S.f.g.
C.A. de Valparaíso

Valparaíso, seis de mayo de dos mil veinte.

Visto:

A folio 1, comparece Ignacio García Morales, abogado, quien actuando por el afectado **Patricio Marcelo Péndola Sáez**, médico siquiatra, interpone acción constitucional de protección en contra del **Banco Bilbao Viscaya Argentaria** (BBVA), persona jurídica de Derecho Privada, Sociedad Anónima Bancaria, representada legalmente por su Gerente General señor Manuel Antonio Olivares Rossetti.

Indica que el afectado es cliente del Banco Scotiabank (Ex BBVA) desde hace aproximadamente dos años, y es titular de una cuenta corriente número 0504-0327-0100020228, línea de crédito, una tarjeta de débito y dos tarjetas de crédito (Visa y MasterCard), precisando que éste posee esa cuenta corriente solamente en relación con un crédito hipotecario contraído con el banco, por lo tanto, su uso es muy acotado.

Explica que al momento del fraude el recurrente mantenía en la cuenta por concepto de ahorros la suma de $3.222.819; agregando que éste solo usaba con cierta frecuencia la tarjeta de débito para compras de bajos montos y nunca había activado ni usado las tarjetas de crédito asociadas. Así, el jueves 7 de noviembre del 2019 a las 8 de la mañana, al revisar su correo electrónico, verifica varias notificaciones de Banco Scotiabank, por transacciones de altos montos hechas durante la madrugada del mismo día (transferencias electrónicas y solicitud de avances de dinero en las tarjetas antes mencionadas). Llamó inmediatamente al Call-Center del banco, procediendo a solicitar el bloqueo de todos sus productos (código de bloqueo SD071119), y a las 9 de la mañana del mismo día, concurrió personalmente a la sucursal del banco de Avenida Libertad con 9 Norte, Viña del Mar, donde verifican que durante el día 6 de noviembre y la madrugada del 7 de noviembre, se llevaron a cabo una serie de transacciones fraudulentas desde su cuenta corriente por un monto aproximado de $70.000.000.

Refiere que los responsables del fraude hicieron uso de su saldo de la cuenta corriente y la línea de crédito que en conjunto sumaban casi $6.000.000, posteriormente solicitaron un crédito de consumo por un monto de $56.636.800 y solicitaron dos avances de dinero, uno en la tarjeta VISA y otro en la tarjeta MasterCard, de $2.850.000 cada uno. El dinero fue gastado en al menos 4 trasferencias electrónicas a cuentas desconocidas de otros bancos de $5.000.000 cada una, compras en línea en diversos portales de compras, así como pagos de cuentas a través de portales de pagos, quedando un saldo restante al momento de bloquear la cuenta de aproximadamente $34.000.

VGXCPMVTCM

Destaca que durante las horas que fueron realizadas estas transacciones, el afectado no tuvo conocimiento de éstas, y nunca hubo un llamado de alerta de movimientos sospechosos por parte del banco. Por otro lado, resulta evidente la violación de las medidas de seguridad del banco, puesto que pudieron solicitar un crédito sin la verificación de identidad ni solicitud de claves adicionales, hacer uso de tarjetas que jamás habían sido activadas y hacer transferencias electrónicas a cuentas desconocidas por montos de $5.000.000 en 4 ocasiones en menos de 24 horas.

Señala que teniendo conocimiento de lo sucedido el afectado se dirigió a la oficina de la Policía de Investigaciones, parte policial número 7509. Y antes de las 14 horas del día 7 de noviembre, volvió al banco e inicia los trámites para hacer la denuncia interna de fraude y activar el seguro de protección contra fraudes que tenía contratado. Precisando que durante la tarde se pone en contacto por teléfono y por mail la Directora de Experiencia de Clientes quien recién le informa al afectado sobre una serie de "movimientos sospechosos" en su cuenta.

Menciona que hasta la fecha el afectado no ha recibido una respuesta formal sobre su situación financiera en relación con el fraude del que fue víctima, no ha existido respuesta del banco en relación de cuál sería la responsabilidad del banco en este siniestro. En cuanto al seguro para fraude le notifican el día 29 de noviembre del 2019 que su solicitud ha sido rechazada en relación a las tarjetas de crédito por no estar dentro de la cobertura del seguro, y luego el día 4 de diciembre notifican que se ha aceptado que los hechos están dentro de la cobertura en relación a la cuenta corriente, pero esta cubre sólo 150 UF.

Expresa que ya se han facturado los montos incluidos en el fraude, por lo que la fecha de pago de la primera cuota del crédito de consumo, así como de las tarjetas de crédito, están fechados para los primeros días de diciembre. Por lo que el Banco, de forma ilegal y arbitraria, puso de cargo del patrimonio del señor Péndola, como un pasivo, la obligación de solventar los dineros por los que fue defraudado el mismo Banco, debido al actuar de terceros y su propia deficiente seguridad. A lo anterior, se añade el hecho de que el Banco, hasta la fecha, se niega a eliminar el pasivo desde el patrimonio del señor Péndola, pese a reconocer el fraude.

Seguidamente, en cuanto a cómo se fragua el fraude bancario, explica que durante la tarde del día 06 de Noviembre de 2019, contacta al recurrente, un ejecutivo del Banco para señalarle que producto del contexto de fusión del Banco BBVA a Scotiabank azul y en el proceso de migración de clientes debía realizar una actualización de sus claves de ingreso a la página web del Banco, mediante una serie de instrucciones que replicaban métodos de uso común en materia de transacciones bancarias vía telefónica, el ejecutivo en cuestión le solicita al afectado digitar su clave de acceso a su cuenta corriente en el teléfono, procurando ser muy claro en que el Banco no solicita claves

VGXCPMVTCM

vía telefónica y que, por ello, ésta debía ser digitada en el teléfono. Posterior a ello, durante la noche del día 6 de noviembre y la madrugada del día 7 del mismo mes, se produce todo el movimiento bancario denunciado.

En consecuencia, el recurrido arbitrariamente, genera un pasivo en el patrimonio del señor Péndola, con el objeto de cubrir los efectos del fraude de que ha sido víctima el propio Banco; negándose éste a restituir los fondos que le fueren arrebatados desde la cuenta corriente. Finalmente, señala que lo expuesto afecta y vulnera el derecho de propiedad del recurrente, contemplado en el N° 24 del artículo 19 de la Constitución Política de la República.

Por tanto, en virtud de lo expuesto, solicita se ordene al banco recurrido que restablezca los fondos retirados de la cuenta corriente del recurrente, que tome las medidas necesarias para sacar del pasivo de éste los créditos y avance en efectivo sacados subrepticiamente de los productos contratados con el banco, que ordene de forma inmediata el cobro de intereses asociados al fraude informático de que fuere víctima el banco recurrido, sin perjuicio de las medidas de protección que se estime del caso adoptar, con costas.

A folio 11, informa la recurrida **Scotiabank Chile S.A.**, (continuador legal de BBVA), solicitando el rechazo del presente recurso, con costas.

En primer lugar, señala que, este recurso fue establecido como un mecanismo de emergencia, concebido para salvaguardar y restablecer el imperio del derecho frente a la vulneración de determinados derechos fundamentales, pero no constituye una vía para conocer asuntos delictuales, cuyo conocimiento, juzgamiento y ejecución de la eventual sanción es de competencia exclusiva de los tribunales penales.

En segundo lugar, niega la existencia de cualquier incumplimiento en las medidas de seguridad adoptadas por el banco en los hechos; añadiendo que el fraude sólo pudo ocurrir con motivo de la entrega que se hizo de su información personal a terceros; no por culpa de un actuar culpable o negligente de su representado, sino por una falta en la obligación del cliente de custodiar sus claves. Lo anterior queda de manifiesto, mediante los propios dichos del recurrente, el cual en su recurso reconoce expresamente haber entregado telefónicamente su clave de acceso a un tercero. Precisa que es un hecho público y ampliamente difundido por los bancos a los clientes, que estos NO DEBEN proporcionar sus claves a terceros y que sólo deben usarla en las páginas web de cada entidad. Se informa además a los mismos clientes que no empleen sus claves a través de los denominados "link" de correos ni los entreguen por teléfono.

En base a lo anterior y realizada la investigación correspondiente, en virtud del reclamo realizado por el Sr. Péndola, la Gerencia de Servicios Forenses Digitales del Banco Scotiabank, pudo concluir que el cliente habría sido engañado, proporcionando su clave

VGXCPMVTCM

personal y secreta, permitiendo a terceros acceder a su sitio personal, suplantando al cliente y efectuando las transacciones. Por lo tanto, no hubo vulneración a los sistemas de seguridad del banco, sino que estamos en presencia del llamado "cuento del tío". Explicando que se investigó el origen de las transacciones objetadas por el cliente, determinando que éstas fueron realizadas a través del canal Scotiaweb, siendo correctamente validadas por los sistemas de seguridad del banco. Se evidencia la autorización mediante el uso de dispositivo KeyPass.

Sin perjuicio de lo indicado anteriormente, hace presente que su representado, una vez que tomó conocimiento del posible fraude denunciado, procedió de inmediato al bloqueo de todos los productos del cliente y gracias a un rápido actuar logró reversar una gran cantidad de las operaciones realizadas y desconocidas por el recurrente. Si bien el texto del recurso, no es preciso y detallado en relación a los montos de las distintas operaciones llevadas a cabo los días 06 y 07 de noviembre de 2019, las cuales el cliente desconoce, éste indica que las transacciones fraudulentas desde su cuenta corriente fueron por un monto aproximado de $70.000.000.-

En base a la información obtenida, el monto objetado por el cliente fue de $68.084.474.- de los cuales, producto de la gestión realizada por el área de Prevención de Fraude en conjunto con el área de tecnología, se alcanzaron a reversar $44.987.006.- de los $48.084.456 que correspondían a pagos de servicios.

Añade que además, se alcanzó a retener $1.200.000.- en el Banco Santander, producto que la receptora de las transferencias alcanzó a retirar parte de los fondos el mismo día, mediante giro por caja y transferencias hacia otro banco. Asimismo, fue posible retener $9.800.000.- en Banco BCI, gracias a las gestiones en conjunto con el Banco Santander, quien inmediatamente solicitó la retención por fondos provenientes de su representado.

Refiere, por otra parte, en base a los Informes de Liquidación N°TJS/11- 2019/01021062 y N°TJS/11-2019/01022872, la Compañía de Seguros indemnizó al recurrente, de acuerdo al plan contratado, con la suma de $4.236.750.- siendo rechazado uno de los siniestros denunciados por no estar contemplado dentro de la cobertura del seguro contratado.

Indica que de acuerdo a lo expuesto, no existe un actuar arbitrario por parte de su representado. Las transferencias electrónicas y avances se hicieron a través del sitio privado del Banco, ingresando los datos y claves personales y secretas del cliente, quien está obligado a custodiarlas. El Banco, notificado por el recurrente de los hechos, tomó las medidas necesarias y bloqueó la cuenta, para luego remitir todos los antecedentes a la compañía de seguros contratada por éste para el caso de fraudes y, además, está llana a aportar todos los antecedentes que sean solicitados en una futura investigación penal. Destacando que la sola existencia de un fraude o una estafa cometida

VGXCPMVTCM

por un tercero no significa, de por sí, la concurrencia de responsabilidad del Banco. Seguidamente, señala que no existe un actuar ilegal del banco; en el contrato suscrito por el actor se le informa la necesidad de resguardar sus claves y de jamás entregárselas a terceros; agregando que tampoco existe actuar alguno de su representado que haya vulnerado el derecho de propiedad del actor. En efecto, quien lo ha hecho es, de acuerdo a su propio relato, el delincuente que urdió un esquema para obtener sus datos personales y datos bancarios; razón por la cual, solicita rechazar el recurso de protección interpuesto, con costas.

A folio 28, informa el **Banco de Crédito e Inversiones**, indicando que en virtud de la impugnación requerida por Banco Scotiabank- Banco Santander, este último en calidad de puente transaccional, con fecha 7 de noviembre 2019, mediante correo electrónico y expresando que cliente de origen Banco Scotiabank, Sr. Patricio Péndola Sáez, desconocía transacciones originales, el BCI mantiene retención de $9.800.000.

A folio 30, informa el **Banco Santander Chile**, señalando que efectivamente se encuentra retenida la suma de $1.200.000 en la cuenta 7058059409 asociada al Rut N° 202731074, producto de solicitud efectuada por Banco Scotiabank en el marco del proceso de validación realizada por la entidad bancaria.

A folio 36, se ordenó traer los autos en relación.

Con lo relacionado y considerando

Primero: Que la acción constitucional de protección, consagrada en el artículo 20 de la Constitución Política de la República, ha sido establecida a favor de quien, por causa de actos u omisiones arbitrarios o ilegales, sufra privación, perturbación o amenaza en el legítimo ejercicio de los derechos y garantías establecidas en el artículo 19 de la Carta Fundamental.

Segundo: Que el recurrente hace consistir su arbitrio constitucional en la ilegalidad o arbitrariedad de la conducta desplegada por la recurrida, en cuanto a que genera un pasivo en el patrimonio del Sr. Péndola Sáez, con el objeto de cubrir los efectos del fraude de que ha sido víctima el propio banco, y que éste además se ha negado a restituir los fondos que le fueren arrebatados desde la cuenta corriente, y que fueren sustraídos producto de las evidentes deficiencias en materia de seguridad del banco recurrido.

Por su parte, el Banco Scotiabank, ha alegado en primer lugar que la acción de protección no constituye una vía para conocer asuntos delictuales, en este caso específico, un delito económico, cuyo conocimiento, juzgamiento y ejecución de la eventual sanción es de competencia exclusiva de los tribunales penales. Y en segundo lugar, niega la existencia de cualquier incumplimiento en las medidas de seguridad adoptadas por el banco, precisando que el fraude solo pudo ocurrir por una falta en la obligación del cliente de custodiar sus claves.

VGXCPMVTCM

Tercero: Que la acción incoada tiene por objeto restablecer el imperio del derecho y asegurar la debida protección del afectado, mediante un procedimiento extraordinario, rápido y concentrado, lo que supone la existencia de una vía de hecho o de un acto ilegal que de manera evidente vulnere derechos indubitados del afectado.

Cuarto: Que la Excma. Corte Suprema ha sostenido en casos similares al de la especie, 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 que, para cada caso, resulta relevante analizar si los eventos que originaron las transferencias cuestionadas no han tenido como única causa la voluntad del depositante o cuentacorrentista, o han ocurrido otros que llevan a sostener que se han incumplido las obligaciones de resguardo y seguridad que recaen en la institución bancaria respectiva" (causas Rol N°s. 31.744-2018, 32.864-2018 y 2. 196-2018).

Quinto: Que sin perjuicio de lo incontrovertible que sería para el cliente el perjuicio patrimonial que representaría el giro de dinero no consentido desde su cuenta bancaria, del mérito de los antecedentes hasta ahora reunidos, no puede determinarse en forma fehaciente la forma en que se efectuaron los giros que se cuestionan desde la cuenta corriente del recurrente, existiendo controversia al respecto, toda vez que lo declarado por el actor y lo informado por el Banco Scotiabank, se tratan de hechos que deben ser materia de prueba.

Que así, no existe un derecho indubitado que justifique proceder mediante la vía extraordinaria del recurso de protección, pues se requiere de un juicio declarativo que permita, con las pruebas que cada una de las partes aporte, establecer las medidas de seguridad reglamentarias y contractuales que debían implementarse por la recurrida para evitar fraudes, determinar el origen o causa de las transferencias electrónicas y si ello obedece a negligencia del banco o del actor, por lo que corresponde desestimar el recurso de protección.

Sexto: Que a mayor abundamiento, de acuerdo a los dichos del propio recurrente, el día 6 de noviembre 2019, a través de una llamada telefónica recibida supuestamente por parte de un ejecutivo del Banco Scotiabank, facilitó su clave de acceso, digitando ésta a través de su celular.

Por estas consideraciones y visto, además, lo dispuesto en el artículo 20 de la Constitución Política de la República y Auto Acordado de la Excma. Corte Suprema sobre la materia, **se rechaza**, el recurso de protección deducido por don **Patricio Marcelo Péndola Sáez**, en contra del **Scotiabank Chile S.A.**, (continuador legal de BBVA).-

Acordada con el **voto en contra** del Ministro Suplente don Erik Gonzalo Espinoza Cerda, quien estuvo por acoger la presente acción de protección, en razón de las siguientes consideraciones:

VGXCPMVTCM

Primero: Que, entiende este juez 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, interpretación que también ha sido aceptada por la Exma Corte Suprema (en fallo de de 20/06/18, rol Nº 2.196-2018); Que, a su vez este juez entiende que de la tarjeta de crédito, deriva una especie de mutuo, donde una de las condiciones de la esencia es que el titular de ella manifieste su voluntad en su uso, y que es de cargo del banco el verificar si aquello efectivamente ocurrió, y que, para cada caso, resulta relevante analizar si los eventos que originaron las transferencias cuestionadas no han tenido como causa la voluntad libre del recurrente, o han ocurrido otras circunstancias que llevan a sostener que se han incumplido las obligaciones de resguardo y seguridad que recaen en la institución bancaria respectiva.

Segundo: Que, en efecto, la variedad de las formas como se intenta vulnerar los sistemas de seguridad y la dificultad probatoria inmediata obligan a realizar un juicio acerca de indicios sobre la ocurrencia de los hechos y confrontar aquellos con las diversas normas que determinan las obligaciones de seguridad de las instituciones bancarias. Así, para el caso de transferencias electrónicas, el Capítulo 1-7, punto 4.2, de la Recopilación de normas de la Superintendencia de Bancos indica que: "Los bancos deberán contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible aquellas operaciones con patrones de fraude, de modo de marcar o abortar actividades u operaciones potencialmente fraudulentas, para lo cual deberán establecer y mantener, de acuerdo a la dinámica de los fraudes, patrones conocidos de estos y comportamientos que no estén asociados al cliente. Estos sistemas o mecanismos deberán permitir tener una vista integral y oportuna de las operaciones del cliente, del no cliente (por ejemplo en los intentos de acceso), los puntos de acceso (por ejemplo direcciones IP, Cajero Automático u otros), hacer el seguimiento y correlacionar eventos y/o fraudes a objeto de detectar otros fraudes, puntos en que estos se cometen, modus operandi, y puntos de compromisos, entre otros."

Tercero: Que, de lo expuesto, se concluye que la recurrida señala en su informe que las transferencias y/o asunción de un crédito, se realizaron debido la actividad de la cliente, lo cual es efectivo, pero que conforme a la situación de comunicación supuesta del banco que no fue tal, que se desprende de la actividad del recurrente y de la propia recurrida que le dan cuenta al cuentacorrentista de movimientos extraños en su cuenta, una vez ya realizadas las transferencias indicadas en el presente recurso, lo cual ya da cuenta de un sistema de hackeo, ante lo cual se ingresaron sus datos y número de digipass y ya tenia las transacciones por ella no realizadas a favor de una tercera persona no determinada, planteando la recurrida que todo se debió a la

VGXCPMVTCM

intervención de la demandante, y que si algo estaba mal era de su cargo y responsabilidad.

Cuarto: Que, teniendo presente los hechos asentados resulta que se advierte que la recurrida le devolvió una serie de sumas de dineros por ser efecto de un fraude, pero el saldo que no devolvió, indica que no sería propio de fraude de la operación cuestionada, lo cual es una situación antagónica que argumentalmente no tiene sustento. A su vez se advierte descartar que los hechos se han debido única e inequívocamente a una actividad dolosa o negligente de la recurrente, ya que no aparece que se le pueda achacar que por su actividad únicamente se produjo esta situación, por cuanto si no se contacta al cuentacorrentista para verificar su aquiescencia en un crédito de esta magnitud, unido a que por razones de buena fe, el demandante por lo que pudiera internamente creer sobre que se estaba comunicando efectivamente con la recurrente, dando sus datos en razón de ello.

Quinto: Que además, las obligaciones de monitoreo y control de fraudes recaen expresamente en la institución recurrida, donde los patrones de conducta del cliente son elementos de juicio, para la determinación de una operación para producir engaño, sobre todo si las tarjetas de crédito no habían sido activadas, cuestión que no fue informada en detalle por el Banco recurrido. Sobre la institución bancaria recae la obligación de vigilancia y el análisis de la correlación de eventos y seguridad de las operaciones, por lo que, una vista general de las operaciones del cliente en la cuenta corriente respectiva otorgan verosimilitud a la intervención de terceros en los sistemas de seguridad de la recurrida.

Sexto: Que asentado lo anterior, a juicio de este sentenciador, no queda más que calificar el actuar de la recurrida como ilegal y arbitrario, puesto que al no asumir el perjuicio económico trasladando los efectos del fraude bancario al actor, afecta directamente el patrimonio de éste, vulnerando así el artículo 19 N° 24 de la Constitución Política.

Regístrese, notifíquese y archívese en su oportunidad.

N°Protección-40.433-2019.-

Pablo Andres Droppelmann Cuneo
MINISTRO
Fecha: 06/05/2020 12:51:46

Erik Gonzalo Espinoza Cerda
MINISTRO(S)
Fecha: 06/05/2020 12:51:59

VGXCPMVTCM

Monica Milagros Gonzalez Alcaide
Fiscal
Fecha: 06/05/2020 12:54:22

VGXCPMVTCM

Pronunciado por la Segunda Sala de la C.A. de Valparaíso integrada por Ministro Pablo Droppelmann C., Ministro Suplente Erik Gonzalo Espinoza C. y Fiscal Judicial Monica Milagros Gonzalez A. Valparaiso, seis de mayo de dos mil veinte.

En Valparaiso, a seis de mayo de dos mil veinte, notifiqué en Secretaría por el Estado Diario la resolución precedente.

VGXCPMVTCM

Este documento tiene firma electrónica y su original puede ser validado en http://verificadoc.pjud.cl o en la tramitación de la causa.
A contar del 05 de abril de 2020, la hora visualizada corresponde al horario de invierno establecido en Chile Continental. Para la Región de Magallanes y la Antártica Chilena sumar una hora, mientras que para Chile Insular Occidental, Isla de Pascua e Isla Salas y Gómez restar dos horas. Para más información consulte http://www.horaoficial.cl