C.A. de Concepción
xsr
Concepción, veinticuatro de junio de dos mil veinte.

VISTO:

En estos antecedentes Rol Corte 8120-2020 comparece deduciendo recurso de protección el abogado Rodrigo Padilla Bernedo, en representación de doña Luz María Jaureguiberry Labbé, dueña de casa, ambos domiciliados para estos efectos en Tucapel 142, Concepción. Lo dirige en contra del Banco Scotiabank Chile, institución financiera del giro de su denominación, representada legalmente por su gerente general Francisco Sardón De Taboada, de nacionalidad peruana, o por quien lo subrogue o reemplace en el cargo, con domicilio para estos efectos en la sucursal bancaria ubicada en calle Barros Arana N°345, de Concepción.

El fundamento del recurso lo constituye la actuación ilegal y arbitraria del Banco frente al fraude de que fuera objeto el 21 de diciembre de 2019 debido a la vulneración del sistema de seguridad del mismo por terceros, con el uso fraudulento de sus tarjetas, realizándose transacciones por un monto total de $17.108.000, no por su persona y desde luego sin su conocimiento ni consentimiento, sin que el Banco se haga responsable de las sumas de dinero defraudadas desde el saldo de su cuenta corriente a través de transferencias directas y también con la utilización de sus tarjetas de crédito solicitando avances de dinero para posteriormente usar el mismo en pagos por internet; y, en cambio, haciendo el Banco recurrido de cargo de la afectada el fraude, aduciendo que para efectuar las transferencias se requiere validación de claves, que son de exclusiva responsabilidad de la cliente desde la entrega y activación de sus productos.

Afirma que el sábado 21 de diciembre de 2019, recibió una llamada telefónica de quien se individualizó como Francisco Garrido, trabajador del departamento de seguridad del Banco Scotiabank, quien le consultó si estaba realizando transacciones desde su cuenta corriente y tarjetas de crédito, ya que el Banco había detectado movimientos inusuales. La actora se contactó con el call center del Banco, siendo atendida por Diana Barreros, quien le confirmó los movimientos inusuales detectados por parte del Banco. Ante dicha confirmación, solicitó que se bloquearan sus tarjetas. Igualmente, desde el call center le indicaron que debía hacer la denuncia por fraude ante Carabineros y concurrir el día lunes al Banco para hacer el reclamo respectivo y hacer entrega del parte policial. Siguiendo las instrucciones del call center, concurrió a Carabineros el mismo 21 de diciembre de 2019 para hacer la denuncia respectiva, según da cuenta el parte policial n°1381. Luego, el lunes 23 de diciembre concurrió al Banco Scotiabank, sucursal O'Higgins de la ciudad de Concepción, a realizar los reclamos por el fraude sufrido y solicitud de devolución de dineros. En dicha oportunidad, personal de atención al cliente le informó que

respecto de las tarjetas de crédito debía formular el reclamo por fraude y solicitud de restitución del dinero una vez que éstas se facturaran, lo que ocurriría los días 18 y 20 de enero de 2020, procediendo finalmente de tal manera.

El Banco recurrido respondió el reclamo que formuló, señalando que concluida la investigación interna, se determinó que no existió vulneración a los sistemas de seguridad del Banco, no accediendo entonces al reclamo formulado ni a la restitución de los montos defraudados.

Añade que el monto defraudado asciende a la suma de $17.108.000, consistentes en $1.005.000 por concepto de cinco transferencias electrónicas desde su cuenta corriente a terceros desconocidos, y de $16.103.000 por concepto de seis pagos o compras por internet. El fraude consistió en trasferencias directas desde la cuenta corriente a terceros desconocidos por ella, y en la utilización de sus tarjetas de crédito solicitando avances de dinero para posteriormente utilizar el mismo en pagos por internet.

Agrega que las operaciones y movimientos recién descritos son totalmente atípicos tanto en su naturaleza como en su monto, en relación a la conducta que doña Luz ha mantenido a lo largo de su relación contractual con Banco Scotiabank.

Dice que junto con hacer el reclamo respectivo al Banco, informó del siniestro en razón de los seguros que tenía contratados en esta materia con BNP Paribas Cardif Seguros Generales S.A. Es del caso que los informes de liquidación solamente determinaron la devolución de $1.050.000 previo pago de un deducible de $85.320 por concepto de monto defraudado en la cuenta corriente. Respecto al monto defraudado por vulneración en las tarjetas de crédito, se determinó que no correspondía devolución alguna ya que el siniestro no estaría cubierto por el seguro contratado. Sin perjuicio de lo anterior, doña Luz no activó el seguro, toda vez que le corresponde al Banco restituir los montos defraudados en razón de la fragilidad y vulnerabilidad de su sistema de seguridad.

A la fecha persiste la afectación del derecho de propiedad de la clienta afectada, pues el recurrido no ha accedido a la restitución de los dineros defraudados como corresponde al haber sido vulnerado su sistema de seguridad. Y, es más, en un escrito posterior, con ocasión de una orden de no innovar solicitada, hace presente el letrado recurrente que doña Luz sigue recibiendo llamados a su teléfono celular y de red fija por parte de personal del departamento de cobranza del Banco Scotiabank, entre ellos doña Alejandra Latorre, con objeto de requerir insistentemente el pago de los montos facturados en sus cuentas bancarias. Dichos llamados, tienen lugar varias veces al día e inclusive los fines de semana. El Banco recurrido, no obstante estar al tanto del presente recurso de protección y de la afectación de derechos que ha sufrido la recurrente, no ha tomado las medidas mínimas en orden a

detener estos cobros telefónicos que perturban y amenazan no solo el derecho de propiedad de la señora Jaureguiberry al pretender que asuma una obligación que no le corresponde, sino que también afectan sus derechos a la integridad psíquica y a la protección de su vida privada.

Denuncia el letrado recurrente que la defraudación cibernética descrita se ha debido a una actuación negligente del Banco Scotiabank, quien no tomando todas las medidas de seguridad en los servicios prestados a sus clientes ha permitido que terceros, vulnerando sus sistemas, realicen actividades u operaciones fraudulentas. El comportamiento del Banco de desconocer su responsabilidad por la vulneración de las medidas de seguridad de sus productos bancarios, constituye abiertamente una actuación arbitraria e ilegal, que infringe precisamente el deber de seguridad en la prestación de sus servicios que resulta inherente a la actividad bancaria. El propio recurrido advirtió que se estaban realizando movimientos inusuales en la cuenta bancaria de la recurrente, razón por la cual se contactó con ella personal de su departamento de seguridad el 21 de diciembre de 2019, y no obstante, pese a detectarse tales movimientos inusuales, Scotiabank no tomó las medidas tendientes a impedir que éstos se materializaran y finalmente derivaran en una afectación grave en su patrimonio. Luego, constando ello, ha resultado completamente arbitraria su negativa a restituir el dinero que corresponde.

Pide que se acoja el recurso, con costas, y se ordene al banco recurrido la inmediata restitución de la suma de $17.108.000 más los intereses e impuestos asociados al uso automático de la línea de crédito.

Cita jurisprudencia el apoyo a su pretensión.

Informó el recurso la sociedad BNP Paribas Cardif Seguros Generales S.A., a través del abogado Gian Carlo Lorenzini Rojas, con domicilio en Av. Alonso de Córdova N°2860, oficina 504, comuna de Vitacura. Dijo que la recurrida contrató, el 27 de abril de 2009, con esa Compañía, la póliza N°10406179, la cual contemplaba dentro de sus coberturas la de robo, hurto o extravío de cheques; utilización forzada por terceros de tarjeta redbanc o de crédito; mal uso y clonación de tarjetas bancarias; transferencias remotas cuentas bancarias; y transferencias remotas tarjeta de crédito. Dentro de las condiciones de la póliza se establecía un monto tope de indemnización para la cobertura de transferencias remotas de cuentas bancarias un monto único y total de UF 48 (cuarenta y ocho Unidades de Fomento). Se contemplada también un deducible de UF 3 (tres Unidades de Fomento) aplicable a cada evento y a cada pérdida sufrida por el asegurado. El 23 de diciembre de 2019, la recurrente fue objeto de una solicitud de avance de dinero en su tarjeta de crédito por parte de terceras personas que no se habrían encontrado autorizadas para ello por una suma única y total de $17.108.000

(diecisiete millones ciento ocho mil pesos), de los cuales $1.005.000 (un millón cinco mil pesos) fueron transferidos electrónicamente a cuentas bancarias de terceros desconocidos, y el monto de $16.103.000 (dieciséis millones ciento tres mil pesos) utilizados por terceros para realizar compras por internet. Una vez tomado conocimiento de este hecho, la recurrente procedió a denunciar el siniestro que la afectó, ocasión en que la Compañía dio inicio al proceso de liquidación de dicho siniestro, asignando como liquidador oficial encargado del proceso a la compañía Segured Ltda. Esta última apertura el siniestro N°3219596 respecto a las transferencias bancarias realizadas a cuentas de terceros y el siniestro N°3219597 respecto a las compras realizadas con los fondos obtenidos por medio del avance de dinero realizado por medio de la tarjeta de crédito de la recurrente. Terminado el proceso de liquidación de los siniestros, el liquidador oficial Segured Ltda., emitió el informe de liquidación N°TJS/02- 2020/1058488 respecto del siniestro N°3219596, estimando pertinente acoger la solicitud de cobertura realizada por la recurrente, procediendo al pago del monto defraudado con motivo de las transferencias electrónicas realizadas a las cuentas de terceros, indemnizando el monto único y total de $919.680 (novecientos diecinueve mil seiscientos ochenta pesos), el cual es el resultado de la resta del monto total de lo defraudado, es decir, $1.005.000 (un millón cinco mil pesos) menos el monto del deducible de UF 3 (tres Unidades de Fomento), el cual a la fecha de liquidación del siniestro ascendía a la suma de $85.320 (ochenta y cinco mil trecientos veinte pesos). En lo que respecta al siniestro N°3219597, Segured Ltda. emitió el informe de liquidación N°TJS/02-2020/10058489 estimando pertinente rechazar la cobertura solicitada por la recurrente, toda vez que las compras realizadas por internet no se encontraban amparadas en la póliza por ella contratada. Recibida la petición de informe de este recurso de protección, la Compañía ha decidido revaluar el siniestro N°321597 referente a las compras realizadas por terceros no autorizados por la recurrente, y finalmente ha estimado entregar, de forma excepcional, la cobertura que solicitó, por lo que se procederá a cubrir la pérdida sufrida por las compras realizadas por terceros no autorizados por la recurrente por el monto tope la cobertura de "transferencias remotas cuentas bancarias" amparada en la póliza contratada, esto es, un monto total de UF 45, el cual es el resultado de la resta del monto máximo de cobertura (UF 48) menos el monto de deducible contemplado en el mismo contrato (UF 3), emitiéndose el correspondiente informe de liquidación en dicho sentido. En consideración de lo anterior, y tomando en cuenta el valor de la Unidad de Fomento a la fecha de emisión del referido informe, se procederá al pago de un monto único y total de $1.291.727 (un millón doscientos noventa y un mil setecientos veintisiete pesos). El pago efectivo del monto antes señalado se llevará a cabo dentro de plazo de 10 días hábiles contados a partir de su fecha de emisión.

A su informe acompañó a) Copia simple de la póliza Nº10406179 contratada por la recurrente; b) Endoso Nº 3/2011 a la póliza Nº10406179; c) Informe de liquidación NºTJS/02/2020/01058488 emitido por Segured Ltda.; d) Informe de liquidación NºTJS/02/2020/01058489 emitido por Segured Ltda., y e) Informe de liquidación emitido por BNP Paribas Cardif Seguros Generales S.A.

También informó el recurso la compañía Liquidadores de Seguros en Red Carvallo Limitada, Segured Ltda., a través del abogado Rodrigo Enrique Oyarzún Rojas, ambos domiciliados para estos efectos en calle Monseñor Sótero Sanz N° 55, Piso 11, comuna de Providencia. Explica que su misión en el ámbito asegurador y sus consecuentes procedimientos de comercialización, liquidación de siniestros, impugnaciones, está regulado normativamente en el Decreto Supremo 1.055 y que existe un ente regulador el cual es la Comisión Para El Mercado Financiero (CMF). Que el actuar del liquidador se materializará en una liquidación técnicamente fundada que debe pronunciarse sobre la ocurrencia de un siniestro, luego determinar si el riesgo está bajo cobertura de una compañía de seguros determinada, y el monto de la indemnización a pagar, todo ello en conformidad al procedimiento establecido en la ley. El propio Decreto Supremo 1.055 establece un procedimiento reglado para reclamar o impugnar un informe de liquidación, o cualquier rechazo indemnizatorio por parte del Liquidador, el cual puede llegar incluso a la justicia arbitral u ordinaria, según corresponda.

Respecto del caso de la recurrente, doña Luz suscribió la póliza 10406179 con la Compañía BNP Paribas Cardif Seguros Generales S.A., el 27 de abril de 2009, la que contemplaba entre sus coberturas, las de robo, hurto o extravío de cheques; utilización forzada por terceros de tarjeta redbanc o de crédito; mal uso y clonación de tarjetas bancarias; transferencias remotas cuentas bancarias; y transferencias remotas tarjeta de crédito. En las condiciones de la póliza se estableció un monto tope de indemnización para la cobertura de transferencias remotas de cuentas bancarias de 48 Uf y un deducible de 3 Uf aplicable a cada evento. Respecto del fraude materia de este recuso de protección, los $17.108.000 que se desglosan en $1.005.000 en trasferencias a terceros desconocidos y $16.103.000 en compras por internet.

La compañía BNP Paribas Cardif designó a Liquidadores de Seguros en Red Carvallo Limitada, Segured Ltda., para que llevara a cabo la liquidación del siniestro. Actuando en el ámbito de las funciones que la ley le otorga como compañía de liquidación de seguros, Segured procedió a la apertura del siniestro N°3219596 y N°3219597 para conocer de las transferencias y las compras vía internet respectivamente. Emitió el informe de liquidación TJS/02-2020/01058488 respecto del siniestro N°3219596, estimando que el relato de la asegurada contaba con la cobertura respectiva

recomendando la aprobación de este y la consecuente indemnización de $919.680 (luego de aplicado el deducible mencionado en párrafos anteriores). En el siniestro N°3219597, Segured determinó que las transacciones impugnadas no estaban amparadas por ninguna de las coberturas contratadas y en consecuencia emitió el informe de liquidación TJS/02-2020/01058489 con el rechazo en comento, sin perjuicio de la decisión que pueda adoptar por su parte la compañía de seguros BNP Paribas Cardif Seguros Generales S.A.

A su informe allegó copia de los Informe de liquidación N° TJS/02/-2020/01058489 (siniestro N°3219597) y N° TJS/02-2020/01058488 (siniestro N°3219596), ambos emitidos por Segured Ltda.

Informó el recurso el recurrido Banco Scotiabank Chile, a través del abogado Enrique Tapia Rivera, y pidió el rechazo del mismo.

Luego de hacer una síntesis del recurso, señala que el banco realizó la investigación pertinente para determinar si en los hechos (1) existió una vulneración a los sistemas del banco; o (2) si los fondos fueron transferidos utilizándose los datos privados y las claves de la cliente, las que sólo son conocidas por ella, y lo anterior para determinar si las transacciones se realizaron a través del canal Scotiaweb y validada por los sistemas de seguridad del Banco, mediante el correcto ingreso del número de Rut y Clave Scotiaweb y Scotiapass y/o Keypass. Del análisis realizado se concluye 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 de la recurrente; determinándose que no era procedente la devolución que se solicitaba. Las operaciones fueron realizadas ingresando la información privada de la cliente y las claves, que sólo deben ser conocidas por ella. En este caso, el Banco no tiene cómo 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.

Agrega el informante que si es que existió un fraude, éste sólo pudo ocurrir pues la recurrente no fue suficientemente diligente en la custodia de sus claves y datos personales. Que el contrato celebrado entre la actora 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. Que 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 éstos deben tomar, existiendo extensas campañas publicitarias en diarios, redes sociales, televisión, radio e internet, ya sea en el Facebook del

Banco, en el hashtag #quenotepillenvolandobajo.

Sobre las formas cómo pueden ocurrir los fraudes, como el que le sucedió a la actora, dice que básicamente acontecen por dos vías: (1) con vulneración de los sistemas del Banco o (2) sin vulneración de los sistemas del Banco, suplantándose digitalmente la identidad del cliente por un tercero, quien obtuvo sus claves y datos a través de los mecanismos de fraude habituales: Pharming, Fishing, llamados telefónicos, instalación de malware, etcétera, hechos en los cuales el Banco no tiene ninguna injerencia. El cuidado y resguardo de los clientes de su información personal y claves es tanto o más importante incluso que la implementación de medidas de seguridad por parte de los Bancos. De nada sirve que las instituciones financieras tengan los últimos sistemas de seguridad si es que los clientes, voluntariamente, entregan sus datos y claves de acceso, permitiendo a los delincuentes suplantarlos digitalmente.

Respecto de las medidas de seguridad del Banco para las operaciones no presenciales, dice que los clientes del Banco Scotiabank pueden acceder a la aplicación "Scotiabank Go Chile" 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 móvil "Scotiabank Keypass" que se utiliza para autorizar transacciones desde su cuenta, generando 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, aplicación que para ser activada requiere del ingreso de una serie de claves que le son entregada en forma confidencial solo al cliente. Es una aplicación segura pues todos los clientes cuentan con un PIN de seguridad que eligieron al momento de activar la aplicación, 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 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. Pero además el uso de estas aplicaciones permiten "bloquear" temporalmente las tarjetas y productos de los clientes.

Añade que en el caso de la actora, el supuesto tercero realizó el avance desde la tarjeta de crédito y luego hizo transferencias como si fuera el cliente, porque seguramente la recurrente entregó información personal a terceros, desconociendo el Banco 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. No existe, en consecuencia, vulneración a los sistemas del Banco. Las operaciones sólo pudieron realizarse por la propia clienta o por un tercero que haya obtenido sus claves directamente de ella. 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.

En resumen, estima que el recuso debe rechazarse porque es un asunto de lato conocimiento, siendo los tribunales ordinarios de justicia los encargados de determinar los estados de cuenta en caso de diferencias entre las partes. Asimismo, porque la acción de protección no procede frente a un supuesto incumplimiento contractual; se trata, en consecuencia, de un asunto de lato conocimiento frente a una controversia entre partes, y de acogerse esta acción cautelar tendría que declararse que el banco ha incumplido el contrato de cuenta corriente, lo que importaría obviar -y por esa vía infringir- las normas generales que señalan que dicha materia es necesariamente objeto de un procedimiento de lato conocimiento. Paradojalmente se estaría vulnerando el derecho al debido proceso del Banco. Tratándose de un fraude, como acusa la recurrente, debiera discutirse en sede penal quién o quiénes son los responsables del fraude y su participación en los hechos, para luego, como señala el artículo 680, determinar las indemnizaciones pertinentes. Además, como antes dijo, siendo de cargo de la recurrente el resguardo de sus claves bancarias, no existe acto arbitrario o ilegal de Scotiabank, ni privación, perturbación o amenaza de un derecho de la actora, y por lo tanto, tampoco existen otras medidas que esta Corte pueda adoptar.

En apoyo a su defensa, cita copiosa jurisprudencia.

Acompañó con su informe 1.- Copia de contrato Tarjeta Visa 0050402675000047656, denominado "Contrato de afiliación al sistema y uso de tarjeta de crédito visa y apertura de línea de crédito en moneda nacional" de 30/06/2013, firmado por la recurrente; 2.- Copia de contrato denominado "Contrato de operaciones bancarias para personas naturales" de 21/04/2009, firmado por la recurrente; 3.- Copia de contrato Tarjeta Visa 0050402675000000133, denominado "Contrato de afiliación al sistema y uso de tarjeta de crédito visa y apertura de línea de crédito en moneda nacional" de 22/04/2009, firmado por la recurrente; 4.- Copia de contrato Tarjeta Visa denominado "Contrato de afiliación al sistema y uso de tarjeta de crédito visa y apertura de línea de crédito en moneda nacional" de 13/10/2010, firmado por la recurrente; 5.- Copia de publicaciones realizadas en Twitter por Scotiabank Chile, con el objeto de promover la seguridad; 6.- Ciberseguridad: Información, consejos, y todo lo necesario para estar protegido e informado; 7.- Copia del documento que informa acerca de cómo Scotiabank enfrenta los riesgos en Ciberseguridad; 8.- Copia del Informe de Ciberseguridad en la banca; 9.- copia del ABIF: Lo que necesito saber de mi tarjeta de crédito; 10.-

copia del Contrato único de cliente persona natural con Scotiabank; copia del Contrato de operaciones bancarias para personas naturales, BBVA, y 12.- copia de la Minuta GSFD Nº 041-2019, Gerencia Servicios Forenses Digitales, que complementa minutas por fraude web a clientes, mediante técnicas de phishing y pharming.

Informó también el recurso la Comisión para el Mercado Financiero. Dijo que habiendo buscado en los sistemas de correspondencia de esta Comisión, se encontró la presentación de fecha 23 de enero de 2020, la que se encuentra en el correspondiente proceso de tramitación. Y describe luego su misión. La Comisión ha dispuesto en el Capítulo 1-7 de su Recopilación Actualizada de Normas sobre Transferencia Electrónica de Información y Fondos, las instrucciones para 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, tales como cajeros automáticos, teléfonos, PINPAD u otros; que dichos servicios comprenden tanto las transferencias electrónicas de fondos como cualquier otra operación que se realice utilizando documentos o mensajes electrónicos o dispositivos que permiten a los clientes del Banco la ejecución automática de operaciones; que, además, dichas normas abarcan las comunicaciones por vía electrónica que no den origen a una operación propiamente tal, cuando la información transmitida esté sujeta a secreto o reserva de acuerdo con lo establecido por el artículo 154 de la Ley General de Bancos. Agrega, que los sistemas tecnológicos de que disponga el Banco, como requisito general, 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; 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; que, adicionalmente, 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; que cada sistema que opere en línea y en tiempo real, debe permitir dicho bloqueo también en tiempo real; 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, y, sin perjuicio de lo indicado, los bancos habrán de 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; que los Bancos deben 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 éstos y comportamientos que no estén asociados al cliente; que estos sistemas o mecanismos deben permitir tener una vista integral y oportuna de las operaciones tanto de clientes como de no clientes, de los puntos de acceso, 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.

Finaliza señalando que la forma en que dicha Comisión fiscaliza a las entidades bancarias, es a través de 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.

Se trajeron los autos en relación.

CON LO RELACIONADO Y CONSIDERANDO:

PRIMERO: Que, el recurso de protección de garantías constitucionales establecido en el artículo 20 de la Constitución Política de la República, constituye jurídicamente una acción constitucional de urgencia, de naturaleza autónoma, destinada a amparar el legítimo ejercicio de las garantías y derechos preexistentes que en esa misma disposición se enumeran, mediante la adopción de medidas de resguardo que se deben tomar ante un acto u omisión arbitrario o ilegal que impida, amague o perturbe ese ejercicio.

Por consiguiente, resulta requisito indispensable de la acción de protección la existencia de un acto u omisión ilegal, esto es contrario a la ley, o arbitrario, o sea, producto del mero capricho de quien incurre en él, y que provoque algunas de las situaciones o efectos que se han indicado, afectando a una o más de las garantías preexistentes protegidas, consideración que resulta básica para el análisis y la decisión del recurso que se ha interpuesto.

En el caso de autos, el actuar ilegal o arbitrario que la recurrente imputa al Banco recurrido, es la negativa de este último a restituir en la cuenta corriente y tarjeta de crédito de la primera, los dineros sustraídos fraudulentamente, sin su conocimiento ni consentimiento,

aun incluso cuando el seguro de fraude contratado por la recurrente ha dispuesto el pago, hasta por los montos cubiertos por la póliza, menos los deducibles, por los siniestros que fueron denunciados.

SEGUNDO: Que, es un hecho establecido en autos que efectivamente la señora Luz María Jaureguiberry es cliente del Banco recurrido y mantiene en éste algunos productos, y, en lo que interesa, es titular de una cuenta corriente y tarjeta de crédito asociada a dicha cuenta, desde la primera se realizaron cinco transferencias electrónicas a terceros desconocidos hasta por un monto de $1.005.000 y seis pagos o compras por internet hasta un monto de $16.103.000, desde la segunda, lo que suma la cantidad de $17.108.000.-

Relativamente a dicho contenido fáctico, la actora sostiene que esos movimientos y transferencias fueron producto de un fraude del cual es el Banco quien debe responder y, por su parte, la entidad bancaria recurrida aduce que esos movimientos dinerarios son de responsabilidad de la clienta, dado que bajo su custodia se encuentran las medidas de seguridad que indica: las claves personales, el uso de la 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.

TERCERO: Que, en lo concerniente a la cuestión medular discutida, la Excma. Corte Suprema ha señalado (por ejemplo en roles 2196-2018 y 15126-2019) que el contrato de cuenta corriente bancaria constituye una especie de depósito irregular, respecto de un bien eminentemente fungible, y que es de cargo del depositario el riesgo de pérdida de la cosa depositada durante la vigencia de la convención, y que, para cada caso, resulta relevante analizar si los eventos que originaron las transferencias cuestionadas no han tenido como única causa la voluntad del depositante o cuentacorrentista, o han ocurrido otros que llevan a sostener que se han incumplido las obligaciones de resguardo y seguridad que recaen en la institución bancaria respectiva.

Y ha agregado nuestro Excmo. Tribunal, que la variedad de las formas como se intenta vulnerar los sistemas de seguridad y la dificultad probatoria inmediata, obligan a realizar un juicio acerca de indicios sobre la ocurrencia de los hechos y confrontar aquellos con las diversas normas que determinan las obligaciones de seguridad de las instituciones bancarias.

Así, para el caso de transferencias electrónicas, el Capítulo 1-7, punto 4.2, de la Recopilación de normas de la Superintendencia de Bancos, indica que: "Los bancos deberán contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible aquellas operaciones con patrones de fraude, de modo de marcar o abortar actividades u operaciones potencialmente fraudulentas, para lo cual deberán establecer y mantener, de acuerdo a la dinámica de los fraudes, patrones conocidos

de estos y comportamientos que no estén asociados al cliente.

Estos sistemas o mecanismos deberán permitir tener una vista integral y oportuna de las operaciones del cliente, del no cliente (por ejemplo en los intentos de acceso), 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".

CUARTO: Que, en la situación de autos, el Banco recurrido solamente adujo que sus medios electrónicos no fueron vulnerados. Sin embargo, aparte de esta negativa, nada señaló acerca del modo en que pudo verse vulnerada su página web o los enlaces que conducían hacia su página de internet y donde se pudieron capturar los datos de su clienta, la señora Jaureguiberry, situación que conduce a esta Corte a estimar que carece de asidero, ya desde un plano normativo, ya desde un plano de racionabilidad, la negativa del Banco a cubrir las pérdidas sufridas por su aludida clienta, en la medida que ningún antecedente proporcionó en orden a que la situación denunciada en el recurso no haya ocurrido con ocasión de la sustracción de las claves por parte de terceros y precisamente por una vía distinta a la obtención de las mismas a través de su página web oficial.

QUINTO: Que, teniendo en consideración los antecedentes colacionados en la especie, adquieren notoria importancia las obligaciones de monitoreo y control de fraudes que recaen expresamente en la institución bancaria recurrida, donde los patrones de conducta del cliente son elementos de juicio para la determinación de una operación engañosa, cuestión que no fue informada en detalle por el Banco recurrido.

Sobre la institución bancaria recae la obligación de vigilancia y el análisis de la correlación de eventos y seguridad de las operaciones, por lo que, una vista general de las operaciones de la cliente en la cuenta corriente respectiva, otorgan verosimilitud a la posible intervención de terceros en los sistemas de seguridad que otorgó la recurrida.

No es posible soslayar que, en el caso de autos, el sistema de seguridad del Banco detectó operaciones irregulares en los productos de su clienta, tanto así que funcionarios del Banco llamaron a la cliente para alertarle y ello motivó que la clienta ordenara al Banco el bloqueo de sus productos, haciendo la correspondiente denuncia ante Carabineros, como se lo sugirieron los funcionarios del Banco, para luego, al día hábil siguiente formular la denuncia ante el Banco y solicitar la restitución de su dinero sustraído. Entonces, el mismo llamado, pudo haber sido efectuado a la clienta antes de materializar las operaciones sospechosas, evitando así el fraude, caso en el cual la actuación del Banco habría sido todo lo diligente que se espera y requiere.

SEXTO: Que, así las cosas, ha de calificarse el actuar del Banco

recurrido como arbitrario, al no asumir el perjuicio económico reclamado, trasladando los efectos del fraude bancario a su clienta, afecta directamente el patrimonio de ésta, vulnerando así su derecho de propiedad garantizado en el artículo 19 N°24 de nuestra Carta Fundamental.

La protección impetrada, entonces, habrá de ser otorgada del modo que se dirá.

Por estas consideraciones y de conformidad con lo que dispone el artículo 20 de la Constitución Política de la República y el Auto Acordado de la Excma. Corte Suprema sobre la materia, **se decide que:**

SE ACOGE, con costas, el recurso de protección interpuesto en estos autos, en cuanto el **Banco Scotiabank Chile** deberá restituir a doña **Luz María Jaureguiberry Labbé** la suma de **$17.108.000** (diecisiete millones ciento ocho mil pesos), menos la cobertura efectivamente proporcionada por el seguro contratado.

Acordada con el voto en contra del abogado integrante Hugo Tapia Elorza, quien fue de parecer de desestimar la acción constitucional de protección intentada, teniendo para ello presente que, en su concepto, en el caso de autos no se está en presencia de garantizar adecuadamente un derecho indubitado, objeto propio del recurso enderezado, sino de obtener la declaración de un derecho, tanto así que lo perseguido es propiamente una indemnización de perjuicios, lo que exorbita absolutamente el ámbito de aplicación del recurso de protección, motivo más que suficiente para su rechazo.

Regístrese, comuníquese para los efectos del numeral 14 del aludido Auto Acordado, y archívese, en su oportunidad.

Redacción del ministro Hadolff Gabriel Ascencio Molina.

N° Protección 8120-2020.

Hadolff Gabriel Ascencio Molina
MINISTRO
Fecha: 24/06/2020 12:25:19

Rodrigo Alberto Cerda San Martin
Ministro
Fecha: 24/06/2020 11:57:56

Hugo Fernando Tapia Elorza
Abogado
Fecha: 24/06/2020 13:12:10

Pronunciado por la Sexta Sala de la Corte de Apelaciones de Concepción, integrada por los ministros titulares Hadolff Gabriel Ascencio Molina, Rodrigo Alberto Cerda San Martín y el abogado integrante Hugo Fernando Tapia Elorza. Concepción, veinticuatro de junio de dos mil veinte.

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