Concepción, veintidós de septiembre de dos mil veinte.

VISTOS:

Comparece el abogado Roberto A. Coloma Del Valle, domiciliado en Concepción, calle Aníbal Pinto 265, en representación procesal de Brenda Julieta Flores Jarpa, médico cirujano, domiciliada en Concepción, Sector Collao, calle Tegualda Nº 55, Casa K, Condominio Los Naranjos, interponiendo recurso de protección de garantías constitucionales en contra del Banco Scotiabank, representado por su Agente en Concepción Alfredo Ormeño Smith, ambos domiciliados en Concepción, calle Barros Arana Nº 345.

Fundamentando el recurso, señala que su representada es titular de la cuenta corriente bancaria Nº 971922079 del Banco Scotiabank y que en el mes de agosto de 2019 recibió un incentivo al retiro por parte de su empleador por una suma cercana a los $40.000.000, oportunidad en que por sugerencia de su ejecutiva procedió a la apertura de una "Cuenta Renta Diaria", asociada a la cuenta corriente que ya tenía.

Explica que, en circunstancias que su representada se encontraba fuera del país, el 14 de enero de 2020 fue notificada por medio de un correo electrónico enviado desde el Departamento de Monitoreo de Fraudes del Banco Scotiabank, casilla electrónica monitoreo.fraudes@Scotiabank.cl del hecho de registrase con esa fecha 6 transferencias desde su cuenta corriente Nº 971922079, por la suma de $300.000 cada una, requiriéndosele confirmar si dichas transferencias estaban correctas o no, ante lo cual su representada respondió desconocerlas completamente. Acto seguido, procedió a revisar sus productos financieros comprobando que el día anterior, esto es, el día 13 de enero de 2020, se realizó una transferencia desde su Cuenta Renta Diaria Nº 975810534 por la suma de $38.000.000 (treinta y ocho millones de pesos) a su Cuenta Corriente Nº 971922079, y con esa misma fecha se realizaron una serie de transferencias y pagos desde esta última cuenta con destino desconocido, por un monto total de $39.471.521.

Señala que su representada mantiene todas sus claves para operar sus productos financieros en su poder, sin que ninguna otra persona tenga conocimiento ni menos acceso a ellos, de modo que la única forma en que las transacciones y pagos referidos en el párrafo anterior pudieron ocurrir fue por medio de la vulneración por terceros del sistema informático que el Banco Scotiabank pone a disposición de sus clientes para operar los distintos productos financieros que ofrece.

Expone que llama poderosamente la atención que los sistemas de seguridad del Banco Scotiabank hayan advertido de las maniobras fraudulentas correspondientes a las 6 transferencias realizadas el día 14 de enero de 2020, por la suma de $300.000 cada una, dando la alerta por

medio de un correo electrónico, pero nada hayan alertado acerca de las casi 50 operaciones fraudulentas realizadas el día inmediatamente anterior.

Añade que, hecho el reclamo en el Banco recurrido se activó el seguro contra fraudes que tenía contratado y vigente para casos como éstos, el que determinó la efectividad del fraude informático de que fue víctima y con fecha 4 de marzo de 2020, pagó la suma de $2.845.780, que corresponde al monto cubierto por el seguro.

Refiere que su representada ha solicitado en reiteradas ocasiones al recurrido la restitución de los fondos comprometidos en las operaciones fraudulentas y que no fueron cubiertos por el seguro, suma que asciende a $ 36.625.741, sin tener respuesta satisfactoria y que con fecha 14 de mayo de 2020 recibió una comunicación escrita del Banco recurrido, en que luego de señalar que su institución seguía revisando los antecedentes del caso, indica lo siguiente “Sin perjuicio de lo mencionado, debemos señalar que las transacciones denunciadas necesariamente requirieron su usuario (RUT), clave de ingreso y, además, su clave Scotiapass o Keypass, antecedentes que son personales e intransferibles, cuya custodia y uso es de exclusiva responsabilidad del cliente”, desconociendo en consecuencia su responsabilidad como institución bancaria obligada a resguardar los fondos depositados en ella por su representada.

Expresa que el acto arbitrario e ilegal denunciado consiste en que hasta la fecha el Banco recurrido se ha negado a restituirle los fondos comprometidos en las referidas operaciones en la parte no cubierta por el seguro contra fraudes, por un monto que asciende a $36.525.741, al extremo que, con fecha 14 de mayo de 2020 le informa que su caso sigue en estudio, eludiendo toda responsabilidad en los hechos.

Afirma que la conducta del Banco recurrido además de arbitraria es también ilegal toda vez que infringe las disposiciones reglamentarias existentes sobre la materia, específicamente las contenidas en la Recopilación de Normas de la Superintendencia de Bancos.

Menciona como garantía constitucional vulnerada el derecho de propiedad en sus diversas especies establecida en el artículo 19 Nº 24 de la Constitución Política.

Concluye solicitando acoger el recurso, declarando que el recurrido vulneró la garantía constitucional invocada, ordenándole restituir a la brevedad a su representada la suma de $36.625.741, que le fuera sustraída de su Cuenta Corriente No 971922079 (Producto No C048) y Cuenta Renta Diaria No 975810534 (Producto No V007), disponiendo las demás medidas que se estimen conducentes al pleno restablecimiento del derecho, con costas.

Informó la Comisión para el Mercado Financiero, exponiendo la regulación que rige a las empresas bancarias en materia de transferencias de fondos.

Explica que dicha normativa indica que los sistemas tecnológicos de que disponga el banco deben proveer un perfil de seguridad que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, además, la privacidad o confidencialidad de la información transmitida o procesada por ese medio y que los procedimientos deberán impedir que tanto el originador como el destinatario, en su caso, desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse métodos de autentificación para el acceso al sistema y al tipo de operación, que permitan asegurar su autenticidad e integridad.

Añade que las instituciones financieras deben mantener permanentemente abierto y disponible un canal de comunicación que permita al usuario ejecutar o solicitar el bloqueo de cualquier operación que intente efectuarse utilizando sus medios de acceso o claves de autenticación.

Expresa, asimismo, que los canales electrónicos que sean dispuestos por las empresas bancarias deben contar con apropiados privilegios de autorización y medidas de autentificación, controles de acceso lógico y físicos, adecuada infraestructura de seguridad para observar el cumplimiento de las restricciones y límites que se establezcan para las actividades internas y externas, así como para cuidar la integridad de los datos de cada transacción y la privacidad de los registros e información de los clientes.

Además, los bancos deben incorporar en sus procesos las mejores prácticas para la administración del riesgo operacional, de banca electrónica y los estándares internacionales que existen sobre la materia.

También la norma en comento exige a los bancos 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 con 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 tanto de clientes, como de no cliente (por ejemplo, en los intentos de acceso), de los puntos de acceso (v.gr. 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.

Estima pertinente consignar que dicha Comisión realiza una labor permanente de fiscalización y evaluación de los bancos bajo un modelo de supervisión basada en riesgo, actividad que implica la revisión y análisis de las políticas, métodos y procedimientos de que disponen las empresas bancarias con el objeto de mitigar y precaver los riesgos inherentes a su actividad.

Concluye expresando que la Comisión no tiene otros antecedentes que aportar, toda vez que no se ha formulado reclamo alguno por parte de la recurrente respecto a los hechos sometidos a la resolución de esa corte.

Informó el abogado Enrique Tapia Rivera, en representación de Scotiabank Chile, solicitando el total rechazo del recurso de protección, con expresa condena en costas.

Expresa, en primer término, que, respecto de los hechos y su ocurrencia, no existió vulneración de los sistemas del banco y que la recurrente se identificó con sus credenciales de seguridad.

Indica que, recibido el reclamo de la recurrente, se efectuó la investigación del caso, determinando que todas las transacciones objetadas fueron realizadas utilizando las claves personales e intransferibles del actor, a través del sitio web privado de la recurrente, ingresando en la sección de acceso al sitio privado, el Rut del recurrente y su clave personal y exclusiva, que es de su responsabilidad administrar y resguardar y que las operaciones se realizaron mediante la aplicación móvil Keypass, que había sido correctamente enrolada.

Afirma que no existió vulneración a los sistemas de seguridad de la institución y la recurrente se identificó correctamente como tal frente al Banco, de cara a las transacciones objetadas, ingresándose los datos y claves privadas y confidenciales del cliente, cuya custodia es su responsabilidad y que son indispensables para poder operar y administrar los productos y servicios financieros proveídos por el Banco a sus clientes en forma remota, a través de su sitio web o aplicación para dispositivos móviles.

Dice que no le consta que la actora haya sido efectivamente víctima de un fraude, por lo que ella deberá acreditar íntegramente lo anterior y declararlo así el tribunal pertinente, en un procedimiento de lato conocimiento y que podríamos estar frente a un caso de auto-fraude, o de un uso indebido de claves por terceros cercanos a la actora, de estafa o de fraude informático fraguado por terceros, etc.

Agrega que, del análisis realizado por Banco se pudo concluir que las transacciones objetadas por la clienta fueron realizadas a través del aplicativo Scotiaweb, siendo correctamente validadas por los sistemas de seguridad del Banco; se evidenció un eventual patrón de fraude informático por un tercero que habría afectado a titular de cuenta corriente, con el objeto de apropiarse de sus credenciales y claves con que operan por canales no presenciales del Banco; que las transacciones objetadas y que fueron cursadas por Scotiabank, corresponden a operaciones a través de canal Scotiaweb o Scotiabank Go respectivamente, donde los clientes habrían sido suplantados digitalmente por terceros y que no existe responsabilidad de Scotiabank en el accionar fraudulento de terceros, ya que se utilizan las credenciales y claves proporcionadas por el propio cliente.

Destaca que el Banco no tiene como saber si es que las transacciones fueron efectuadas por la propia cliente y recurrente en autos; o por un tercero, quien engañándola obtuvo sus claves y la suplantó digitalmente.

Por lo explicado considera que no es procedente la devolución de monto alguno, pues no existe vulneración alguna de los sistemas del Banco.

Afirma que su representado tiene a disposición de sus clientes un sitio web seguro, que permite acceder a cada cliente a sus productos financieros, mediante la incorporación del usuario y la clave de seguridad, personal e intransferible, que es definida por cada cliente. Explica las características y funcionamiento del sitio web de Scotiabank Chile que, en su concepto, es seguro y que la administración y resguardo de las claves de seguridad personales es de responsabilidad de los clientes.

Hace referencia a las campañas de autocuidado que ha desarrollado y que la Banca y los reguladores se han encargado recurrentemente de alarmar a los clientes sobre estos riesgos y, por tanto, de la importancia de su obligación de custodiar sus claves y datos personales.

Explica la importancia del deber de custodia de sus claves que pesa sobre los clientes el que, en su opinión es tanto o más importante incluso que la implementación de medidas de seguridad por parte de los Bancos.

Respecto de la forma cómo un tercero podría haber realizado el avance desde la tarjeta de crédito y luego hacer transferencias como si fuera el cliente, luego de explicar la forma de operar, concluye afirmando que Scotiabank Chile 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, incluyendo además una aplicación que permite el monitoreo y control por parte de los propios clientes sobre el uso de sus cuentas y tarjetas, desde su teléfono móvil.

Asevera que la recurrente entregó información personal a terceros, desconociendo si ello fue o no de manera intencional y que 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.

Afirma, asimismo, que no existió vulneración a los sistemas del Banco.

Alude a las obligaciones de los bancos en materia de ciberseguridad y que las normas correspondientes establecen las obligaciones de los Bancos en la materia, pero, además, dan cuenta de que el regulador entiende que la seguridad no es una obligación únicamente de los Bancos, sino también de los clientes.

Alega que son los tribunales ordinarios de justicia los encargados de determinar los estados de cuenta en caso de diferencias entre las partes y que la acción de protección no procede frente a un supuesto incumplimiento contractual y que se trata de un asunto de lato conocimiento frente a una controversia entre partes.

Expresa, asimismo, que no existe acto arbitrario o ilegal de Scotiabank Chile y que no existe privación, perturbación o amenaza de un derecho de la actora por parte de Scotiabank Chile.

Niega, igualmente, la existencia de un acto arbitrario o ilegal de Scotiabank Chile, así como la privación, perturbación o amenaza de un derecho de la actora por parte de Scotiabank Chile.

Finalmente, manifiesta que no existen medidas que esta corte pueda adoptar.

Informó el abogado Gian Carlo Lorenzini Rojas, en representación de la sociedad Bnp Paribas Cardif Seguros Generales S.A..

Expresa que con fecha 27 de noviembre de 2012, la recurrente contrató la póliza Nº 112072255, la cual contemplaba las siguientes coberturas: a) protección por mal uso o clonación de tarjetas, b) robo, asalto, hurto o extravío de talonarios de cheques y/o cheques individuales, c) utilización forzada por terceros de tarjetas bancarias, y d)

transferencias no reversables a través de sitios de internet de institución bancaria o financiera.

Hace presente que el monto máximo de indemnización contemplada para la cobertura de transferencias no reversables a través de sitios de internet de institución bancaria o financiera, ascendía al monto único total de UF 100 (cien unidades de fomento).

Agrega que, con fecha 13 de febrero de 2020, la recurrente fue objeto de una serie de transferencia electrónicas no reversables realizadas por terceros desconocidos y no autorizados para ello, por la suma única y total de $39.471.521 y que denunció el siniestro, motivo por el cual se procedió a activar la cobertura de transferencias no reversables a través de sitios de internet de institución bancaria o financiera amparada en la póliza por ella contratada, dando origen al siniestro Nº 3222751.

Explica que, una vez recibida la denuncia del siniestro antes señalado su representada solicitó copia de todos los documentos y antecedentes necesarios para lograr determinar la procedencia de la cobertura solicitada y que, terminado el proceso de liquidación, con fecha 25 de febrero de 2020, procedió a emitir informe de liquidación del siniestro de la referencia, por medio del cual estimó pertinente acoger la solicitud de cobertura e indemnización solicitada por la recurrente procediendo al pago del monto máximo de cobertura amparado en la póliza contratada.

Se dispuso traer los autos en relación.

CONSIDERANDO:

1º. Que, tratándose de una acción constitucional de protección, para su precedencia se precisa la concurrencia copulativa de los siguientes presupuestos: **a)** Una conducta –por acción u omisión– ilegal o arbitraria; **b)** la afectación, expresada en privación, perturbación o amenaza, del legítimo ejercicio de determinados derechos esenciales asegurados en la Constitución y que se enuncian en el mencionado precepto; **c)** relación de causalidad entre el comportamiento antijurídico y el agravio a la garantía fundamental; **d)** la posibilidad del órgano jurisdiccional de adoptar providencias de tutela adecuadas, para resguardar el legítimo ejercicio del derecho comprometido y **e)** que la pretensión constitucional se haya interpuesto oportunamente;

2º. Que, en la presente acción constitucional de protección se sindica como acto arbitrario e ilegal la negativa de la entidad bancaria recurrida restituir los fondos comprometidos en operaciones fraudulentas realizadas en perjuicio de la recurrente, por un monto que asciende a $36.525.741, solicitándose, en consecuencia, como medida de

protección, la condena a la recurrida a la restitución de las sumas sustraídas;

3º. Que, son hechos establecidos en el proceso los siguientes:

a) que la recurrente es titular de dos productos financieros contratados con el Banco Scotiabank: Cuenta Corriente Nº 971922079 y Cuenta Renta Diaria Nº 975810534;

b) que, con fecha 13 de enero de 2020 se realizó una transferencia desde su Cuenta Renta Diaria Nº 975810534 por la suma de $38.000.000 a su Cuenta Corriente Nº 971922079 y con esa misma fecha se realizaron un conjunto de aproximadamente 50 operaciones de transferencias y pagos desde esta última cuenta con destino desconocido, por un monto total de $39.471.521;

c) que la recurrente tenía contratada una póliza con cobertura por protección por mal uso o clonación de tarjetas y transferencias no reversables a través de sitios de internet de institución bancaria o financiera, entre otras;

d) que, una vez activada la señalada cobertura, la compañía aseguradora estimó procedente la indemnización solicitada por la recurrente procediendo al pago del monto máximo de cobertura amparado en la póliza, esto es, la suma única y total del equivalente 100 unidades de fomento;

4º. Que, el Capítulo 1-7 de la recopilación actualizada de normas sobre **transferencia electrónica de información y fondos**, contiene un conjunto de instrucciones relativas a la prestación de servicios bancarios y la realización de operaciones interbancarias que se efectúan mediante transmisiones de mensajes o instrucciones a un computador conectado por redes de comunicación propias o de terceros, efectuadas desde otro computador o mediante el uso de otros dispositivos electrónicos (cajeros automáticos, teléfonos, PINPAD, etc.).

Entre otras exigencias, en su numeral 2 letra C) exige 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 resguardar, además, la privacidad o confidencialidad de la información transmitida o procesada por ese medio".

Se agrega que "Los procedimientos deberán impedir que tanto el originador como el destinatario, en su caso, desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse métodos de autentificación para el acceso al sistema y al tipo de operación, que permitan asegurar su autenticidad e integridad".

También establece en la letra E) que "Para todos los sistemas de transferencia automática de fondos deberá establecerse un límite en los

montos de transferencia con respecto a cada cliente con acceso al sistema. Cuando se trate de un servicio de uso masivo que no contempla la posibilidad de efectuar transacciones importantes, dicho límite podrá fijarse en forma general para todos los usuarios".

En el capítulo 4.2, relativo a la **Prevención de fraudes**, se establece 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.

Se agrega que 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), de 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;

5º. Que, a la luz de los hechos establecidos y de las instrucciones antes señaladas, es posible concluir que la recurrida incumplió las disposiciones de la Comisión para el Mercado Financiero, toda vez que la realización de 50 operaciones transferencias de fondos que prácticamente vaciaron la cuenta corriente de la actora, no puede sino ser considerada como una operación potencialmente fraudulenta, considerando la capacidad económica de la cuentacorrentista y su comportamiento habitual.

Frente a estos movimientos en las cuentas de la recurrente que, evidentemente aparecían revestidas de los caracteres de un fraude, los sistemas del banco no funcionaron porque no permitieron su oportuna detección e identificación, como lo exigen las instrucciones de la autoridad financiera y la naturaleza del contrato de cuenta corriente, que impone al banco la obligación de restituir las sumas depositadas, esto es la misma cantidad de dinero que ha recibido, aunque no se trate de las mismas monedas y billetes, por cuanto se trata de un depósito de cosas fungibles, cuya propiedad adquiere éste y en el que la confianza entre los contratantes resulta esencial;

6º. Que no está de más agregar que, de acuerdo a lo informado por la Compañía Aseguradora, ésta consideró que los hechos denunciados cumplían los requisitos necesarios para hacer procedente una indemnización según la cobertura contemplada en la póliza suscrita por la recurrente, pagándole la correspondiente indemnización, con el tope previsto en la póliza;

7º. Que, en consecuencia, la conducta imputable al recurrido puede considerarse antijurídica porque incumplió las instrucciones emanadas de la Comisión para el Mercado Financiero y es, asimismo, arbitraria al negarse a restituir los fondos que le fueron desviados de la esfera de resguardo del propio banco, sin una causa que justifique su negativa, todo lo cual le ha provocado a la recurrente un menoscabo significativo en su patrimonio, vulnerándole la garantía constitucional consagrada en el N° 24 del artículo 19 de la Constitución Política de la República.

Por estas consideraciones y de acuerdo con lo dispuesto en los artículos 19 y 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, se declara que **se acoge, con costas**, el deducido por el abogado Roberto A. Coloma Del Valle, en representación de Brenda Julieta Flores Jarpa, en contra del Banco Scotiabank, ordenándose al recurrido la restitución a la actora de la suma de $36.625.741, en su cuenta corriente N° 971922079, que mantiene en dicha institución bancaria o en la que indique la recurrente.

Regístrese, comuníquese y archívese.

Redactó el abogado integrante Gonzalo Cortez Matcovich.

Rol Nº 10633-2020. Recurso de Protección.

Juan Angel Munoz Lopez
MINISTRO
Fecha: 22/09/2020 14:29:22

Gonzalo Luis Rojas Monje
MINISTRO(S)
Fecha: 22/09/2020 13:40:43

Gonzalo Alonso Cortez Matcovich
ABOGADO
Fecha: 22/09/2020 11:25:59

Pronunciado por la Segunda Sala de la C.A. de Concepción integrada por Ministro Juan Angel Muñoz L., Ministro Suplente Gonzalo Rojas M. y Abogado Integrante Gonzalo Alonso Cortez M. Concepcion, veintidós de septiembre de dos mil veinte.

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