar tales transferencias, consignando si el Banco cumplió o no con las normas que establecen los contratos y normativa aplicable al efecto: Los registros de las transacciones tal como se indicó en el punto 4 desarrollado, no tienen

vulneraciones de la seguridad, ya que registraron y validaron el ingreso de los datos correctos y autorizados para realizar transferencias de fondos de esta empresa por lo tanto se puede indicar que terceros NO vulneraron el sistema de seguridad del Banco para realizar tales transferencias. Las normas que establecen los contratos y normativas si fueron cumplidas por el banco ya que el anexo firmado por el cliente indica los Rut autorizados para realizar cada paso de una transferencia. Este anexo fue revisado por este perito del sitio Web del portal judicial en los archivos subidos en esta causa.

Respecto de la pregunta: El perito deberá informar a S.S. sobre el funcionamiento del sistema Banconexión Web que el Banco pone a disposición de sus clientes: El funcionamiento del sistema Banconexion WEB se encuentra desarrollado en el punto 1 de este informe pero en resumen consiste en: El sistema Banconexion 1.0 donde se realizaron las transacciones motivo de esta causa, funciona desde un portal WEB, es decir funciona como sitio Web en los computadores del Banco de Chile, NO se instala ningún programa o aplicación en los computadores de los clientes. Este sistema Banconexion, posee como seguridad para poder acceder a él solicita 3 datos que deben ingresarse en forma correctamente para conectarse y hacer algún tipo de consulta o transacción con las cuentas corrientes bancarias, los datos son: a. RUT EMPRESA; b. RUT USUARIO; c. CLAVE DE USUARIO. Donde en caso que la clave no sea correcta, el sistema NO PERMITE SU ACCESO. Una vez ingresados los datos anteriores en forma correcta se accede al menú que permite hacer las siguientes operaciones o transacciones: Emergencias Bancarias, Administración contrato, Administración Claves, Certificados Digitales, Comisiones Confianza, Cuentas Corrientes, Línea de Crédito, Tarjeta Visa, Selección de Filiales, Transferencias de Fondos, Pago cuentas Servicios, Pago en Otros Sitios, Pago Proveedores, Pago con Nominas, Pagos Pensiones, Proveedores, Pagos a Su favor, Factura Electrónica, Recaudación Cuotas, Fin de Sesión.

Noveno: Que en la presente causa se ha interpuesto acción de cumplimiento de contrato e indemnización de perjuicios, por responsabilidad contractual, alegando la demandante que la demandada habría incumplido sus obligaciones al actuar con negligencia en relación a los dineros de la actora, depositados en la cuenta corriente mantenida en el Banco de Chile, de la cual fue retirada la cantidad que indica.

Al efecto era indispensable que se acreditara ese incumplimiento en el cual se funda la demanda de autos, el cual consiste, conforme lo indicado en los números 1 y 2 de la resolución que recibió la causa a prueba, en haber sufrido la actora un acceso no autorizado a su cuenta bancaria, y que producto del mismo, se efectuaron uno o más giros de dinero de su propiedad, y que dicho acceso se produjo por falencias técnicas de seguridad, en los sistemas informáticos de manejo de cuentas bancarias de la demandada, todo ello, en infracción al contrato de cuenta corriente celebrado entre las partes.

La parte demandante acompañó la cartola de la cuenta corriente que mantiene en la institución bancaria demandada, correspondiente al mes de diciembre del año 2017, en la cual aparece que el día 5 de ese mes y año se efectuaron tres transferencias por la suma de $4.999.999 a una misma persona, indicada como Rene la court. El resto de la prueba rendida por la actora dentro de plazo legal, no dice relación con estas transferencias.

El peritaje rendido en estos autos, emitido por la perito Karen Alaluf, concluye que esas tres transferencias. que constan de la cartola acompañada por la parte demandante, fueron efectuadas sin vulneración del sistema

bancario de protección de la demandada, con acceso desde la cuenta de la sociedad demandante y con utilización de sus claves para la validación de la transacción

Del resto de la prueba rendida dentro de plazo legal no hay antecedentes que acrediten la injerencia de terceros en las transferencias detalladas en el motivo segundo de este fallo y en las que se funda la demanda.

Así las cosas, no habiéndose probado el hecho fundante de la acción, en forma y oportunidad legal, la demanda no podrá prosperar.

Décimo: Que el resto de la prueba rendida y no analizada en particular no varía lo concluido.

Por lo expuesto y visto, además, lo dispuesto en los artículos 1437, 1438, 1441, 1489, 1545, 1556, 1557, 1698 y siguientes, todos del Código Civil; artículos 144, 160, 170, 327, 342, 346, 348, 425 todos del Código de Procedimiento Civil; **se declara:**

1.- Que se rechaza la objeción de documentos opuesta por la parte demandante en la presentación agregada en el folio 38.

2.- Que **se rechaza**, en todas sus partes, la demanda interpuesta por Emiliano Zelada Silva, en representación de Mecagri-Chile E.I.R.L., en contra del Banco de Chile, representada por el agente Jaime Cáceres López, todos ya individualizados.

3.- Que cada parte pagará sus costas.

Regístrese, notifíquese y archívese en su oportunidad.

Dictada por Alexandra Yáñez Jara, juez del Juzgado de Letras de Casablanca.

Se deja constancia que con esta fecha se dio cumplimiento a lo dispuesto en el artículo 162 del Código de Procedimiento Civil.