Providencia, a veintiséis de septiembre de dos mil veinticuatro.

VISTOS:

La querella interpuesta en lo principal de la presentación de fojas 6 y siguientes, por el abogado Maximiliano Andrés Fuentes Cid, con domicilio en Valentín Letelier 16, Santiago, en representación de [redacted] domiciliada en [redacted] Providencia, en contra de **BANCO ITAU CORPBANCA S.A.**, Rut N°97.023.000-9, representado legalmente por su gerente general [redacted] ambos domiciliados en Av. Presidente Riesco 5537, Las Condes, por infracción a los artículos 3° letras b) y d), 12 y 23 de la Ley 19.496, sobre Protección de los Derechos de los Consumidores.

Fundamenta la querella exponiendo que su representada es clienta del Banco Itaú, sin perjuicio que también es clienta del Banco Security, con quien realiza la mayoría de sus transacciones, únicamente utiliza su cuenta del Banco Itaú por mantener un crédito hipotecario, sin registrar mayores movimientos de dinero con dicha entidad. Con fecha 30 de mayo de 2023, a las 13:22 horas ella se encontraba en su lugar de trabajo, ubicado en calle [redacted] Providencia, con dirección IP [redacted] lugar donde recibe una llamada telefónica de una persona que se identifica como ejecutivo del área de fraudes del Banco Itaú, de nombre [redacted] quien, tras la investigación en curso de la Fiscalía, hoy se sabe que era [redacted] (imputado/delincuente), que cuenta con otra causa por uso fraudulento de tarjeta de crédito o medio de pago. Esta persona le comenta que estaban intentando realizar una compra por internet que parecía sospechosa, la clienta responde que ella no estaba realizando ninguna compra, por lo que el supuesto ejecutivo le dice que no se preocupe, que procederían a realizar el bloqueo de sus productos durante 48 horas; para ello, debe validar algunos datos, menciona su nombre completo, Rut, dirección y correos electrónicos, tanto personal como laboral, la clienta sólo debía señalar si éstos eran correctos o erróneos. Todo era correcto, es decir, el delincuente contaba con información comercial, personal y sensible con respecto a la consumidora, información que se encuentra bajo el resguardo del Banco Itaú. Posterior a ello, el supuesto ejecutivo procede a leer los últimos movimientos bancarios, consultándole si desconocía alguna transacción, lo que

no era el caso, puesto que todas eran compras realizadas por ella. Es decir, el supuesto ejecutivo tenía acceso a toda la información de su cuenta corriente. Después, durante la conversación le señala que iba a necesitar un medio de verificación, por política del banco no podía entregar sus claves, sino que las claves de coordenadas debían ser digitadas en su teléfono, las que él le iba señalando; ante la urgencia de solucionar un eventual fraude, accede a digitar las claves de coordenadas en su teléfono celular. Tras lo anterior, se le señala que se contactarían con ella para hacer entrega de los nuevos plásticos; es decir, tal era el nivel de sofisticación que los delincuentes se preocuparon de todos los detalles para que la consumidora creyera que estaba siendo atendida realmente por un ejecutivo del banco.

El día 1° de junio de 2023, dos días después del llamado del falso ejecutivo, se comunica con ella su ejecutivo de cuentas, [redacted] señalándole que había un movimiento sospechoso en su cuenta, siendo un avance en efectivo por $3.230.500.-, el cual fue bloqueado por el banco al haber sido detectado como sospechoso. En ese momento se da cuenta que había sido defraudada por el antisocial que se hizo pasar por ejecutivo del Banco Itaú. Pero, [redacted] comete el error grave de no comentarle que el día anterior, 31 de mayo, el delincuente había realizado una transferencia de $1.248.- a su cuenta, para luego, esa misma mañana, 1° de junio, el delincuente había realizado una segunda transferencia por $4.750.000.- a su cuenta del Banco Falabella, además de haber solicitado el avance o abono en su cuenta corriente por el monto de $3.230.500.-, sólo éste último fue catalogado por el Banco como movimiento sospechoso e informado a la clienta. Recién, cuando [redacted] llama al Banco para dar aviso y desconocer esas transacciones, pudo tomar conocimiento del movimiento millonario, pues en ningún momento le llegaron SMS por parte del Banco, avisando de las transacciones.

El ejecutivo le comenta a doña [redacted] que se trataba de transferencias entre sus cuentas, lo que no tiene sentido, pues ella no tiene cuenta en el Banco Falabella, sólo aparece su nombre de pila y otro Rut. Agrega que la demandante nunca ha realizado transferencias millonarias en dicha cuenta.

Posteriormente, realizó la correspondiente denuncia ante la PDI y un reclamo en el SERNAC. También, denuncia vulneración a los datos personales, de conformidad a la Ley 19.628, ante la CMF.

Agrega que, la consumidora no hacía uso de la aplicación ITAUPASS, y sólo ingresaba al Banco desde su hogar o su trabajo, operando siempre con su tarjeta de coordenadas, la cual en ningún momento fue apartada de su esfera de control, o expuesta a terceros. Así se confirma de la IP utilizada por los delincuentes. Destaca que el Banco solicita clave alfanumérica, la que es imposible digitar mediante teclado con llamada telefónica simultánea, recalca que ésta nunca fue entregada a los delincuentes.

Con fecha 12 de junio de 2023, el Banco da respuesta al desconocimiento de los movimientos bancarios, señalando que no se observan patrones de fraude, y que, por el contrario, se advierte el ingreso de forma correcta y sin errores en las claves secretas y demás credenciales de seguridad requeridas, las que son de conocimiento exclusivo de los clientes.

El 15 de junio se hace entrega de una nueva tarjeta de coordenadas, donde le vuelven a asegurar que todo se encuentra bien; pero, al día siguiente intenta ingresar a su cuenta y no le solicita su tarjeta de coordenadas, sino el Itaú Pass, es decir, esta aplicación seguía abierta en el dispositivo del delincuente, no había sido bloqueada por el Banco. Preocupada y nerviosa de volver a ser víctima de fraude, se contacta con su ejecutivo de cuenta, pero no recibe respuesta, por lo que llama a la unidad de atención del cliente, atiende [redacted] con quien procede a bloquear la aplicación, le dan un número de reclamo; hasta el día de hoy no recibe respuesta de aquello.

Alega que el Banco permitió que terceros no sólo accedieran a sus datos personales, sino que, además, a 16 días de haber ocurrido la estafa la aplicación seguía abierta en un dispositivo que no era de la clienta, ya que se había ingresado otro número telefónico, en circunstancia que el número del cual es titular hace años figuraba en el mismo Banco. Impidiendo que la clienta recibiera los SMS de alerta. Es decir, el mismo sistema del Banco jugó en contra de la seguridad de las operaciones, al permitir, sin medios de verificación de segundo paso, como la tarjeta de coordenadas, el que se cambiara el número telefónico asociado a su cuenta del Banco.

Por otra parte, el Banco no observó patrones de fraude, lo hace de forma tardía, no alertó de los otros movimientos completamente extraños y no habituales de transferencias millonarias a una cuenta nueva. Recalca que el Banco comete un imperdonable error en su investigación, pues la clienta nunca ha utilizado la aplicación Itaú Pass, la cual fue utilizada por primera vez por los delincuentes para cometer fraude. Por otro lado, las IP desde donde se realizaron las operaciones que se desconocen no corresponden a las IP usuales de la consumidora, las operaciones fueron realizadas desde un lugar del sector sur de Santiago.

La demanda de indemnización de perjuicios deducida en el primer otrosí de fojas 6 y siguientes, por el abogado Maximiliano Fuentes Cid, en representación de [redacted] en contra de **BANCO ITAU CORPBANCA S.A.**, todos ya individualizados, por los mismos hechos antes expuestos, los que da por reproducidos. Señala que fue víctima de una estafa sumamente sofisticada, no recibió el respaldo ni la protección de parte del Banco, quienes han profundizado su vulneración, tanto de sus datos personales como de su patrimonio, e incluso su estabilidad emocional, ya que, de forma negligente mantuvieron abierta la aplicación pese a la denuncia, además de proceder a demandarla en calidad de victimaria.

Se vio privada de gran parte de su dinero, sumado al deber impuesto de pagar un crédito que nunca solicitó, con los intereses que conlleva, ha debido recurrir a profesionales, tanto legales [redacted] Debió endeudarse con su hermana, quien retiró anticipadamente un depósito a plazo a fin de prestárselo para pre-pagar el crédito de manera que no generara más intereses, además de poder hacer frente a sus gastos habituales, por lo que recibió $4.850.000.-, con los cuales junto a la primera cuota de $330.451.- pudo pagar el crédito que el delincuente solicitó a su nombre por medio de las plataformas digitales del Banco, más intereses e impuestos; en definitiva, los $3.230.500.- solicitados como avance en la tarjeta de crédito generó un daño efectivo de $3.463.860.-, a lo que se debe sumar los $4.750.000.- sustraídos por los antisociales, menos el abono obligatorio de las 35 Unidades de Fomento que realizó el Banco. Por último, ha debido desembolsar importantes sumas de dinero para un [redacted] el cual al momento de presentar

la demanda asciende a $550.000.- por concepto de [redacted] sin perjuicio que de seguir avanzando el [redacted] dicho monto seguirá aumentando. En efecto, el daño patrimonial directo a la fecha asciende a la suma de $8.888.145.-, correspondiente al mutuo conseguido con su hermana para afrontar los gastos del mes y del crédito contratado por los delincuentes, y las transferencias a sus cuentas que el mismo delincuente realizó, junto con el valor de las [redacted]

En cuanto al daño moral, además de haber sido víctima de fraude, ha sido demandada por el mismo Banco, en vez de querellarse en contra del verdadero responsable, por lo que estima que el daño extra-patrimonial sufrido asciende a la suma de $4.500.000.-.

La audiencia de contestación y prueba se llevó a efecto en rebeldía de la parte de Banco Itaú Corpbanca, según consta del acta que rola a fojas 151 y siguiente.

La prueba documental y testimonial rendidas en la audiencia.

Según petición de la querellante y demandante de autos, se tiene a la vista la causa Rol N°37.762-4-2023 de este mismo tribunal.

A fojas 159 y siguientes, las abogadas María Fernanda González Tobar y Catalina Unda Rodríguez, en representación de Banco Itaú Chile S.A. asumen el patrocinio y poder en la causa.

CONSIDERANDO Y TENIENDO PRESENTE:

En materia infraccional:

1.- Que, como se ha visto, la parte de[redacted] se querella en contra de Banco Itaú por haber incurrido en infracción a los artículos 3°, 12 y 23 de la Ley 19.496, atendido que se realizaron 2 transferencias electrónicas de fondos a una cuenta desconocida del Banco Falabella, y se efectuó un avance en efectivo de su tarjeta de crédito, todas operaciones realizadas sin su autorización. Alega que cómo una persona ajena puede manejar su información bancaria confidencial; registrar en su celular la aplicación del Banco y enrolar el dispositivo de seguridad Itaú Pass, lo que permitió que se ejecutaran las operaciones que ella desconoce frente al Banco. Señala que se utilizó una IP desconocida y la Itaú Pass, en circunstancias que ella siempre se conectaba a través de dos IP conocidas, las de su casa y lugar de trabajo, además de utilizar

siempre una tarjeta de coordenadas para realizar sus operaciones bancarias. El Banco activa las alertas en forma tardía, cuando se realiza el avance en efectivo.

2.- Que, en orden a acreditar los fundamentos de su querella, acompaña los siguientes documentos: carpeta investigativa que lleva la Fiscalía de Ñuñoa, con la denuncia realizada ante la PDI, el día 2 de junio de 2023, por uso fraudulento de tarjetas o medios de pago, y la posterior investigación penal (fojas 56 a 92); cartas dirigidas a la clienta con la respuesta dada por el Banco (fojas 93 a 95); correo electrónico del ejecutivo de cuentas (fojas 96); correo electrónico de fecha 16/06/2023, enviado al ejecutivo donde consta que la clienta no puede entrar a su cuenta porque se le pide el Itaú Pass (fojas 97); correo electrónico de fojas 99; consulta de transferencias realizadas en la cuenta de [redacted] (fojas 101 a 103); registro de IP e información del dispositivo iPhone (fojas 107 y 109 a 112); informe de prepagos (fojas 144); y estados de cuenta nacional de la tarjeta de crédito (fojas 145 a 150).

3.- Que, por su parte, el Banco Itaú no rindió prueba alguna en la causa.

4.- Que, analizados los diversos antecedentes de autos, en especial el informe emitido por el propio banco querellado, consta que las operaciones desconocidas se realizaron desde IP no habituales y fueron autorizadas a través de la Itaú Pass en circunstancia que la clienta operaba exclusivamente con la tarjeta de coordenadas; es decir, el Banco permitió que se enrolara el dispositivo de seguridad en un teléfono celular desconocido, lo que posibilitó que terceros operaran en la cuenta corriente y tarjeta de crédito de la querellante.

5.- Que, por otra parte, también consta de los antecedentes, que luego de haber realizado [redacted] el correspondiente reclamo frente al banco, días después, seguía operativo el Itaú Pass en un teléfono celular que no era de la clienta.

6.- Que la Superintendencia de Bancos e Instituciones Financieras, hoy Comisión para el Mercado Financiero, ha puntualizado en sus respectivas circulares, que los bancos están obligados a garantizar la seguridad de las transacciones y transferencias electrónicas de dinero. Asimismo, deben asegurar que las operaciones de que se trata sólo puedan ser realizadas por personas autorizadas para ello, debiendo recabar todas las validaciones previas que sean necesarias para resguardar la operación, manteniendo sistemas y

procedimientos que les posibiliten identificar, evaluar, monitorear y detectar 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, 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 compromiso, entre otros.

7.- Que la Ley 20.009, modificada por la Ley 21.234, que establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude, dispone que en los casos en que el usuario desconozca haber autorizado una operación, corresponderá al emisor probar que dicha operación fue autorizada por el usuario y que se encuentra registrada a su nombre. El solo registro de las operaciones no bastará, necesariamente, para demostrar que ésta fue autorizada por el usuario, ni que el usuario actuó con culpa o descuido que le sean imputables. (artículo 4°)

8.- Que, atendido lo antes expuesto, a juicio de este Tribunal, queda de manifiesto que el Banco Itaú infringió lo dispuesto en los artículos 3° letra d) y 23 de la Ley 19.496, ya que no cumplió con su deber de prestar el servicio con seguridad, al que se obligó con la consumidora en virtud del contrato celebrado entre ambas partes, no operaron los resguardos o mecanismos de control que el banco debía implementar, a fin de poder detectar vulneraciones a la seguridad de sus sistemas, tomando en consideración además, de que se trataba de una conducta inusual por la naturaleza de las operaciones cuestionadas y su monto, lo que hacen responsable al banco al permitir el uso malicioso o fraudulento de sus productos financieros por parte de terceros ajenos, causando menoscabo a la consumidora por fallas de seguridad en el servicio prestado.

En materia civil:

9.- Que la conducta infraccional imputada en el considerando precedente a Banco Itaú Chile S.A., en cuanto ocasionó perjuicios a terceros, da origen a una

indemnización regulada según lo previsto en el artículo 3º letra e) de la Ley 19.496, sobre Protección de los Derechos de los Consumidores.

10.- Que, se ha tenido a la vista el proceso Rol N°37.762-2023, seguido entre las mismas partes, por infracción a la Ley 20.009, cuya sentencia definitiva fue dictada con fecha 7 de junio del año en curso, que resolvió rechazar la demanda declarativa de existencia de dolo o culpa grave del artículo 5 de la Ley 20.009, y se ordena al Banco Itaú restituir a [redacted] a suma de $3.489.393.-, saldo retenido, debidamente reajustado aplicando la tasa de interés máximo convencional, con costas. Esta sentencia fue apelada por el Banco y se encuentra actualmente en tramitación en la Corte de Apelaciones de Santiago, bajo el Rol 2967/2024.

11.- Que, atendido lo antes expuesto este tribunal ya ordenó la devolución de los dineros que fueron defraudados, descontando las 35 Unidades de Fomento que la consumidora reconoce haber recibido.

12.- Que, en cuanto al avance en dinero de la tarjeta de crédito a la cuenta corriente, este dinero no salió de la esfera de control de la consumidora, por lo que no corresponde su indemnización.

13.- Que, en cuanto al daño moral, resulta evidente que la afectación económica que sufrió la consumidora por la indisponibilidad financiera y alteración a sus productos bancarios, le produjo natural molestia, dolor, preocupación y angustia, con [redacted] que constituye lo propio del daño moral, más si se considera que tuvo que afrontar una demanda del banco lo que puso en tela de juicio su honradez, por lo que se regulará de modo prudencial una indemnización de conformidad con las reglas de la sana crítica.

Y atendido lo dispuesto en los artículos 1 y 13 de la Ley 15.231, Orgánica de los Juzgados de Policía Local; artículos 14, 17 y 23 de la Ley 18.287 de Procedimiento ante los mismos; artículos 3°, 12, 23, 24 y 27 de la Ley 19.496, sobre Protección de los Derechos de los Consumidores; y Ley 20.009 que establece un Régimen de Limitación de Responsabilidad para Titulares o Usuarios de tarjetas de Pago y Transacciones Electrónicas en caso de Extravío, Hurto, Robo o Fraude.

SE DECLARA:

A. Que se hace lugar a la querella interpuesta en lo principal de la presentación de fojas 6 y siguientes, y se condena a **BANCO ITAU CHILE S.A.**, antes individualizado, a pagar una multa de 5 U.T.M. (Cinco Unidades Tributarias Mensuales) por haber incurrido en infracción a los artículos 3° letra d) y 23 de la Ley 19.496, sobre Protección de los Derechos de los Consumidores.

B. Que se acoge la demanda de indemnización de perjuicios deducida en el primer otrosí de fojas 6 y siguientes, po[redacted] en contra de **BANCO ITAU CHILE S.A.**, ya individualizados, sólo en cuanto se condena a ésta última a pagar a la demandante la suma de $550.000.- (Quinientos cincuenta mil pesos) por concepto de daño moral. Sin costas.

ANÓTESE Y NOTIFÍQUESE

ROL N°94.926-7-2023

Dictado por la Juez Subrogante, **María Isabel Brandi Walsen**

Secretaria Subrogante, **Silvana Costa Moreno**.