Poder Judicial

MERES, BERNARDO C/ NUEVO BANCO DE SANTA FE S.A. S/ DAÑOS Y PERJUICIOS

21-12639238-6

Juzg. 1ra. Inst. Civil y Comercial 18va. Nom.

ROSARIO, 05 de Octubre de 2023

Nº Rosario,

**Y VISTOS**: Los presentes autos caratulados **"MERES BERNARDO C/ NUEVO BANCO DE SANTA FE SA S/ DAÑOS Y PERJUCIOS" CUIJ.21-12639238-6** de trámite por ante este Juzgado de Primera Instancia de Distrito en lo Civil y Comercial de la 18° Nominación de Rosario, venidos a despacho para el dictado de definitiva.

A fs. 8, en fecha 20 de diciembre de 2021, el Dr. Ezequiel Pinilla, en su carácter de apoderado de BERNARDO MERES DNI N°36.987.547, inicia demanda contra NUEVO BANCO DE SANTA FE CUIT N°30-69243266-1, estimando el monto de la pretensión resarcitoria en la suma de $229.000.-, con más intereses y costas.

Manifiesta que en fecha 12 de julio de 2021, a las 18:31hs, su mandante procede a enviar un mensaje a la cuenta de Instagram del Banco de Santa Fe Oficial a los fines de realizar una consulta por el pago de un producto que se había devengado repetidamente. Que recibe una respuesta de un supuesto representante del banco que le solicitó el número celular para evacuar la consulta y que minutos después recibe una llamada vía Whatsapp donde la supuesta representante le solicita datos de la cuenta bancaria. Que su mandante al advertir que se trataba de una representante del banco, procedió a otorgar dichos datos. Y que posteriormente siendo las 19:30hs, recibe un mail de RED LINK donde se encontraba adjunto un comprobante de una transferencia hecha desde su homebanking hacia una cuenta desconocida por la suma total de $129.000.- que en ese momento era la totalidad de los fondos que poseía la cuenta.

Explica que ante ello, ingresa al homebanking, y que se encuentra con su

cuenta bancaria en cero y con todos sus datos personales vulnerados y modificados. Detalla luego los intentos de cancelación de la transferencia y los reclamos y denuncias realizadas al respecto. Destaca que al día siguiente solicita un turno presencial en el Banco en la cual es atendido por un representante que no le brinda la ayuda correspondiente para bloquear su cuenta y restituir sus datos. Resume los trámite que debió realizar para que finalmente el gerente del banco se disponga a hacer lo que debía.

Expresa luego que el actor fue informado por correo de los métodos de estafa que estaban sucediendo, sosteniendo que el banco pudo prevenir al Sr. Meres de la estada sufrida y no lo hizo sino después de que dicha estafa se produjo en una clara negligencia del deber de información y seguridad al cual el banco está obligado.

Seguidamente refiere a la legitimación activa y la aplicación del régimen de defensa del consumidor. A la atribución de responsabilidad civil, deber de seguridad, comunicaciones del BCRA. Cita también jurisprudencia a los fines de avalar su postura.

Detalla los daño reclamados, el daño emergente estableciendolo en la suma de $129.000.- y el daño punitivo en la suma de $100.000.-

Por último ofrece la prueba de la que habrá de valerse y reserva derechos.

A fs. 24, en fecha 30 de marzo de 2022, se dicta el primer decreto de trámite ordinario (art. 398 CPCC).

A fs. 33, en fecha 19 de mayo de 2022, comparece el Dr. Juan Esteban Cantón, en su carácter de apoderado del NUEVO BANCO DE SANTA FE SA.

A fs. 37, en fecha 27 de julio de 2022, se corre traslado de la demanda.

A fs. 69, en fecha 8 de septiembre de 2022, el Dr. Cantón contesta la demanda negando todos y cada uno de los hechos, documental y el derecho argüido por la parte actora que no sea objeto de reconocimiento expreso.

Explica que su mandante dio debida respuesta a todos y cada uno de los reclamos realizados por el actor y sostiene la inexistencia de presupuestos de responsabilidad.

Seguidamente brinda su versión de los hechos manifestando que el actor es

cliente de su mandante. Refiere a los productos contratados por el mismo, afirmando que operó y opera los mismos con absoluta normalidad, conforme acreditan los resúmenes de cuenta. Entiende que la operación realizada el día 12 de julio de 2021 también fue parte de la operatoria normal realizada por el actor, detallando la misma y aclarando los factores de autenticación que requiere la operatoria. Repasa asimismo las medidas de seguridad. También refiere a las modalidades DEBIN.

Explica que conforme lo convenido contractualmente de ninguna manera se puede operar desde los cajeros automáticos ni homebanking y solicitar y realizar los productos y operaciones realizadas sin su tarjeta de débito y su clave personal. Concluye que las operaciones son genuinas. También refiere a cláusulas contractuales particulares. Y demás detalles de la operación.

Sostiene que de la sola lectura de la demanda deriva la incongruencia y lo desajustado a derecho del reclamo. Cita jurisprudencia y normativa a los fines de avalar su postura.

Por último ofrece la prueba de la que habrá de valerse.

En fecha 8 de septiembre de 2022 se abre la causa a prueba (fs. 97), fijándose audiencia de proveído de prueba en el marco del Plan Piloto de Oralidad en los Procesos Civiles, impulsado por la Corte Suprema de la Provincia de Santa Fe, el Ministerio de Justicia y Derechos Humanos de la Provincia de Santa Fe y el Ministerio de Justicia y Derechos Humanos de la Nación, protocolo de actuación recomendado por Acuerdo Ordinario - Acta 48/2017 de fecha 5 de diciembre de 2017 de la Excma. Suprema Corte de la Provincia de Santa Fe.

A fs. 101, en fecha 23 de septiembre de 2022, ofrece prueba la demandada. A fs. 106, en fecha 12 de octubre de 2022, la actora ratifica su prueba.

A fs. 108, en fecha 12 de octubre de 2022, se toma audiencia de proveído de pruebas en el marco del protocolo referido, fijándose audiencia de producción de prueba.

A fs. 149, en fecha 28 de febrero de 2023 se toma audiencia de producción de prueba. En la misma se fija audiencia complementaria.

A fs. 157, en fecha 27 de marzo de 2023, se agrega pericial.

A fs. 200, en fecha 4 de abril de 2023, se toma audiencia complementaria de producción de pruebas. En la misma se presentan las partes y el perito ingenierio en sistemas de información, quien contesta aclaraciones efectuadas. Se produce asimismo confesional y absolución de posiciones.

A fs. 201, en fecha 24 de abril de 2023, se clausura el periodo probatorio y pasan los autos por su orden para alegar.

A fs. 203, en fecha 26 de abril de 2023, se agrega alegato de la parte actora. Y a fs. 207, en fecha 22 de mayo de 2023, acompaña alegato la parte demandada.

A fs. 208, en fecha 22 de mayo de 2023, se dicta el llamamiento de autos para sentencia, el cual se notifica a fs. 209-210.

A fs. 216, en fecha 23 de junio de 2023, se agrega dictamen de la Sra. Agente Fiscal.

Cumplimentados los requisitos formales y no constando escritos sueltos para agregar según informe, quedan los presentes en estado de resolver.

**Y CONSIDERANDO**: Que conforme lo normado por el art. 243 CPCC, “los hechos constitutivos de la litis son los que proceden jurídicamente de la demanda y su contestación y de las peticiones formuladas en ella”. Por consiguiente, corresponde analizar los hechos invocados, las constancias de autos y el derecho aplicable en la especie. (C.C.C. de Santa Fe, sala 1ra., Zeus, Tomo 12, p.R-33).

Que la cuestión litigiosa queda integrada con la contestación de la demanda. "El esquema temático de cuestiones jurídicas propuesto por el actor al promover la demanda, que en definitiva serán objeto litigioso y constituirán el thema decidendum, se completa con la contestación de la demanda, porque sobre las admisiones y negaciones del demandado se determina cuales serán los hechos controvertidos ("cuestión litigiosa") y la forma en que se distribuirá la carga de la prueba." ("La demanda y la defensa en el proceso

civil", Víctor De Santo Bs.As., edit. Universitaria, l981, p.459).

Que es entonces que de los escritos constitutivos del proceso ha quedado reconocido en autos: 1) Que el actor es cliente del Nuevo Banco de Santa Fe S.A.- 2) Que el mismo ha operado con normalidad tanto de manera presencial como a través del homebanking los productos que posee contratados con la entidad bancaria.- 3) Que el día 12/07/21 se realizó un débito en la Caja de Ahorro Nro. 076071064104 de titularidad del actor por la suma de $. 129.000.- y se procedió a modificar los datos personales del actor – tel. de contacto y mail – de su homebanking.

Que resulta controvertido al presente: 1) Si dicho débito fue realizado por el propio actor o producto de un supuesto de pishing.- 2) En el segundo caso, si existe responsabiidad achacable a la entidad bancaria demandada.- 3) De ser afirmativa la respuesta a dicho interrogante, es menester analizar si resultan procedentes los rubros y montos reclamados.-

Que en primer lugar, resulta necesario recordar que el tribunal interviniente no tiene la obligación de analizar y resolver las cuestiones planteadas por los justiciables en base a la totalidad de argumentos, consideraciones y elementos que los mismos aporten a la causa, bastando a tal fin se pondere los relevantes a los fines de dirimir el thema decidendum. En este sentido, se ha señalado que “los jueces no están obligados a considerar una por una todas las pruebas de la causa, sino sólo aquellas que estimen conducentes para fundar sus conclusiones, como tampoco están constreñidos a tratar minuciosamente todas las cuestiones expuestas por las partes ni analizar los argumentos que a su juicio no posean relevancia. La exigencia constitucional de que los fallos judiciales sean motivados, sólo requiere una fundamentación suficiente, no una fundamentación óptima por lo exhaustiva” (CCyC de Rosario, sala 3, 29/7/2010, “Piancatelli c/ Ryan deGrant”, www.legaldoc.com.ar.)

Como marco téorico previo al análisis de las probanzas arrimadas a esta causa es preciso señalar que el vínculo jurídico habido entre el actor y el banco

demandado es una relación de consumo (art. 3 ley 24.240; art. 1384, 1093 del Cód. Civ. y Comercial) lo que obliga a ponderar las constancias de esta causa con una mirada protectora de los derechos (arts. 42, 72, inc. 23 de la CN, 38 de la Const. Pcial., 1, 2, 36, 65 y cctes. de la Ley 24.240) con especial atención al régimen tuitivo expresamente establecido en las normas de los arts. 5, 6 y 53 de la ley 24.240 y 1106, 1107 sigs. y conc. del CCCN.

Que por su parte el Banco Central de la República Argentina, en su carácter de regulador del funcionamiento de los bancos comerciales, en los términos del artículo 21 de la Ley N° 21.526, y como consecuencia de la numerosísima reiteración de hechos como los que motivan la presente, ha emitido diversas comunicaciones mediante las cuales, entre otras cuestiones, se enumeran las obligaciones de las entidades bancarias en miras a garantizar la efectiva protección de los intereses económicos de los usuarios en operaciones de servicios financieros.

Así, con fecha 15 de noviembre de 2019, el Ente regulador dispuso un Texto Ordenado de los “Requisitos Mínimos de Gestión, Implementación y Control de los riesgos relacionados con Tecnología Informática, Sistemas de Información y Recursos Asociados para las Entidades Financieras”, en el cual destaca en su artículo 6.3.2.1, que las “Las entidades deben desarrollar, planificar y ejecutar un plan de protección de sus activos, procesos, recursos técnicos y humanos relacionados con los Canales Electrónicos bajo su responsabilidad, basado en un análisis de riesgo de actualización periódica mínima anual, en su correspondencia con la Matriz de Escenarios y en los requisitos técnico operativos detallados en los puntos 6.7. y subsiguientes ”, enumerando seguidamente, una serie de funciones y tareas relacionadas con los procesos estratégicos de seguridad para sus Canales Electrónicos, de conformidad con lo que surge del artículo 6.3.2.2.  Ellos son, entre otros, los de “contar con un programa de concientización y capacitación de seguridad informática anual, medible y verificable, cuyos contenidos contemplen todas las necesidades internas y externas en el uso, conocimiento, prevención y denuncia de incidentes, escalamiento y responsabilidad de los Canales Electrónicos con los que cuentan (...) adquirir, desarrollar

y/o adecuar los mecanismos implementados para la verificación de la identidad y privilegios de los usuarios internos y externos, estableciendo una estrategia basada en la interoperabilidad del sistema financiero, la reducción de la complejidad de uso y la maximización de la protección del usuario de servicios financieros (...) garantizar un registro y trazabilidad completa de las actividades de los Canales Electrónicos en un entorno seguro para su generación, almacenamiento, transporte, custodia y recuperación" (cfme. Art. 6.3.2.2.).

En dicho contexto, la norma citada define "Concientización y Capacitación"

como "aquel proceso relacionado con la adquisición y entrega de conocimiento en prácticas de seguridad, su difusión, entrenamiento y educación, para el desarrollo de tareas preventivas, detectivas y correctivas de los incidentes de seguridad en los Canales Electrónicos"; a la vez que entiende por "Control de Acceso" al "proceso relacionado con la evaluación, desarrollo e implementación de medidas de seguridad para la protección de la identidad, mecanismos de autenticación, segregación de roles y funciones y demás características del acceso a los Canales Electrónicos " (cfme. Arts. 6.2.1. y 6.2.2., respectivamente).

Del mismo modo, la Comunicación citada, en su artículo 6.7.1., reza lo siguiente: "los contenidos del programa de concientización y capacitación deben incluir: técnicas de detección y prevención de apropiación de datos personales y de las credenciales mediante ataques de tipo 'ingeniería social', 'phishing', 'vishing' y otros de similares características".

Asimismo, es menester mencionar la Comunicación "A" Nº 6.878, de fecha 24 de enero de 2020, la cual puntualmente en el artículo 3.8.5., dispone que, "las entidades deberán prestar atención al funcionamiento de las cuentas con el propósito de evitar que puedan ser utilizadas en relación con el desarrollo de actividades ilícitas", agregando que "deberán adoptarse normas y procedimientos internos a efectos de

verificar que el movimiento que se registre en las cuentas guarde razonabilidad con las actividades declaradas por los clientes". Asimismo, destaca en reiteradas oportunidades la "implementación de mecanismos de seguridad informática que garanticen la genuinidad de las operaciones". Ello, de conformidad con los artículos 1.6.2, 1.6.3, 1.7.2, 1.7.3 y 3.4.5. de la Comunicación citada.

Por su parte, la Comunicación A Nº 7.072, de fecha 16 de julio de 2020, dispone en su art. 2.2.2.11. "Política "conozca a su cliente": recaudos especiales a tomar de manera previa a la efectivización de una transferencia, a los fines de continuar con la política de minimizar el riesgo, particularmente con respecto a las cuentas que presenten algunas de las siguientes características: • Cuentas de destino que no hayan sido previamente asociadas por el originante de la transferencia a través de cajeros automáticos, en sede de la entidad financiera o por cualquier otro mecanismo que ella considere pertinente. • Cuentas de destino que no registren una antigüedad mayor a 180 días desde su apertura. • Cuentas que no hayan registrado depósitos o extracciones en los 180 días anteriores a la fecha en que sea ordenada la transferencia inmediata. (…) En caso de no producirse la justificación del movimiento en el término previsto, la entidad receptora deberá proceder al rechazo de la transferencia (…)".

Que la Comunicación "A" 7370 de fecha 24/9/21 sobre " Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras. Adecuaciones" dispuso, con relación a las normas sobre "Sistema Nacional de Pagos– Transferencias" en su punto 5.1.2. que las entidades financieras pueden aplicar, bajo su responsabilidad, el diferimiento, rechazo o reversión de débitos y/o créditos como medidas adicionales a las medidas de seguridad que hayan adoptado de acuerdo con los perfiles de sus clientes, las características de sus cuentas, los movimientos que efectúen normalmente y otros criterios. Adicionalmente, en el punto 5.1.3. en materia de la política "conozca a su cliente" se contempla la posibilidad de tomar recaudos especiales, de manera previa a la efectivización de una transferencia, con el fin de minimizar el riesgo.

(www.bcra.gob.ar/Pdfs/PublicacionesEstadisticas/InformeproteccionpersonasusuariasSF2021.pdf)..

Que en igual sentido, más recientemente, se dictó la Comunicación A 7777 BCRA- de fecha 01/06/23 sobre “Requisitos Mínimos para la Gestión y Control de los Riesgos de la Tecnólogía y Seguridad de la Información.

Todas dichas circulares aquí referenciadas dan cuenta del interés y preocupación de esa entidad por prevenir situaciones como las que denunció el actor en autos y la obligación en cabeza de las entidades financieras de extremar las medidas de capacitación, información, prevensión, control y minimaización de riesgos y daños en el uso de medios y canales informáticos.

Cabe entonces analizar si de las probanzas aportadas a esta causa puede concluirse que la accionada cumplío con su deber de seguridad e información conforme la normativa reseñada.

De la prueba pericial informática realizada en autos y agregada a fs. 157/163 y en lo que aquí resulta relevante, se extraen las siguientes conclusiones: El perito informa que: 1) para ingresar al Homebanking se requiere usuario y contraseña. 2) Preguntado el perito a fin de que verifique si al momento de realizar el pago de un nuevo servicio, una trasnferencia a cuenta de otro bancos, el alta de una nueva cuenta para transferir, la solicitud de préstamos (estando logeado en la plataforma) el sistema solicita un código de autenticación y/o segundo factor de autenticación, y cual es el mismo. El experto responde: Se realizó una simulación de alguna operaciones y funcionalidades de las condiciones actuales del Homebanking del NBSF y se detallan a continuación las medidas de seguridad que se solicitan al momento de realizarlas:... **Pagos debin:** (operación relizada en los presentes) una vez ingresado al Hombanking (usuario/contraseña/Captcha/Avatar) se solicita código de seguridad, fecha de vencimiento de la tarjeta de débito y segundo factor (SMS o mail).

Al ser preguntado el experto si han existido cambios en los datos

incluídos en el usuario de homebanking del actor (telefono y correo electrónico) en todo el mes de Julio de 2021 y si para realizar la transferencia objeto de la demanda de autos y cualquier otra actividad realizada a dichos fines se han aplicado segundos factores de autenticación, y, en su caso, indique cúales y cómo fueron efectivizados (puntos de pericia 12 y 13 de la demandada). El perito responde: Según informa el NBSF en un archivo PDF proporcionado, el 12/07/21 el usuario modificó en el Homebanking el número de teléfono y correo electrónico, para ello cumplimentó con la validaación del segundo factor, pero del análisis del LOG proporcionado no surge claramente cual fue el segundo factor utilizado. Agrega el experto: 1) El día 12/07/21 a las 19.07 hs. se modifica el número de teléfono del celular del usuario por el número 3516426286 .- 2) El días 12/07/21 a las 19,15 hs. se modifica el mail del usuario por el mail leonsergio7933@gmail.com.3) El día 13/07/21 a las 7.55 se modificó el número del celular del usuario por el nro. 2364587732 y el mismo día a las 13,01 se modificó el mail del ususario por el de bernardmeres@gmail.com. El segundo factor fue enviado a los números de celular 3516426286 y 2364587732.

Agrega el perito que se observa modificación de dispositivo los siguientes días: El 12/07/21 a las 19.16 se modificó por un dispositivo marca Motorola – Modelo Moto g (6) se envío segundo factor al nro. 3516426286 para la autorización. El día 22/07/21 a las 17,03 se modificó a un dispositivo Samsung – Modelo SM-A505g remitiendo segundo facor al Nro. 2364587732. Aclarando nuevamente el experto que toda dicha información no surge claramente del LOG proporcionado, resultando el mismo incompleto y con información confusa (fs. 162 vta.)

Que dichas respuestas fueron materia de observaciones por parte del banco accionado a fs. 168/170, las cuales fueran evacuadas por el perito contador en oportunidad de la audiencia de producción de pruebas celebrada en autos en fecha 04 de Abril de 2023 (fs. 200), otorgándose al accionado el plazo de 10 (diez) días corridos a fin de que entregue información complementaria, lo cual el Banco no cumplimentó (ver decreto de fs. 201).

Siguiendo con el análisis del informe del perito infromático antes citado. se concluye también que las medidas de seguridad del Banco ceden si el usuario brinda datos

de su tarjeta de débito y contraseñas a terceros. Aclarando el experto que las mismas, a su criterio, resultan insuficientes, realizando un detallado y minuciosos análisis a fin de dar fundamento a su respuesta. (punto de pericia Nro. 11) .

Por último, y en lo que aquí resulta relevante, de la respuesta brindada por el perito al punto de pericia Nro 2 y 3 de la actora surge que la página de la red social Instagram con la cual se comunicó el actor a fin de obtener información sobre su reclamo, es una página validada y corresponde el Nuevo Banco de Santa Fe.

Que dicho contacto fue respondido por un BOT el cual solicitó al actor un número de contacto telefónico a fin de continuar la comunicación vía wapp (fs. 162/163).

En conclusión, ante la duplicación de un débito en la caja de ahorro del actor, de lo cual dá cuenta la propia documentación agregada a autos por la demandada (fs. 64), el accionante se comunicó vía internet con la pagina oficial del banco demandado en la red social Instagram habiendo obtenido la respuesta de un BOT el cual le solicitó el número de telefono de contacto. El actor, en el convencimiento de encontrarse en comunicación con un agente de cuentas de la demandada, le brndó su datos de tarjeta de débito y contraseña, lo cual permitió al “tercero” acceder a su hombanking, cambiar el número de telefono de contacto y el mail.

Que el banco demandado no acreditó de manera alguna cual fue el segundo factor de validación que utilizó para autorizar dichas operaciones. Pero aún más, tomando por cierto que el 2° factor se envió al Nro de celular 3516426286, conforme manifiesta el accionado, se concluye que dicha validación resulta absolutamente insuficiente. Nótese que enviando el factor de validación al nuevo número ingresado se esta remitiendo el factor de validación al propio tercero estafador. Coadyunvando así el propio banco a la realización de la operacipon fraudulenta.

Que tal maniobra sucedió en el marco de lo que los medios califican como un aumento exponencial de los delitos de este tipo lo que se refleja en el informe

de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) conforme al cual las denuncias por fraude y estafa bancaria aumentaron casi un 3.000% entre 2019 y 2020 (https://eleconomista.com.ar/2021-07-bcra-obligara-a-bancos-mas-medidas-de-seguridad/ último día de visita 14/07/2021), lo que, como ya se adelantó, ha tenido como consecuencia la decisión del BCRA de aumentar las medidas de seguridad en este tipo de operaciones.

Justamente, en torno al crecimiento del empleo de medios informáticos en la actividad bancaria, se ha señalado que "La recurrente comisión de fraudes vinculados con la prestación de servicios financieros que se valen de la informática (considérese, por ejemplo, las plataformas electrónicas de pagos, los cajeros automáticos, y los portales de home banking), así como las reiteradas fallas que aquejan a dichos mismos servicios, refleja con elocuencia el nivel considerable de exposición que acompaña a buena parte del negocio bancario actual.

"Es en base a tales circunstancias que se argumenta que el oficio bancario, en tanto y en cuanto se encuentre atravesado por sistemas informáticos, se perfila como una actividad riesgosa. Aun antes del dictado del Cód. Civ. y Comercial (...) ya se afirmaba que el sistema (software y hardware) que permite operar una red de cajeros automáticos podía ser calificado de cosa riesgosa y que en rigor esta calificación podía ser asignada, en este punto, al sistema informático que opera las transacciones remotas, sea mediante el denominado homebanking sea por el uso de cajeros automáticos (...) Habida cuenta de que el sustrato de la prestación bancaria no siempre conlleva un peligro intrínseco, opinamos que la potencialidad dañosa deriva de la mismísima informatización, conformando, por ende, una actividad riesgosa a razón de los medios empleados (...) si bien los bancos establecen y perfeccionan medidas tendientes a fortalecer la seguridad de sus servicios (...) su sola puesta en marcha no trae aparejada eximición alguna dado que, en principio, las entidades financieras continuarán siendo responsables si tales hechos lesivos no logran ser neutralizados. Sucede que, al tratarse de actividades riesgosas, únicamente podrán desentenderse comprobando causa ajena." (De Núñez, Rodrigo, "La responsabilidad objetiva en la actividad bancaria" SJA 27/06/2018, 27/06/2018, 5 - Cita Online:

AR/DOC/3012/2018).

“El deber de información para el correcto uso de los medios electrónicos para la celebración de un contrato de consumo, contemplado expresamente por el Legislador en el art. 1107 del Cód. Civ y Comercial y que recae en el proveedor, parte del supuesto de que el consumidor carece del conocimiento tecnológico que ostenta el primero y no necesariamente conoce o sabe desenvolverse en la Internet, por lo que su situación de vulnerabilidad se ve aumentada por la complejidad técnica de los sistemas y la imposibilidad que tiene de verificar todos los aspectos de la contratación en sí y del producto o servicio antes de efectuar la contratación (conf. Tambussi, C.E. en “Código Civil y Comercial de la Nación y normas complementarias. Análisis doctrinal y jurisprudencial”, Bueres A.J. (dir.), Hammurabi, Bs. As., 2018, T° 3-C, ps. 649/650; arts. 1093, 1094, 1107, 1384 y ccs. del Cód. Civ. y Comercial, seg. Ley 26.994; art. 1, 3, 37 y ccs. de la Ley 24.240 y arg. arts. 195, 232, 260 y ccs. del Cód. Proc. Civ. y Comercial; cit. por la Cámara de Apelación, Sala II, La Plata, en causa 274.696 el 06/04/2021).

En función de lo aquí expuesto, se concluye que existió responsabilidad achacable a la accionada por violación de su deber legal de seguridad e información, no habiendo el banco accionado acreditado de manera alguna la causa ajena por la cual se vería eximido de responder. Siendo menester a esta altura del análisis destrañar la procedencia de los rubros e importes reclamados.

Que el actor reclama en concepto de año patrimonial emergente la restitución de la suma de $. 129.000.- (Pesos ciento veintinueve mil) indebidamente detraída de su Caja de Ahorro. Dicho rubro corresponde sea admitido con más intereses desde el momento del débito indebido y hasta su efectivo pago.-

En lo relativo al daño puitivo pretendido por la accionante se adelanta desde ya que el mismo ha de ser rechazado.

Ello así por cuanto de la regulación que de la misma hace el estatuto del

consumidor se interpreta que ha de quedar reservada a supuestos de graves incumplimientos dolosos o al menos de notorio menosprecio al eventual perjuicio que el consumidor pudiera padecer.

Asi se afirma que para la procedencia de esta clase de sanción debe verificarse la conducta gravemente reprochable del demandado, de modo que no basta un mero incumplimiento para que resulte procedente la sanción, sino que debe tratarse de una conducta particularmente grave caracterizada por la presencia de dolo o grave negligencia.

Existe consenso mayoritario en que las inmdenizaciones por daño punitivo solo proceden en casos excepcionales o supuestos de particular garvedad, en los que el agente ha desplegado una conducta marcadamente reprochable signada por el dolo o la culpa grave que justifican la imposición de la condena (Stiglitz, Rubén Y Pizarro, Ramón D.en “Reformas a la ley de Defensa del Consumidor L.L. 2009-B-949; Picasso, Sebastían, Ley de defensa del Consumidor comentada y anotada, Vazques Ferreyra, R. director, Sebastían Picasso, coordinador, L.L. 2009, T.1. p.625; Ariza, A. Contratos y Responsabilidad por daños en el Derecho del Consumo, en “Reforma al Régimen de Defensa del Consumidor por ley 26,361, Ariel Ariza coordinador, Abeledo Perrot, 2008 pag.134/135, entree muchas otras.

No habiéndose acreditado en autos que la conducta de la demandada haya sido realizada maliciosamente sino más bien producto de un descuido, negligencia o de su impericia, la sanción punitiva peticionada ha de ser rechazada.

En lo que respecta a los intereses moratorios y toda vez que el art. 1747, CCC, expresa que "*El resarcimiento del daño moratorio es acumulable al del daño compensatorio o al valor de la prestación (...)*",1) la sumas indemnizatorias establecidas en esta sentencia devengarán intereses desde la mora -fecha del débito indebido - y hasta su efectivo pago por aplicación de la tasa activa capitalizada que publica el BCRA (art. 768 inc c del CCCN).

Por todo lo hasta aquí expuesto; **RESUELVO:** 1) Hacer lugar parcialmente a la demanda de autos y, consecuentemente: 1) Condenar a la demandada al pago de los

**Poder Judicial**

daños patrimoniales reclamados por la sumá de $.129.000.-(Pesos ciento veintinueve mil), en el plazo de 10 (diez) días de notificada la presente, con más los intereses fijados en los considerandos.- 2) Rechazar el rubro daño punitivo.- 3) Costas a la accionada vencida (art. 53 LDC) habiendo tenido el consumidor razones suficientes para litigar.- 4) Honorarios, una vez practicada planilla en autos.-

Insértese y hágase saber

…….. ……..……..

DRA. PATRICIA ANDREA BEADE — **Secretaria**

DRA. SUSANA SILVINA GUEILER — **Jueza**