

Concepción, dos de junio de dos mil veinte.

Vistos:

Compareció en estos antecedentes **Rol N° 6.909-2020**, Sebastián Alejandro Vásquez Olcese, abogado, domiciliado para estos efectos en Avenida Costanera N° 7.488, of. 206 A, de la comuna de San Pedro de la Paz, ciudad de Concepción, en favor de Álvaro Rodrigo Mardones Urra, ingeniero mecánico, chileno, domiciliado en calle Parque Nacional Tolhuaca N°6830, comuna de San Pedro de la Paz, de la ciudad de Concepción, y dedujo acción de protección constitucional en contra de Banco Scotiabank Chile -Ex Banco Bilbao Vizcaya Argentaria Chile- (en adelante, conjunta o indistintamente "Banco", "Banco Scotiabank" o "Recurrido"), sociedad del giro de su denominación, representado por Francisco Sardón de Taboada, Gerente General, ambos domiciliados en calle Morandé N° 226, comuna de Santiago.

Expone, en síntesis, que en el contexto de la fusión de las entidades bancarias BBVA y Scotiabank, el día 11 de junio de 2019, alrededor de las 18:20 horas, mientras su representado se encontraba en su oficina, "lo contactó telefónicamente un ejecutivo del Banco", informando que a propósito del proceso de migración de clientes producto de la fusión, para advertir del cambio que experimentaría la plataforma computacional debido a la migración de los clientes, necesitaba ratificar sus datos personales de conocimiento del Banco, confirmado si eran ciertos. A las preguntas realizadas por dicho ejecutivo, su patrocinado contestó afirmativamente. Luego el mismo "ejecutivo", le indicó que por el mismo motivo debía cambiar su clave de acceso web, la cual era enviada de manera automática a su celular de confianza en conocimiento de BBVA mediante mensaje de texto, y



otra clave numérica de confirmación de cuatro dígitos que le llegó por correo electrónico desde la casilla scotianbank@skotiabank.cl, como se acreditaría con copia de dicho correo acompañada en un otrosí de este recurso.

Agrega que la nueva clave fue actualizada por su representado mientras conversaba con el “ejecutivo”; y, que con ella pudo acceder a su información bancaria a través de internet. Dice que en la misma llamada el “ejecutivo” le indicó que podía guiarlo en el proceso de activación sin tener que dar sus claves a viva voz, ya que el Banco nunca pide las claves para evitar fraudes, sino que debía seguir el procedimiento indicado por él, escribiendo sólo por teclado en el celular.

Luego dice que a las 18:40 del mismo día, su representado recibió un correo electrónico del banco, cuya copia se acompaña, indicando que la "*activación de mi Scotiabank Azul Pass fue exitosa*". En ese momento, su patrocinado no comprendió bien de qué se trataba esta aplicación, puesto que nunca había sido advertido de su existencia ni por su ejecutiva ni por otra persona del Banco. Entonces a las 19:00 horas aproximadamente llamó reiteradamente a la mesa de ayuda al teléfono 600 600 1100, para ratificar la autenticidad del llamado y la aplicación, pero nadie contestó, pese a su insistencia. Después de tres intentos desistió, ingresando al día siguiente a su cuenta sin notar nada extraño, por lo que se sintió más tranquilo y se olvidó momentáneamente del tema.

Dice que conforme a lo hasta ahora relatado, se puede observar tres elementos de importancia ocurridos entre el 11 y el 13 de junio de 2019: a) primero el Banco procede a autorizar transferencias desde su cuenta corriente sin usarse tarjetas de “coordinadas”; b) Siendo casi la medianoche del 12 de junio de



2019, sin la presencia de un ejecutivo ni consulta previa a su representado, el recurrido otorgó un crédito millonario, llamado “Avance en Línea TC” con cargo a su patrimonio, registrado en su cartola recién el 13 de junio de 2019, sin indicar la hora de otorgamiento ni comunicado al cliente mediante aviso por ningún medio; y, c) Autorizó una serie de transacciones millonarias a distintas cuentas de terceros, por los mismos montos solicitados, más la mayor parte del sueldo de su defendido que se encontraba depositado en la cuenta corriente.

Agrega que los dos hechos ocurridos entre el 11 y 12 de junio, fueron seguidos inmediatamente de “sospechosas transferencias bancarias” que, a pesar de ello, no causaron alarma alguna en el mismo Banco recurrido, lo que permitió que entre las 23:42 horas del 12 de junio y las 00:16 horas del 13 de junio de 2019 (esto es en el transcurso de 34 minutos), se realizaran transferencias de fondos desde la cuenta de su representado a personas desconocidas de la lista habitual de transferencias, más pagos de servicios o compras a través de internet, por la suma total de \$15.826.900, tal como se acreditaría con documentos que se acompañan en un otrosí de su presentación.

Arguye que el 13 de junio de 2019, a las 8:20 a.m., mientras su patrocinado desayunaba, revisó su correo electrónico y se percató que había varios avisos de transferencias. Inmediatamente después de percatarse de las irregularidades, llamó al “*Call Center*” del Banco y procedió a informar y solicitar el bloqueo de la cuenta corriente, enviando un correo seguidamente a su ejecutiva de cuenta.

Dice que luego, se dirigió a la comisaría más cercana a su domicilio y realizó la denuncia en Carabineros en la Tenencia de



San Pedro de la Paz. Posteriormente fue a la sucursal de Scotiabank de esa misma comuna para ingresar el reclamo al Banco e informó el siniestro a la compañía de seguros por recomendación de la ejecutiva de mesón.

Agregó que al momento en que se realizó el actuar fraudulento por estos terceros, su representado tenía otros \$892.931 correspondiente a su sueldo, los que fueron utilizados casi en su totalidad, quedando un saldo de sólo \$86.031 pesos. Dice que en este sentido es preciso comentar que al momento del fraude era de conocimiento del Banco la situación económica de su defendido, toda vez que su empleador efectuaba un depósito automático de su renta, por una suma de \$880.000 pesos, los que eran depositados los días 05 de cada mes.

Expresa que el mismo Banco recurrido reiteradamente habría reconocido el fraude, pero lo atribuyó al mal uso de las claves por parte de su representado o un supuesto virus en el computador desde el cual se realizaron las operaciones, tal como se acredita con los documentos que se acompañan en un otrosí de esta presentación, especialmente en la última respuesta que se da formalmente mediante la Asociación de Bancos e Instituciones Financieras de Chile A.G. (ABIF) el 27 de febrero de 2020, fecha en que su representado entiende que no tendrá solución alguna de parte del Banco recurrido.

Luego el recurrente hace una relación circunstanciada de los reclamos que ha efectuado ante el Banco recurrido, los que en los últimos meses han derivado en respuestas desfavorables.

Argumenta que el Banco recurrido incurrió en dos actos que originan esta acción constitucional, los que configuran un actuar arbitrario e ilegal: a) por una parte, la generación por el Banco de un pasivo en el patrimonio de su representado, solventando en el



mismo los efectos de un fraude de que el mismo Banco recurrido fue víctima; y, b) negativa del Banco a restituir los fondos defraudados o eliminar el pasivo generado.

Agrega que el Banco recurrido, sin mediar consentimiento alguno por parte de su patrocinado, generó créditos a su favor con cargo a su patrimonio, tanto al otorgar casi a la media noche del 12 de junio de 2019 a un tercero defraudador un crédito de consumo *on line* bajo su titularidad; y, permitiendo a estos terceros, durante un breve periodo (35 minutos), acceder a su cuenta y efectuar una serie de transferencias bancarias a sujetos desconocidos.

Explica que a la fecha, la parte recurrente ha efectuado varios reclamos en las diferentes instancias administrativas habilitadas para obtener respuesta del Banco recurrido, sin embargo, hasta ahora todas las respuestas entregadas por dicha institución han sido negativas, quedando sólo pendiente respuesta al reclamo a la Comisión para el mercado Financiero ("CMF"), cuyo proceso aún no se encuentra cerrado. Sin perjuicio de lo anterior, habida consideración de la última respuesta entregada el 27 de febrero de 2020, y a los graves perjuicios que se están generando en el patrimonio de su representado en virtud de este acto arbitrario e ilegal de rechazar la devolución íntegra de los fondos sustraídos, es que decidió interponer este recurso de protección.

Concluye solicitando que se acoja, con costas, el recurso se ordene la disposición de los fondos en la Cuenta Corriente de su representado para solventar el pasivo generado, o bien, derechamente la eliminación de este pasivo; y/o, adoptando cualquier otra medida que esta Corte estime pertinente.



Acompañó al recurso los siguientes documentos: 1) Hecho Esencial informado por el BBVA a la Superintendencia de Bancos e Instituciones Financieras el 2 de agosto de 2018; 2) Copia de correos electrónicos Scotiabank de 11 de junio de 2019, por cambio de clave Scotiabank Azul Pass; 3) Copia de correo electrónico de 26 de noviembre de 2019, del Servicio Atención al Cliente de Scotiabank dirigido al recurrente, donde se detallan las transacciones realizadas; 4) Copia de correo 16 de septiembre 2019 del Centro Atención al Cliente de Scotiabank solicitando documentación para procesar reclamo; 5) Copia respuesta entregada por el Banco mediante la Asociación de Bancos e Instituciones Financieras AG de 27 de febrero de 2020; 6) Copia de sentencias dictadas por la Excelentísima Corte Suprema de Justicia en causas roles de ingreso números 2.196-2018, 23.188-2019 y 28.892-2018.

Informó Gian Carlo Lorenzini Rojas, abogado, en representación de la sociedad BNP PARIBAS CARDIF SEGUROS GENERALES S.A., señalando, en síntesis, que el 07 de junio de 2018, el recurrente contrató con la Compañía informante la póliza N°117117230, la cual contemplaba dentro de sus coberturas, las de transferencias electrónicas no reversables a través de los sitios de internet de institución bancaria o financiera, y la de compras fraudulentas realizadas por vía telefónica o internet.

Posteriormente, el 12 de junio de 2019, el recurrente fue objeto de una llamada telefónica realizada por un tercero desconocido, el cual haciéndose pasar por un ejecutivo de cuentas de la recurrida, logró hacerse con las claves de acceso a la plataforma digital personal que el recurrente poseía en dicha institución.



Luego de ocurrido el hecho antes relatado el tercero procedió a solicitar un avance de dinero con cargo a la cuenta corriente del recurrente Álvaro Mardones por la suma de \$15.020.000 (quince millones veinte mil pesos). Una vez que el dinero solicitado por medio del avance solicitado fue obtenido, el tercero procedió a realizar, sin la autorización del señor Mardones, una serie de giros bancarios a favor de cuentas bancarias de terceros, los cuales habrían ascendido a la suma única y total de \$15.826.900.

Agrega que tras haberse percatado de la defraudación de la cual habría sido objeto, el recurrente procedió a denunciar el siniestro que lo afectó, ocasión en la cual su representada dio inicio al proceso de liquidación de éste, ocasión en la cual asignó como liquidador oficial del mismo a Segured Ltda.

Expresa que una vez asumido su cargo, Segured Ltda., procedió a la apertura de la carpeta de siniestro N°3118929, relativa a la cobertura de compras fraudulentas realizadas por vía telefónica o internet; y al siniestro N°3117680 respecto de la cobertura de transferencias no reversables a través de los sitios de internet de institución bancaria o financiera.

Dice que terminado el proceso de liquidación antes señalado, Segured Ltda., en su calidad de liquidador oficial, estimó pertinente acoger la solicitud de cobertura realizada por el recurrente, procediendo a otorgar el tope máximo de cobertura contemplada en la póliza contratada para cada siniestro, esto es, UF 150 para cada uno de ellos, monto el cual a la fecha de pago ascendía a la suma única y total de \$4.180.500 (cuatro millones ciento ochenta mil quinientos pesos) para cada uno de ellos, correspondiendo ello al tope de cada una de las coberturas amparadas en la póliza contratada por el recurrente, cuyo monto



fue pagado por su representada dentro del plazo legal establecido para ello y respetando los términos y condiciones del seguro contratado.

Informó la Comisión para el Mercado Financiero, señalando, en síntesis, que en razón de lo dispuesto en el artículo 5°, número 21 del Decreto Ley N° 3.538, modificado por la Ley N° 21.000, que creó la Comisión para el Mercado Financiero, dicho Organismo no cuenta -como principio general- con los antecedentes particulares de las operaciones bancarias realizadas entre los bancos y sus clientes. Sin embargo, en el caso del recurrente de autos, revisados sus sistemas de correspondencia, consta la presentación de un reclamo en contra del recurrido referido a la materia que es objeto del presente recurso, el que se encuentra en tramitación.

Informó Enrique Tapia Rivera, abogado, en representación de Scotiabank Chile, quien, en síntesis, señala que Scotiabank Chile realizó la investigación pertinente para determinar si es que existió una vulneración a los sistemas del banco; o si los fondos fueron transferidos utilizándose los datos privados y las claves del cliente, las que sólo son conocidas por este último¹; como da cuenta en Informe GSFC n°267-2019 que se acompaña en esta presentación.

Sobre el particular señala que el análisis que el Banco realiza debe determinar si las transacciones se realizaron a través del canal Scotiabank Azul y validada por los sistemas de seguridad del Banco, mediante el correcto ingreso del número de R.U.T y Clave Scotiaweb y Scotiapass y/o Keypass. Dice que dicho informe concluyó lo siguiente:

1. Las Transacciones objetadas por Álvaro Mardones, fueron correctamente validadas por los sistemas de seguridad del Banco,



Éstas fueron aprobadas con los factores de autenticidad administrados por él.

2. El proceso realizado para ejecutar las transacciones objetadas por el cliente, no constituyen una vulneración a los sistemas o medidas de seguridad implementadas por Scotiabank Azul para evitar fraudes y/o validar transacciones a través de canales no presenciales. Lo anterior, sugiere a un patrón de posible fraude asociado a técnicas de ingeniería social, posibilitando de esta manera la captura de sus credenciales y claves, facilitando con ello que las transacciones reclamadas fueran recibidas y cursadas por Scotiabank Azul como legítimas.

3. Se efectúa retención de fondos, por un monto total de \$ 2.967.000 en banco de destino.

Dice que habiéndose concluido en la investigación del Banco que no hubo vulneración de sus sistemas de seguridad, que los fondos fueron transferidos vía internet a través de la página web del Banco, (canal Scotiaweb), usando los datos personales e intransferibles del recurrente, se determinó que no era procedente la devolución que se solicitaba.

En consecuencia, se determinó que no existió una vulneración de los sistemas del Banco. Las operaciones fueron realizadas ingresando la información privada del cliente y las claves, que sólo deben ser conocidas por este último. Destaca, de acuerdo a los hechos descritos, que el Banco no tiene cómo saber si es que las transacciones fueron efectuadas por el propio cliente y recurrente en autos; o por un tercero, quien engañándola obtuvo sus claves y la suplantó digitalmente.

Concluye señalando que es por este motivo que no es procedente la devolución de monto alguno, pues, como ya se explicó, no existe vulneración alguna de los sistemas del Banco.



Dice que el contrato celebrado entre el actor y el Banco recurrido, señala como una responsabilidad del cliente el tomar medidas especiales de resguardo para proteger sus tarjetas, documentos bancarios y transferencias por internet, especialmente respecto a sus claves o números secretos que son de su exclusiva responsabilidad, personales e intransferibles.

Añade que si es que existió un fraude, este sólo pudo ocurrir porque el recurrente no fue suficientemente diligente en la custodia de sus claves y datos personales, pues como ya se explicó, las operaciones objetadas fueron realizadas usando las claves y datos personales del cliente. Así, sólo existen dos posibilidades: (1) el cliente efectivamente fue víctima de un fraude, pero en que no existió vulneración de los sistemas de seguridad del Banco, sino que se obtuvieron sus claves a través de la instalación de un *malware* en sus dispositivos electrónicos o usando otro mecanismo fraudulento; o, (2) No existe fraude y quien realizó las operaciones fue el propio cliente.

Al respecto el Banco, en cumplimiento de sus obligaciones normativas y contractuales, permanentemente informa a sus clientes sobre los distintos mecanismos usados actualmente por los delincuentes y los resguardos que estos deben tomar, existiendo extensas campañas publicitarias en diarios, redes sociales, televisión, radio e internet.

Añade que los clientes del Banco BBVA podían, en dicha época, acceder a la aplicación del Banco que funciona como la plataforma en que el cliente puede revisar y manejar su cuenta corriente desde ordenadores o aparatos móviles, además existe la aplicación "BBVA PASS" que se utiliza para autorizar transacciones desde su cuenta. Hace presente que ésta es una aplicación móvil que genera claves únicas para que los usuarios



autoricen transacciones, o incluso puedan contratar productos desde el teléfono celular, sin necesidad de utilizar una tarjeta de coordenadas ni una tercera clave, entregando un mayor dinamismo y velocidad, sin comprometer la seguridad en las transacciones bancarias. Explica que esta aplicación, para ser activada, requiere del ingreso de una serie de claves que le son entregadas en forma confidencial sólo al cliente. Agrega que ésta es una aplicación segura, pues todos los clientes cuentan con un PIN de seguridad, que eligieron al momento de activar la aplicación. Este PIN, que es personal y confidencial, es requerido para generar la clave automática que autoriza las transacciones desde el celular o desde el sitio web.

Además, Scotiabank Chile (ex BBVA) tiene a disposición de sus clientes, en el uso de estas aplicaciones, la opción de recibir notificaciones instantáneas en el móvil de los movimientos realizados con las tarjetas de crédito y débito del Banco, lo que permite a los usuarios llevar un control en línea de todas las transacciones de forma eficiente y segura. Por lo demás, el uso de estas aplicaciones permiten "bloquear" temporalmente las tarjetas y productos de los clientes.

Concluye señalando que su representada ha puesto 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 dispositivo de claves; y una aplicación que permite el monitoreo por parte de los propios clientes sobre el uso de sus cuentas.

Controvierte que se esté efectivamente frente a un fraude, cuestión que debe ser resuelta por la justicia ordinaria, ya sea por un juez penal o un juez civil, luego de la investigación o etapa de prueba respectiva.



Afirma que en este caso el actor Mardones entregó información personal a terceros, desconociendo su representado si ello fue o no de manera intencional. Así, terceros habrían capturado sus credenciales y posteriormente la habrían suplantado por los canales no presenciales del Banco, concretando de esta manera las transacciones objetadas por ella, por lo cual no existe vulneración a los sistemas del Banco. Insiste en que las operaciones sólo pudieron realizarse por el propio cliente o por un tercero que haya obtenido sus claves directamente de ella y que es imposible para una institución bancaria hacerse cargo de la seguridad de cada computador o teléfono personal de cada cliente o que cada cliente decide usar para la realización de operaciones bancarias.

Finaliza diciendo que los hechos, en la forma en que han sido descritos, no pudieron ocurrir sino de una de dos formas: (i) o con el consentimiento del cliente, o (ii) con la entrega culpable o negligente de sus claves, ya sea entregándolas con motivo de un llamado telefónico o por la falta de cuidado en la custodia de estas y de sus datos personales, hechos en los cuales el Banco no tiene ninguna injerencia.

Luego se refiere latamente a las obligaciones de los Bancos en materia de *ciberseguridad*.

Dice que, en primer lugar, los Bancos deben contar con sistemas de seguridad. 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".

Arguye que el Banco cuenta con estos sistemas y sí ha detectado patrones de fraudes. Así por ejemplo, no es posible realizar transferencias a un usuario recientemente inscrito por más de \$300.000 sino hasta 24 horas después de su inscripción; no se pueden transferir diariamente más de \$5.000.000; se envían correos y mensajes a las aplicaciones instaladas en los teléfonos de los clientes y a su mail para informarlos en todo momento de las transacciones que se están realizando, etc. Lo que ocurre, dice, es que producto de la entrega (voluntaria o no) que el cliente hizo de sus claves (lo que permitió su suplantación de identidad digital), su representado no tenía cómo detectar que quien realizaba las distintas operaciones objetadas no era el cliente. Nada hacía presumir que quien efectuaba las operaciones no era el cliente. Agrega que como ya se explicó, el cliente fue, presuntamente, víctima del engaño de terceros, quienes vulneraron sus dispositivos de seguridad (y no los del Banco), lo que habría permitido a estos supuestos terceros realizar las operaciones objetadas.

Se trajeron los autos en relación.

Con lo relacionado y considerando:

1º) Que el recurso de protección de garantías constitucionales establecido en dicha norma, constituye una acción constitucional de urgencia, autónoma, destinada a amparar el legítimo ejercicio de las garantías y derechos preexistentes que la misma enumera, mediante la adopción de medidas de resguardo que se deben tomar ante un acto u omisión arbitrario o ilegal que impida, amague o perturbe su ejercicio. Así, resulta



requisito indispensable de la acción constitucional de protección, la existencia de un acto u omisión ilegal, esto es, contrario a la ley, o arbitrario, es decir, producto de una voluntad no gobernada por la razón, sino por el capricho y que provoque algunas de las situaciones o efectos indicados, afectando a una o más de las garantías protegidas por el constituyente;

2°) Que el recurrente hace consistir el acto que reprocha por esta vía, en síntesis, en el hecho que entre el 11 y el 13 de junio de 2019 el Banco recurrido procedió a autorizar transferencias desde su cuenta corriente sin usarse tarjetas de “coordinadas”. Precisa que siendo casi la media noche del 12 de junio de 2019, sin la presencia de un ejecutivo ni consulta previa a su representado, la entidad bancaria recurrida otorgó un crédito millonario, llamado “Avance en Línea TC” con cargo al patrimonio del actor, el que fue registrado en su cartola recién con fecha 13 de junio de 2019, sin indicar la hora de otorgamiento ni comunicado al cliente y sin enviarse aviso alguno. Luego autorizó una serie de transacciones millonarias a distintas cuentas de terceros, por los mismos montos solicitados, más la mayor parte del sueldo del actor que su empleador le depositaba mensualmente en su cuenta corriente;

3°) Que, a su turno, el representante del recurrido señala, en síntesis, que este recurso debe ser rechazado, por cuanto:

a- La ley señala que son los tribunales ordinarios de justicia los encargados de determinar los estados de cuenta en caso de diferencias entre las partes.

b- La acción de protección no procede frente a un supuesto incumplimiento contractual.

Se trata, en consecuencia, de un asunto de lato conocimiento.

c- No existe acto arbitrario o ilegal de Scotiabank Chile.



d- No existe privación, perturbación o amenaza de un derecho del actor por parte de Scotiabank Chile.

e- No existen medidas que esta Corte de Apelaciones pueda adoptar ante lo pedido en lo conclusivo del recurso;

4°) Que antes que todo debe decirse que según se advierte de lo petitorio de esta acción constitucional, lo que pretende la actora es que esta Corte “ordene la disposición de los fondos en la Cuenta Corriente de su representado para solventar el pasivo generado, o bien, derechamente la eliminación de este pasivo”; y/o, adoptando cualquier otra medida que esta Corte estime pertinente.

5°) Que aparece del tenor del recurso y el informe del Banco recurrido, que en la especie se trata de una controversia entre partes, desde que la recurrente -por las razones que detalla- estima que se realizaron transferencias de fondos desde la cuenta de su representado a personas desconocidas de la lista habitual de transferencias, más pagos de servicios o compras a través de internet, por la suma total de \$15.826.900 desde su cuenta corriente a terceros extraños, operaciones que, en su opinión, fueron realizadas vulnerando las medidas de seguridad que el Banco recurrido habría implementado para proteger los productos financieros de sus clientes; en tanto que el recurrido controvierte tal aseveración señalando que no se ha acreditado que las medidas de seguridad del Banco recurrido respecto de los productos financieros de sus clientes fueran vulneradas, o bien que ello se habría producido por descuido o falta de cuidado del actor, por lo que ninguna responsabilidad tiene el recurrido en los hechos descritos por el recurrente;

6°) Que la naturaleza propia de la acción constitucional de protección y el procedimiento inquisitivo dispuesto para su



tramitación, hace que constituya un arbitrio destinado a resolver situaciones en que los hechos esgrimidos y los derechos constitucionales que se dicen afectados estén indubitados y no discutidos, lo que no sucede en el caso propuesto.

En efecto, la acción intentada es de naturaleza cautelar, urgente y no declarativa, de modo que no es procedente este arbitrio para discutir y resolver materias propias de un procedimiento declarativo, en que lo discutido es si el Banco recurrido ha incumplido su obligación de resguardar debidamente los dineros del recurrente;

7°) Que, asimismo, no debe olvidarse que el recurso de protección es un procedimiento excepcional que *“Se aplica sólo cuando existe una amenaza, perturbación o privación del legítimo ejercicio de un derecho esencial producida por una acción u omisión arbitraria o ilegal de un tercero, sea este público o privado, existiendo una manifestación de dicha actuación que no requiere de un proceso de prueba complejo, la afectación del derecho debe ser relativamente clara o evidente. En caso contrario, debe utilizarse el procedimiento ordinario o sumario correspondiente.”* (Nogueira Alcalá, Humberto; El Recurso de Protección en el Contexto del Amparo de los Derechos Fundamentales Latinoamericano e Interamericano, en Revista Ius et Praxis, 13 (1): 75 - 134, 2007);

8°) Que, en conclusión, no es este recurso la vía idónea para resolver la controversia surgida entre recurrente y recurrido, la que trasciende los fines de la acción de protección de garantías constitucionales, y no se condice con el carácter extraordinario y de tramitación breve y urgente que tiene el arbitrio de que se trata.

Al respecto la Excelentísima Corte Suprema de Justicia en recurso de protección, similar al de autos, interpuesto contra el



Banco Santander Chile señaló en causa Rol N° 26.627-2018, en lo que interesa a estos efectos: *“QUINTO: Que si bien esta corte ha sostenido- como lo propone el recurrente- que el contrato de cuenta corriente 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 las convención (SCS de 20/06/18, Rol N° 2.196-2018) ello ha sido en el entendido que tal pérdida se ha producido por causa ajena a la voluntad del depositante o cuenta correntista, circunstancia de hecho que dista o difiere de los presupuestos fácticos enumerados en el motivo precedente , pues, como allí consta, en el caso concreto ha sido el recurrente quién proporcionó a terceros los mecanismo de seguridad indispensables para concretar los giros cuestionados, matiz que determina la legalidad de la conducta del banco recurrido, pues para tal entidad , así como para esta Corte, no resulta posible establecer la involuntariedad de tal traspaso de información entre el cuenta correntista y el tercero que habría realizado los movimientos bancarios cuya restitución se pide”;*

En idéntico sentido resolvió el Excelentísimo Tribunal en recurso de protección Rol 32.718-2018;

9°) Que por todo lo reflexionado y concluido precedentemente, esta acción constitucional debe ser desestimada, por lo cual resulta innecesario entrar al análisis de las garantías constitucionales que se indican como conculcadas, como también al examen detallado de los documentos acompañados por las partes.

Por estas consideraciones, normas constitucionales, legales y reglamentarias citadas, y de conformidad, además, con lo dispuesto en el artículo 20 de la Constitución Política de la



República de Chile y Auto Acordado de la Excelentísima Corte Suprema de Justicia sobre Tramitación y Fallo del Recurso de Protección, **se rechaza**, sin costas, el deducido por Álvaro Rodrigo Mardones Urra, en contra de Banco Scotiabank Chile -Ex Banco Bilbao Vizcaya Argentaria Chile.

Regístrese, notifíquese y en su oportunidad, archívese virtualmente.

Redacción del ministro Claudio Gutiérrez Garrido.

No firma el ministro interino señor Waldemar Koch Salazar, quien concurrió a la vista de la causa y al acuerdo, por haber cesado su interinato.

Rol N° 6.909-2020. Protección.-

Enoc Claudio Gutierrez Garrido
Ministro
Fecha: 02/06/2020 15:26:45

Carlos del Carmen Aldana Fuentes
MINISTRO
Fecha: 02/06/2020 16:20:27



Pronunciado por la Quinta Sala de la C.A. de Concepción integrada por Ministro Presidente Claudio Gutierrez G. y Ministro Carlos Del Carmen Aldana F. Concepcion, dos de junio de dos mil veinte.

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



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>