Santiago, diez de julio de dos mil veintiséis.

Vistos:

En estos autos Rol Corte Suprema N° 51.579-2024, se ha conocido el recurso de queja deducido por el abogado Rodrigo Lezana Toledo, en contra de los integrantes de la Décima Tercera Sala de la Corte de Apelaciones de Santiago, Ministros señor Carlos Farías Pino, señora Carolina Vásquez Acevedo y señor Patricio Martínez Benavides, por las faltas o abusos graves en que han incurrido al dictar la sentencia de segundo grado, de fecha treinta de septiembre de dos mil veinticuatro, en sus autos Rol 1.308-2022, por la que se revocó el fallo dictado en los autos Rol N° 28.181-2020 del Primer Juzgado de Policía Local de Ñuñoa, caratulados “Lezana con Banco Scotiabank”, que acogió parcialmente la querella y demanda civil intentada por infracción a la Ley de Protección al Consumidor, disponiendo, en su lugar, el rechazo de dichas pretensiones.

Solicita, se acoja el recurso de queja, se deje sin efecto la sentencia recurrida y, en su reemplazo, se confirme el fallo apelado que condenó al Banco Scotiabank al pago de una multa de 25 Unidades Tributarias Mensuales y, en lo civil, al pago de $17.389.624 por concepto de daño emergente, con declaración de que se condene además a la demandada a pagar al actor la suma de $15.000.000 (quince millones de pesos) por concepto de daño moral, más reajustes y costas.

Informando los jueces recurridos al tenor del recurso, refirieron que la resolución dictada por la Corte de Apelaciones cumple con su obligación de fundamentar adecuadamente su decisión, expresando, sucintamente, los motivos de hecho y de derecho, y los antecedentes en que se sustenta la sentencia revocatoria.

Encontrándose en estado, se trajeron los autos en relación.

Considerando:

Primero: Que el quejoso en su libelo recursivo, refiere que los recurridos, con falta grave y abuso, revocaron la sentencia de primera instancia dictada por el Primer Juzgado de Policía Local de Ñuñoa, de fecha 2 de febrero de 2022, que acogía la querella y demanda de indemnización de perjuicios interpuesta en contra de Banco Scotiabank, por incumplimiento del deber de seguridad en el consumo, previsto en el artículo 23 de la Ley N° 19.496, con ocasión de las transacciones fraudulentas realizadas por terceros, en su cuenta corriente y tarjeta de crédito, el día 19 de marzo de 2020, quienes vulneraron las medidas de seguridad informática dispuestas por el Banco, provocando que el Sr. Lezana fuese víctima de un fraude de $17.389.624.

Las faltas graves y abuso se verificaron con ocasión de una falsa apreciación de los antecedentes del proceso, atendido a que se acreditó en autos que el Banco no desplegó las medidas de seguridad que le exige la ley y se contravino formalmente la ley, por cuanto la magistratura soslayó que el Banco Scotiabank omitió el deber de detectar patrones de fraude y monitoreo de operaciones que no respondan a las habituales del usuario, de conformidad a lo establecido en el artículo 6 letra a) de la Ley N°21.234 y Circular N°3.444 de la Superintendencia de Bancos e Instituciones Financieras (actual CMF).

Explica que en el mes de septiembre de 2019, el Sr. Lezana abrió una cuenta corriente y productos asociados en Banco Scotiabank. Entre esa fecha y el 19 de marzo de 2020, la actividad de la cuenta fue un abono asociado a un crédito de consumo que le fue otorgado al abrir la cuenta corriente y tres transferencias de monto inferior a $300.000 cada una, todas debidamente notificadas al correo seguro registrado.

Sin embargo, continúa, el 19 de marzo de 2020 recibió un correo electrónico proveniente de la casilla *“comprobantes.info@scotiabank.cl”*, con logo y tipografía institucional del Banco, solicitando *"sincronizar el dispositivo de seguridad"*, por lo que actuando de buena fe, ingresó al enlace. Al día siguiente, al no poder acceder a la plataforma, contactó al servicio de atención

telefónica del Banco, generó una nueva clave y constató que se habían efectuado cuatro transacciones no autorizadas por más de $17.000.000. La primera de ellas consistió en un traspaso de fondos desde su tarjeta de crédito a la cuenta corriente, por $3.712.619, que abultó artificialmente el saldo disponible y, seguidamente, tres transferencias correspondientes a pagos efectuados a la Tesorería General de la República y al Servicio de Impuestos Internos, por concepto de pago de impuestos asociados al número 126441290, correspondiente a una empresa sin vínculo alguno con el actor, por un total de $17.389.624.

Asegura que las referidas operaciones dan cuenta de un patrón de fraude, por cuanto en un espacio temporal acotado, fueron realizadas cuatro operaciones de alto monto, frente a un histórico de operaciones menores y, por tanto, no habituales del cliente. Por otra parte, según el propio informe forense realizado por el Banco Scotiabank, se comprobó que el acceso a la plataforma fue desde dos direcciones IP distintas, ninguna asociada al cliente; se desinstaló la aplicación KeyPass del dispositivo registrado y se reinstaló en otro celular no registrado con anterioridad.

En opinión del quejoso, de la secuencia de hechos antes reseñada se desprende que el Banco Scotiabank no notificó al correo seguro que el cliente tenía registrado, como tampoco a través del envío de mensajería a su teléfono, la desinstalación de KeyPass del dispositivo registrado, la reinstalación de KeyPass en un dispositivo nuevo, el código o coordenadas de validación que el propio protocolo del Banco exige. Tampoco informó el traspaso de fondos desde la tarjeta de crédito a la cuenta corriente, ni las tres transferencias fraudulentamente efectuadas. Las omisiones incurridas por la entidad bancaria, conducen a concluir que el cliente no pudo haberlas recibido y, por tanto, tampoco pudo entregarlas a terceros, pues no las recibió.

Precisa que el Primer Juzgado de Policía Local de Ñuñoa, por sentencia de 2 de febrero de 2022, acogió la querella infraccional, tras estimar

comprobada la infracción del deber de seguridad que le asiste a la institución denunciada, condenando al Banco a una multa y a la restitución de $17.389.624. Sin embargo, rechazó el daño moral y no concedió a reajustes ni intereses.

Apelada esa determinación por ambas partes, los jueces recurridos la revocaron, absolviendo al Banco Scotiabank, por considerar, en lo medular, que la defraudación no se produjo por insuficiencia de las medidas de seguridad del Banco, sino *"por el actuar del denunciante",* y que la entidad acreditó haber prestado información suficiente y clara mediante publicaciones y contenido en su plataforma web sobre prevención de fraudes.

El quejoso asegura que la sentencia de segundo grado descansa en una errónea ponderación de la prueba, al haber omitido consideraciones esenciales, como son, el patrón anómalo de operaciones, que por sí solo activaba el deber de monitoreo y alerta; y que el Banco no acreditó haber notificado al correo seguro del cuentacorrentista, la desinstalación/reinstalación de KeyPass, ni el envío de las claves de validación. De contrario, el Banco sólo acompañó el informe de servicios forenses digitales y las publicaciones generales preventivas realizadas en su web, material probatorio que resulta insuficiente para acreditar el cumplimiento del deber de seguridad y dejan en evidencia el conocimiento del Banco sobre los patrones de fraude, lo que agrava su responsabilidad, invirtiendo con ello la carga probatoria.

Por su parte, el quejoso denuncia la contravención formal de la ley a los artículos 3 letra d) y 23 de la Ley N° 19.496 sobre Protección de los Derechos de los Consumidores, que prevé el deber de seguridad en el consumo y responsabilidad del proveedor por fallas en la calidad del servicio; al artículo 12 A del mismo cuerpo de normas, en cuanto establece la obligación de enviar confirmación escrita al consumidor de los contratos celebrados por medios electrónicos, lo que no ocurrió respecto del traspaso de fondos desde la tarjeta de crédito a su cuenta corriente. Además, se denuncia la trasgresión a la

Circular N° 3.444 de la Superintendencia de Bancos (hoy CMF), sobre detección de patrones de fraude y al artículo 6 letra a) de la Ley N° 21.234, referido al deber de las entidades financieras de contar con sistemas de monitoreo que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual del usuario. Además, se trasgrede el artículo 6 inciso segundo de la Ley N° 20.009, que establece para los emisores u operadores deberes específicos de seguridad y artículo 1547 del Código Civil.

Solicita se acoja el recurso de queja, enmendando en todas sus partes la sentencia de segunda instancia y, en su lugar, se confirme la sentencia dictada por el Primer Juzgado de Policía Local de Ñuñoa, con declaración de que se acoja, además, la indemnización por daño moral, condenando a la demandada a pagar por tal concepto la suma de quince millones de pesos, además de los reajustes, intereses y costas, imponiendo las sanciones disciplinarias que correspondan.

Segundo: Que, en cumplimiento de lo ordenado por esta Corte, los jueces recurridos informaron que efectivamente con fecha treinta de septiembre de dos mil veinticuatro, en los autos Rol Corte de Apelaciones N°1.308-2022, revocaron la sentencia apelada, dictada por el Primer Juzgado de Policía Local de Ñuñoa, en los autos Rol 28.181-2020, por estimar que el banco denunciado no incurrió en las infracciones que se le atribuyeron, conforme a los fundamentos que se contienen en la sentencia impugnada, que dicen relación con el derecho aplicable a los hechos establecidos, conforme la ponderación realizada del material probatorio, sin que ello signifique haber incurrido en falta o abuso grave, como lo sostiene el quejoso, tratándose más bien de una mera discrepancia interpretativa de los hechos y el derecho, por lo que solicitan su rechazo.

Tercero: Que el recurso de queja está regulado en el Título XVI del Código Orgánico de Tribunales, denominado “De la jurisdicción disciplinaria y

de la inspección y vigilancia de los servicios judiciales", y su párrafo primero, intitulado de "Las facultades disciplinarias", contiene el artículo 545 que lo consagra como un medio de impugnación que tiene por exclusiva finalidad corregir las faltas o abusos graves cometidos en la dictación de sentencias definitivas e interlocutorias que ponga fin al juicio o hagan imposible su continuación, que no sean susceptibles de recurso alguno, ordinario o extraordinario.

Cuarto: Que, para un adecuado escrutinio de las objeciones planteadas en el recurso en examen, es preciso tener presente que, según se desprende de las piezas principales del proceso en el que incide, no resultó controvertido entre las partes o fueron hechos que se han tenido por acreditados por la judicatura del fondo, según se desprende del basamento tercero de la sentencia de primer grado, que los jueces recurridos tienen por reproducido, los siguientes:

1. Entre las partes existe un contrato de cuenta corriente bancaria, cuya apertura data de septiembre de 2019, registrándose como abono únicamente el préstamo otorgado ese año al quejoso y el realizado el 19 de marzo de 2020, que se ha tachado por las partes como fraudulento, ascendente a la suma de $3.712.619, que corresponde a un traspaso de fondos desde la tarjeta de crédito a la cuenta corriente del actor.

2. El miércoles 18 de marzo de 2020, a las 23:55 horas, el cuentacorrentista Sr. Rodrigo Lezana Toledo, recibió un correo electrónico de comprobantes.info@scotiabank.cl, que en el asunto se indica "Sujeto a bloqueo si no sincroniza su dispositivo", con el logo característico de la entidad bancaria y en el que se informa:

"Estimado cliente:

Le informamos que nuestros sistemas han detectado un inconveniente con su dispositivo de seguridad, por lo que se requiere sincronizarlo de manera inmediata. Este procedimiento solo será solicitado por única vez, ya que

garantiza la protección de sus datos y no será necesario solicitarla nuevamente.

Estado de Dispositivo – No Sincronizado

Sincronizar Dispositivo

Recuerde que solo tiene 48 horas después de recibir este email para realizar dicho proceso, de lo contrario su cuenta será bloqueada y tendrá que acercarse a la sucursal más cercana para solicitar una nueva tarjeta.

Has recibido este correo porque figura como E-mail de tu cuenta Scotiabank. Para modificarlo contáctate con tu ejecutiva o visita una de nuestras sucursales. Infórmese sobre la garantía estatal de los depósitos en su banco o en www.cmfchie.cl 2020 Scotiabank.com Todos los derechos reservados" (SIC).

3. El jueves 19 de marzo de 2020, desde la cuenta corriente del actor, que contaba con mayor disponibilidad de fondos producto de los obtenidos desde su tarjeta de crédito, se efectuaron tres transacciones, consistentes en pagos de impuestos a la Tesorería General de la República y al Servicio de Impuestos Internos, por la suma total de $17.389.624, asociados a los Rut 76.757.057-0, 76.828.866-6 y 76.064.647-4.

4. Las transacciones descritas obedecerían a un fraude informático, en que terceros, usando un correo electrónico fraudulento, habrían suplantado al Banco proveedor para sustraer las claves del cuentacorrentista y, engañando al banco, suplantan al cliente desde otra ubicación IP, sin que ese fraude haya sido procesado a tiempo por el Banco proveedor. De esa forma, terceros accedieron a los productos bancarios del cliente, obtuvieron fondos desde la tarjeta de crédito del actor, traspasan ese dinero a su cuenta corriente y, finalmente, extrajeron la mayor parte del saldo contable de la cuenta, pagando los impuestos adeudados por terceros, beneficiando a personas jurídicas no asociadas con el actor.

5. El Banco Scotiabank no comunicó al actor la ocurrencia de las transacciones antes reseñadas. Tampoco acreditó que activó la alerta de operación fraudulente, ni que ésta haya sido comunicada al cuentacorrentista.

Quinto: Que, en consideración a esos hechos, la judicatura de segundo grado, en el considerando 4°, estimó: *"Que en tales condiciones, es posible tener por establecido, que el actor fue víctima del actuar de terceros, que obtuvieron del propio denunciante las claves necesarias para operar su cuenta corriente, por medio de la técnica denominada "phishing", al simular un correo electrónico como proveniente de la entidad bancaria, y de ese modo, obtener los códigos e implementos necesarios para operar electrónicamente sobre los productos financieros del actor."* (SIC).

Luego, en el considerando 5°, agrega: *"…no es posible atribuirle responsabilidad al banco demandado, pues conforme la manera que se verificó el acto fraudulento denunciado, según fue establecido, no consta que el banco haya incumplido las normas antes referidas, por cuando la defraudación sufrida por el denunciante, no se produjo por una insuficiencia de las medidas de seguridad del demandado, o por vulneración de sus sistemas de seguridad, sino por el actuar del denunciante, lo que a juicio de esta Corte, sobrepasa la esfera de cuidado que debió otorgar el banco; en efecto, con la prueba rendida en autos, es posible tener por demostrado que la demandada prestó información suficiente y clara, advirtiendo a sus clientes de esta manera de realizar defraudaciones. Así fluye de las copias de publicaciones realizadas en dicho sentido, y de la información que aloja en su plataforma web."*

Finalmente, en el considerando 6° de la misma sentencia, concluye: *"Que, de esta forma, no es posible atribuirle responsabilidad al banco denunciado, en la defraudación de que fue objeto el actor, puesto que con los medios probatorios mencionados, su actividad de cuidado debida, se encuentra acreditada, por lo que corresponde absolver a la denunciada de la*

acusación de vulneración de lo preceptuado en los artículos 3 d) y 23 de la Ley N°19.496." (SIC).

Sexto: Que, como es sabido, el contrato de cuenta corriente bancaria constituye una especie de depósito respecto de un bien eminentemente fungible, de manera que es de cargo del depositario el riesgo de pérdida de la cosa depositada durante la vigencia de la convención. Asimismo, resulta relevante analizar si los eventos que originaron el otorgamiento de un crédito y las transferencias cuestionadas han tenido como única causa, el actuar del cuentacorrentista o si, por el contrario, existen antecedentes que demuestren la ocurrencia de hechos que permitan asentar un incumplimiento de las obligaciones de resguardo y seguridad que recaen en la institución bancaria respectiva, al no adoptar las medidas de resguardo para detectar e impedir los fraudes cibernéticos.

Séptimo: Que, en este orden de consideraciones, se debe tener presente que la variedad de las formas en las que se vulneran los sistemas de seguridad y la dificultad probatoria inmediata, obligan a la judicatura, en acciones como las planteadas, a realizar un juicio sobre indicios acerca de la ocurrencia de los hechos y confrontarlos con las 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, actual Comisión para el Mercado Financiero, que complementa la normatica aplicable al caso, al tratarse de un mercado altamente regulado, 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.".

El objetivo de la normativa legal y administrativa, vigente a la fecha de ocurrencia de los hechos, estriba en que se implemente un sistema que maximice la eficiencia en la prevención de fraudes en las transferencias electrónicas bancarias. Para dichos efectos, pone a cargo de quién esté en mejores condiciones, en términos de contar con recursos tecnológicos, la obligación de seguridad informática de la custodia del patrimonio ajeno. Frente a la sofisticación de los sistemas informáticos es la parte más fuerte y no la más débil, a la que se impone un deber primario en su cumplimiento y de alto estándar para la detección de los comportamientos fraudulentos, antes de que se verifiquen los desplazamientos patrimoniales, lo que se concreta en cierta clase de acciones que primero debe cumplir la entidad bancaria por deber administrativo, precaviendo inclusive cierta torpeza derivada de la falta de comprensión del uso de los sistemas informáticos y de transferencias electrónicos, por la gran masa de usuarios del sistema financiero. Entonces, en tiempo previo a la denuncia de fraude al banco por parte del contratante, la entidad financiera ya se encuentra vinculada jurídicamente a la obligación administrativa, en consonancia con la obligación de seguridad del artículo 3 letra d) de la Ley del Consumidor.

Además, en este sentido, la carga de la prueba del cumplimiento de sus obligaciones legales y administrativas recae, según el art. 1698 del Código Civil, en quien beneficia el cumplimiento, por lo que es la parte demandada la que deberá acreditar la apropiada actuación de cumplimiento de la obligación administrativa. Por contrapartida, la eximición de responsabilidad, como

excepción que interfiere con dicho resultado, se asigna a factores de imputación del titular de los productos financieros.

Octavo: Que es importante señalar que la entidad crediticia denunciada no controvirtió que efectivamente el banco tiene el dispositivo denominado “Keypass”, que permite realizar transferencias y pagos de manera remota, sin necesidad de utilizar su tarjeta de coordenadas. Por su parte, no consta en estos antecedentes, que la institución financiera haya enviado al actor un correo electrónico en que informe cada una de las transacciones realizadas, objeto de la controversia, debiendo hacerlo.

Lo anterior reviste la máxima relevancia, toda vez que la sentencia impugnada reprocha al actor haber entregado su clave de seguridad a terceros; sin embargo, el actor no señaló aquello, por el contrario, refirió que el banco envió un correo electrónico el día 18 de marzo de 2020, requiriéndole sincronizar el dispositivo de seguridad, lo que realizó.

Pues bien, en este punto del análisis, la sentencia de segundo grado, sustenta su decisión en que el actor no habría cumplido su deber de custodia y cuidado de las claves y datos para acceder a los productos bancarios, en que el ahora quejoso habría *“entregado sus datos”,* permitiendo que terceros accedieran a sus productos financieros. Empero, tal circunstancia se opone a lo reconocido por el propio Banco Scotiabank y, en todo caso, no implica aceptar que el dinero o actividades bancarias del actor queden desprotegidos, menos aún que el banco se libere del cumplimiento de la obligación de seguridad en relación a la custodia de los dineros que se depositan en la cuenta corriente.

Así, si a través de un proceso fraudulento vinculado con el mecanismo de seguridad Keypass, terceros obtuvieron la clave secreta del actor (ScotiaWeb) y el código que arroja el Keypass, incumbe exclusivamente al banco recurrido la obligación de adoptar todos los resguardos que sean necesarios para impedirlo, comunicando oportunamente al cuentacorrentista

las transacciones realizadas, alertando las operaciones sospechosas que no se ajusten a las transacciones habituales del cuentacorrentista, sin que haya acompañado al proceso antecedente alguno que permita concluir que cumplió con aquello.

Noveno: Que, asentado lo anterior, se debe precisar que, en el caso de autos, es posible avizorar que el banco fue objeto de dos fraudes. El primero se relaciona con una transferencia desde la tarjeta de crédito del cuentacorrentista, vía web, realizada el jueves 19 de marzo de 2020, circunstancia que por sí sola es sospechosa, operación que no fue comunicada al cliente. Lo anterior lleva a la estimación jurídica, que si el banco recurrido tiene por práctica comercial entregar este tipo de créditos de manera remota, a cualquier hora del día, debe asumir los riesgos que aquello entraña, debiendo destacar que no acompañó antecedente alguno al proceso que permita respaldar la circunstancia de haber requerido el actor el otorgamiento del referido crédito que supone la operación, elemento de juicio que los sentenciadores del fondo debieron ponderar y que pasaron completamente por alto.

Ahora bien, depositados en la cuenta corriente del quejoso los fondos correspondientes al referido crédito, el Banco Scotiabank no negó que, en un breve espacio de tiempo se realizaron tres operaciones que implicaron cargos en la cuenta corriente del quejoso y, con ello, la disposición de casi la totalidad del saldo contable del cuentacorrentista, por $11.480.043, $3.356.561 y $2.553.020, desde un número de IP no habitual del cliente. Es evidente, que tal situación, por el estándar de seguridad del banco, debió activar las alertas de seguridad de aquél, máxime si estas operaciones tuvieron características de que se realizaban sin claves de la tarjeta de coordenadas, de forma remota, se trataron de transacciones no habituales del cliente, a lo que se suma que todo ello ocurrió sin que se haya enviado las comunicaciones de seguridad de cada una de ellas al correo electrónico registrado por el cliente.

Cabe destacar que la entidad bancaria tampoco acompañó antecedente probatorio de la investigación realizada en relación con el caso, más allá del informe que contiene su dictamen, limitándose a sostener que existió una negligencia del cliente, sin demostrar que adoptó efectivamente todos los resguardos que, en su calidad de institución bancaria, estaba obligada a activar.

Décimo: Que, aún más, desde la perspectiva del modo global involucrado, las cuestionadas operaciones corresponden a tres pagos por una suma que en total supera los diecisiete millones de pesos, lo que fue tenido por válido por el Banco, bajo las circunstancias mencionadas. Todo ello deja en evidencia su pasividad en el cumplimiento de su deber de seguridad, soslayando el deber de cuidado en la prestación de sus servicios financieros, infracción que se relaciona causalmente con las tres transacciones realizadas, en un breve plazo, desde la cuenta corriente del quejoso.

Undécimo: Que, en las condiciones descritas, el banco recurrido no pudo excusarse de hacerse cargo del menoscabo patrimonial generado al quejoso, dado que no acreditó, estando en posición de hacerlo, que el siniestro ocurrió por el aprovechamiento de las debilidades del resguardo de la información antes evidenciadas, como tampoco acreditó que en el espacio de ejecución de tales transacciones, adoptó todas las providencias que permitieran establecer que las mismas respondían a un patrón de conducta de su cliente al tratarse de transacciones regulares, ni, finalmente, que ello habría sucedido exclusivamente con ocasión de un descuido grave del cuentacorrentista capaz de superar las solvaguardas bancarias exigibles.

En este contexto, se debe reiterar y enfatizar que las obligaciones de monitoreo y control de fraudes jurídicamente recaen, de manera expresa, en la entidad bancaria, donde los patrones de conducta del cliente son elementos de juicio para la determinación de una operación engañosa, cuestión que, como se señaló, no fue informada en detalle por el Banco Scotiabank.

Duodécimo: Que las consideraciones antes anotadas no fueron advertidas por los jueces del fondo, quienes desatendiendo el mérito de los hechos del proceso asentados en la propia sentencia recurrida y los no discutidos por las partes, descartaron la responsabilidad infraccional denunciada respecto del Banco Scotiabank, por incumplimiento al deber de seguridad en el consumo, establecido en el artículo 3 literal d) de la Ley N°19.496, limitando el análisis a la supuesta entrega de los mecanismos de seguridad a terceros que el quejoso realizó, con la que aquellos accedieron en forma fraudulenta a sus productos bancarios, pero omitieron examinar la conducta desplegada por la entidad bancaria, en quien recae el deber de resguardo de los fondos depositados, el de contar con las herramientas informáticas idóneas para pesquisar operaciones sospechosas y quien, en definitiva, otorgó un crédito en forma digital y permitió la realización de tres pagos electrónicos por más de diecisiete millones de pesos, pese a que se trata de operaciones no habituales para el cliente, realizadas desde un número de IP no utilizado por éste y sin alertar su ocurrencia a través de mensajería o correos electrónicos que el cuentacorrentista tenía registrados; configurándose de esa manera la falta o el abuso grave denunciados en el recurso de queja, puesto que con ello se ha impuesto al quejoso asumir el perjuicio económico, trasladando los efectos del fraude bancario a éste, desatendiendo las obligaciones de resguardo que pesan sobre las entidades financieras, y particularmente el artículo 3 letra d) de la Ley 19.496, afectando directamente el patrimonio del recurrente.

Décimo Tercero: Que en consecuencia, se hará lugar al recurso de queja deducido contra los Ministros de la Corte de Apelaciones de Santiago, invalidando la sentencia impugnada y dictando en su reemplazo una que confirme la de primer grado, que condenó a la denunciada conforme a lo previsto en los artículos 3 letra d) y 24 de la Ley N° 19.496, al pago de una

multa a beneficio fiscal de 25 Unidades Tributarias Mensuales, por estimar que ella resulta proporcional a la infracción constatada.

Décimo Cuarto: Que, además, se confirmará la sentencia dictada por el Primer Juzgado de Policía Local de Ñuñoa, en cuanto hizo lugar parcialmente a la demanda civil deducida por el quejoso, condenándose a Banco Scotiabank a pagar al actor, por concepto de daño emergente, la suma de $17.389.624, que corresponde al monto transferido desde su cuenta corriente, el día 19 de marzo de 2020, debidamente reajustada conforme a la variación que experimente el índice de precios al consumidor desde la fecha de los hechos hasta su efectivo pago, más los intereses que el actor pagó al Banco con ocasión de la transferencia fraudulentamente realizada desde su tarjeta de crédito.

Décimo Quinto: Que, en cuanto al daño moral demandado, atendidos los elementos de juicios ponderados en el basamento 17° de la sentencia dictada por el tribunal de primer grado, que esta Corte comparte, se confirmará su rechazo.

Décimo Sexto: Que no se condenará en costas al Banco demandado, por no haber sido totalmente vencido.

Por estas consideraciones y conforme lo dispone el artículo 549 del Código Orgánico de Tribunales, **SE ACOGE** el recurso de queja deducido en contra de los integrantes de la Corte de Apelaciones de Santiago, Ministros señor Carlos Farías Pino, señora Carolina Vásquez Acevedo y señor Patricio Martínez Benavides, por haber dictado con falta o abuso la sentencia de treinta de septiembre de dos mil veinticuatro y, en consecuencia, se la deja sin efecto y se decide, conforme lo previamente razonado, que **SE CONFIRMA** la sentencia apelada de dos de febrero de dos mil veintidós, dictada en los autos Rol 28.181-2020-RB del Primer Juzgado de Policía Local de Ñuñoa, sin costas.

No se dispone la remisión de estos antecedentes al Pleno de este Tribunal, por tratarse de un asunto en que la inobservancia constatada no

puede ser estimada como una falta o abuso que amerite disponer una medida de carácter disciplinario.

Acordado con el voto en contra del Ministro Sr. Valderrama, quien estuvo por rechazar el recurso de queja impetrado, en virtud de las siguientes consideraciones:

1°) Que, como cuestión previa, conviene tener en cuenta que el recurso de queja, en tanto persigue modificar, enmendar o invalidar resoluciones judiciales pronunciadas con falta o abuso, constituye un medio extraordinario destinado a corregir la arbitrariedad judicial, mediante la imposición de medidas disciplinarias a los recurridos ante la existencia de un perjuicio que afecte al recurrente, manifestado en un error grave y notorio de hecho o de derecho.

2°) Que, como evidencia una atenta lectura del recurso intentado, en éste se cuestionan las conclusiones que alcanzan los jueces recurridos, al exonerar de responsabilidad al banco querellado en la defraudación que afecto al actor, tras haber ingresado a un link fraudulento que le fue entregado a través de un correo electrónico, actuar que permitió que terceros capturaran sus datos y claves, con las que se efectuaron las transacciones, todos elementos de juicio que no han sido controvertidos entre las partes. En consecuencia, resulta inconcuso que el actuar del consumidor del servicio financiero y el engaño del que fue víctima, es el hecho que permitió que terceros se apoderaran de los fondos que existían en su cuenta corriente, sin que las omisiones en que pudo incurrir el Banco denunciado, en la comunicación de las operaciones y alertas, aparezcan como determinantes en la producción del daño causado, pues no existen elementos de juicio de los que se pueda inferir que de haber dado cumplimiento a tales deberes de información, los efectos de la defraudación no se habrían producido.

3°) Que, en tal entendimiento, la decisión de los recurridos, contrastada con las argumentaciones de la quejosa, claramente representa una legítima diferencia en la determinación de sí los hechos establecidos en el fallo

configuran las infracciones denunciadas por el consumidor, diferencia interpretativa que no llega a constituir una falta o abuso grave que amerite la interposición de un recurso de la naturaleza de que se trata, según constante jurisprudencia de esta Corte.

Es más, lo cierto es que los sentenciadores, ajustándose a los planteamientos esgrimidos por los intervinientes en torno a las infracciones de los artículos 3 inciso primero, letra d) y 24 de la Ley 19.496 calificaron los hechos del proceso, interpretando y dando aplicación a las disposiciones legales atingentes a la materia, de manera tal, que como ha sostenido reiteradamente este Tribunal, el no compartir la parte reclamante una determinada posición frente al sentido o alcance de una norma jurídica, no puede constituir falta o abuso grave que amerite la imposición de sanciones por la vía disciplinaria, pues se trata de la aplicación del derecho a los hechos sentados, actuación propia de la labor jurisdiccional.

Regístrese y agréguese copia autorizada de esta resolución al proceso Rol N° 1308-2022 de la Corte de Apelaciones de Santiago y Rol N° 28.181-2020, seguido ante el Primer Juzgado de Policía Local de Ñuñoa. Hecho, archívese.

Rol N° 51.579-2024

Pronunciado por la Segunda Sala de esta Corte Suprema integrada por los Ministros Sr. Manuel Antonio Valderrama R., Sras. María Teresa Letelier R. María Cristina Gajardo H., y los Abogados Integrantes Sres. Juan Carlos Ferrada B., y Eduardo Gandulfo R. No firma la Ministra Sra. Letelier y el Abogado Integrante Sr. Ferrada, no obstante haber estado en la vista de la causa y acuerdo del fallo, por haber cesado de sus funciones y por estar ausente, respectivamente.

MANUEL ANTONIO VALDERRAMA REBOLLEDO
MINISTRO
Fecha: 10/07/2026 14:17:08

MARIA CRISTINA GAJARDO HARBOE
MINISTRA
Fecha: 10/07/2026 14:17:09

EDUARDO NELSON GANDULFO RAMIREZ
ABOGADO INTEGRANTE
Fecha: 10/07/2026 14:17:09

En Santiago, a diez de julio de dos mil veintiséis, se incluyó en el Estado Diario la resolución precedente.