

Antofagasta, a veintitrés de julio de dos mil veinte.

VISTOS:

La comparecencia de IVÁN BRITO BOBADILLA, domiciliado para estos efectos en Antofagasta, en calle Washington n° 2562, oficina 309, quien interpone recurso de protección en contra de Banco Scotiabank Chile, para que se ordene la restitución de \$45.136.865, que corresponde a movimientos fraudulentos y no reconocidos y que la entidad bancaria se niega a devolver, lo que estimó arbitrario e ilegal, por lo que pide restablecer el imperio del Derecho en este sentido.

Informó la recurrida, solicitando el rechazo del recurso.

Puesta la causa en estado, se trajeron los autos en relación para dictar sentencia.

CON LO RELACIONADO Y CONSIDERANDO:

PRIMERO: Que en su calidad de cuenta correntista del Banco Scotiabank Chile, del cual es cliente hace más de veinte años, vulnerando los posibles dispositivos de seguridad informáticos del Banco, terceros desconocidos lograron la transferencia de todos los fondos disponibles, a un tercero de acuerdo al siguiente detalle:

1.- Trasferencia desde la línea de crédito de la cuenta corriente N° 3090016427 por la suma de \$9.124.214. La cuenta



corriente tenía un saldo contable de \$3.211.214 y no tenía ninguna necesidad de utilizar la línea de crédito.

- 2.- Transferencia de la cuenta corriente N° 309009051 a la cuenta corriente N°3090016427 por un monto de \$6.600.000. Esta transferencia va desde una cuenta que mantiene por adjudicación de un Proyecto Fondecyt N°1170256, la cual sólo se puede usar para gastos del proyecto estando prohibido por las bases del concurso Fondecyt. Destaca que en dos ocasiones por error del Banco, se pagaron cuentas personales (créditos hipotecarios), para lo cual el Banco entregó dos constancias asumiendo su error, constancias que fueron entregadas al programa Fondecyt, para regularizar la situación financiera del proyecto, lo que demuestra que quien efectuó esta transferencia fue un tercero.
- 3.- Pago por SWEB (servicio de transferencia por internet del Banco) SERV (se desconoce a que corresponde esta sigla) por la suma de \$18.854.700.
- 4.- Transferencia de tarjeta de crédito VISA 4301 a la cuenta corriente personal la suma de \$6.125.000
- 5.- Transferencia de tarjeta de crédito Master Card 4336 a la cuenta corriente personal la suma de \$6.611.000
 - 6.- Pago por SWEB de SERV por la suma de \$5.843.854
- 7.- Se realiza pago por SWEB de SERV por la suma de \$5.647.243
- 8.- Transferencia de tarjeta de crédito Mastercard 9628 a la cuenta corriente personal la suma de \$13.686.000
 - 9.- Pago por SWEB de SERV por la suma de \$2.963.281.



- 10.- Pago por SWEB de SERV por la suma de \$3.023.371.
- 11.- Pago por SWEB de SERV por la suma de \$2.549.741.
- 12.- Pago por SWEB de SERV por la suma de \$2.375.912.
- 13.- Pago por SWEB de SERV por la suma de \$3.878.763.

Agrega que sus cuentas corrientes quedan en cero pesos el mismo día y solo se percató el lunes 16 de diciembre de 2019 a las 18:20 horas aproximadamente, al acceder a su cuenta bancaria desde su computador personal al sitio web www.scotiabank.cl e ingresar del modo habitual, es decir con su cedula de identidad y clave personal de internet, advirtiendo que las transferencias de las línea de crédito de las cuentas corrientes y de las tarjetas de crédito por SWEB a su cuenta corriente personal por SWEB, se hicieron pagos por "SWEB a SERV", lo que ascendió a un monto total de \$45.136.865, respecto de movimientos no reconocidos.

El dinero correspondía a depósitos realizados en la cuenta corriente y que tenía bajo su custodia, así como también otros obtenidos a través de la línea de créditos asociados a dicha cuenta y tarjetas de crédito.

El día 16 de diciembre de 2019, dice que llamó de inmediato al Banco activando el bloqueo de todos los productos y concurrió a la Tercera Comisaría de Carabineros de Antofagasta, donde mediante parte 2170 de la misma fecha, denunció estos hechos, iniciándose la causa RUC 1901362556-8 en la Fiscalía Local de Antofagasta.

Posteriormente, el día martes 17 de diciembre de 2019, se comunicó por correo electrónico con su ejecutiva de cuentas en el Banco Scotiabank, María Soledad Guerra,



informándole de la situación, quien le respondió al siguiente que derivaría la información al área de Fraudes del Banco. El 20 de diciembre de 2019, llenó el formulario de fraude respectivo en el Banco entregando toda la información de los hechos a la Sra. Yoselin Araya encargada en el servicio de atención al cliente del Banco Scotiabank, quien remitió a la semana siguiente, los documentos al área que tiene el Banco para hacer la investigación del siniestro, asignándose los siguientes códigos numéricos: 1638629; 1638574; 1638740; 1640441. Relata además que solicitó en numerosas ocasiones a su ejecutiva de cuentas antes señalada, que hiciera envío del contrato de la póliza y los contratos de cuenta corriente, sin resultados positivos, indicándole, que producto de la fusión del Banco BBVA y Scotiabank, los documentos solicitados están en Santiago y no los encuentran, por lo que, el 21 de diciembre de 2019, realizó reclamo en SERNAC solicitud N° R2019W3425287, la que recibió respuesta negativa el 17 de enero de 2020, en la que se indica, que el Banco está investigando el asunto, debiendo esperar esta resolución y que al ser titular de una cuenta corriente bancaria Premium, está en conocimiento que tiene una póliza de seguros contra fraude, por consiguiente se contactó el día lunes 23 de diciembre de 2019, con Germán Nienhufer a través del portal del Banco, quien le indica que la Póliza de seguro Premium lleva el número 10908491 y se encuentra vigente. Idéntica información le entregó telefónicamente Antonio Escobar a través del portal de la compañía aseguradora BNP PARIBAS CARDIFF SEGUROS, quien le indica que el seguro tiene cobertura por fraude de clonación y por Transferencias No reversables a sitios de internet.



Luego la ejecutiva del Banco María Soledad Guerra, niega la información precedente, indicándole que no tenía seguro. Posteriormente, el 23 de enero de 2020, se realiza reclamo ante la Comisión para el Mercado Financiero, cuyo requerimiento fue registrado con el correlativo número 01122.

El 02 de marzo de 2020, la analista del Banco Scotiabank envía comunicación a la jefa del departamento de Atención de Público de la Comisión para el Mercado Financiero, indicando que los montos fueron sustraídos sin su autorización corresponden a dos transacciones, la primera por \$1.- y la segunda por \$1.350.000, añadiendo en la misma comunicación "se ha concluido que el hecho relatado no constituye una 105 vulneración а sistemas 0 medidas de seguridad implementadas por Scotiabank para evitar Fraudes, dado que no advirtieron irregularidades las en transacciones realizadas."

Posteriormente, el Banco disculpa se por información falsa en respuesta final del 26 de mayo de 2020. A su vez, el 05 de marzo de 2020 la analista Banco Scotiabank envía respuesta en referencia a la solicitud ${\tt N}^{\circ}$ 1638629, en indica "Los antecedentes documentos la que se У proporcionados por usted se encuentran en evaluación por parte de la Compañía de Seguros Cardif, quien decidirá si los hechos denunciados cumplen los requisitos necesarios para hacer procedente una indemnización según cobertura, tope por evento y exclusiones; entre otros requisitos, contemplados en la póliza suscrita por usted con dicha compañía". Agrega "Realizada la investigación pertinente, se concluyó que no existió una vulneración a los sistemas de seguridad del Banco, pues las transacciones fueron validadas la



información antes referida. Presumimos en consecuencia, la existencia de un Malware (virus) en sus dispositivos electrónicos..."

El lunes 13 de abril de 2020 recibió respuesta de parte de la compañía de seguros, respecto a la póliza contratada por fraude Bancario, de tal modo le envía informe de liquidación N°: TJS/03-2020/01073755, el que concluye luego de la investigación realizada "se determinó el uso malicioso de los documentos siniestrados en las oportunidades que se mencionan". Otorgando el pago de la cobertura total.

Expone que aceptó esta liquidación el 15 de abril aceptándola, pero sin renunciar a ningún tipo de acción contra el banco, ya que el monto cubierto por el seguro, no alcanza ni al 10% de lo que desconocidos lograron sustraer al banco, y que es aquello que el banco no pretende ni solucionar motu proprio ni devolverle.

Finalmente, el 26 de mayo de 2020, recibió confirmación última y definitiva sobre investigación del Banco Scotiabank, donde se le señala que 1) la compañía de seguros pagará la póliza de acuerdo al tope máximo, 2) solicitan disculpas por toda la información falsa que han entregado a la Comisión para el Mercado Financiero y 3) finalizan indicando que en ningún caso procede responsabilidad de parte del Banco.

En definitiva, señala que desconocidos sustrajeron la totalidad de los fondos depositados en las cuentas corrientes, líneas de crédito y tarjetas de crédito a su nombre, todo ello, porque lograron vulnerar todos los dispositivos de seguridad informática que el Banco Scotiabank Chile dice contar, quien, con sus omisiones en entregar



información, su desorden administrativo y derechamente, con la negativa de existir seguros contratados a su nombre que cubran estos hechos, amenazan mi derecho de propiedad, afectan directamente mi derecho a la honra y a la integridad psíquica e incluso física, como se expone más adelante.

Por otra parte, indica que Banco Scotiabank Chile mantiene una serie de restricciones a las transferencias de fondos, al menos, para que sus sistemas eviten operaciones sospechosas y consecuentemente se eviten fraudes. La más relevante de estas medidas en la especie, es la imposibilidad de transferir más de \$5.000.000 diarios existente para las personas naturales y un monto máximo de \$300.000 como primera transferencia, lo que hace más evidente aún la vulneración de los sistemas de seguridad informática de Banco Scotiabank Chile, la que es depositaria de los fondos depositados en sus cuentas, y por tanto, del contrato de cuenta corriente celebrado nacen para el Banco señalado, obligación de cuidado y entrega en los términos allí señalados.

Sostiene que el día 26 de mayo de 2020, recibió un correo electrónico de Paula Canessa Rossi, Jefe Atención Clientes del Banco Scotiabank, informándose la negativa a restituir los dineros sustraídos por terceros desde la plataforma web que dicha institución maneja y proporciona a los usuarios, señalado lo siguiente: "Junto con saludar y en relación al correo recibido, en el cual manifiesta su molestia por la respuesta entregada a la Comisión para el Mercado Financiero (CMF), cumplo con informar: A continuación se detallan las transacciones por usted reclamadas. Además se adjunta la cartola de cuenta corriente, donde se visualizan las mismas operaciones: Una vez recibida su denuncia se



derivaron los antecedentes correspondientes a la compañía de seguros, quienes determinaron el pago del siniestro, de acuerdo a las condiciones de la póliza contratada, en cuanto a cobertura y tope por evento. Lo anterior, en ningún caso presume alguna responsabilidad de nuestra Institución en las transacciones objetadas, ya que tal como se respondiera a usted con fecha 05 de marzo de 2020, la totalidad de éstas, se realizaron con las claves necesarias de seguridad, las que son de uso y confidencialidad del cliente, correspondiendo este pago, a las condiciones propias del producto contratado con la aseguradora, por lo cual se paga mensualmente una prima. Cabe precisar que la finalidad de contar con un seguro fraude es que el cliente se libere de un riesgo determinado, como puede ser en este caso, la eventual utilización de terceros los productos bancarios. en le solicitamos disculpas por la Finalmente, incorrecta información enviada a la CMF ante la presentación por usted efectuada a dicho organismo, en cuanto los involucrados, como también a la existencia de seguros involucrados."

Expone que la comunicación precedente enviada por la misma recurrida, la compañía aseguradora accedió al pago de la póliza. Siendo de mayor contundencia lo resuelto en informe de liquidación N°: TJS/03-2020/01073755, emitido por la Empresa liquidadora de seguros SEGURED la que indica que existió fraude y autorizó el pago de la prima completa asegurada (50 UF). Si bien el monto pagado no cubre la totalidad de lo sustraído, toma gran relevancia que un ente externo y especializado en la materia, estableció que existió fraude en los productos bancarios de su nombre.



Alega que la respuesta del Banco constituye un acto ilegal y arbitrario, toda vez que le priva del derecho de propiedad del dinero depositado, líneas de crédito y tarjetas de crédito, así como también afecta la integridad psíquica, ya que en la actualidad, y producto de esta privación de sus fondos, debió pagar los intereses y otros cargos derivados de la sustracción de la que fue víctima y que corresponde a la línea de crédito y tarjetas de crédito ya referidas, pagos que en modo alguno me corresponde asumir.

cuanto a los antecedentes de derecho, En expone que es titular de un contrato de cuenta corriente suscrito con la recurrida, el que se rige por el DFL ${
m N}^{\circ}707$ de 7 de octubre de 1982 y que la obligación de la recurrida es la devolución del dinero conforme al artículo 2212 del Código Civil. Cita sentencia de la Excma. Corte Suprema, causa Rol 2196-2018, que ordenó restituir los dineros sustraídos de la del requirente, transcribiendo cuenta corriente considerandos pertinentes. Concluye que los sustraídos de la cuenta corriente y línea de crédito asociada a ésta y sus tarjetas de créditos, son propiedad del banco, debiendo éste asumir el costo y pérdida generado por el fraude informático. Siendo un acto ilegal y arbitrario porque la negativa del Banco se funda en que el recurrente sustrajo el dinero, lo que sería imposible, toda vez que el monto máximo para la primera transferencia es de \$300.000 \$5.000.000 como máximo diario a transferir, además no se le advirtió de las operaciones inusuales. Agrega que la página web, los digipass o tarjetas de transferencia y el acceso a los mismos, son diseñados, elaborados y proporcionados por el Banco, por lo que es totalmente contrario a derecho



también a la lógica) que el recurrente deba asumir el riesgo de una actividad cuyo control es del Requerido, ni tampoco respecto de la sustracción de dineros.

Explica que el acto ilegal y arbitrario del requerido, en atención a negarse a la restitución en igual género y cantidad respecto de los dineros que entregó en mérito del contrato de cuenta corriente, ha perturbado y vulnerado su derecho de propiedad, consagrado en el artículo 19 N°24 de la Constitución Política de la República.

Asimismo, se vulnera su derecho a la honra, consagrado en el Art. 19 N° 4 del estatuto constitucional, al imputarse maniobras dolosas destinadas a engañar al Banco recurrido, desconociendo transacciones fraudulentas que le han privado de su patrimonio, lo que implica que el Banco ha infringido su obligación de resguardar y dar seguridad a las transacciones efectuadas en la cuenta corriente, dado que no logró evitar que ésta sea utilizada sin vulnerar los sistemas informáticos existentes para ese fin.

lado, la Superintendencia de 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 y transferencias electrónicas transacciones de dinero. Conforme a ello, los Bancos deben garantizar que las operaciones solo puedan realizadas personas ser por autorizadas para ello, debiendo recabar todas 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.

Concluye que la actuación del Banco recurrido resulta arbitraria, en cuanto por las razones señaladas y que en su oportunidad se le hicieron valer al propio Banco, son antojadizas y caprichosas, contraria a la razón; e ilegal, al infringir la normativa sobre seguridad de las transacciones electrónicas y lo dispuesto en el Art.3 de la Ley 19.496, 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. Afirma su tesis citando sentencia de la Excelentísima Corte Suprema en fallo ROL 2196-2018.

Para la ilegalidad del acto, agrega que el Banco ha afectado su integridad psíquica, padeciendo la molestia y miedo por la sustracción y negativa de restitución de \$45.136.865. (cuarenta y cinco millones ciento treinta y seis mil ochocientos sesenta y cinco pesos), provocándole un cuadro agudo de estrés, el que a su edad es perjudicial para su salud. Así desde el mes de diciembre de 2019, tuvo que realizar infinidad de gestiones ante el Banco y otros incontables situaciones organismos, negándosele en la restitución inmediata de los fondos, con una espera de la investigación y resoluciones internas por seis meses, lo que le provocó gran agobio la interacción del Banco con la CMF (Comisión para el Mercado Financiero), en que incluso la recurrida envió información falsa, señalando que solo fueron sustraídos dos transacciones, la primera por \$1.- y segunda por \$1.350.000.



SEGUNDO: Que informó el abogado Emilio González Corante, en representación del recurrido Banco Scotiabank, solicitando el rechazo del recurso, porque los derechos cuya protección se reclama, no tienen el carácter de indubitados, lo cual es un requisito esencial de la acción.

En efecto, conforme al "contrato de operaciones bancarias para personas naturales" que suscribió recurrente con el banco, se establece el procedimiento para estos casos, así como también el grado de responsabilidad que pudiera tener el Banco o el cliente en el manejo de los canales remotos por donde circula la información, tales como internet o conexión telefónica. Así, para determinar si la actuación del banco ha infringido la relación contractual con la recurrente, el conflicto debe ventilarse en una instancia en que las partes procesalmente acrediten en forma legal sus pretensiones, como por ejemplo, el procedimiento contemplado en la Ley N°19.496, u otras acciones que pueda interponer la recurrente ante los Tribunales ordinarios, cuestión que excede la competencia de la Corte, ya que lo que se alega es en un supuesto incumplimiento contractual.

subsidio, se argumentó que no se está en presencia de un contrato de depósito irregular y que hay responsabilidad del recurrente respecto de los dineros sustraídos de su cuenta. En consecuencia, se trata de un contrato típico, bilateral conmutativo, denominado У "contrato operaciones bancarias", que contempla de la responsabilidad por la custodia de las claves, lo que implica una diferencia con el contrato de depósito irregular, ya que auien asume el riesao en caso de incumplir esta responsabilidad, es el cliente y no el banco.



En subsidio, se alegó la inexistencia de acción u omisión ilegal o arbitraria por parte de la recurrida. Consta en el "INFORME DE CASO 1937509" de la Gerencia de servicios Forenses Digitales de Scotiabank, que la causa de la defraudación obedece a "Malware del dispositivo utilizado por el cliente". Según el informe, este tipo de defraudaciones se puede hacer de dos formas, a través del medio del phishing, que utiliza el correo electrónico como soporte material para reconducir a la víctima a un sitio "web falso" o en el pharming, lo que se introduce es un malware o un gusano en el servidor de internet del usuario para reconducirlo mediante la manipulación del "Domain Name Server" (DNS) a una página "web" falsa.

En consecuencia, las normas de la Superintendencia de Bancos e Instituciones Financieras, señalan frente a situaciones como las expuestas dos cuestiones completamente diversas: la primera, consiste en la intervención directa y por parte de terceros de la página web del Banco y, la segunda, la intervención de terceros, ya no de la página web del Banco, sino del computador o pantalla del cliente o usuario, bajo la modalidad del phishing. Para evitar lo primero - intervención por terceros de la página web del Banco y, por ende, suplantación a través de ella del cliente - el Organismo Supervisor dispone que el sistema debe proveer un perfil de seguridad que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resquardar la privacidad la información transmitida o procesada por ese medio. Lo anterior, con la finalidad de evitar que se desconozca la autoría de las transacciones o mensajes, utilizándose claves de acceso al



sistema, que permitan asegurar autenticidad, sin intervención de terceros.

Agrega que los canales electrónicos que ofrezcan las instituciones bancarias para realizar transferencias deberán contar con apropiados privilegios de autorización y medidas de autentificación, e infraestructura de seguridad para cuidar la integridad de los datos de cada transacción y la adecuada privacidad de los registros e información de los clientes. Asimismo, se indica por la superintendencia los bancos deberán que contar procedimientos que permitan detectar todas las operaciones con patrones de fraude, para marcar o abortar operaciones potencialmente fraudulentas, para lo cual deberán establecer patrones conocidos de estos y comportamientos que no estén asociados al cliente.

Por lo señalado, hizo presente que los sistemas de seguridad del Banco no fueron transgredidos, ya que las transferencias no se ejecutaron vulnerando sistemas de seguridad del Banco.

La segunda cuestión prevista por la normativa, es la intervención de terceros, ya no de la página web del Banco la comunicación entre ambos, y por ende de dispositivo móvil empleado por el cliente, bajo la modalidad del "phishing" antes descrito u otra similar; operación en la que el delincuente ingresa a la página web del Banco, ya con todos los datos personales adulterados y procede a efectuar transferencias a terceros. Εn este caso, existe comunicación auténtica para estos efectos entre el Banco y el cliente, con la salvedad de que quien opera las claves no es el titular, sino, un tercero quien las extrajo previamente.



Por ello, lo que ha ocurrido es que el cliente ha proporcionado sus claves - probablemente en forma inadvertida- a un tercero.

En el último caso, no hay un problema de autenticidad de comunicación o de violación de la página del Banco, ningún error u omisión administrativo, sino mal uso que terceros hacen de las claves confidenciales del cliente, quien ha perdido el dominio de ellas en virtud de una acción anterior, correspondiente al bloqueo de su equipo.

Por lo expuesto, estima que no se ha quebrantado derecho de la recurrente, como tampoco cometido acto arbitrario o ilegal en su contra.

TERCERO: Que de conformidad a lo establecido en el inciso primero del artículo 20 de la Constitución Política de República el recurso de protección de constitucionales constituye jurídicamente una acción naturaleza cautelar, destinada а amparar el legítimo ejercicio de las garantías y derechos preexistentes que en esa misma disposición se enumeran, mediante la adopción de medidas de resquardo que se deben tomar ante un acto arbitrario o ilegal que impida, amaque o moleste ese ejercicio.

CUARTO: Que el recurso de protección, como acción cautelar de urgencia, carece de las garantías procesales de un juicio declarativo de lato conocimiento, razón por la que sólo ampara derechos no controvertidos o indubitados.

En este sentido, un acto u omisión es arbitrario cuando carece de razonabilidad, de fundamentación suficiente, de sustentación lógica, es decir, cuando no existe razón que lo fundamente y quien actúa lo hace por mero capricho.



El acto u omisión será ilegal cuando no reúne los requisitos legales, es contrario a derecho o a la ley o no se atiene estrictamente a la normativa legal vigente.

QUINTO: Que de las presentaciones efectuadas por las partes se desprende que el objeto de la acción deducida es determinar la existencia de un acto ilegal o arbitrario de la institución bancaria recurrida, consistente en negarse a hacer devolución de los montos sustraídos mediante fraude.

SEXTO: Que de los antecedentes expuestos por la recurrente, del contenido del informe evacuado por el banco recurrido y especialmente del INFORME DE CASO de la Gerencia de servicios Forenses Digitales, se desprende que existieron transacciones en las cuentas del recurrente, efectuadas por desconocidos mediante la utilización de ingeniería social y/o por malware del dispositivo del obteniendo así sus credenciales y claves de acceso, logrando suplantar su identidad, mediante la modalidad de "phishing". se señala que se efectuó la reclamación correspondiente y el consecuente bloqueo de tarjetas, que dio inicio a la investigación.

10 anterior, resulta indubitado que la recurrida no adoptó las medidas de seguridad suficientes para impedir que se afectara el patrimonio del actor, al no ser efectivas o eficientes dichas medidas que permitieron el ingresos a la cuenta corriente y las demás cuentas asociadas, sin respetar las mínimas medidas que pudieren advertir estas defraudaciones, desde que los movimientos en parte se excedieron de los límites que el propio banco impone, por lo que puede afirmarse que la entidad bancaria no tuvo el resquardo elemental para evitar estos fraudes y al no



responder denegando la devolución de los montos defraudados, medidas de ante la omisión de adoptar las seguridad pertinentes, ha incurrido en una arbitrariedad palmaria porque la decisión de no devolver dinero retirado a través de sin autorización del terceros cuenta correntista antojadiza y sin respaldo alguno, sobre todo que su misma investigación administrativa no es unívoca frente responsabilidad que podría tener el recurrente y no explica cómo se burlaron las normas de seguridad general para todos los usuarios, incluso con los instrumentos autorizados, sobre el máximo de montos en las transacciones.

La ilegalidad deviene del desconocimiento de las obligaciones básicas que impone la Ley frente a situaciones subrepticias, particularmente la Ley 21.234, que impone a la institución bancaria la carga de acreditar que la transacción fue autorizada por el cliente y; también a los reglamentos e instrucciones que le obligan a adoptar medidas concretas frente a este tipo de acciones arbitrarias, discrecionalmente denegó su devolución, razón por la cual acoger la presente acción constitucional, corresponde disponiendo la devolución de todas las sumas de dinero referidas por el recurrente, dentro de tercero día en que quede ejecutoriada la sentencia, más intereses corrientes fijados para operaciones de dinero no reajustables a partir la fecha de la sustracción que aparece en la misma comunicación del banco, porque se ha privado en la forma señalada el derecho de propiedad representado por el dinero sustraído irregularmente, sin que sea posible estimar afectada la honra de las personas, pues la sola referencia a esta garantía no es suficiente.



Finalmente, no habiéndose discutido la calidad de ser titular de una cuenta corriente como tampoco de los demás servicios que le otorgó la entidad bancaria, surgen derechos indubitados sobre el patrimonio que el librado en este tipo de actividades debe resguardar, más aun si se sobrepasó de las reglas mínimas de seguridad en cuanto algunas transacciones estaban sobre el limite corriente impuesto por entidades bancarias, sin que sea un obstáculo las existencia de otros procedimientos destinados a recuperar las sumas de dinero retiradas subrepticiamente de la cuenta corriente. Pues el artículo 20 inciso primero parte final de la Constitución Política de la República, permite y regula esta cautelar, "sin perjuicio de los demás derechos que pueda hacer valer ante la autoridad o tribunales correspondientes", el recurrente y afectado.

Por estas consideraciones y de acuerdo, además, con lo dispuesto en el artículo 20 de la Constitución Política de la República y Auto Acordado de la Corte Suprema sobre Tramitación del Recurso de Protección de Garantías Constitucionales, SE ACOGE con costas, el recurso deducido por IVÁN BRITO BOBADILLA en contra de Banco Scotiabank S.A., y se dispone que la entidad bancaria deberá reintegrar dentro de tercero (3°) día en que quede ejecutoriada la sentencia, la suma de \$45.136.865 (cuarenta y cinco millones ciento treinta y seis mil ochocientos sesenta y cinco pesos), más intereses corrientes fijados para operaciones de dinero no reajustables, entre el 13 de diciembre de 2019 y el día del pago efectivo, más los gastos e intereses o gravámenes que se hubiesen cobrado por el giro o transferencia de estas sumas,



incrementadas con los mismos intereses entre la fecha del cobro y el día del pago efectivo.

Se regula en dos (2) ingresos mínimos mensuales incrementados para efectos remuneracionales las costas personales causadas en esta instancia.

Se deja constancia que se hizo uso de la facultad contenida en el artículo 82 del Código Orgánico de Tribunales.

Registrese y comuniquese.

Rol 2508-2020 (PROT)

Redacción del Ministro Titular Sr. Óscar Clavería Guzmán.



Pronunciado por la Segunda Sala de la C.A. de Antofagasta integrada por los Ministros (as) Oscar Claveria G., Virginia Elena Soublette M., Dinko Franulic C. Antofagasta, veintitrés de julio de dos mil veinte.

En Antofagasta, a veintitrés de julio 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