

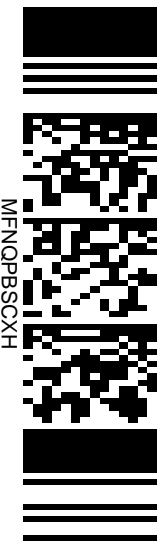
Arica, treinta de marzo de dos mil veinte.

**VISTO Y TENIENDO PRESENTE:**

**PRIMERO:** Que, el abogado Milton Rojas Cancino en favor de doña Claudia Dinora Molina Flores, interpuso recurso de protección en contra del Banco Scotiabak S.A, empresa del giro de su denominación, Rut N° 97.018.000-1, representada por don Francisco Sardón de Taboada, ambos con domicilio en calle 21 de mayo N° 187, Arica, por haber vulnerado su garantía constitucional del N° 24 del artículo 19 de la Constitución Política de la República.

Señala que la recurrente es cuentacorrentista del banco recurrido y que el 6 de diciembre de 2019, mientras se encontraba de vacaciones en esta ciudad, alrededor de las 10:00 horas, intentó efectuar desde su computador (notebook), una transferencia electrónica desde su cuenta corriente a un tercero, a través del sitio web del Banco Scotiabank. Agrega que siguió todos los pasos que señala el sistema del banco e ingresó al ambiente que éste ofrece a sus clientes, para ello digitó su número de cédula de identidad y clave, ya registrados, con la intención de realizar el pago de su gimnasio a una cuenta que ya tenía registrada como destinatario habitual. Sin embargo, el sistema no le permitió realizar la operación, pues no pudo digitar los números claves de su “digipass”. Finalmente cerró todas las ventanas de su computador portátil.

Complementa que de manera casi instantánea la llamaron por teléfono desde el banco recurrido, preguntándole si había realizado una transferencia, a lo que indicó que no, explicándole al funcionario de la institución financiera, que trató de hacer una transferencia pero que no fue posible, debido a que el sistema quedó detenido. Acota, que de manera instantánea le llegó un correo electrónico del banco que decía: “[Informaciones@scotiabank.cl](mailto:Informaciones@scotiabank.cl) Estimado CLAUDIA DINORA MOLINA FLORES La transferencia de fondos instruida por usted con fecha 06/12/2019, desde su cuenta nro. 00000000000971928557 al sr(a) Javier Pérez Cruz, cuenta nro. 00000000000974202719 de Scotiabank por un monto de \$ 4.210.000 fue Aceptada Sus consultas favor realizarlas al 600 6 700 500 Atentamente Scotiabank Chile 4.”.



Afirma que jamás realizó ni intentó una transferencia electrónica a Javier Pérez Cruz, a quien no conoce ni tampoco lo tenía registrado como destinatario habitual de sus depósitos, de modo que por ser la primera transferencia a ese destinatario, el banco debió haberla aceptado sólo por \$ 300.000 con 24 horas de anticipación; señalando, además, que por el monto dicha transferencia, \$ 4.210.000, la debieron haber contactado, lo que no ocurrió, sino que ella copó el saldo de su cuenta corriente afectando la totalidad de su línea de crédito, la cual ascendía a la suma \$2.500.000.

Refiere que realizó gestiones con el banco, solicitando la devolución de su dinero, recibiendo el día 3 de febrero del año en curso, la siguiente respuesta: “Estimada Claudia. Junto con saludar y en relación al reclamo por desconocimiento de transacciones realizadas en su cuenta terminada en los dígitos 8557, por un monto total de \$4.210.000, informo lo 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 Scotiapass o Keypass, 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.

Le recordamos que Banco Scotiabank nunca lo llamará para solicitar sus claves por ningún motivo. Tampoco le enviará correos con enlaces de ningún tipo, ni siquiera a un sitio web, o botones de suscripción; y nunca le pedirá su clave Scotiapass o KeyPass antes del ingreso a su Banco en Línea. Sugerimos además, verificar los datos registrados en el sitio web de sus



destinatarios inscritos y/o transferencias programadas, ante la posibilidad de que hayan sido adulterados, es importante que usted los actualice. Finalmente y de acuerdo a lo conversado, damos por atendida la solicitud.”

Indica que la respuesta del banco, es una clara y directa omisión de responsabilidad, basada en atribuir problemas al propio cliente, sin exponer de manera clara como se produjo la presunta falla.

Solicita que se acoja la presente acción constitucional, debiéndole restituir a la cuenta corriente de la recurrente la suma de \$4.210.000.- (cuatro millones doscientos diez mil pesos), con costas.

**SEGUNDO:** Que, en su oportunidad el abogado Raúl Soto Paredes, en representación del Banco Scotiabank Chile, evacuando el informe solicitado por esta Corte, señaló, que la recurrente es poco precisa sobre los hechos supuestamente ocurridos el 6 de diciembre del año 2019.

Alude que de acuerdo al procedimiento establecido por el Banco Scotiabank, para hacer transferencias, es necesario: Ingresar con la clave personal a la página web privada del Banco, con el nombre de usuario y su clave única, la cual es conocida por el cliente, debiendo utilizar un dispositivo digital personal, denominado “Scotiapass”, el cual genera una clave dinámica numérica de 8 dígitos, la cual permanece activa por 30 segundos, para cada operación. Sin este último elemento de seguridad, es imposible realizar una transferencia electrónica. En consecuencia, el resguardo de las claves por parte del cliente es fundamental y sin ellas, ninguna transacción puede realizarse. Agrega que como no se detectaron fallas del sistema de seguridad del banco, asumen que el cliente fue víctima de alguna estafa o de un “malware” (virus en dispositivos del cliente que capturó claves).

Añade que existe una circunstancia importante que la recurrente omite señalar en su recurso, que el 6 de diciembre del año 2019, ella activó un nuevo dispositivo digital, en consecuencia, la transacción que se impugna por esta vía constitucional fue autorizada mediante el dispositivo Scotiapass o el KeyPass, el cual fue activado el mismo día de la transacción impugnada. Complementa, que para la activación de este nuevo dispositivo, Claudia Molina Flores utilizó: " Su Rut + Su Clave Web + Clave enviada al correo electrónico del cliente + 8 últimos dígitos de una de sus tarjetas",



datos que la propia recurrente aplicó en la página Web del Banco.

Acota el recurrido, que el límite superior de giro de cualquier cuenta bancaria personal diaria alcanza a la suma de \$ 5.000.000, motivo por el cual el banco no debe realizar ningún tipo de notificación al cliente.

Indica, además, que la recurrente interpuso una denuncia por fraude, por este motivo a juicio del recurrente, el recurso de protección “es inconducente”, por cuanto, ya se puso en ejercicio una acción penal con el fin de determinar las responsabilidades, debiendo en dicho proceso ejercerse las acciones pertinentes.

Concluye que los hechos descritos anteriormente, sólo pudieron ocurrir de dos formas: la primera, con el consentimiento del cliente por medio de un fraude o la instalación de un virus informático que capturó las claves y, la segunda, con la entrega culpable o negligente de sus claves, ya sea con motivo de un llamado telefónico o por la falta de cuidado en la custodia de éstas y de sus datos personales; hechos en los cuales el banco no tendría ninguna injerencia.

Indica que los hechos alegados por la recurrente son controvertidos, no existiendo un derecho de carácter indubitado, que se pueda proteger por esta vía constitucional, además de no existir una infracción de ley o arbitrariedad imputable al Banco Scotiabank.

Finalmente solicita el rechazo del recurso de protección, con costas.

**TERCERO:** Que, la acción de protección contemplada en la Carta Fundamental, existe con el propósito de cautelar debidamente los derechos fundamentales de rango constitucional, para lo cual prevé que cualquier persona por sí o a favor de un tercero puede recurrir ante el órgano jurisdiccional para su amparo, cuando estos derechos sean amagados por actos arbitrarios o ilegales de terceros, debiendo la Corte de Apelaciones respectiva adoptar las medidas conducentes para restablecer el orden jurídico quebrantado, si de los antecedentes proporcionados se establece que existe lesión a los derechos constitucionales de quien recurre.

**CUARTO:** Que, en la especie, cabe analizar si el actuar del banco recurrido fue arbitrario o ilegal, y establecido esto, si se ha vulnerado alguna de las garantías protegidas por este arbitrio, de conformidad con lo dispuesto en el artículo 20 de la Constitución Política de la República.



**QUINTO:** Que, la recurrente le atribuye una actuación arbitraria al Banco Scotiabank, por no restituir la suma de \$4.210.000 a su cuenta corriente, lo cual afecta su patrimonio, siendo ello resultado de la falta de seguridad y resguardo de dicho banco.

**SEXTO:** Que, por su parte, Banco Scotiabank sostiene que no ha incurrido en una actuación arbitraria e ilegal, pues las transferencias se ejecutó sin que se detectara fallas en el sistema de seguridad del banco, por instrucciones recibidas con aplicación de los sistemas de seguridad, lo cual fue posible por la información confidencial que le entregó el recurrente a un tercero o bien, con la instalación de un virus informático en el dispositivo del cliente o debido a un actuar negligente o culpable en la custodia de sus claves de seguridad por parte de su clienta.

**SÉPTIMO:** Que como ha sostenido la Ilustrísima Corte de Apelaciones de Santiago en sentencia de protección ROL N°44.191-2017, cada vez que las instituciones bancarias o financieras ofrecen a sus clientes la posibilidad de desarrollar por vía electrónica operaciones de transferencias de fondos u otras, se asume que aquéllas deben asegurar sus fines sustrayendo de cualquier menoscabo a quienes, guiados por los beneficios de rapidez y precisamente mayor reserva y seguridad, deciden utilizar estos métodos.

Mismo sentido en el que la autoridad fiscalizadora de dichas entidades oferentes, la Superintendencia de Bancos e Instituciones Financieras ha puntualizado en sus respectivas Circulares, a saber, la N°3.451 de 2008, que los bancos están obligados a garantizar la seguridad de las transacciones y transferencias electrónicas de dinero. Asimismo, deben asegurar que las operaciones de que se trata sólo puedan ser realizadas por personas autorizadas para ello, debiendo recabar todas las validaciones previas que sean necesarias para resguardar la operación, manteniendo “sistemas y procedimientos” que les posibiliten “identificar, evaluar, monitorear y detectar” movimientos con “patrones de fraude”, de manera que puedan abortar actividades u operaciones potencialmente dolosas.

**OCTAVO:** Que de la sola lectura del informe evacuado por la Institución Bancaria recurrida, se desprende meridianamente que ésta no ha dado cabal cumplimiento a la circular referida en el motivo precedente,



toda vez que si efectivamente hubiese mantenido los sistemas y procedimientos que le permitiesen “identificar, evaluar, monitorear y detectar movimientos con patrones de fraude” necesariamente habría dado una respuesta certera a la recurrente respecto a lo acontecido, y no “presumir la existencia de un malware (virus) en sus dispositivos electrónicos, lo que habría permitido a los supuestos terceros efectuar las operaciones objetadas”.

**NOVENO:** Que sobre el particular, es menester tener presente que el contrato de cuenta corriente no exige como obligación esencial, que el cuentacorrentista deba utilizar un sistema de antivirus para entender que el banco pueda eximirse de sus obligaciones de custodia del dinero depositado ante éste.

**DECIMO:** Que, aún más allá de la regulación aludida en el considerando séptimo, la propia naturaleza de los negocios que un particular, como lo es la recurrente, efectúa en su calidad de titular de una cuenta corriente, línea o tarjeta de crédito, con una sociedad bancaria, si bien impone para el primero, por cierto, el seguimiento de los cuidados e instrucciones básicos y razonables para el uso de los productos dentro de los márgenes contractuales a los que adhirió, para la segunda ello conlleva, sin duda, un extremo cuidado, que nace de su rol como depositario y garante de los fondos de que debe hacerse cargo y en virtud del cual, necesariamente, no sólo debe atender los mandatos de pago que se formulen debidamente con cargo a los mismos, sino también, custodiarlos y asegurarlos en pos de los fines que sus titulares tienen a su respecto, y de la confianza en la correcta operatividad del sistema. Es en ese sentido que, adicionalmente a las indicaciones que las propias autoridades vigilantes de las operaciones financieras han determinado, subyace en ellas la necesidad de reserva, de seguridad en torno a los valores confiados, de las transacciones sobre ellos, de los datos personales, etcétera, la que si bien pudiese precaverse por parte del usuario particular mediante diversos mecanismos instruidos por el banco, por ejemplo, el uso de claves personales o telefónicas, dadas las características de la plataforma digital de acceso remoto o por internet que se ofrece y propicia en estos ámbitos, cuyo fue el caso en la especie, es el segundo organismo al que cabe extremar las



precauciones que eviten los errores, interferencias o derechamente fraudes en el sistema por parte de terceros ajenos. En tanto ello supone tareas de implementación, seguimiento y perfeccionamiento de los programas que implementa para sus propios servicios y que en modo alguno procede asignar a sus clientes.

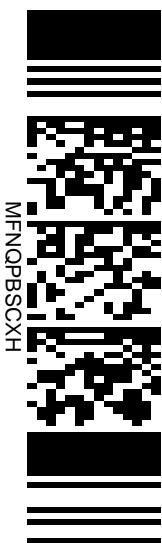
**UNDECIMO:** Que según lo que se viene razonando, el giro cuestionado mediante la presente acción cautelar, lo fue a través de los propios medios que entrega el banco a sus clientes para el desarrollo de sus operaciones electrónicas, particularmente su plataforma digital o página web, sin que operaran los resguardos o mecanismos de control que a ella le caben en relación a los fraudes de terceros, como por ejemplo el límite máximo de \$300.000- aplicable a toda primera transferencia dentro del plazo de 24 horas, sin que pueda sostenerse que se libere de toda responsabilidad ante su contratante y pretenda, imponerle a ésta la pérdida patrimonial que los sucesos descritos implican, soslayando la confianza y buena fe que aquella mantenía en sus procedimientos y mecanismos de seguridad, y en consideración a las cuales actuó.

**DUODECIMO:** Que acorde a lo anteriormente reflexionado, no cabe sino calificar el actuar del Banco recurrido como ilegal y arbitrario, puesto que al no asumir el perjuicio económico ocasionado a la recurrente, trasladándole a ésta los efectos del fraude bancario de que fue objeto, mismo que le afectó su patrimonio, vulnerándose así su derecho de propiedad, contemplado en el artículo 19 N°24 de la Constitución Política de la República.

Por estas consideraciones y visto, además, lo dispuesto en el artículo 20 de la Constitución Política de la República y en el Auto Acordado de la Excma. Corte Suprema sobre Tramitación y Fallo del Recurso de Protección de las Garantías Constitucionales, se resuelve:

I.-Que **SE ACOGE** la acción constitucional deducida por el abogado Milton Rojas Cancino en favor de doña Claudia Dinora Molina Flores, en contra del Banco Scotiabank, debiendo este último reincorporar a la cuenta corriente del recurrente la suma de \$4.210.000.

II.-Se deja sin efecto la orden de no innovar, decretada el seis de marzo del año en curso.

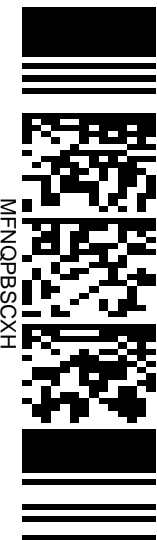


Cúmplase, oportunamente, con lo establecido en el numeral 14° del referido Auto Acordado.

Redacción de la Ministra María Verónica Quiroz Fuenzalida.

Regístrese, notifíquese, y archívese en su oportunidad.

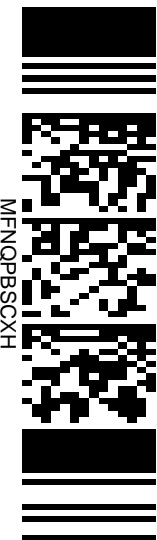
Rol N° 232-2020 Protección.





Pronunciado por la Segunda Sala de la C.A. de Arica integrada por Ministro Presidente Mauricio Danilo Silva P. y los Ministros (as) Maria Veronica Quiroz F., Marco Antonio Flores L. Arica, treinta de marzo de dos mil veinte.

En Arica, a treinta de marzo 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 08 de septiembre de 2019, la hora visualizada corresponde al horario de verano establecido en Chile Continental. Para Chile Insular Occidental, Isla de Pascua e Isla Salas y Gómez restar 2 horas. Para más información consulte <http://www.horaoficial.cl>