C.A. de Rancagua

Rancagua, diecisiete de marzo de dos mil veinticinco.

Vistos:

Se reproduce la sentencia en alzada.

Y se tiene, además, presente:

1.- Que, la parte querellante y demandante civil dedujo recurso de apelación en contra de la sentencia de primer grado, en cuanto rechazó la querella y demanda civil, absolviendo a Angélica Iturrieta Cereceda, por no existir antecedentes suficientes que acrediten la existencia de dolo o culpa grave de su parte.

2.- Que, para la adecuada decisión del presente arbitrio, cabe precisar que las acciones ejercidas en autos por la institución bancaria en contra de la clienta Iturrieta Cereceda corresponden a las previstas en los incisos 2° y 3° del artículo 5 de la 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.

3.- Que, en particular, el Banco persigue que la clienta restituya las 35 UF que debió pagarle con motivo de la reclamación de cargos no reconocidos, efectuada por la Sra. Iturrieta Cereceda, respecto de transacciones efectuadas entre el 11 de marzo al 23 de junio del año 2022, respecto de operaciones de pago efectuadas vía on line, para pagar juegos y apuestas en línea, por un total de $2.302.237, por estimar que aquella actuó con dolo o al menos con culpa grave en tales transacciones, por cuanto se efectuaron a través de los accesos y claves secretas de la demandada, las que de alguna manera habría facilitado a terceros que burlaron los fondos desde su cuenta RUT y chequera electrónica.

4.- Que, al efecto, cabe tener presente que el inciso 3° del artículo 5 de la Ley 20.009, dispone que: "*Si en el plazo anterior, el emisor recopilare antecedentes que acrediten la existencia de dolo o culpa grave por parte del usuario, podrá ejercer ante el juez de policía*

local todas las acciones que emanan de esta ley, siendo competente aquel que corresponda a la comuna del domicilio del usuario".

5.- Que, del contenido de dicha norma resulta patente que es el Banco quien debe probar que las transacciones cuestionadas se deben exclusivamente a dolo o culpa grave del usuario, carga probatoria que no ha sido cumplida en la especie.

En efecto, el informe técnico recabado en la investigación interna del Banco, acompañado como documento al juicio a fojas 34 y siguientes, no resulta bastante para dicho fin, por cuanto no permite asentar la tesis de que las operaciones cuestionadas se concretaron únicamente por el actuar negligente de la clienta, desde que la institución bancaria no logró probar que cumpliera con todas las medidas de seguridad implementadas para mitigar fraudes informáticos.

6.- Que, en efecto, 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.".

En el mismo sentido, cabe recordar que el artículo 6 de la Ley 20.009, dispone: *"Los emisores, operadores, comercios y otros establecimientos afiliados a un sistema de tarjetas de pago, así como las demás entidades que intervengan o presten servicios asociados a pagos y transacciones electrónicas, u otros sistemas de características similares, incluyendo los proveedores de servicios de iniciación de pagos, deberán adoptar las medidas de seguridad necesarias para prevenir la comisión de los ilícitos descritos en esta ley y el resguardo de la privacidad de los datos de los titulares o usuarios de medios de pago conforme a la legislación y normativa que les resulte aplicable, y velarán por la prestación segura del respectivo servicio en los términos señalados por el artículo 23 de la ley N°19.496.*

En el caso de los emisores u operadores, según corresponda, dichas medidas de seguridad deberán considerar, al menos, lo siguiente: a) Contar con sistemas de monitoreo que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual del usuario; b) Implementar procedimientos internos para gestionar las alertas generadas por dichos sistemas de monitoreo; c) Identificar patrones de potenciales fraudes, conforme a las prácticas de la industria y recomendaciones, los que deberán incorporarse al sistema de monitoreo de operaciones; d) Establecer límites y controles en los diversos canales de atención que permitan mitigar las pérdidas por fraude. Los referidos límites y controles deberán basarse en consideraciones de riesgo objetivas, generales y no discriminatorias, en relación con la naturaleza del medio de pago y la clase de operaciones que permita efectuar".

7.- Que, de la norma recién transcrita, se colige que las medidas de seguridad que los Bancos deben adoptar para evitar y en su caso mitigar los fraudes bancarios, no se limitan a entregar a los clientes claves secretas de transferencias y a efectuar campañas informativas

sobre potenciales fraudes, sino que involucran otras obligaciones, como monitorear y alertar operaciones que no corresponden al comportamiento habitual del usuario, además de establecer límites y controles en los diversos canales de atención que permitan mitigar las pérdidas por fraude.

8.- Que, en el presente caso, a pesar de que en el propio informe técnico que hace valer la parte apelante, se indica que dentro de las medidas de seguridad de la APP, se encuentran la gestión de alerta de monitoreo, los límites de primera transferencia, límites de inscripción de nuevos destinatarios, así como la inscripción de pagos de servicios, consignándose expresamente que: "*no se podrá realizar movimientos de fondos que superen el límite diario establecido*", como también la existencia de notificaciones al correo del cliente y límites y control de montos en las transacciones, la institución bancaria no logró acreditar que tales medidas se cumplieran en autos, existiendo, en cambio, antecedentes que dan cuenta que las mismas no fueron aplicadas o bien que fueron derechamente vulneradas.

En efecto, es del caso que precisar que las operaciones desconocidas por la clienta y que corresponden a pagos de juegos y apuestas en aplicaciones por la suma de $2.302.237, efectuados mediante Google Play store, entre los días 11 d marzo a 23 de junio del año 2022, cargos que no corresponden a operaciones habituales de la usuaria, tal como se aprecia de las cartolas de la chequera electrónica y cuenta Rut de los meses previos, acompañadas por ambas partes y que rolan a fojas 60 y siguientes, en la que no se aprecian pagos a través de dicho medio ni por tales montos. Tampoco se demostró por parte del Banco que se enviaran a la usuaria las notificaciones de tales transferencias ni que se activara alerta alguna antes del llamado telefónico de la clienta.

A ello, se agrega que la institución bancaria tampoco se hizo cargo de la alegación de la clienta relativa a no encontrarse activadas las tarjetas que contienen las coordenadas necesarias para efectuar

transacciones en línea desde las cuentas de la clienta, circunstancia que fue considerada por el juez a quo al momento de resolver.

9.- Que, sobre lo dicho, resulta ilustrativo lo sostenido por los autores Munita y Aedo, al decir: *"¿le es imputable al banco la ineficacia del sistema de transferencias seguras? Pensamos que sí, aunque nuestra postura no debe ser entendida, como hemos dicho, como reflejo de una responsabilidad sin culpa o estricta u objetiva. Fundamos nuestra opinión tanto en el derecho común como en la jurisprudencia. Una rápida lectura al art. 1547 del CC nos advierte que la culpa en el cumplimiento de las obligaciones, a saber, en este caso, la de seguridad y vigilancia, es posible presumirla. De tal manera que es al banco a quien le cabe demostrar su diligencia. Por lo demás, en relación con el art. 1546 del CC, es posible considerar que es la buena fe la que habilita al cliente a exigir un riguroso cumplimiento de la obligación de seguridad que pesa sobre la entidad bancaria, idea que ya presentamos"* (Renzo Munita Marambio y Cristian Aedo Barrena. Responsabilidad civil de los Bancos por fraudes informáticos, en Revista Actualidad Jurídica N°42 - Julio 2020, Universidad del Desarrollo, pág. 89).

10.- Que, en este sentido, si bien el Banco demandado ha pretendido exonerarse de su responsabilidad, alegando que las operaciones bancarias cuestionadas se llevaron a cabo con las claves y medidas de seguridad entregadas a la cliente, quien habría obrado de manera descuidada en el resguardo de ellas, lo cierto es que el fraude de que fue víctima la usuaria pudo ser mitigado por el Banco si hubiesen operado las demás medidas de seguridad disponibles y, en particular, el límite de transferencia a nuevos destinatarios impuesto como medida de seguridad, sin que el demandado haya rendido prueba alguna para demostrar que la ineficacia de dichas medidas no le es atribuible.

11.- Que, en conclusión, no es posible enfocar el infortunio del cliente en el pretendido manejo descuidado de sus claves o contraseñas,

pues de lo obrado en autos resulta patente que el Banco también contribuyó al daño provocado por el fraude, escenario en el que no puede pretender la restitución de las 35 UF enteradas de conformidad al artículo 5 inciso 2°, siendo imperativo ordenar, además, la obligación del emisor de restituir al usuario el saldo retenido, debidamente reajustado, aplicando para ello la tasa de interés máxima convencional calculada desde la fecha del aviso, por lo que no cabe más que confirmar el fallo apelado, con declaración en dicho sentido.

Por estas consideraciones y de conformidad con lo dispuesto, además, en los artículos 14 y 32 y siguientes de la Ley 18.287, **se confirma**, en lo apelado, la sentencia definitiva dictada el cuatro de julio de dos mil veintitrés, en la causa Rol 1909-2022, escrita de fojas 194 a 206 de autos del Juzgado de Policía Local de Graneros, **con declaración** de que se ordena al Banco recurrente, restituir a la usuaria el saldo retenido, debidamente reajustado, aplicando para ello la tasa de interés máxima convencional calculada desde la fecha del aviso.

Regístrese, comuníquese y devuélvase.

Rol I. Corte 53-2024-Policía Local

Se deja constancia que esta sentencia no reúne los presupuestos del Acta 44-2022 de la Excma. Corte Suprema para ser anonimizada.

Michel Anthony González Carvajal
Ministro
Corte de Apelaciones
Diecisiete de marzo de dos mil veinticinco
11:52 UTC-3

Álvaro Javier Martínez Alarcón
Fiscal
Corte de Apelaciones
Diecisiete de marzo de dos mil veinticinco
11:53 UTC-3

Claudia Andrea Álvarez Sepúlveda
Abogado
Corte de Apelaciones
Diecisiete de marzo de dos mil veinticinco
12:04 UTC-3

Pronunciado por la Primera Sala de la C.A. de Rancagua integrada por Ministro Michel Anthony Gonzalez C., Fiscal Judicial Alvaro Javier Martinez A. y Abogado Integrante Claudia Alvarez S. Rancagua, diecisiete de marzo de dos mil veinticinco.

En Rancagua, a diecisiete de marzo de dos mil veinticinco, notifiqué en Secretaría por el Estado Diario la resolución precedente.