FOJA: 57 .- .-

NOMENCLATURA : 1. [40]Sentencia
JUZGADO : 25º Juzgado Civil de Santiago
CAUSA ROL : C-29061-2019
CARATULADO : HALPERN/BANCO SANTANDER - CHILE

Santiago, treinta y uno de Agosto de dos mil veintidós

VISTOS:

En folio 1, compareció don JOSÉ MIGUEL MEDINA LARRAÍN, RUT N°17.628.561-3, abogado, en representación judicial de doña NICOLE HALPERN MAGER, RUT N°15.958.860-2, psicóloga, ambos domiciliados para estos efectos en Av. Américo Vespucio Sur N°1982, Depto. 203, comuna de Las Condes; quien, en la representación investida, dedujo en juicio ordinario de menor cuantía, una acción de cumplimiento de contrato, en contra del BANCO SANTANDER-CHILE, representado legalmente por su gerente general, don MIGUEL MATTA HUERTA, ambos domiciliados para estos efectos en calle Bandera N°140, comuna de Santiago; en virtud de los hechos y fundamentos de derecho que se reproducen a continuación:

LOS HECHOS:

1) El ilícito:

Sostuvo que su representada es clienta del Banco Santander, en el cual al día de hoy mantiene cuenta una corriente cuyo número es el 73027160. En este contexto, con fecha 7 de noviembre de 2018 la Sra. Halpern recibió un llamado de una persona que se identificó como colaborador del ejecutivo de cuentas del Banco Santander que monitorea su cuenta corriente. Esta persona, identificada como Francisco Morales, procedió a mencionar toda su información personal y confidencial con el fin de demostrar que efectivamente era quién decía ser. Entre la información que manejaba sobre su persona, estaba: nombre completo, RUT, dirección personal, nombre de su ejecutivo de cuenta corriente, número de su cuenta corriente y número de su tarjeta de coordenadas (utilizada para autenticarse en operaciones bancarias). Hecho esto, utilizando como pretexto la actualización de la aplicación del Banco Santander, procedió a solicitar

números de su tarjeta de coordenadas. Considerando la validación que efectuó quien decía llamarse Francisco Morales, la Sra. Halpern accedió a entregar la información requerida. Con ella, se realizaron sin su autorización las siguientes operaciones el mismo día 7 de noviembre de 2018: a) Transferencia de crédito a pasivo en su cuenta corriente por la suma de $6.000.000; b) Transferencia electrónica por $100.000, a las 12:53 horas; c) Transferencia electrónica por $1.600.000, a las 12:58 horas; d) Transferencia electrónica por $1.700.000, a las 12:59 horas; y e) Transferencia electrónica por $1.600.000, a las 13:01 horas; señaló.

Refirió que la persona que vulneró los sistemas de seguridad del Banco Santander solicitó un crédito consumo a nombre de su representada por $6 millones y procedió a transferir 5 de ellos a tres cuentas distintas del Banco Estado, ninguna de las cuales pertenecen, o tienen relación alguna con la demandante.

Indicó que, una vez que se percató de éstos ilícitos, ese mismo día 7 de noviembre, la demandante a las 17:50 denunció el ilícito en la 17° Comisaría de Las Condes bajo el número 10331705. Asimismo, suscribió acta de reconocimiento de especies por la suma de 5 millones. Ese mismo día también notificó al Banco Santander de los hechos y procedió a requerir de inmediato la restitución de los dineros que le corresponden, indicó.

Alegó que nunca en su historial de actividades con el Banco Santander su representada ha solicitado un crédito de consumo por una suma semejante para proceder a transferirla casi inmediatamente a cuentas distintas del Banco Estado, por medio de transferencias sucesivas. Sumado a ello, nunca ha realizado transferencias sin individualizar debidamente a los receptores. El detalle de transferencias emitido por el Banco Santander indica que los destinatarios de las transferencias son “Diego”, “Cxt” y “Wawa”. Además, las transferencias se realizaron desde un dispositivo cuya dirección de IP nunca pudo relacionarse al uso de su representada de sus productos bancarios, refirió.

Sostuvo que, adicionalmente, al día de hoy existe un proceso penal vigente contra tres personas, imputadas por el delito de estafa residual contemplado en el artículo 473 del Código Penal, en grado de ejecución consumado. La causa es seguida ante el 4° Juzgado de Garantía de Santiago bajo el RIT 3805-2019 y actualmente se encuentra fijada audiencia de juicio oral simplificado para el próximo día 29 de agosto de 2019, mencionó.

2) Tramitación de seguro de fraude:

Afirmó que, ante esta situación, dentro de plazo su representada suscribió “formulario único de siniestro fraude canales a distancia transacciones no reconocidas en cuenta corriente” del Banco Santander. Al siniestro se le asignó el número 443061 en la aseguradora Zurich Santander Seguros Generales Chile. Así, con fecha 29 de noviembre de 2018, la aseguradora emitió informe de liquidación número 122704. En él, realizó el siguiente razonamiento: “En el presente caso y de acuerdo al relato de los hechos, el asegurado no cumple con su obligación, ya que incurre en una infracción a su deber de diligencia para prevenir el siniestro, cuando entrega en forma voluntaria las combinaciones de su tarjeta de coordenadas a terceros desconocidos, sin tomar los resguardos necesarios.”, según citó.

Expuso que, en consecuencia, por disposición del Banco Santander a su representada no se le restituyó suma alguna, lo que significó ser defraudada definitivamente por la suma de $5 millones. Esto, sin perjuicio que fue engañada por una persona que manejaba sus datos personales y confidenciales; y que se realizaron las acciones en su cuenta corriente vulnerando estándares de seguridad mínimos exigidos por la Superintendencia de Bancos e Instituciones Financieras. Esta situación, obligó a la demandante a recurrir a la vía judicial.

EL DERECHO:

1) Sostuvo que la demandante no ha actuado negligentemente:

Al respecto, indicó que recientemente la Excma. Corte Suprema ha descartado la negligencia de la víctima de una estafa de similares características, puesto que existían “antecedentes demostrativos de patrones de fraude”, entre ellos “falta de habitualidad de las operaciones que se ejecutan de forma inmediata” y “[falta de] una dirección IP asociada al uso de dispositivos”. En ese mismo pronunciamiento, el máximo Tribunal agregó que “las obligaciones de monitoreo y control de fraudes recaen expresamente en la institución recurrida”, según citó.

Alegó que, como fue mencionado en los hechos, en el caso de autos concurrieron diversos antecedentes demostrativos de fraude. Entre ellos: a) La falta de habitualidad de las operaciones que se ejecutan: La demandante nunca ha solicitado un crédito de consumo de magnitud similar para transferirlo inmediatamente a cuentas ajenas.

Su representada, jamás ha realizado 4 transferencias consecutivas, mucho menos a destinatarios indebidamente individualizados como “Wawa” o “Cxt”; b) Falta de una dirección de IP asociada al uso del dispositivo que realizó las operaciones en cuestión. Asimismo, debe agregarse que quienes defraudaron a la demandante contaban con su información personal y confidencial. Entre ella, su nombre completo, RUT, número de teléfono, nombre de ejecutivo de cuentas, número de cuenta corriente y número de tarjeta de coordenadas.

Estimó que, en consecuencia, pese a la hipótesis sostenida por la aseguradora en su informe de liquidación, debe descartarse que la demandante haya actuado con dolo o negligencia en el caso de autos. Producto de ello, y conforme lo dispuesto en el artículo 707 del Código Civil, su buena fe debe presumirse, indicó.

2) Alegó que la demandada se encuentra en mora y procede solicitar cumpla forzadamente con su obligación correlativa de restituir la suma de dinero a la demandante:

Expuso que la demandada no ha restituido o pagado los 5 millones de pesos chilenos que pertenecen a la demandante, pese a que ella así lo ha requerido reiteradamente a contar del 7 de noviembre de 2018. El deber de entregar estos dineros que pertenecen a su representada, corresponde a una obligación del Banco Santander en virtud de lo dispuesto en el contrato de cuenta corriente que une a las partes y, en consecuencia, la demandada se encuentra en mora dado lo prescrito en el artículo 1551 del Código Civil, indicó.

Refirió que, así las cosas, habiendo además su representada cumplido sus obligaciones de buena fe y de forma diligente, según lo presume el artículo 707 y lo ordena el artículo 1546 del Código Civil, ésta se encuentra facultada para solicitar en esta sede el cumplimiento forzado de las obligaciones de la demandada, conforme lo dispuesto en el artículo 1489 del Código Civil.

Sostuvo que, en consecuencia, solicita se ordene al Banco Santander cumpla con sus obligaciones correlativas emanadas del contrato de cuenta corriente suscrito entre las partes, específicamente la de restituir o pagar a la demandante la suma de 5 millones de pesos, debidamente reajustada y con los intereses legales que correspondan.

Petitorio de la demanda: previas citas legales, solicitó que en definitiva se ordene a la demandada que cumpla su obligación

correlativa de restituir o pagar a su representada la suma de $5.000.000 (cinco millones de pesos chilenos) más intereses legales y reajustes, con costas.

En folio 6, consta el emplazamiento de la parte demandada.

En folio 7, compareció don FELIPE BARRERA SANCHO, abogado, en representación del BANCO SANTANDER - CHILE, sociedad anónima bancaria, del giro de su denominación, ambos domiciliados en esta ciudad, calle Bandera 140, comuna de Santiago; quien **contestó la demanda** entablada en contra de su mandante, solicitando su rechazo total, con costas, en virtud de las alegaciones y defensas que se reproducen a continuación:

I.- PRIMERA DEFENSA: INEXACTITUD E INEFECTIVIDAD DE LOS HECHOS FUNDANTES DE LA DEMANDA:

1.- Señaló que la exposición de hechos contenida en la presentación de la demandante es inexacta, y en lo substancial inefectiva. La veracidad de los hechos que relata no le consta ni le puede constar a su representado por cuanto no ha tenido participación en los mismos, que se refieren a un tercero desconocido que la actora afirma que la defraudó, haciéndose pasar por un funcionario del Banco. De hecho, ni la propia actora le atribuye participación a algún funcionario del Banco en estos acontecimientos, sostuvo.

Alegó que en consecuencia, su parte no puede darle crédito a la actora en este punto y ella deberá acreditar sus dichos.

Indicó que, su parte niega categóricamente que los datos de que ha dispuesto el supuesto ciber delincuente hayan podido ser obtenidos mediante la vulneración de los registros del Banco o de su sistema de seguridad.

Expuso que, por el contrario, lo que sí le consta a su parte es que el supuesto fraude, si existió, no ha tenido lugar en la plataforma que el Banco entrega a sus usuarios y desde la cual atiende a sus requerimientos, esto es desde su página web. Los sistemas del Banco no han sido vulnerados y las transacciones efectuadas cumplieron con todos los requisitos que el protocolo de seguridad exige para que pudiera dárseles curso, indicó.

2.- Expresó que, en efecto, de la investigación interna que el Banco llevó a efecto en su Departamento de Fraudes Electrónicos, área técnica y especializada en estas materias, luego de ingresado el reclamo de la actora, concluyó que los hechos denunciados no

constituyeron una vulneración a los sistemas de seguridad implementados por Banco Santander Chile para evitar fraudes en el uso y/o transacciones realizadas a través de la plataforma digital, pues se respetaron y aplicaron todas las medidas de seguridad establecidas para las operaciones de ese tipo, no existiendo responsabilidad de Banco Santander Chile en los hechos reclamados, por lo que no se pudo acceder a su reclamo. Similar parecer tuvo la compañía aseguradora que estimó que el hecho reclamado no estaba cubierto por el seguro contratado, cuestión que, en todo caso, no le empece a su parte por tratarse de una persona jurídica distinta del Banco.

Indicó que, se concluyó asimismo que, de haber existido el fraude, éste pudo materializarse mediante la captura o entrega a terceros de las claves secretas por parte de la actora a través de la intervención fraudulenta de su equipo computacional y/o de su teléfono, permitiendo el conocimiento y manipulación por parte de terceros de la información personal. Posteriormente, según vimos, la propia actora facilitó su súper clave a un tercero desconocido y ello habría permitido finalmente, la utilización correcta de sus claves y autorizaciones recibidas por el Banco como legítimas, lo que permitió que las operaciones pudieran ser materializadas, refirió.

3.- Expuso que ya es de conocimiento general y común el hecho que al no poder acceder a los sistemas operativos de los bancos, que están especialmente preparados para rechazar cualquier tipo de intervención o vulneración de sus sistemas, para lo cual cuentan con protocolos de seguridad altamente sofisticados y que operan también en el ámbito internacional bajo reglas muy estrictas, de aplicación común en los demás países del mundo, los ciber delincuentes locales optan por “cortar por lo más delgado”, esto es, vulnerar la frágil seguridad que presentan los usuarios en el manejo de sus claves y datos personales.

Indicó que es así como crean páginas web muy similares a las de los bancos a las que acceder a través de links de muy fácil utilización (un simple “click” en el supuesto logo del banco) y esperan a que usuarios descuidados ingresen a ellas y desde allí obtienen todos sus datos personales para luego utilizarlos en sus fraudes bancarios. Este sistema de fraude es comúnmente conocido como phishing (pescando), refirió.

Mencionó que los usuarios facilitan que pueda darse esta figura al no digitar en forma completa la dirección correcta de la página del Banco, incluido el protocolo https. Prefieren conectarse con un simple

“click” a estas páginas que se parecen a las verdaderas y luego caen en la ya conocida trampa citada, indicó.

Señaló que al phishing le sigue la figura del vishing, que es un tipo de estafa informática, muy similar al phishing, consistente en el uso delictivo del teléfono. Según indica su término, que proviene de la unión de dos palabras en inglés voice y phising, el ciberdelincuente, valiéndose de la telefonía, se hace pasar por una fuente fiable y alegando supuestas razones de seguridad, intenta engañar a sus víctimas para hacerse con sus datos personales. La finalidad que persigue es robarles la identidad, o bien hacerse con su información bancaria, mencionó.

Expuso que, para ello, previamente han obtenido la información básica de la víctima a través de bases de dato que están a disposición de cualquiera, a lo que se agrega la información obtenida a través del Phishing.

Indicó que otro tanto sucede con sus teléfonos celulares, que son permeados con relativa facilidad debido a los resguardos poco seguros de las empresas telefónicas que ofrecen estos servicios. En este caso las víctimas son suplantadas en su uso y reciben los mensajes y coordenadas que van dirigidas a ellas por cuanto su teléfono (normalmente celular) ha sido intervenido, refirió.

Estimó que esto es lo que pudo haber sucedido en el caso de la especie, de ser cierto lo expuesto en la demanda, lo que a su parte no le consta.

Alegó que en lo que no cabe duda es que todas estas circunstancias han podido tener lugar antes de la intervención del Banco y de sus sistemas de seguridad.

4.- Refirió que es necesario tener presente que los sistemas de seguridad que provee el Banco Santander Chile, así como cualquiera otra institución bancaria, para el uso electrónico de los productos que ofrece, están estandarizados en el sistema financiero y son regulados por la Superintendencia de Bancos. En el desarrollo de estos sistemas de seguridad se ha llegado al consenso general de que la mejor forma de resguardar la seguridad de las transacciones electrónicas es mediante la entrega de una clave personal intransferible, que solo puede ser establecida por el propio usuario y debe ser conocida únicamente por éste. Sin esta clave no es posible acceder a ninguna transacción electrónica como las que han sido objeto de la presente acción de protección, indicó.

Señaló que, en particular, el Banco Santander Chile ha implementado un sistema de seguridad para acceder electrónicamente a través de su página web a las cuentas corrientes y efectuar operaciones en ella, que puede llegar a involucrar el uso de hasta tres tipos claves de seguridad sucesivas, dependiendo de las operaciones de que se trate, según el siguiente detalle: 1) Clave secreta: Esta es la clave que el propio usuario determina y permite el acceso electrónico a la cuenta corriente a través de la página web del Banco Santander Chile. Como ya hemos visto, es de responsabilidad del usuario no darla a conocer a terceros y cambiarla regularmente para su propia seguridad. Su uso se restringe a tener acceso a la información que entregue el portal electrónico sobre los movimientos y saldos de la cuenta corriente y demás productos asociados y permite también hacer pagos y traspasos entre las propias cuentas del usuario cuenta correntista y tarjeta-habiente; 2) Súper Clave: Esta se obtiene a partir de una tarjeta que el Banco entrega al usuario al momento de contratar una cuenta corriente, la que contiene hasta 50 números distintos que se pueden relacionar aleatoriamente mediante coordenadas. Para tener acceso a ella, el usuario debe solicitarla al sistema, el que le pide aleatoriamente 3 números de los contenidos en la citada tarjeta, indicando sus respectivas coordenadas. Al examinar la tarjeta el usuario encontrará con la coordenada señalada por el sistema cada uno de los números requeridos, formando de esta manera la súper clave. Sólo puede tener acceso a esta súper clave, quien esté en posesión material de la correspondiente tarjeta. Con esta súper clave, el usuario puede operar su cuenta corriente transfiriendo fondos a destinatarios ya conocidos, esto es, a quienes antes y en forma regular se les ha transferido fondos por montos equivalentes y en un período regular, hasta determinadas sumas; 3) Clave 3.0: Esta clave es exigida por el Banco para determinadas operaciones que involucran transferencias a terceros ya conocidos de sumas de dinero más altas de lo habitual o por cualquier suma a terceros desconocidos que no hayan sido antes destinatarios de fondos. Se obtiene una vez que es requerida por el sistema, cuando detecta que el usuario quiere realizar alguna de las operaciones antes descritas. Una vez solicitada por el usuario, el sistema le envía una clave aleatoria siempre distinta a su teléfono móvil y desde allí debe rescatarla la cuenta correntista para poder operar con ella en los casos ya señalados; señaló.

5.- Sostuvo que, en la especie, en la investigación interna del Banco se pudo establecer que se instruyeron aparentemente por el titular de la cuenta diversas transferencias desde su cuenta corriente a

terceros no habituales. Siendo así, para darles curso fue necesario entonces requerir las tres claves de seguridad, y solo ingresadas correctamente las mismas pudo llevarse a efecto las transacciones que la actora reclama. Revisados el ingreso de estas tres claves, se pudo constatar que tanto la clave de acceso a la cuenta corriente, como la súper clave y la clave 3.0 fueron ingresadas correctamente al sistema y ello permitió que se solicitara un avance de la tarjeta de crédito y luego se giraran los fondos desde la cuenta corriente de la recurrente en que fueron depositados, expresó.

Indicó que, evidentemente, el ingreso al sistema mediante el uso correcto de las tres claves a través de la verdadera página web del Banco no importa una violación de su seguridad, sino que el cumplimiento íntegro del protocolo para el ingreso a la cuenta corriente y su posterior operación.

Sostuvo que la violación habría tenido lugar si se hubiera ingresado al sistema sin el uso de las claves o con claves incorrectas o inexistentes, lo que no tuvo lugar en este caso.

6.- Expresó que se concluyó en la investigación en comento que, de ser efectivo lo señalado en el recurso, el fraude habría tenido su origen en la violación de la propia seguridad implementada por la actora, por un descuido de ésta que permitió que terceros tuvieran acceso a las tres claves de seguridad. Esto no puede ser producto de una casualidad o mera mala suerte, menos en este caso, en que se han tenido que vulnerar tres diferentes tipos de claves a las que solo ha debido tener acceso la recurrente. Como ya ha señalado, normalmente esto tiene lugar porque los usuarios ingresan a páginas falsas que no pertenecen al Banco por su propia desidia, negligencia o descuido, de las cuales son capturados sus datos que luego permiten ingresar correctamente al sistema del Banco, o bien a los teléfonos celulares de los afectados, desde donde capturan la información almacenada en dicho aparato o recibida en éste a requerimiento de quien lo está utilizando, refirió.

7.- Hizo presente, además, que de los propios dichos de la recurrente queda establecido que su denuncia tuvo lugar una vez efectuadas las transferencias que estima fraudulentas y no antes, lo que es determinante al momentos de establecer responsabilidades, según veremos en el acápite siguiente.

8.- Alegó que, por otra parte, no forma parte de los procedimientos de verificación del Banco que este le pida a sus clientes la entrega de los tres números claves de su tarjeta de

coordenadas para obtener la Súper Clave cuando los ejecutivos llaman por teléfono, como reconoce la actora que sucedió en este caso. Por el contrario, según consta de las advertencias publicadas por el Banco Santander Chile a los usuarios, que la actora también ha reconocido expresamente conocer y de las cuales transcribe en parte, entre las actuaciones que se advierten como falsas se incluye precisamente aquella en que se le solicita al cliente por teléfono los tres números claves de su tarjeta de coordenadas, en los siguientes términos: “Nunca, Jamás, te llamaremos para pedir tus claves bancarias o tus coordenadas, ni las pediremos por email ni por SMS”. Estas publicaciones están contenidas en la página web del Banco y siempre están a disposición de sus clientes y para su debido conocimiento y resguardo.

Sostuvo que, en la especie, existe reconocimiento expreso de la actora que, antes de producirse el fraude que denuncia, fue ella quien entregó a un desconocido los números de su tarjeta de coordenadas.

II.- SEGUNDA DEFENSA: EXCEPCIÓN DE FALTA DE LEGITIMACION PASIVA:

1.- Al respecto, alegó que para poder actuar y figurar eficazmente como parte, en un proceso determinado y específico, no basta con disponer de la aptitud general de la capacidad o legitimatio ad processum, sino que es necesario además poseer una condición más precisa, referida en forma particularizada al proceso individual de que se trate. Tal condición se denomina legitimatio ad causam o legitimación procesal. Afecta al proceso no en su dimensión común, sino en lo que tiene de individual y determinado. En efecto, la capacidad de ser parte supone también, en principio, la aptitud de ser titular de los derechos materiales o sustantivos en controversia o, dicho de otro modo, la aptitud para afirmar en un proceso que se tiene la calidad de titular de tales derechos. También se dice que quien es parte en un proceso es quien tiene la legitimatio ad causam. Lo importante es que el hecho de ser parte importa pretender ser titular de un derecho en conflicto amparado por la ley, pues, recién en la sentencia se determinará si en efecto quien hizo la referida afirmación es realmente el titular del derecho alegado o no, refirió, citando enseguida doctrina y jurisprudencia sobre la legitimación procesal.

2.- Refirió que, en el caso planteado por la actora no es posible que el Banco Santander Chile pueda ser sujeto pasivo de esta acción toda vez que no ha participado como tal, por sí, ni a través de sus funcionarios, en los hechos que han motivado esta acción, ni forma

parte de los sujetos que han podido intervenir en el supuesto fraude en que se sustenta la demanda de restitución de autos. Por otra parte, no existe ningún antecedente entregado por la actora que permita relacionar al Banco con el supuesto uso de información personal de la actora, ni que éste haya podido entregarla a terceros para que éstos hagan mal uso de la misma. La imputación que hace la actora al Banco Santander Chile se sostiene únicamente en sus propias y gratuitas afirmaciones, sin entregar antecedente alguno en que pueda sustentarla, sostuvo.

Expuso que, por el contrario, todo indica que ha sido la propia actora la que, en forma descuidada, ha permitido que terceros pudieren acceder a sus datos personales a través de la citada figura del “phishing” y/o del “vishing” a lo que se une su reconocimiento expreso y espontáneo de que entregó su súper clave a un tercero extraño, luego del o cual habría sufrido el fraude que reclama.

Alegó que la responsabilidad en la custodia de las claves le corresponde a la demandante y no al Banco.

3.- Señaló que, de lo expuesto se desprende que del ingreso por parte de la Sra. Halpern a una página que no era del Banco y luego de la entrega, también por su parte de la Súper Clave a un tercero, se habría originado el engaño que reclama. Se trata entonces de hechos que han tenido lugar antes de que se ingresaran las operaciones cuestionadas al sistema del Banco, de los cuales su parte estuvo en total desconocimiento hasta después de consumadas las transferencias, una vez que la actora hizo su tardía denuncia, indicó.

5.- Alegó que, ante la masificación en el uso de los sistemas digitales se ha debido regular sobre la responsabilidad que le cabe a cada uno de los participantes frente a la posibilidad de que terceros en forma fraudulenta puedan acceder a las claves personales, causándole perjuicios. Es así como la Ley 20.009 sobre extravío, robo o hurto de tarjetas de créditos establece en su artículo 1° lo siguiente: "Artículo 1º.- Los tarjetahabientes de tarjetas de crédito emitidas por instituciones financieras o casas comerciales, podrán limitar su responsabilidad en los términos establecidos por esta ley, en caso de hurto, robo o extravío, dando aviso pertinente al organismo emisor”, citó.

Refirió que, luego, los arts. 3° y 4° del mismo cuerpo legal estatuyen lo que sigue: “Artículo 3º.- En el caso que las tarjetas sean operadas con posterioridad al aviso de extravío, hurto o robo, corresponderá al emisor probar que las operaciones fueron realizadas

por el tarjetahabiente titular o los adicionales autorizados por éste. Las cláusulas de los contratos que impongan el deber de prueba sobre el tarjetahabiente, por operaciones realizadas con posterioridad al aviso de extravío, hurto o robo, se tendrán por no escritas."; "Artículo 4º.- El tarjetahabiente no tendrá responsabilidad por las operaciones realizadas con posterioridad al aviso o noticia entregada al emisor, sin perjuicio de la responsabilidad penal que corresponda"; según citó.

5.- Mencionó que, de las disposiciones transcritas queda meridianamente claro que el titular de la tarjeta responde de las operaciones que con ella se realicen hasta tanto no informe sobre su extravío, robo o hurto. A su vez, solo en el caso que las tarjetas sean operadas con posterioridad a dicho aviso, corresponderá al emisor probar que las operaciones fueron realizadas por el tarjetahabiente titular o los adicionales autorizados por éste. Resulta evidente que dentro de la aplicación de estas normas, se incluye todo mal uso que se haga de una tarjeta de crédito sin la anuencia o autorización de su titular, derivado de cualquier tipo de engaño o fraude, indicó.

6.- Señaló que, en la misma línea, al momento de contratar estos servicios y según se acreditará oportunamente, los clientes deben suscribir un contrato que se rige, entre otras, por las estipulaciones aplicables al Contrato para operar a través de Cajeros Automáticos y demás Medios Electrónicos o Sistemas Bancarios Automatizados y Remotos, que son normas comunes que rigen en todo contrato celebrado con el Banco, las que se entienden incorporadas a todo contrato que permita la utilización de canales remotos, que como condiciones particulares suscriban el Banco y los Clientes.

Mencionó que, conforme a dichas normas comunes el Banco presta diversos servicios a sus Clientes por medio de plataformas de transmisión electrónica de datos, directamente o a través de terceros, que le permiten a los Clientes, entre otros, acceder a información, utilizar los servicios y/o productos, contratar y/o realizar operaciones bancarias, transferir información, fondos y/o contenidos, en adelante los "Servicios Automatizados". Se dispone asimismo que, para acceder y operar los Servicios Automatizados el Cliente debe utilizar los procedimientos y/o medios de seguridad, identificación e integridad que el Banco tenga dispuestos o implemente en el futuro, y que pudieren estar asociados a los elementos requeridos para su utilización, tales como tarjetas magnéticas, número de RUT y/u otros. Entre éstos, y a título meramente ilustrativo, se pueden citar los códigos o claves secretas, firmas electrónicas, avanzadas o no, y cualquier otro mecanismo de seguridad de acceso y/u operativo que el

Banco o los operadores de los Sistemas Automatizados hubiesen establecido o establezcan en el futuro, que se denomina “Firma Electrónica.”, manifestó.

8.- Indicó que, otra norma de común aplicación que rige la relación entre el Banco y el cliente en esta materia es que, en caso de extravío, hurto, robo, o mal uso, de la Firma Electrónica, el Cliente queda obligado a dar aviso inmediato y por escrito al Banco, en cualquiera de sus oficinas. Cesa la responsabilidad del cliente desde el momento en que el Banco reciba el aviso escrito antes señalado, en cualquiera de sus sucursales a lo largo del país o bien, por cualquier otro medio que el Banco desarrolle en el futuro para tales efectos. Por otra parte, se establece la responsabilidad del cliente por los perjuicios derivados del extravío del soporte en que el éste mantenga guardada la información relacionada con la Firma Electrónica, o de cualquier otra circunstancia, sea que ellos provengan de su hecho o culpa ocurridos antes de que el Banco reciba el citado aviso, señaló.

9.- Expuso que, en consecuencia, desde el mismo inicio de la relación contractual entre el cliente y el Banco queda determinado por la ley del contrato que la responsabilidad en el uso, resguardo, custodia y confidencialidad de la clave personal queda en manos exclusivas del usuario, como asimismo, la exención de responsabilidad del Banco mientras el cliente no le hubiere informado personal y previamente el hecho de la pérdida o sustracción de su clave secreta que permita su mal uso por terceros.

Señaló que, en el caso de autos, la propia afectada reconoce en su demanda que solo dio aviso de las transferencias cuya ilegitimidad reclama, cuando ya había entregado la súper clave al tercero extraño y una vez que éstas ya se habían realizado, lo que exime de toda responsabilidad al Banco en las consecuencias negativas que el mal uso de las claves pudiere haber causado a la recurrente.

Mencionó que, de acuerdo a lo anterior, la custodia de las claves secretas ha quedado legal y contractualmente en manos de la actora y no del Banco y sobre ella pesa la obligación de resguardo y la responsabilidad por su eventual mal uso por tercero, como se reclama en este caso, no pudiendo ser el Banco sujeto pasivo de una acción que persiga una responsabilidad de custodia de información que no le corresponde.

III.- TERCERA DEFENSA: EL BANCO NO HA PODIDO DEJAR DE CURSAR LAS OPERACIONES RECLAMADAS SIN INCURRIR EN UNA INFRACCIÓN LEGAL Y REGLAMENTARIA:

1.- Manifestó que, sin perjuicio de lo anterior, conforme lo dispone el art. 1° de la Ley Sobre Cuentas Corrientes Bancarias y Cheques, 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. En el caso de autos, como ya hemos dicho, suponiendo la veracidad de lo señalado por la demandante, resulta evidente que la obtención fraudulenta de las tres claves de cada una de su cuenta corriente y tarjeta de crédito señaladas por la actora habría tenido lugar con antelación al ingreso a los sistemas del Banco, por un descuido de la propia actora. Pues bien, una vez cumplidos los requisitos para que operaran las transferencias cuestionadas por la Sra. Halpern, esto es, una vez ingresadas correctamente las tres claves de seguridad en este caso a la plataforma verdadera del Banco, éste no podía sino cumplir con su obligación legal de dar curso a dichas órdenes de transferencia que había recibido, según entendía, del titular de la cuenta, pues, como ya alegó, todas las claves que debían estar en su solo conocimiento fueron correctamente ingresadas al sistema para este efecto.

2.- Expuso que, en el mismo sentido, la letra C) del punto 2 del Capítulo 1- 7, de la Recopilación Actualizada de Normas de la Superintendencia de Bancos, referido a las transferencias electrónicas, dispone lo siguiente: “Los procedimientos deberán impedir 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 métodos de autentificación para el acceso al sistema y al tipo de operación, que permitan asegurar su autenticidad e integridad.”, citó.

Señaló que lo anterior importa que una vez entregada la clave al usuario y siendo éste el custodio de la misma, cada vez que mediante su uso se genere una orden de transferencia electrónica, ni el usuario, ni el Banco pueden desconocer la autoría de las transacciones o mensajes, ni la conformidad de su recepción, todo ello mientras no se haya recibido una notificación en contrario de parte del cliente, según ya vimos.

Expresó que, de acuerdo a esta normativa, los sistemas de seguridad que provee el Banco no pueden considerarse vulnerados si se ha utilizado el procedimiento correcto, esto es, el ingreso del RUT y de la clave secreta correcta reconocida en el mismo sistema y además, en este caso particular, de la súper clave y luego de la clave 3.0.

3.- Alegó que, dentro de las estipulaciones aplicables al Contrato para operar a través de Cajeros Automáticos y demás Medios Electrónicos o Sistemas Bancarios Automatizados y Remotos incorporadas en el contrato suscrito entre ellas, las partes acordaron y aceptaron asimilar jurídicamente todas las firmas electrónicas y claves a la firma manuscrita del cliente, y que la utilización de los Servicios Automatizados importará una manifestación de voluntad del cliente.

4.- Indicó que, según los antecedentes a que ha tenido acceso el Banco, no existía indicio alguno de patrón de fraude que pudiere haberse detectado con antelación a la solicitud de avance en la tarjeta de crédito y las transferencias efectuadas a su cuenta corriente, salvo por los dichos de la actora, cuya veracidad no le puede constar a su parte, por tratarse de circunstancias que habrían acaecido fuera de su ámbito de acción y control. Por el contrario, ha podido confirmarse internamente que operaron todas las medidas de seguridad y que se respetaron y aplicaron en cada caso los procedimientos determinados para las operaciones de este tipo. Establecidos los hechos anteriormente relatados, no es posible atribuir a su representado una actuación ilegal al negarse a restituir los fondos que según la recurrente le fueron defraudados, toda vez que no se puede desconocer el efecto obligatorio de ley que tiene para las partes lo estipulado en el contrato que las vincula, al tenor de lo dispuesto en el art. 1545 del Código Civil, alegó.

IV: CUARTA DEFENSA: IMPROCEDENCIA DE LA RESTITUCION DEMANDADA:

1.- Argumentó que, consecuencia inevitable de lo expuesto es que resulta del todo improcedente la restitución demandada por la actora, según se pasa a exponer. La demanda de restitución de la actora se sustenta en la aplicación de la figura del “depósito irregular” al contrato de cuenta corriente, según se sostiene en un fallo de la Excma. Corte Suprema que cita al efecto, en función de lo cual se estima que el contrato de cuenta corriente bancaria constituye una especie de depósito respecto de un bien eminentemente fungible, y que es de cargo del depositario el riesgo de pérdida de la cosa depositada durante la vigencia de la convención, y en consecuencia el Banco está obligado a restituir el dinero sustraído que estaba en depósito, señaló.

2.- Señaló que ninguno de los fallos citados de contrario se refiere a un caso en que la cuenta correntista haya reconocido haber entregado los números de su súper clave a un tercero desconocido,

como en la especie. Esto hace una diferencia determinante entre los casos analizados en dichos fallos y el presente juicio. En aquellos casos, referidos a recursos de protección en que no ha existido la posibilidad de contar con un espacio mínimo para realizar una prueba que determine la imposibilidad técnica de que sea franqueado por parte de terceros el acceso a la plataforma de los bancos, sin la autorización de los usuarios titulares de productos contratados con ellos, pero en ninguno de ellos ha tenido lugar la figura en que el propio usuario reconozca que entregó sus claves a un tercero desconocido, en forma previa al fraude, lo que exime de toda responsabilidad a su parte y se aleja sustancialmente del supuesto de hecho sobre los cuales dichos fallos se han dictado, indicó.

3.- Estimó que, en todo caso, existe una errada interpretación de la especial convención que constituye el contrato de cuenta corriente, que se rige por normas especiales, las cuales no se relacionan con la citada figura del depósito irregular. En primer término, conforme a lo dispuesto en los artículos 2211 y siguientes del Código Civil, para que opere la figura del depósito éste debe ser gratuito, por expresa aplicación del art. 2219 del mismo cuerpo legal, que dispone lo siguiente: “El depósito propiamente dicho es gratuito. Si se estipula remuneración por la simple custodia de una cosa, el depósito degenera en arrendamiento de servicio...”, citó. Pues bien, en atención a que por el contrato de cuenta de corriente se cobra una comisión por parte del Banco, se hace inaplicable entonces la figura del depósito en cualquiera de sus especies -sea regular o irregular- por cuanto en este caso el contrato es de carácter oneroso, al establecerse una prima mensual que el cliente debe pagar a la institución financiera. De esta manera, la figura que operaría en la especie sería la del arrendamiento de servicio, de acuerdo a la correcta aplicación de la norma legal citada, indicó.

3.- Señaló que, a lo anterior se agrega que, en el caso del arrendamiento de servicios, como señala la norma legal citada, la responsabilidad que le asiste al que presta el servicio es de culpa leve. Sin embargo, la teoría esgrimida en el fallo citado de contrario, al asimilar el contrato de cuenta corriente a un depósito irregular, porque entiende que el Banco hace suyos los dineros -título traslaticio de dominio- lo hace responsable de la culpa levísima, al entender -erradamente- que la institución bancaria es la única beneficiaria (artículo 1547 del Código Civil), sostuvo. En consecuencia, también resulta errada la aplicación del depósito irregular al contrato de cuenta corriente, pues por la propia naturaleza y características esenciales de

éste no es posible invocar tal figura al momento de determinar las responsabilidades aplicables al Banco, estimó.

4.- Alegó que, por último, resulta un contrasentido que se sostenga que la propiedad del dinero depositado en una cuenta corriente le corresponde al Banco Santander Chile, por lo que la institución bancaria debe asumir la pérdida de dicho dinero, y al mismo tiempo se pretenda obtener la restitución de dicho dinero por parte de la actora, que lo estima propio. Sobre el particular debe recordarse que el derecho de dominio sólo puede recaer sobre cosas determinadas. Por ello el artículo 700 del Código Civil señala que la posesión –que es la cara visible del dominio- "es la tenencia de una cosa determinada con ánimo de señor o dueño", citó. En el caso que nos ocupa es precisamente el actor quien se atribuye la condición de propietario de los dineros sustraídos desde su cuenta corriente y sustentado en este supuesto demanda su restitución, refirió.

5.- Expuso que el Banco Santander Chile no tiene un derecho de dominio sobre determinadas especies monetarias. Por consiguiente, mal se puede aseverar que el Banco Santander Chile es el propietario del dinero depositado en la cuenta corriente de la actora. Precisamente, en razón de esa evidente circunstancia, los autores que se han ocupado de los depósitos bancarios de dinero han resaltado la inexistencia de una obligación de custodia o cuidado respecto de la suma depositada. Así, Garrigues destaca que al limitarse la obligación del Banco a devolver una cantidad igual a la recibida y no ídem corpus, "…es indudable que la obligación de custodia se esfuma y llega a desaparecer, sobre todo si se concibe como una actividad encaminada a la conservación y protección de la cosa. Parece entonces que esta obligación queda sustituida por la pura obligación de restituir", citó.

6.- Manifestó que, la obligación de custodia es reemplazada por la obligación de restituir, con lo cual resulta un error aludir al deber de custodia del Banco sobre el dinero depositado. Precisamente en congruencia con ello, cuando se trata del usufructo de dinero, el artículo 775 del Código Civil sólo admite la posibilidad de caución de restitución, pero no de conservación, y el nudo propietario, en tal caso, no es propietario del dinero objeto de usufructo sino sólo acreedor personal de la obligación de restituir. En consecuencia, el depositante tiene un crédito o derecho personal en cuya virtud puede exigir del Banco la restitución de los fondos depositados, pero ello en ningún caso importa que el Banco depositario tenga la propiedad de los

dineros depositados, como quiera que se trata de bienes determinados sólo genéricamente, sostuvo.

7.- Afirmó que lo que sí tiene el Banco depositario es, en principio, una obligación de restituir el mismo monto depositado, pero evidentemente que cesa esta obligación restitutoria si el depositante, previamente, ya ha hecho uso de los caudales depositados (en este caso por medios electrónicos, a través de sus claves secretas). Por ello no es posible traspasar la responsabilidad al Banco Santander Chile por las transacciones realizadas con las claves del actor, bajo el pretexto de que el Banco depositario es el dueño de los dineros depositados, indicó.

8.- Señaló que, en suma, en el caso que nos ocupa, las transferencias de dinero impugnadas se llevaron a cabo con las claves de acceso y de coordenadas de la actora –claves que sólo ésta conoce- y, además, con la clave 3.0 o clave dinámica, la cual fue enviada para cada una de las transferencias en cuestión al número de teléfono que ésta tiene registrado en el Banco Santander Chile, por lo que no se detectó ningún viso de irregularidad en dichas transacciones. En consecuencia, la responsabilidad por el uso de tales claves es exclusivamente de la demandante, estimó.

9.- Agregó que su parte niega categóricamente lo aseverado por la actora, en el sentido que el supuesto fraude que acusa habría sido realizado a resultas de una vulneración de los sistemas de control y seguridad del Banco. En este sentido su parte insiste que en la especie se cumplieron con todas las medidas de seguridad y que todas las operaciones se efectuaron correctamente con las claves de la recurrente (clave de acceso, claves de tarjeta de coordenadas y clave 3.0). Por lo mismo, no puede imputársele al Banco Santander Chile haber omitido adoptar las respectivas medidas de seguridad o haber incumplido su obligación de custodiar debidamente los dineros de la cuenta corriente de la demandante, expresó.

Petitorio de la contestación: pidió que, en definitiva, se niegue lugar a la demanda de autos, en todas sus partes, con costas.

En folio 15, se celebró la audiencia de conciliación, notificada en folios 12 y 13, con asistencia del apoderado del actor y en rebeldía del demandado, motivo por el cual no se produjo acuerdo, previo llamado de rigor.

En folio 17 se dictó la interlocutoria de prueba, debidamente notificada a las partes, contra la cual no se interpusieron recursos, siendo reactivado el probatorio en definitiva según consta en folio 49.

En folio 60, se citó a las partes a oír sentencia.

CONSIDERANDO:

PRIMERO: Que doña NICOLE HALPERN MAGER, por intermedio de su apoderado, dedujo en juicio ordinario de menor cuantía, una acción de cumplimiento de contrato, en contra del BANCO SANTANDER-CHILE, todos ya individualizados en autos, y, en virtud de los hechos y fundamentos de derecho que se reproducen en la parte expositiva, solicitó que en definitiva se ordene a la demandada que cumpla su obligación correlativa de restituir o pagar a su representada la suma de $5.000.000 (cinco millones de pesos chilenos) más intereses legales y reajustes, con costas.

SEGUNDO: Que el demandado contestó el libelo dirigido en su contra, y, en virtud de los fundamentos, alegaciones y defensas reseñados en la parte expositiva, pidió que, en definitiva, se niegue lugar a la demanda de autos, en todas sus partes, con costas.

TERCERO: Que, del análisis del contenido de los escritos que componen la etapa de discusión, se advierte que es un hecho pacífico o no controvertido entre las partes, que entre ambas partes se celebró un contrato de cuenta corriente bancaria, actualmente vigente, teniendo la demandante la calidad de cuentacorrentista del banco demandado.

CUARTO: Que la controversia de hecho ventilada en el proceso, radica en dirimir acerca de la efectividad y contenido de los hechos denunciados por la actora y que se relacionan al uso, por parte de un tercero, de su cuenta corriente bancaria; las cláusulas, condiciones, estipulaciones y alcances del contrato de cuenta corriente suscrito por las partes y del seguro de fraude contratado por la demandante; el cumplimiento dado por las partes a las obligaciones emanadas de los contratos de cuenta corriente y de seguro de fraude referidos; y la efectividad de que fueron vulneradas las medidas de seguridad, establecidas por la demandada, para el uso y realización de transacciones en su plataforma digital para usuarios.

QUINTO: Que la demandante, a fin de comprobar sus dichos, aportó al proceso la PRUEBA DOCUMENTAL no objetada por su contraparte, acompañada en folios 29 y 52, la que consiste en:

1. Correo electrónico, asunto: “POLIZA DE SEGURO”.

2. Documento titulado “CERTIFICADO DE COBERTURA DE INCENDIO Y SISMO PARA CRÉDITOS HIPOTECARIOS (EN UF) MODALIDAD PRIMA RECURRENTE BANCO SANTANDER / LICITADA SEGUN ART. 40 DFL 251”.

3. Correo electrónico, “Transacción no reconocida, N° de reclamo 23385254. Nicole Halpern Mager”.

4. Copia de cédula de identidad de la demandante.

5. Documento titulado “FORMULARIO ÚNICO DE SINIESTROS FRAUDE CANALES A DISTANCIA / TRANSACCIONES NO RECONOCIDAS EN CUENTA CORRIENTE”.

6. Documento titulado “DENUNCIA”, de fecha 7 de noviembre de 2018.

7. Documento emitido por Banco Santander, referido a transferencia de fecha 7 de noviembre de 2018.

8. Documento titulado “DETALLE DE TRANSFERENCIAS” emitido por Banco Santander.

9. Documento titulado “CONSULTA DE MOVIMIENTOS” emitido por Banco Santander Santiago.

10. Copia de Parte Denuncia N°5780 de fecha 11 de julio de 2018, ante Carabineros de Chile, Pref. Stgo Andes, 17° Comisaría de Las Condes.

11. Escrito en cuya suma se lee “REQUERIMIENTO DE PROCEDIMIENTO SIMPLIFICADO”.

12. Acta de audiencia de preparación de juicio oral simplificado, de fecha 10 de julio de 2019, ante el 4º Juzgado de Garantía de Santiago, causa RIT 3805 – 2019, RUC 1801095631-1.

13. Acta de audiencia de juicio oral simplificado, de fecha 16 de enero de 2020, ante el 4º Juzgado de Garantía de Santiago, causa RIT 3805 – 2019, RUC 1801095631-1.

14. Documento titulado “Consulta un nuevo requerimiento”.

SEXTO: Que la demandada aportó al proceso la PRUEBA DOCUMENTAL no objetada por su adversaria, acompañada en folio 46, y que consiste en:

1. Documento titulado “CONTRATO DE PLAN DE SERVICIOS FINANCIEROS”.

2. Documento titulado “CONDICIONES COMUNES AL CONTRATO PARA OPERAR A TRAVÉS DE CAJEROS AUTOMÁTICOS Y DEMÁS MEDIOS ELECTRÓNICOS O SISTEMAS BANCARIOS AUTOMATIZADOS Y REMOTOS”.

3. Documento titulado “Informe Dpto. Gestión de Fraudes RTO-2021”.

4. Documento titulado “Informe pericial”, emitido por FRANCISCO JAVIER VARAS UNDURRAGA, en calidad de ingeniero, a solicitud del BANCO SANTANDER CHILE.

SÉPTIMO: Que, del análisis del contenido de las pruebas incorporadas al proceso, consistentes en instrumental acompañada legalmente por ambas partes, no objetada por su respectiva oponente, y valorada en forma legal conforme a la naturaleza de cada documento agregado, se tienen por acreditados los siguientes hechos:

1.- Que con fecha 7 de noviembre del 2018, el Departamento de Gestión de Fraudes de la Gerencia de Riesgo Tecnológico y Operacional del BANCO SANTANDER CHILE, gestionó el reclamo N°23385254 presentado por la cuentacorrentista del banco, doña NICOLE HALPERN MAGER, en el cual ella indicó desconocer 4 transacciones realizadas con cargo en su cuenta por un total de $5.000.000, efectuadas el 7 de noviembre de 2018. Tras ello, y de acuerdo a los antecedentes analizados, evidencia y trazabilidad obtenida de los sistemas, el Departamento de Gestión de Fraudes de la Gerencia de Riesgo Tecnológico y Operacional del Banco Santander Chile, emitió el informe RTO-2021, de fecha 18 de mayo de 2021, no objetado por la demandante, en el cual establece que se evidenció, a través de la revisión de los Aplicativos del Banco, las conexiones (direcciones IP) y dispositivos del cliente afectado, y el análisis de Logs (sic) de Auditorías de los Sistemas del Banco, que las transacciones desconocidas por la cliente por un total de $ 5.000.000, fueron autorizadas a través del aplicativo Santander Pass, enrolado a nombre de la cliente NICOLE HALPERN MAGER, Rut 15958860-2, el cual requirió de todos los mecanismos de seguridad (log-in, TSC y

Clave 3.0 –sic) para activar este aplicativo, agregando que no se identificó algún intento fallido de vulneración.

2.- Que los hechos expuestos precedentemente fueron denunciados ante la autoridad policial por la demandante, y tras la correspondiente investigación penal, se ventilan ante el 4° Juzgado de Garantía de Santiago, en causa RIT 3805 – 2019, RUC 1801095631-1, cuya sentencia no ha sido acompañada al presente juicio ordinario.

OCTAVO: Que, abordando el fondo de la acción de cumplimiento contractual forzado interpuesta, se debe tener presente que, en conformidad con lo previsto en el artículo 1698 del Código Civil, en relación con el artículo 1489 del mismo cuerpo legal, es carga de la parte demandante acreditar la existencia y el contenido de la obligación cuyo cumplimiento reclama de su contraparte, y, a su vez, es carga de esta última, comprobar que la respectiva obligación se encuentra extinguida o es inexigible.

NOVENO: Que, de las pruebas rendidas y de lo concluido respecto al contenido de éstas en el motivo séptimo, no se advierten elementos de convicción suficientes, precisos, graves y concordantes, que permitan determinar que el banco demandado hubiese incumplido sus obligaciones impuestas por el contrato de cuenta corriente celebrado con la demandante, en relación con la seguridad de sus plataformas y transacciones digitales, particularmente en el caso de las transacciones objetadas por la actora. En efecto, de las pruebas rendidas no se advierte en forma suficiente que dicho tercero u otro, hubiesen accedido ilegítimamente a la plataforma digital del banco demandado, mediante una vulneración de los sistemas de seguridad que se encuentra obligado a implementar y mantener. Y, a mayor abundamiento, la demandante reconoce en su libelo que fue ella misma quien entregó la respectiva clave de acceso al tercero que se la solicitó telefónicamente, simulando ser funcionario del banco demandado, engañando de esta manera a la demandante para que entregase dicha información.

Por otro lado, es un hecho de pública notoriedad, al amparo de lo previsto en el artículo 89 del Código de Procedimiento Civil –disposición común a todo procedimiento-, que tanto el banco demandado como la mayoría de los bancos que operan en el mercado nacional, realizan campañas de información masivas a sus clientes y al público general, en las cuales advierten que el banco jamás solicita claves personales por vía telefónica o similar.

Finalmente, de las pruebas aportadas, tampoco se advierten antecedentes de una decisión judicial ejecutoriada en relación con el proceso penal incoado por la demandante, que pudiese determinar la participación del tercero que engañó a la demandante, en una eventual vulneración a los sistemas de seguridad del banco demandado, y que en virtud de dicha vulneración, hubiese obtenido las claves necesarias para efectuar las transacciones objetadas en la demanda.

En consecuencia, por los motivos dados, y siendo, en consecuencia, insuficientes las pruebas rendidas para determinar el incumplimiento de las obligaciones del banco demandado en relación con una supuesta vulnerabilidad informática que hubiese permitido el engaño del que fue víctima la demandante, corresponderá desestimar la demanda, sin perjuicio de otros derechos.

DÉCIMO: Que, en consecuencia, dada la insuficiencia probatoria señalada en el motivo anterior, corresponderá desestimar la excepción de falta de legitimación pasiva opuesta por la demandada, y también las restantes defensas y alegaciones opuestas por ella en la contestación.

UNDÉCIMO: Que, habiéndose desestimado las pretensiones de ambas partes, conforme a lo dispuesto en los motivos noveno y décimo, cada una de ellas pagará sus respectivas costas.

Por estas consideraciones, y visto, además, lo dispuesto en los preceptos legales citados por las partes y los reseñados a lo largo del presente fallo; y, además, en los artículos 160 y 170 del Código de Procedimiento Civil, **se resuelve:**

A) Que se desestima la excepción de falta de legitimación pasiva y las demás defensas y alegaciones opuestas por la demandada, en virtud de lo dispuesto en el motivo undécimo.

B) Que se **desestima la demanda entablada**, conforme a lo dispuesto en el motivo noveno.

C) Que cada parte pagará sus costas.

Regístrese, notifíquese a las partes y en su oportunidad archívense estos antecedentes.

ROL C-29.061-2019.

PRONUNCIADA POR DOÑA SUSANA RODRÍGUEZ MUÑOZ, JUEZA.

C-29061-2019

Foja: 1

Se deja constancia que se dio cumplimiento a lo dispuesto en el inciso final del art. 162 del C.P.C. en **Santiago**, **treinta y uno de Agosto de dos mil veintidós**