Santiago, dieciséis de junio de dos mil veinte.

Visto y considerando.

Primero: Que, comparece Claudia Andrea Cañas Pinochet, factor de comercio, y deduce recurso de protección en contra del Banco Scotiabank Chile Sab, sociedad del giro de su denominación, por el acto ilegal y arbitrario que cometió en el correo electrónico de 17 de febrero de 2020, remitido por Daniel Espinosa Fernández, analista del Banco. La decisión contenida en dicho correo, perturba y vulnera su derecho de propiedad, consagrado en el N° 24 del artículo 19 de la Constitución Política de la República, además amenaza y perturba su derecho a la integridad psíquica asegurado en el N° 1 del artículo 19 de la Carta Fundamental.

Explica que el 17 de febrero de 2020, recibió un correo electrónico de Scotiabank, el que contiene la decisión ilegal y arbitraria del Banco, en orden a que debe asumir el costo de transacciones bancarias, que no consintió y que corresponden a un fraude bancario, tal decisión resulta ilegal y arbitraria, pues no se condice con las normas aplicables al contrato de cuenta corriente bancaria, que le impone asumir un costo que no le corresponde.

Expresa que es titular de la cuenta corriente bancaria del Banco recurrido, N° 973149709, y ocurre que el 4 de diciembre de 2019, estando de viaje en República Dominicana, fue informada por correo electrónico que se realizó una transferencia fraudulenta de dinero con cargo a su cuenta corriente, por $4.999.890.-, cuyo destino era una cuenta corriente del mismo Banco, N° 1170154486 a nombre de Yuri Barraza Bahamondes, Rut 16.619.757-0, transacción que no realizó, ya que no solo desconoce la cuenta corriente a la que se realizó ésta, con la que nunca ha tenido contacto, ni la conoce. Precisa que, de la cartola emitida por el banco, el 11 de diciembre de 2019, los $ 4.999.890.-, fueron traspasados a su cuenta corriente desde la tarjeta de crédito, de la que es titular, asociada a la misma cuenta corriente, esto es, tarjeta de crédito MasterCard Black Nº 5587 27110022 0083 del banco Scotiabank, la que no activó, siendo una operación fraudulenta, que fue la primera y única operación realizada con ella.

Añade que al enterarse de esa situación, de inmediato, tomó contacto con su ejecutiva bancaria Marcela Sepúlveda para indicarle qué desconocía esa transacción y, le pidió que aclarara el origen del movimiento bancario y, que tal situación fuera resuelta, pues le causaba un perjuicio, por cuanto disminuye de manera fraudulenta y sin causa alguna su patrimonio. La ejecutiva, le confirmó la

transferencia fraudulenta detectada, y de otras seis compras fraudulentas realizadas vía internet con cargo a su cuenta corriente, todas del 4 de diciembre de 2019, por un monto total de $ 1.009.880.-, por compras realizadas a una misma sociedad llamada FYX Limitada, con cargo a los fondos de su cuenta corriente.

De esta manera, y a pesar de los avisos que dio al banco, éste se limitó a indicar que debía dejar constancia en Carabineros para que se inicie la respectiva investigación en contra del presunto autor del fraude. Acto seguido, realizó la denuncia en Carabineros, después fue al Sernac Financiero y a la Comisión de Mercado Financiero (CMF).

Sostiene que el fraude se realizó mediante transacciones vía internet suplantándola y utilizando sin su autorización y aprovechando su total desconocimiento, tanto sus datos personales como las claves propias del sistema bancario asociados a su cuenta, información que solo eran de su conocimiento y de la institución bancaria de la que es cliente.

Agrega que el 11 de diciembre de 2019, mediante un formulario, formalizó ante el Banco Scotiabank la denuncia del fraude, también lo denunció en Carabineros, que derivó en una investigación en la Fiscalía Local de Las Condes, con la expectativa de obtener un reembolso íntegro del dinero defraudado, toda vez que se trata de una transferencia electrónica y de seis compras por internet que, no fueron realizadas por ella, ni por orden o tolerancia suya, ya que no ha compartido su clave personal de ingreso a la sesión de la cuenta bancaria, y tampoco se le ha perdido, robado o extraviado su tarjeta de débito o su clave *"Keypass", toda vez* que jamás ha pedido ni ha tenido sistema de pago por Keypass. lo que tiene como base, el poco uso que le ha dado a esa cuenta corriente del Scotiabank, la que usa solo para el pago del dividendo de un crédito hipotecario que mantuvo con el banco hasta el año 2018, a propia solicitud de éste, y para la recepción de algunos arriendos, por lo que el uso ordinario de la cuenta corriente para otro tipo de pagos, como las compras en el comercio, ha sido siempre muy escueto y por montos muy menores, que no se comparan a la magnitud de lo defraudado, razón por la que nunca tuvo la necesidad de activar las tarjetas de crédito, de donde se transfirió dinero a su cuenta corriente, o de usar el mencionado Keypass, empleando para algunas

transferencias, un dispositivo entregado por el propio banco llamado ScotiaPass, para efectos de validar las transacciones electrónicas, el que cumple una función de validación distinta al referido Keypass, ya que tal como se desprende de la información sacada de la página web del Banco Scotiabank, el Keypass está asociado al teléfono celular, distinto al Scotiapass, bajando una App y activando el servicio con el banco, lo que no ha realizado, que según las propias políticas del banco, no se puede realizar sin dar de baja el sistema antiguo, esto es, el Scotiapass.

Enfatiza que no sabe la forma y/o manera de operar que permitió a él o los autores del fraude perpetrar su acción delictiva, ya que ha custodiado debidamente, sus tarjetas relacionadas con su cuenta corriente, como los medios de verificación de su identidad y claves, salvo, lo que respecta a la clave *Keypass* pues no cuenta ni ha contado con dicho sistema, por lo que no hay forma de que el dinero transferido desde su cuenta se deba a voluntad o negligencia suya, por lo que cabe responsabilizar al banco por esta situación, debiendo el mismo banco solucionar y resarcir los perjuicios que le ha provocado.

Acota que realizada la investigación interna del Banco, el 17 de febrero de 2020 se le dio respuesta por Daniel Espinoza Fernández, cuyo contenido es del siguiente tenor: *"En lo que respecta a la revisión efectuada por el Banco, se detectó que las transacciones fueron realizadas a través de internet. Para la realización de las transacciones objetadas, necesariamente se debe ingresar con su usuario (Rut), la clave personal de ingreso a su sesión y, además, su clave Kevpass, información cuya custodia y uso, son de responsabilidad exclusiva del cliente. Realizada la investigación pertinente, se concluyó que no existió una vulneración a los sistemas de seguridad del Banco, pues las transacciones fueron validadas con la información antes referida. Presumimos en consecuencia, la existencia de un Malware (virus) en sus dispositivos electrónicos que hubieran podido provocar la captura de sus credenciales de seguridad para acceder a los servicios del Banco, lo que habría permitido a los supuestos terceros efectuar las operaciones objetadas. Es por este motivo que le recomendamos formatear sus equipos y actualizar de forma periódica los*

programas antivirus de los mismos, con el fin de evitar este tipo de situaciones".

Afirma que, con esa respuesta, el Banco declinó efectuar el pertinente reembolso de dinero a su cuenta corriente, por concluirse que no hubo vulneración a los sistemas de seguridad del Banco, y, en definitiva, se le atribuye la exclusiva responsabilidad de custodiar una información que fue utilizada por los defraudadores. Sostiene que jamás ha pedido habilitación del sistema *KEYPASS* en el banco, por lo que es imposible que hubiese realizado dichas transacciones, tanto la transferencia directa a una cuenta corriente del mismo banco, como las otras 6 compras a la sociedad ya individualizada, las que desconoce totalmente, mediante dicho sistema e incluso aún más, es materialmente imposible que por descuido le hubiesen sustraído dichos datos y claves pues estas no existen en atención a que hasta esta misma fecha nunca ha solicitado la habilitación del mismo, y por lo tanto, la única forma en que dicho fraude pudo haber sido cometido es por medio de alguna anomalía, voluntaria o accidental, en el propio sistema del banco, ya que no hay ningún documento que pruebe que alguna vez hubiese solicitado lo anteriormente descrito.

Por otro lado, no ha realizado transacción alguna a la cuenta a la que se dirigió, tanto la primera transacción como las 6 compras. Al respecto, dice que como es de público conocimiento, por política de las instituciones bancarias en general, y del banco Scotiabank en particular, como se lo informaron, cada vez que se realiza una transacción a una cuenta nueva por primera vez, dicha transacción no puede exceder de un cierto monto de dinero, que en este caso asciende a trescientos mil pesos, y solo después de 24 horas, se libera dicha cuenta permitiendo realizar transferencias por montos superiores, transferencias que nuevamente tienen un tope máximo, en este caso de $5.000.000.-, detectando una discordancia, ya que el mismo banco acompañó la primera y única transferencia, realizada el 4 de diciembre de 2019, a la cuenta corriente ya individualizada, que se realizó cuando estaba fuera del país, asciende a $4.999.890.-, suma superior a la señalada como tope por el mismo banco, que autorizó una transacción que no cumplía con sus propios lineamientos.

En virtud de lo anterior, en especial de la conducta del Banco de evadir su responsabilidad de garante y cuidador del dinero que ha dejado a su cuidado, intentando endosarla a su persona, sin

cumplir con su obligación legal y restituir los fondos sustraídos producto de su negligencia, es del todo ilegal y arbitraria, ya que de la sola revisión de los antecedentes, resulta claro que el único responsable de no haber tomado las medidas necesarias para proteger su cuenta corriente y su dinero, es el Banco Scotiabank, cuya decisión, además de ilegal, arbitraria, errada e infundada, le ocasionó una pérdida patrimonial directa superior a los seis millones de pesos, lo que constituye afectación a su derecho de propiedad, ya que se menoscaba, como consecuencia de la negligencia del banco en autorizar transacciones sin los respaldos necesarios. Rechaza la tesis del banco de responsabilizarla del fraude, considerando que se vulneraron los medios de verificación de su identidad, no cumpliendo con los protocolos de seguridad alternativos dispuestos por el propio Banco para estos casos, que permiten detener todo intento de transferencia por un monto mayor a $ 300.000.- a un destinatario de transferencia electrónica no registrado antes por un cliente en una primera operación de transferencia. El banco omitió su principal obligación la de ser garante de los fondos que los cuentacorrentistas depositan para su resguardo.

Hace presente que los hechos, además de denunciarlos al Banco recurrido, también lo hizo ante la Fiscalía Local de Las Condes y, envió una carta a la *Comisión para el Mercado Financiero (CMF),* informando esta situación y de la negativa del banco a restituir el dinero defraudado, carta que a la fecha no tiene respuesta.

Informa que tomó conocimiento que el Banco la ha publicado en Dicom, sin que terminara la investigación interna, haciendo cobro de un pagaré, en relación con las deudas generadas por la propia ineptitud y falencia del banco, situación que le causa desprestigio financiero propio por el solo hecho de figurar publicada en ese boletín, por hechos ajenos a su voluntad.

Añade que con el Banco Scotiabank celebró un contrato de cuenta corriente bancaria, contrato que está definido en el artículo l de la Ley sobre Cuentas Corrientes Bancarias y Cheques, como: *"La cuenta corriente bancaria es un contrato en 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".* La Excma.

Corte Suprema ha resuelto: "*que constituye un elemento esencial en el referido contrato la entrega de ciertas cantidades de dinero al banco, bajo la modalidad de la figura del depósito*". En casos como el de la especie, al recaer el depósito en una suma de dinero que no está destinada a mantenerse en arca cerrada, se presume que se permite emplearlo, quedando obligado el depositario a restituir igual cantidad en la misma moneda. Dando lugar a lo que en doctrina se conoce como depósito irregular, en cuya virtud el Banco se hace dueño de los dineros que recibe, quedando obligado a enterar la misma cantidad de dinero que ha recibido cuando el cuentacorrentista lo requiera.

De esta forma y atendida la regulación aplicable al contrato de cuenta corriente bancaria, no cabe sino concluir que el dinero sustraído por vías fraudulentas no era de su propiedad, sino del Banco; entidad que está obligada a devolverle, por su sola solicitud, la cantidad de dinero equivalente a aquella que depositó en su cuenta corriente. Sin embargo, el Banco ha manifestado su decisión unilateral de asignar el costo del fraude a su cargo, provocando una evidente conculcación de su derecho de propiedad sobre el dinero que pretende lo asuma, y por el monto total de $ 6.009.170.

Comenta que, a similares conclusiones han arribado las Cortes, tales como en Rol 79735-2018 de la I. Corte de Apelaciones de Santiago, rol: 714-2019 de la I. Corte de Apelaciones de La Serena y rol 12093-2019, de la Excma. Corte Suprema, entre otras, en que el Banco ha infringido su obligación de resguardar y dar seguridad a las transacciones efectuadas en su cuenta corriente, de manera tal de evitar que ésta sea utilizada sin vulnerar los sistemas informáticos existentes para ese fin. Por otro lado, la actual Comisión para el Mercado Financiero (ex Superintendencia de Bancos e Instituciones Financieras), se ha esmerado en puntualizar, a través de sus respectivas Circulares (N° 3.451 de 2008), que los bancos están obligados a garantizar la seguridad de las transacciones y transferencias electrónicas de dinero. Conforme a ello, los bancos deben garantizar que las operaciones solo puedan ser realizadas por personas autorizadas para ello, debiendo recabar todas las autorizaciones previas que sean necesarias para cumplir con la seguridad de la operación, como así también deben mantener "sistemas y procedimientos" que les permitan "identificar, evaluar, monitorear y detectar"

operaciones con "patrones de fraude" de manera que puedan abortar actividades u operaciones potencialmente dolosas.

Expone que el Banco no le brindó la seguridad debida, ya que terceros efectuaron transacciones sin inconvenientes en su cuenta corriente, sin que se cumplieran los protocolos y medidas de seguridad destinadas a entregar seguridad a sus clientes, el que lejos de reconocer y asumir la responsabilidad por la falla de seguridad en su sistema electrónico, la responsabiliza y le cobra las sumas de dinero realizadas por terceros, sin su autorización y aprovechándose de su desconocimiento y confianza en los sistemas de seguridad del Banco Scotiabank, de modo que su actuación resulta arbitraria, pues ha sido antojadiza y caprichosa, contraria a la razón; e ilegal, al infringir la normativa sobre seguridad de las transacciones electrónicas y lo dispuesto en el artículo 3 de la Ley 19.146, en cuanto establece como derechos de los consumidores, la seguridad en el consumo de bienes o servicios y el deber de evitar los riesgos que puedan afectarles, en consecuencia, el actuar negligente por parte de la entidad bancaria, atenta contra su derecho fundamental cautelado por la Constitución Política de la República, en el artículo 19 N° 24, referente al Derecho de Propiedad.

Termina pidiendo se restablezca el imperio del derecho y se ordene que se le restituya a su cuenta corriente, como los montos sustraídos desde su tarjeta de crédito MasterCard Black Nº 5587 27110022 0083, del banco Scotiabank, ya mencionada, todos los montos extraídos, producto de las transacciones fraudulentas efectuadas por terceros, y los intereses que estos mismos montos han devengado y, el inmediato retiro de la publicación de morosidad en el boletín Comercial Dicom, y que esta Corte disponga las medidas que juzgue necesarias o convenientes para hacer imperar el imperio del derecho.

Acompaña a su recurso: 1. Copia de denuncia presentada ante el Ministerio Público Fiscalía de Las Condes de fecha 11 de diciembre de 2019. 2. Copia de denuncia presentada ante Banco Scotiabank de fecha 11 de diciembre de 2019. 3. Copia simple de respuesta de Scotiabank recibida vía e-mail con fecha 17 de febrero de 2020 a las 16:06 hrs., desde la cuenta daniel.espinosa ex@scotiabank.cl,perteneciente a Daniel Esteban Espinosa Fernández. 4. Copia simple de Cartela de cuenta corriente de la titular Claudia Andrea Cañas Pinochet, N° 973149709, de 11 de Diciembre de 2019. 5. Información de la página www.scotiabank .cl

que informa los 2 tipos de verificación online para transacciones (ScotiaPass y Keypass) señalando las diferencias entre ellos. 6. Certificado Boletín Comercial Dicom.

Segundo: Que, informando la recurrida pide el rechazo del recurso, y luego de hacer un resumen del mismo, expresa que no hubo vulneración de los sistemas del Banco, tal como lo establece el informe elaborado por su gerencia de seguridad, y la recurrente se identificó correctamente como tal frente al Banco, de cara a las transacciones objetadas, ya que las operaciones fueron realizadas ingresándose sus datos y claves privadas y confidenciales, cuya custodia es su responsabilidad y que son necesarias para operar y administrar los productos y servicios financieros, que el Banco entrega a sus clientes en forma remota, a través de su sitio web o aplicación para dispositivos móviles, que se conoce como *"identificación digital"* del cliente, que, incorporando sus credenciales o claves, le acreditan como titular de sus productos bancarios.

Sostiene que no le consta que la actora haya sido efectivamente víctima de un fraude, por lo que tiene que probarlo y, declararlo así el tribunal pertinente, en un procedimiento de lato conocimiento. Lo que le consta, es que no existió una vulneración de sus sistemas y que la recurrente se identificó digitalmente, utilizando sus claves de seguridad, para realizar las transacciones objetadas, por lo que podría tratarse de un caso de auto-fraude, o de un uso indebido de claves por terceros cercanos a la actora, de estafa o de fraude informático fraguado por terceros, etc. Por ello, plantea que de acuerdo a los hechos descritos y antecedentes recabados, es imposible determinar lo que aconteció, siendo necesaria una investigación penal exhaustiva.

Luego transcribe las conclusiones del informe de fraude del Banco, elaborado a partir de los hechos descritos por la recurrente y sobre el mismo, entrega las observaciones que siguen:

En la parte que dice: *a) Se investigó el origen de las transacciones objetadas por la clienta, determinando que fueron realizadas a través del aplicativo Scotiaweb, siendo correctamente validadas por los sistemas de seguridad del Banco. La autorización fue mediante el uso del aplicativo KeyPass, dado de alta el día 02.DIC.2019.";* manifiesta que, el aplicativo Keypass fue enrolado, a través de las claves de seguridad de la actora y las contraseñas que

el mismo Banco envía a su correo electrónico. El aplicativo fue instalado el día 2 de diciembre, 2 días antes de que ocurriesen las transacciones objetadas.

Sigue, el informe: "*b) En base al análisis de los registros de sistema, se pudo determinar que la clienta eventualmente habría sido engañada mediante el compromiso con malware y /o Phishing del dispositivo utilizado para realizar transacciones por la web, con lo cual, terceros habrían capturado sus credenciales y posteriormente habrían dado de alta el dispositivo KeyPass y suplantado por el canal Scotiaweb, concretando de esta manera las transacciones objetadas por ésta.".* Al respecto, comenta que a consecuencia de los hechos expuestos en su reclamo, si es que efectivamente las transacciones no fueron realizadas por ella, cuestión sobre la que no tiene ningún antecedente que así permita concluirlo, las operaciones sólo pudieron hacerse por un tercero que, previamente, instaló un malware en los dispositivos electrónicos de la actora, ya que la instalación de la aplicación "Keypass" se necesita conocer el usuario del cliente; su clave web; los dígitos de su tarjeta de crédito; las claves que el banco envía al correo previamente registrado.

Siguiendo con el informe interno; "*c) No existe evidencia del uso de técnicas de Ingeniería Social por parte de terceros, producto que el relato de los hechos entregado por la clienta no entrega mayores antecedentes, sin embargo, considerando la casuística observada, no debe descartarse dicho patrón de fraude.".* Explica, que para verificar que los hechos ocurrieron como la actora señala y que se vulneraron sus dispositivos electrónicos, tendría que realizarse un análisis pericial de estos, ya que lo único que le consta, es que no hubo vulneración de sus sistemas y que la recurrente o alguien a su nombre, se identificó con sus claves ante el Banco, pero en los hechos, puede tratarse de un auto-fraude, de un uso indebido de claves por terceros cercanos a la actora, de estafa o de fraude informático fraguado por terceros, etc.

Avanzando en el análisis del informe; "*d) La extracción de fondos se realizó a través de 06 Pagos de servicios en el comercio Fyx Ltda. y 01 transferencia electrónica de fondos. El avance de la tarjeta de crédito se pudo concretar debido a que toda tarjeta*

entregada al cliente, está activa en el sistema para realizar transacciones por Internet; el cliente solo debe activar su uso para cajeros automáticos, mediante el ingreso del pin informado al momento de la entrega del plástico.". Indica que esa parte revela que la tarjeta "nunca haya estado activada", como lo refiere la recurrente, pues lo que ocurrió, es que no activó su clave Pin Pass, al recibir la tarjeta, las que vienen activadas con una clave igual a los primero 4 dígitos del Rut de los clientes, siendo su obligación, cambiar este número, pero la actora no lo hizo, por lo que sólo puede conjeturar, que de existir un tercero involucrado, éste activó la tarjeta e hizo el avance.

Enseguida, en cuanto al punto: "*e) Se determinó que la dirección IP desde donde se realizaron las transacciones objetadas por la clienta fue la 191.96.183.155, considerada No habitual, producto que solo se observa los días 02 y 04.DIC.2019.".* Acota que una IP no sea "habitual", no significa, por sí solo, que se esté en presencia de un fraude, ello significa que la transacción se hizo desde un lugar o dispositivo electrónico distinto al habitual, que es algo común, lo que permite pagar servicios o realizar transferencias desde cualquier computador, donde haya conexión a internet, lo que no implica necesariamente que las transacciones no están siendo realizadas por el titular de la cuenta.

Respecto de lo que se informa en las letras: "*f) No existe evidencia que comprometa los sistemas del Banco en el eventual robo y utilización de las credenciales personales del cliente o de las transacciones objetadas por ésta; g) Respecto de las credenciales y claves dinámicas comprometidas y que los clientes utilizan para realizar transacciones por los canales no presenciales o aplicaciones móviles, éstas son cifradas y no pueden ser recuperadas desde los sistemas del Banco. Es por esto, que ante la eventualidad que un cliente olvide sus credenciales, el Banco reinicia las claves para que el titular las cree nuevamente y de esta manera se evita el compromiso a nivel de los sistemas de Scotiabank. y, h) Los métodos utilizados por los ciberdelincuentes para lograr que titulares de cuentas corrientes entreguen voluntariamente sus credenciales a terceros ajenos a Scotiabank,*

han sido informados a través de los distintos canales de comunicación.". A modo de conclusión, dice que consta que no hubo vulneración a sus sistemas de seguridad y que la recurrente o alguien a su nombre, se acreditó como titular de sus productos y servicios, utilizando sus claves o credenciales de seguridad. Y, las hipótesis posibles son que las transacciones fueron realizadas por la propia cliente, la que pretende obtener un beneficio indebido de ello; las transacciones fueron realizadas por alguien cercano que tenía acceso a las claves de la cliente y no se lo comunicó; o existió un fraude, pero este sólo pudo ocurrir porque terceros vulneraron los sistemas de seguridad de la cliente, no del Banco, suplantando así su identidad digital.

En relación con las transacciones remotas, en la actualidad, existe la posibilidad de validar una transacción ingresando la segunda clave a través de una aplicación móvil, llamada "Keypass", que fue la usada para realizar las transacciones objetadas por la actora y que, de acuerdo a sus dichos, lo que en todo caso no le consta, no habrían sido realizadas por ella. Indica que "Keypass" es una aplicación móvil que genera claves únicas para que los usuarios autoricen transacciones desde el teléfono celular, sin necesidad de utilizar una tarjeta de coordenadas, Scotia Pass o una tercera clave, entregando un mayor dinamismo y velocidad, sin comprometer la seguridad en las transacciones bancarias. En ella los clientes deben descargar la aplicación desde Appstore o Google Play en su teléfono celular o en el dispositivo electrónico mediante el cual se autorizarán las transacciones; una vez instalada, el cliente debe ingresar con su Rut y su clave Scotiaweb, la que se determina cuando se contratan productos con el Banco para operar en el sitio web del mismo. Esta es una clave personal, secreta y confidencial del cliente; luego, el Banco envía al correo registrado por el cliente en el Banco, un código de validación, que se debe digitar en la aplicación; después, el cliente crea una clave de autorización personal, confidencial y secreta, la cuál es su obligación custodiar y no divulgar; por último, si el cliente tiene asociado un dispositivo Scotia Pass, debe ingresar una clave dinámica de 8 dígitos. si no la tiene, debe ingresar los últimos 8 dígitos de su tarjeta de crédito.

Así, continúa el informante, para la autorización de una transacción con KeyPass, se requiere no una, sino 4 contraseñas y códigos para que la misma sea activada. Pero además, y para

mayor seguridad de los clientes, el Banco pone a su disposición la aplicación “Scotiabank Avísame”, disponible desde Marzo de 2018, que permite encender y apagar las tarjetas de crédito al instante y, además, recibir notificaciones inmediatas por cada transacción que se realice con los productos bancarios de un cliente determinado. Finalmente, se envía al correo fijado por el cliente, los comprobantes de todas las transacciones.

En conclusión, Scotiabank Chile pone a disposición de sus clientes una aplicación segura, que permite la realización de transacciones y transferencias, sin tener que recurrir a la tarjeta de coordenadas, incluyendo además una aplicación que permite el monitoreo y control por parte de los propios clientes sobre el uso de sus cuentas y tarjetas, desde su teléfono móvil.

Controvierte la existencia de un fraude, cuestión que debe ser resuelta, por un juez penal o un juez civil luego de la investigación o etapa de prueba respectiva, ya que de los antecedentes reunidos, es imposible saberlo. Sostiene que si no fue la recurrente la que realizó las transacciones, entonces entregó inadvertidamente todos sus datos y un tercero realizó las operaciones fraudulentas, por lo que no hubo vulneración a los sistemas del Banco. Las operaciones sólo pudieron realizarse por el propio cliente o, por un tercero que obtuvo las claves directamente del cliente.

Resalta que la custodia de la clave y de los datos personales no es sólo una obligación de las instituciones financieras, sino que los clientes tienen la obligación contractual de custodiarlas y adoptar todas las medidas de cuidado. Agrega, que un fraude bancario puede ocurrir con vulneración de los sistemas del Banco; o sin vulneración de los sistemas del Banco, suplantándose digitalmente la identidad del cliente por un tercero, quien obtuvo sus claves y datos a través de los mecanismos de fraude habituales: Pharming, Fishing, llamados telefónicos, instalación de malware, etc.

Luego de explicar las distintas formas en que los delincuentes obtienen la información de los clientes, dice que a éstos, se les instruye por distintos medios de comunicación lo que no deben hacer al entrar a la página del banco y los resguardos que deben tomar. El malware compromete el dispositivo utilizado por el cliente, capturando datos de éste o bien redirigiendo la navegación a sitios web falsos que simulan ser de Scotiabank.

En consecuencia, el cuidado y resguardo por parte de los clientes de su información personal y claves, es tanto o más

importante incluso que la implementación de medidas de seguridad por parte de los Bancos. De nada sirve que las instituciones financieras tengan los últimos sistemas de seguridad, si es que los clientes, bajo engaños, voluntariamente, entregan sus datos y claves de acceso, permitiendo a los delincuentes suplantarlos digitalmente.

Detalla las diversas campañas que el Banco realiza, para informar a sus clientes de las medidas que deben adoptar para evitar los fraudes.

Agrega, que los Bancos deben contar con sistemas de seguridad y, en este sentido, el Capítulo 1-7 de la Recopilación Actualizada de Normas de la CMF (RAN) señala que para, para la prevención de fraudes, *"Los bancos deberán contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible aquellas operaciones con patrones de fraude, de modo de marcar o abortar actividades u operaciones potencialmente fraudulentas, para lo cual deberán establecer y mantener, de acuerdo a la dinámica de los fraudes, patrones conocidos de estos y comportamientos que no estén asociados al cliente".*

Expresa que nada hacía presumir que quien realizaba las operaciones no era el cliente: la activación de la aplicación se hizo válidamente; se inscribieron también, válidamente, nuevos usuarios para futuras transacciones; se esperó el tiempo de 24 horas para hacer una transferencia superior al monto mínimo; se enviaron correos y mensajes de texto al teléfono y correos electrónicos registrados por el cliente.

De acuerdo al Capítulo 8-41 de la RAN, *"Los bancos debe instruir a los tarjetahabientes acerca de las precauciones que deben tener en el manejo de sus tarjetas físicas y de los medios en que ellas pueden ser utilizadas, especialmente para mantener en resguardo las claves personales, así como de las principales normas que rigen su uso"*.

Al respecto, los Bancos, a través de distintos medios de comunicación social, informan a los clientes y al público en general sobre los peligros asociados al uso de sus productos bancarios, la importancia de custodiar sus claves, que llamen al Call Center cuando tengan una duda o sospecha, y otras recomendaciones.

En conclusión, hay normas que establecen las obligaciones de los Bancos en la materia, las que al menos Scotiabank cumple a cabalidad. Pero, además, dan cuenta de que el regulador, entendiendo la evolución del contrato de cuenta corriente, establece que la seguridad no es una obligación solo de los Bancos, sino también de los clientes.

Luego se refiere, a que la Excma. Corte Suprema, ha resuelto que la Cuenta Corriente Bancaria es un contrato de depósito irregular, motivo por el cual, como depositario de los dineros de los clientes, tendría la obligación de soportar el riesgo en caso de existir un fraude., a base de lo cual realiza un análisis jurídico sobre el depósito irregular, citando jurisprudencia y doctrina. Después analiza el Contrato de Cuenta Corriente Bancaria, al tenor del DFL N° 707, el Código de Comercio, la Recopilación Actualizada de Normas de la CMF o RAN, y el propio contrato celebrado con cada cliente. Concluye, luego de analizar el contrato de cuenta corriente bancaria y el depósito irregular, que las diferencias que entrega, significan que la interpretación de la Corte Suprema es errónea, por cuanto se exige a los Bancos una obligación que ni legal ni contractualmente les es exigible: que el cliente no entregue su clave. Hacer a los Bancos responsables significa desconocer toda la regulación especial de la cuenta corriente bancaria, que además, implica hacerlos responsables de un hecho que escapa absolutamente de su control: la entrega de claves por parte del cliente.

Refiere que el uso y custodia de las claves es responsabilidad de los clientes, lo que significa una modificación expresa de las partes a los elementos del contrato de depósito irregular. Así, si bien es cierto que en el caso de error o fuerza mayor, quien asume el riesgo es el depositario; ello no es así en el contrato celebrado entre las partes (ya sea de cuenta corriente o de mutuo irregular), pues ellas, libre y voluntariamente acordaron lo contrario para este tipo de casos. Así, son los clientes los responsables de custodiar sus claves. No existiendo una vulneración a los sistemas del Banco, de acuerdo a lo pactado, no es responsabilidad de la recurrida.

Acota que de los hechos descritos por la propia recurrente y, las aclaraciones efectuadas por esta parte, sólo es dable concluir que la acción de protección de autos debe ser rechazada, por cuanto no procede frente a un supuesto incumplimiento contractual. Se trata, en consecuencia, de un asunto de lato conocimiento. No hay acto arbitrario o ilegal de Scotiabank Chile.

No existe privación, perturbación o amenaza de un derecho de la actora por parte de Scotiabank Chile. No existen medidas que la Corte pueda adoptar.

En este caso, no se cumple la más elemental condición de procedencia de esta clase de acciones, pues la recurrente pretende obtener una sentencia en sede de protección, limitándose a invocar un supuesto incumplimiento contractual de esa parte, no es un derecho indubitado, y ello, por cierto, tampoco resulta procedente.

De hecho, la recurrente reconoce que la relación que existe entre las partes, en donde se daría un supuesto incumplimiento de su representada al deber de cuidado, es contractual, lo que habría ocasionado incluso, daños morales y supuestas publicaciones indebidas, señalando expresamente en su libelo: lo que se alega en realidad, es un supuesto incumplimiento al contrato de cuenta corriente celebrado entre las partes, por consiguiente, la intención de la contraria es que, a raíz de un supuesto fraude cometido por terceros ajenos al Banco, este último pague por los perjuicios causados a raíz de un supuesto incumplimiento a las disposiciones del contrato suscrito y de la ley, vulnerando un deber contractual de cuidado. Lo que busca discutir la actora es si es que, en el marco de una relación contractual, existe un incumplimiento de obligaciones que haya causado daño, el cual busca le sea indemnizado.

La arbitrariedad, según la jurisprudencia, *"implica carencia de razonabilidad en el actuar u omitir; falta de proporción entre los medios y el fin a alcanzar; ausencia de ajuste entre los medios empleados y el objetivo a obtener o una inexistencia de los hechos que fundamentan un actuar"*. Conforme la Real Academia Española, arbitrariedad se define como *"acto o proceder contrario a la justicia, la razón o las leyes, dictado solo por la voluntad o el capricho".*

Sin embargo, no hay conducta alguna de su representada que haya vulnerado el derecho de propiedad de la actora ni a su integridad física y psíquica. Es más, del relato de la recurrente aparece que incluso tiene identificada a la persona que recibió el dinero y que habría participado en el supuesto fraude. Además, no puede existir vulneración alguna al derecho de propiedad ni de integridad en el actuar del banco, pues, no hubo vulneración a las medidas de seguridad del Banco: y quien tenía el deber de

custodiar sus claves, era la propia recurrente, fallando en ello, por lo que, de conformidad al contrato celebrado por las partes, debe hacerse responsable por el riesgo.

Tampoco hay medidas que la Corte pueda adoptar, al no ser necesario restablecer el imperio del derecho, desde que no ha existido acto ni arbitrario ni ilegal pues no es posible restituir dineros que no ha recibido, sino que han sido transferidos a terceros, sin vulneración de las medidas de seguridad del Banco, con claves secretas cuya custodia le corresponde a la recurrente, por lo que la acción debe ser rechazada.

Finalmente, dice que no puede adoptarse medidas concretas por la vía constitucional, ya que al ejercer una especie de acción restitutoria que emana de un fraude sufrido por ella, vulnera lo dispuesto en el artículo 680 N° 10 del Código de Procedimiento Civil, puesto que debe discutirse, en sede penal, quien o quienes son los responsables del fraude y su participación en los hechos, para luego, como lo previene el artículo 680, determinar las indemnizaciones pertinentes.

Acompaña al Informe: sentencias dictadas por Cortes de Apelaciones y la Excma. Corte Suprema en que, en casos como este, se han rechazado los recursos de protección por diversos motivos; entre ellos, por tratarse de asuntos de lato conocimiento; Set de publicaciones en redes sociales realizadas por los Bancos en materia de Ciberseguridad.; Publicaciones en el sitio web del Banco sobre Ciberseguridad; Opinión del Comité de Asuntos Jurídicos de la ABIF sobre la jurisprudencia en que la actora basa su recurso; Informe denominado "Ciberseguridad en la Banca", confeccionado por la Asociación de Bancos e Instituciones Financieras y citado en lo principal de este escrito, que explica que la Ciberseguridad es tarea de todos; Documento denominado "Lo que necesito saber de mi tarjeta de Crédito", confeccionado por la Asociación de Bancos e Instituciones Financieras, el que explica, en su página 14, los cuidados que se deben tener con las claves; Contrato de Operaciones Bancarias del Cliente y Contrato de Tarjeta de Crédito.

Tercero: Que, como reiteradamente se ha dicho por esta Corte, el recurso de protección de garantías constitucionales consagrado en el artículo 20 de la Constitución Política de la República, es una acción de carácter cautelar, destinada a amparar el legítimo ejercicio de las garantías y derechos preexistentes que en esa misma disposición se enumeran, mediante la adopción de

medidas de resguardo que se deben tomar ante un acto arbitrario o ilegal que impida, amague o perturbe ese ejercicio.

Surge de lo dicho que es requisito indispensable de la acción cautelar de protección la existencia, por un lado de un acto u omisión ilegal, esto es, contrario a la ley, o bien acto u omisión arbitrario es decir, producto del mero capricho o voluntad de quien incurre en él, y por el otro, debe provocar alguna de las situaciones antes indicadas de impedir, amagar o perturbar el ejercicio de alguna de las garantías que el artículo 20 menciona.

Cuarto: Que, como se reseñó en el apartado primero de este fallo, el acto tildado de ilegal y arbitrario por la recurrente es, la respuesta dada por Daniel Espinoza Fernández, en representación del banco recurrido a su petición de reembolsarle el cargo efectuado a su cuenta corriente el 4 de diciembre de 2019, por la suma de $ 4.999.890 y 5 operaciones de su tarjeta de crédito.

El contenido de dicha respuesta es el siguiente: *"En lo que respecta a la revisión efectuada por el Banco, se detectó que las transacciones fueron realizadas a través de internet. Para la realización de las transacciones objetadas, necesariamente se debe ingresar con su usuario (Rut), la clave personal de ingreso a su sesión y, además, su clave Kevpass, información cuya custodia y uso, son de responsabilidad exclusiva del cliente. Realizada la investigación pertinente, se concluyó que no existió una vulneración a los sistemas de seguridad del Banco, pues las transacciones fueron validadas con la información antes referida. Presumimos en consecuencia, la existencia de un Malware (virus) en sus dispositivos electrónicos que hubieran podido provocar la captura de sus credenciales de seguridad para acceder a los servicios del Banco, lo que habría permitido a los supuestos terceros efectuar las operaciones objetadas. Es por este motivo que le recomendamos formatear sus equipos y actualizar de forma periódica los programas antivirus de los mismos, con el fin de evitar este tipo de situaciones".*

Con la indicada respuesta, el Banco negó realizar el reembolso de dinero a la cuenta corriente de la recurrente, por haberse concluido, de acuerdo a una investigación interna, que no hubo vulneración a los sistemas de seguridad y, en definitiva, se le

atribuye la exclusiva responsabilidad de custodiar una información que fue utilizada por los defraudadores.

Quinto: Que, la recurrida en su informe, reconoce tal hecho, pero sostiene que no le consta que la actora haya sido efectivamente víctima de un fraude, por lo que tiene que probarlo y, declararlo así el tribunal pertinente, en un procedimiento de lato conocimiento. Lo que le consta, es que no existió una vulneración de sus sistemas y que la recurrente se identificó digitalmente, utilizando sus claves de seguridad, para realizar las transacciones objetadas, por lo que podría tratarse de un caso de auto-fraude, o de un uso indebido de claves por terceros cercanos a la actora, de estafa o de fraude informático fraguado por terceros, etc. Por ello, plantea que de acuerdo a los hechos descritos y antecedentes recabados, es imposible determinar lo que aconteció, siendo necesaria una investigación penal exhaustiva.

Sexto: Que, la recurrida concluye que el acceso a la cuenta de la recurrente para fines de ejecutar transacciones de modo remoto, implica necesariamente tener conocimiento, al mismo tiempo, de las cuatro claves de seguridad, que le permiten tener acceso a la tarjeta de crédito y cuenta corriente de la recurrente, contraseñas de las que aquella disponía.

Sin embargo, nada dice acerca de que la tarjeta de crédito no había cambiado de la clave original que esta tiene al ser entregada, que de acuerdo a su política de información al cliente, aconseja su cambio de inmediato por otra; que se hizo una transacción mientras aquella estaba en el extranjero, por el máximo que está permitido realizar, cifra que fue transferida, de inmediato, a la cuenta corriente de otra persona del mismo banco que está plenamente identificada, respecto de la cual no hizo ninguna averiguación en su investigación interna y nada se dice en el informe, al igual que las operaciones efectuadas con la tarjeta de crédito a un mismo establecimiento, respecto del cual, nada averiguó.

El sistema de seguridad del banco y la política de información no puede quedarse en simples anuncios, ante la sospecha cierta que hubo un fraude informático para acceder a las cuentas de una cliente, sin que sea bastante la mera entrega de la tarjeta de crédito, con su clave universal, para que, por sobre las eventuales medidas de seguridad de la institución bancaria, se aprobaran las transacciones impugnadas, revelando la precariedad del protocolo para el ingreso a la cuenta corriente y su posterior operación, las

cuales no extrañaron al banco pese a que contrastaban con la conducta habitual y ordinaria de su cliente, sobre todo advirtiéndose que implicaban al menos una transacción a favor de otra cuenta corriente de un tercero en la misma institución bancaria, muy superior a las transacciones acostumbradas por la recurrente, cuestiones desatendidas en la investigación interna realizada por el banco para determinar si daba o no lugar a la petición de no imputarle los cobros a la cliente, que develan un actuar negligente de la institución en la protección de la cuenta corriente y uso de la tarjeta de crédito de su cliente.

Desde la cómoda posición del Banco recurrido, de endilgarle toda la responsabilidad a la cliente, con una investigación interna incompleta, sin tomar medidas respecto de los datos concretos entregados por la cuentacorrentista, implican no haber dado cumplimiento al deber de protección y resguardo que tiene en razón de contratos válidamente celebrados, lo que torna su proceder en ilegal y arbitrario, por ir en contra de la legislación vigente y, obrar sin razonabilidad.

Séptimo: Que, a mayor abundamiento, conforme al artículo 40 de la Ley General de Bancos, dichas entidades están facultadas para realizar una serie de actos destinados a captar en forma habitual dineros del público con el objeto de darlos en préstamo y realizar otras operaciones, entre ellas, celebrar el contrato de cuenta corriente bancaria. En virtud de éste, el banco se obliga a cumplir las órdenes de pago de otra persona hasta la concurrencia de las cantidades de dinero que se hubieren depositado en aquella (artículo 1° del D.F.L. N° 707 de 1982).

Octavo: Que, de acuerdo a lo antes razonado, se desprende que los dineros sustraídos de una cuenta corriente bancaria en forma tal, que reviste caracteres de un fraude informático, utilizando las claves de acceso a la misma y sin el consentimiento de su titular, como ocurre en la especie, no corresponden a caudales específicos del cuentacorrentista, por tratarse del depósito de un género y no de cuerpos ciertos, que además son bienes fungibles (artículo 575 del Código Civil), esto es, las especies monetarias empleadas para la satisfacción de lo debido están dotadas de igual poder liberatorio y pueden reemplazarse unas a otras o recíprocamente en la ejecución de las obligaciones.

Noveno: Que, de este modo, aun cuando el hecho se haya ejecutado mediante el uso irregular de los datos y claves bancarias personales de la actora, lo sustraído es dinero, bien fungible que se

confunde con otros de igual poder liberatorio, con lo que resulta no sólo jurídica sino físicamente imposible sostener y menos acreditar la exacta identidad de las especies sustraídas mediante el fraude perpetrado a través de la cuenta bancaria de la recurrente, circunstancia que lleva a concluir que en definitiva el único y exclusivo afectado por el engaño referido es el banco recurrido, dada su calidad de propietario del dinero depositado, en quien recae finalmente el deber de eficaz custodia material de éste, debiendo adoptar, al efecto, todas las medidas de seguridad necesarias para proteger adecuadamente el dinero bajo su resguardo.

Décimo: Que, establecido lo anterior, no queda más que concluir que el actuar de la recurrida debe ser calificado como ilegal y arbitrario, puesto que al no asumir el perjuicio económico, trasladando los efectos del fraude bancario a la actora, afecta directamente al patrimonio de ésta, vulnerando así el artículo 19 N° 24 de la Carta Fundamental.

Idéntica calificación tiene la publicación en Dicom de la morosidad proveniente del mismo hecho, debiendo la entidad bancaria retirar la indicada información.

En mérito de lo razonado y de conformidad, además, con lo que dispone el artículo 20 de la Constitución Política de la República y Auto Acordado de la Excma. Corte Suprema sobre la materia, **SE ACOGE**, el recurso de protección interpuesto por Claudia Andrea Cañas Pinochet, ordenándose en consecuencia que el Banco Scotiabank Chile SAB, debe retrotraer y dejar sin efecto las operaciones que figuran en la tarjeta de crédito y cuenta corriente de la recurrida, realizadas el día 4 de diciembre de 2019, junto con todo cargo o cobro accesorio a ellos, tales como, a vía ejemplar, intereses, impuestos, comisiones, etc., eliminándose de todo registro de deuda en el que haya informado a la recurrente como deudora morosa en Dicom, que sean producto de las transacciones fraudulentas a que se refiere la presente acción cautelar.

Regístrese y archívese, en su oportunidad.

Redacción del Ministro Miguel Eduardo Vázquez Plaza.

Rol Corte N° 25.798-2020. Protección.

MIGUEL EDUARDO VAZQUEZ PLAZA
MINISTRO
Fecha: 16/06/2020 08:40:32

MARIO DANILO ALEJANDRO ROJAS GONZALEZ
MINISTRO
Fecha: 16/06/2020 12:15:50

INELIE LEDDA DURAN MADINA
MINISTRO
Fecha: 16/06/2020 08:29:15

KPTXGWZEWS

Pronunciado por la Quinta Sala de la C.A. de Santiago integrada por los Ministros (as) Miguel Eduardo Vazquez P., Mario Rojas G., Inelie Duran M. Santiago, dieciséis de junio de dos mil veinte.

En Santiago, a dieciséis de junio de dos mil veinte, notifiqué en Secretaría por el Estado Diario la resolución precedente.

KPTXGWZEWS