SENTENCIA

Córdoba, catorce de marzo de dos mil veinticinco.

VISTOS:

Estos autos caratulados **"MACHADO, ANA VALERIA C/ BANCO MACRO S.A. – ORDINARIO – OTROS - EXP. N.º 5 846 679"**, de los que resulta.

1) A ff. 1/4 comparece la Sra. Ana Valeria Machado e inicia formal demanda ordinaria en contra del Banco Macro S.A., por la suma de pesos setenta y tres mil trescientos ($ 73 300), mas sus intereses y costas, incluido lo establecido en el Art. 99 inc. 5 de la Ley 9459.

Expresa, que con fecha 15/09/2012 solicitó un crédito personal por el monto de pesos treinta y ocho mil ($ 38 000) en el Banco Macro S.A., en el cual es clienta hace más de 15 años como titular de una Cuenta Corriente n.° 3 350 0940925882-3 y cotitular de otra Cuenta Corriente n.° 3 350 0940179605-3 de la Sucursal Fuerza Aérea de esta Ciudad de Córdoba. Relata, que a los fines del depósito del dinero del préstamo y el posterior pago mensual del crédito, la demandada con fecha 14/09/2014 procedió a abrirle a su nombre una nueva caja de ahorro en pesos n.° 4 350 094 700 4523 4, con el saldo del préstamo otorgado, para lo cual se le solicitó nuevamente todos sus datos personales, entre ellos su correo electrónico, al cual posteriormente se le remite un e-mail con el software malicioso. Continúa relatando, que una semana después le enviaron desde el Banco una tarjeta de débito de la cuenta, que estaba asociada a una caja de ahorro que "le abrieron por error", con un saldo de cero pesos. Indica, que por ello se comunicó con el Banco y le informaron que le iban a dar de baja la segunda caja de ahorro en virtud de que había

habido un error y en esa semana le hicieron crear una clave de cliente para operar por Macro Direct-Home banquing para lo cual le entregaron una tarjeta de coordenadas.

Continúa explicando, que el 12/10/2012 ingresó a su correo electrónico y observó que en su bandeja de entrada había recibido un mail del Banco Macro el cual le proporcionaba un enlace que al hacer un click le conducía a la página del Banco Macro, un sitio, que luego se enteró que era falso, aunque tenía la misma apariencia que el original, por lo que sostiene, que no tenía ninguna forma de darse cuenta que estaba siendo víctima de un engaño.

Relata, que habiendo entrado al sitio que le habían re direccionado, le solicitaron sus datos (D.N.I., clave y contraseña) y luego de que ella los ingresó le saltó una ventana emergente que no la dejaba continuar si no cargaba los datos de la tarjeta, la clave y todos los campos de su tarjeta de coordenadas. Indica, que acto seguido ingreso en la página todos esos datos, vió su resumen y salió del *sitio web*. Explica, que una hora después se comunicaron desde el Banco Macro el teléfono de su trabajo para consultarle si había realizado una transferencia por pesos veinte mil ($ 20 000), a lo que sorprendida le contesto que no, por lo que el agente del banco le explicó que evidentemente había sido víctima de una transferencia fraudulenta, que se trataba de un grupo de estafadores que estaba trabajando a nivel nacional. Señala, que mientras hablaba con el operador, otro empleado del Banco se comunicó con ella a su celular, para preguntarle si acababa de realizar otra transferencia de pesos dieciocho mil trescientos ($ 18 300), a lo que le explicó que no y que ya se estaba comunicando con otro compañero de la entidad, por lo que continuó con la conversación recibida en primer término, pero con gran preocupación. Detalla, que el operador le indicó que se acercara a la sucursal en la que tiene sus cuentas, en donde le explicaron que debía realizar una denuncia penal por lo ocurrido y le extendieron un comprobante del reclamo

que formalizo junto con el n.° de CBU al cual fue destinado el dinero de las transferencias, luego de que el banco hiciera esa gestión con la finalidad de rastrear los fondos.

Explica, que la estafa sufrida consistió en la transferencia de pesos veinte mil ($ 20 000) desde la Caja de Ahorro n.° 4 350 094 700 4523 4 a la Cuenta Corriente n.° 3 350 094 092 5882 3 (n.° de referencia 956383724) de la cual se realizó una transferencia interbancaria al Banco Itau de Viamonte Buenos Aires, C.B.U. n° 2590006620088593430170 y de otra transferencia interbancaria dirigida a la misma caja de ahorro por un monto de pesos dieciocho mil trescientos ($ 18 300) de la cuenta corriente n.° 3 350 0940179605 3 (n.° de referencia 198623).

Continúa señalando, que luego de realizar la denuncia policial, con gran preocupación regreso al Banco y le manifestaron verbalmente que le iban a notificar de la resolución que iba a tomar el banco en un plazo de 7 días, cuestión que no sucedió.

Relata, que ante ese panorama y al no haber obtenido respuesta satisfactoria del banco, el día 21/12/2012 le envió una carta documento a la entidad demandada emplazándola para que en el término de 10 días hábiles hiciera efectivo el reintegro de las sumas extraídas más intereses, en concepto de daño emergente por haber sufrido una estafa informática. A lo que la demandada respondió con otra misiva el 21/02/2013, en la que negaron toda responsabilidad en los hechos ocurridos.

Sostiene, que la responsabilidad del Banco es de tipo objetiva, porque es quien ha creado el riesgo de la utilización del sistema Home Banking para aumentar sus beneficios. Aduce, que en rigor, su obligación principal es la de brindar los servicios que ofrece con total seguridad para el usuario, ya sea cuando lo utiliza en forma personal, como cuando lo realiza por medios electrónicos. Además, solicita la aplicación del estatuto consumeril.

Por otra parte, aclara que no hubo culpa de la víctima, ya que la actora brindó sus datos, pero fue motivado en una necesidad de cuidar su patrimonio, sin tener ninguna herramienta para darse cuenta que estaba siendo víctima de un caso de *"phishing"* o estafa informática. Sostiene, que no hubo ninguna negligencia de su parte, y que mediante un abuso informático, los terceros lograron engañar no solo a varias personas sino también al propio sistema del banco. Señala además, que tampoco podría considerarse que hubo una eximente de responsabilidad por el hecho de un tercero porque el banco debe responder por el uso de los medios electrónicos y que este tipo de estafas ya son previsibles y de reiterada realización, por lo que deberían ser objeto de mayor atención y diligencia por parte de las entidades bancarias.

Reclama como daño emergente, la suma de pesos treinta y ocho mil trescientos ($ 38 300), por daño moral reclama la suma de pesos quince mil ($ 15 000) y por pérdida de chances reclama la suma de pesos veinte mil ($ 20 000).

Funda su pretensión en derecho y cita jurisprudencia.

2) A f. 18 se imprime trámite de juicio ordinario. A f. 19/29 comparece el demandado Banco Macro S.A. a través de su apoderado el Dr. Martín Cortes Olmedo.

3) A f. 34 vta. se corre traslado de la demanda. A ff. 35/38 contesta el traslado la demandada, pidiendo su rechazo con costas. Realiza una negativa genérica y otra específica de los hechos afirmados por la actora. Niega la existencia y validez de parte de la documental acompañada.

Sostiene, que hay una ruptura del nexo causal de responsabilidad fundada en el hecho de la víctima, porque aduce que la actora (que es una persona joven y además instruida) actuó en forma negligente, ya que la misma reconoce que suministró información confidencial en un sitio *web* fraudulento. Aclara, que son muy conocidas las políticas de

concientización del Banco al respecto, a las cuales hizo caso omiso la actora, quien no solo suministro su n.° de D.N.I, nombre de usurario, clave de acceso a *Home Banking* a los terceros, sino que además les dio voluntariamente los 81 dígitos que figuran en su tarjeta de coordenadas, sin llegar a dudar en ningún instante de que la operatoria podía tratarse de una estafa. En subsidio, postula que hay una eximente de responsabilidad por el hecho de un tercero por el que no debe responder, porque el accionar se debió a personas ajenas que estafaron a la actora, constituyendo de esta manera un caso típico de *phishing* o estafa virtual.

En cuanto a los hechos, reconoce la versión dada por la actora, acerca de que el banco se comunicó con ella para confirmar si había realizado las transferencias y explica que se trató de dos llamadas de rigor en función del sistema de seguridad del banco. Reconoce, las transferencias realizadas en la cuenta de la actora. Asimismo, reconoce que cuando la actora le manifestó a un operador que había ingresado todos sus datos en una página web por un correo recibido, inmediatamente se le manifestó que debía hacer la denuncia penal y que se le explicó que había sido víctima de una estafa digital. Explica, que inmediatamente de haber recibido el reclamo de la actora, puso en marcha todo el sistema de seguridad pertinente y realizó una investigación, que arrojó que no hubo ninguna vulneración de los sistemas del banco, por lo que se arribó a la conclusión de que todo lo que sucedió, fue responsabilidad de la actora que negligentemente proporcionó sus datos confidenciales a los terceros. Independientemente de ello, denuncia que el Banco cumplió con todas las actividades tendientes al recupero de los fondos que estipulan los protocolos, lo cual fue infructuoso.

Remarca, que no se trata de un caso de fraude al sistema informático del Banco, ni vulneración de sus sistemas de seguridad, sino de transferencias originadas por errores o

negligencia de la propia clienta, quien hizo caso omiso a las claras recomendaciones de seguridad del Banco y entregó de manera voluntaria o involuntaria sus datos bancarios.

4) A ff. 42/47 comparece la Sra. Fiscal a cargo de la Fiscalía Civil, Comercial y Laboral de Segunda Nominación. Hace presente que en el caso de autos existe una relación de consumo entre la actora y el Banco demandado, por lo que al resolver habrá de estarse a los principios rectores de la normativa consumeril.

5) A f. 48 vta. se abre a prueba la causa, obrando en autos las que fueran diligenciadas.

6) A f. 144 vta. se corre el traslado para alegar. A ff. 152/155 presentó su alegato la parte actora y a ff. 156/159 lo presentó la parte demandada.

7) A f. 160 se dictó decreto de autos y una vez cumplimentada la medida para mejor proveer dictada con fecha 08/03/2018, los presentes quedan en condiciones de ser resueltos con fecha 25/11/2024.

Y CONSIDERANDO:

I) En primer lugar, cabe determinar el marco normativo aplicable a los fines de resolver el *sub lite*. De las constancias de autos, resulta insoslayable que la demandada se encuentra emplazada dentro de la categoría de "proveedor" acorde al art. 2 de la ley 24240 y la actora engasta en la calidad de usuaria de servicios financieros (art. 1 Ley 24240), existiendo entre las partes una vinculación contractual encuadrable en una relación de consumo, en los términos del art. 3 de la Ley 24.240, en consonancia con las expresiones de la Agente Fiscal interviniente.

Por otro lado, el CCC al regular los contratos bancarios, establece en su art. 1384, que las disposiciones relativas a los contratos de consumo son aplicables a los contratos bancarios, de conformidad con lo dispuesto en el art. 1093 del citado cuerpo normativo.

Por lo expuesto, en los presentes deberá aplicarse la Ley de Defensa del Consumidor junto a todos los principios rectores y postulados que iluminan la materia.

II) Así las cosas, se comenzará a delinear la plataforma fáctica y doctrinaria del caso de marras.

En primer lugar y para lograr una ubicación conceptual del caso que nos ocupa, se recordará que la actora sostiene que ha sido víctima de una estafa virtual bajo la modalidad que se ha dado a conocer como "*phishing*".

Con la finalidad de adentrarse en el tema, cabe mencionar que en el ámbito del servicio bancario, desde hace un tiempo se ha instaurado la utilización de entornos digitales, de manera tal que el uso de la tecnología en los productos y servicios financieros viene creciendo significativamente en los últimos años. La gran mayoría de los bancos hace años que ofrece a sus clientes *Apps* (aplicaciones móviles) y distintas plataformas de *Home Banking* para realizar la mayor parte de las operaciones, con lo que ya se encuentra ampliamente instalado, la gestión digital de los diversos productos que ofrecen las entidades financieras. Todo ello, fruto de una innegable ventaja práctica que hace a la rapidez de las operaciones, la comodidad de los usuarios y la indudable mayor fluidez del tráfico bancario.

Asimismo, en este contexto, se ha evidenciado que el aumento del uso de los entornos digitales de las entidades bancarias y financieras, también trajo aparejado el incremento de los *ciber* delitos donde el principal ataque es el uso de la ingeniería social, mediante el engaño. Es lo que se conoce como *phishing*.

Evidenciándose además, un creciente y permanente perfeccionamiento de las maniobras delictivas que obligan a los bancos a tener que tomar constantemente medidas para evitar los crecientes casos de fraude, que son de notorio y público conocimiento.

El *phishing*, traducido al idioma castellano significa cosecha y pesca de contraseñas, definido como el uso de técnicas de ingeniería social, donde se engaña y manipula psicológicamente a la víctima para que revele datos que no brindaría en circunstancias normales. El "*phishing"* no es más que una técnica de manipulación. La maniobra normalmente viene acompañada con la "suplantación de identidad" de alguna empresa, organismo público o personalidad reconocida que podría ser de interés para la víctima, pero el circuito mínimo de "anzuelo y pesca" que propone el *phishing* consta de un llamado de atención (que puede ser la caída de un servicio, el bloqueo de una clave, una oferta de último minuto, un premio, e incluso una multa o un castigo) y un requerimiento de información sensible (usuarios, contraseñas, claves bancarias, tarjetas de coordenadas, tokens, códigos de verificación, códigos de recuperación, números de tarjetas de crédito y de débito, etc.). En resumen, el atacante busca poner en crisis al eslabón más débil de toda la cadena de la seguridad de la información -el usuario final- para inducirlo a realizar determinada acción (completar un formulario, entregar información por teléfono, blanquear una clave, realizar operaciones por cajero automático, consumir desde un sitio web que simula ser otro, etc.). Y la gravedad del caso dependerá luego de la utilidad que el criminal le encuentre a la información obtenida. Porque el perjuicio patrimonial directo es una de las opciones, pero también lo son el acceso indebido, la suplantación de identidad (para engañar a terceros) y la extorsión a la propia víctima, entre otras tantas (MILLER, Christian H., *Los casos de "phishing" en la justicia argentina avanzan favorablemente para los damnificados*, LA LEY 10/11/2021, 7, TR LALEY AR/DOC/3184/2021).

Los "phishers", así son denominados estos estafadores, a menudo simulan pertenecer a entidades bancarias y solicitan a los *ciber* navegantes los datos de tarjetas de crédito o las

claves bancarias a través de un formulario o un correo electrónico, con un enlace que conduzca a una falsa página *web* con una apariencia similar a la original. Al ser engañado, el usuario ingresará sus datos confidenciales sin temor, en tanto desconoce que los está enviando a un delincuente.

Al solo efecto ejemplificativo, se mencionarán algunas de las modalidades en las que pueden evidenciarse los casos de *"phishing".* El denominado *"vishing",* es una práctica fraudulenta que consiste en el uso de la línea telefónica convencional y de la ingeniería social para engañar personas y obtener información delicada como puede ser financiera o cualquier dato útil para el robo de identidad. El término es una combinación del inglés *"voice*" (voz) y *phising*. Por último, el término *"smishing"* refiere a una actividad criminal a base de mensajes de texto dirigidos a usuarios de telefonía móvil. El "robo de identidad", se configura cuando se utiliza la información personal de los usuarios para realizar operaciones como compras con tarjetas de crédito y/o débito, solicitudes de préstamos o apertura de cuentas bancarias. También recientemente ha aparecido otra modalidad, que se ha dado en llamar *"malware"*, la que puede tomar muchas formas, como virus o troyanos, que son virus que se suelen infectar las computadoras de los usurarios o los dispositivos móviles a través de la recepción de correos electrónicos, sitios web o descargas de aplicaciones no seguras.

El denominado "pharming", que es un tipo de ciberataque en el que el atacante intenta redirigir el tráfico web, especialmente los datos de la solicitud a un sitio web fraudulento. Relacionado también con el "Fraude en línea", que es aquel mecanismo que logra que el usuario proporcione información personal en sitios *web* sospechosos. Para evitar éste último, se suele aconsejar a las personas para que identifiquen bien las páginas en las cuales van a ingresar sus datos, por ejemplo que tengan la sigla: https://, o el denominado

“tilde azul”. Asimismo, es de vital importancia, que al ingresar a una página lo hagan directamente tipeando la dirección de la misma, o desde la aplicación previamente descargada en la computadora o en el celular y que nunca lo hagan desde un buscador, porque puede ser redirigido el tráfico a otra página no oficial.

En el caso de marras, del relato de la actora se evidencia que intenta sostener que se trató de un caso de “pharming” o de fraude en línea, ya que sostiene que recibió un mail (que en apariencia se lo enviaba el Banco Macro) que contenía un enlace que la direccionaba a otra página, y que una vez que ingreso a esa segunda página, colocó su D.N.I., clave y contraseña. Y que luego de eso, se comenzó a abrir otra ventana emergente (en esa misma página) en la que ingreso el resto de sus datos confidenciales.

Pero, analizando la plataforma fáctica se observa que la actora no ha logrado acreditar por ningún medio el antecedente fáctico de las supuestas maniobras delictivas, como para tener por configurada la existencia de la estafa digital.

Así las cosas, en primer lugar la actora manifiesta que el 12/10/2012 ingreso a su casilla de correo y observó que en su bandeja de entradas había un mail que le dirigía el Banco Macro. El perito ingeniero informático oficial Iván J. Garro en su dictamen obrante a ff. 93/97 en su respuesta a la pregunta n.° 1 del cuestionario del actor, en la que se le solicitaba que estableciera la existencia de correos electrónicos enviados por el Banco Macro al mail de la actora, dictaminó: *“[…] se ingresó al sitio web www.gmail.com con la cuenta inmoflama@gmail.com y su contraseña y se procedió a realizar búsquedas de correos electrónicos con el siguiente criterio: “@bancomacro.com.ar”; “banco macro”; “macro”. Como se puede ver, no existen correos anteriores a la fecha 31/12/2015, con ese criterio de búsqueda. Posteriormente se realizó una nueva búsqueda únicamente entre fechas, fijando como parámetros entre el día 09/10/2012 y el 16/10/2012, arrojando*

*un resultado negativo, ningún correo ha sido encontrado, el resultado puede verificarse en la siguiente impresión de pantalla […]".*Vinculado a este elemento probatorio, se puede afirmar que las pericias representan la pieza probatoria más apta para dilucidar la cuestión sujeta a decisión, por tratarse de la opinión de un especialista acerca del área propia de su conocimiento, sobre las cuales no es mucho lo que puede conocer el juez. En el caso de marras, la pericia oficial exhibe una innegable calidad probatoria en relación a las cuestiones técnicas para las que fue confeccionada. Asimismo, dicho informe luce claro, preciso en sus términos, coherente en sus conclusiones y está debidamente fundado. Por otro lado, no se encuentra impugnado y ninguna de las partes ha arrimado a la causa ningún informe técnico en disidencia que permitiera inferir alguna conclusión distinta a la arribada. Asimismo, se observa que el perito ha realizado una respuesta muy circunstanciada del punto, ya que primero elaboro una conclusión teniendo en cuenta el período de tiempo anterior al 31/12/2015 y además acompañó un print de pantalla con la respuesta obtenida a su consulta. Asimismo, realizó una segunda consulta, colocando dos fechas próximas al supuesto mail recibido por la actora, para afinar el criterio de búsqueda y obtener un resultado más específico el cual volvió a arrojar una respuesta negativa.

Por otra parte, existe una discordancia en las declaraciones de la actora, puesto que de las copias del sumario penal cuyas copias fueron agregadas con fecha 23/02/2024, no existe constancia de que la actora hubiere manifestado en sede penal que recibió un mail ese día del Banco Macro.

De lo expuesto, se concluye inexorablemente que el día 12/10/2012, la actora no recibió en su casilla de correo ningún mail proveniente del Banco Macro.

Además y continuando con el análisis del relato de los hechos formulados por la actora, no se vislumbran los motivos (y la actora no los manifiesta) por los cuales ella tomó la

decisión de ingresar a un enlace que supuestamente recibió en el primer mail. Es decir, ella manifiesta que recibió un mail con la apariencia de provenir del Banco Macro, que tenía un enlace que la direccionaba a la página oficial del mismo banco y que inmediatamente ella ingresó al enlace proporcionado por la página, sin haber estado realizando ninguna gestión previa en el banco. Aquí, sin lugar a dudas, se comienza a vislumbrar una incipiente actitud por lo menos irreflexiva por parte de la actora. Si bien es cierto que la actora manifiesta que semanas antes solicitó un crédito en la entidad demandada, para lo cual se le abrió una caja de ahorro y se le depositó el monto requerido, no menos cierto es que lo sucedido el día 12/10/2012 fue un hecho totalmente ajeno a las circunstancias que rodearon la concesión del crédito solicitado.

En segundo lugar, la actora manifiesta que en ese mail recibido había un enlace que la conducía a la página del Banco Macro y que una vez que ingresó a esa segunda página, ella colocó su D.N.I., su clave y su contraseña. En relación a esta postulación, cabe recordar que el perito oficial, ante la pregunta n.° 2 de la actora, en la que se solicita que determine si en los mails enviados por la demandada contenían algún enlace o si se le daban algunas indicaciones de pasos a seguir por parte del destinatario del correo electrónico, el perito oficial respondió: *"[…] Determinado que no ha sido encontrado ningún correo electrónico, esta respuesta no puede ser respondida […]".* Cabe recordar aquí, que no existe en autos ninguna otra prueba, documental, testimonial, etc. que aporte ningún elemento probatorio tendiente a acreditar ni siquiera indiciariamente, que la actora ingresó a una segunda página, que tuviere la apariencia de la página oficial del Banco Macro. Es decir, la actora sostiene que el enlace la redirigió a una página determinada que era parecida a la del Banco, pero lo dirimente aquí, es que la actora no acreditó por ningún medio si entró a una página que tuviera la apariencia de la oficial del banco, o si

entró a alguna otra página que fuera a todas luces muy distinta, ni a ninguna otra. Cabe remarcar, que la actora si bien puso a disposición del perito informático su computadora, no ofreció como punto de pericia a fin de que el ingeniero en sistemas pudiera a través del historial de ingresos efectuados en esa computadora, establecer con certeza a que página había entrado la actora el día 12/10/2012, luego de haber recibido el supuesto mail del banco demandado.

Por último, la misma actora sostiene que luego de ingresar esos datos confidenciales en la segunda página, le apareció una ventana emergente que no la dejaba operar, sino ingresaba otros datos más. A lo que ella manifiesta que voluntariamente ingresó los datos de su tarjeta y su clave. Sin perjuicio de que tampoco ha acreditado la actora la existencia de alguna ventana emergente en ninguna página en la que supuestamente hubiere accedido, en este estadio argumental, aparece un dato muy relevante para continuar analizando, esto es, que la actora aduce que le fueron solicitados los campos de la tarjeta de coordenadas y que ella los ingreso en la página para continuar operando. Aquí cabe traer a colación, que la tarjeta de coordenadas, si bien no fue acompañada en el expediente, a ff. 50/51 existen dos copias de los reversos de distintas tarjetas de coordenadas del Banco Macro y del Banco Galicia, las cuales no han sido impugnadas y de las que surge que como recomendaciones de seguridad se explicitan las siguientes leyendas: “nunca se le solicitarán todas las coordenadas juntas”. Así, luce especialmente llamativo que la actora hubiera ingresado todos los campos de su tarjeta de coordenadas en el sitio, como ella misma lo reconoce, tomando todo el tiempo necesario para ello sin haber dudado en algún momento acerca de si estaba operando en un sitio falso, ya que no solo en el mismo plástico de la tarjeta se encuentra la recomendación acerca que nunca se le van a pedir todos los datos juntos, sino que también, es un tipo de tarjeta que contiene

transcripto en la generalidad de los casos numerosos dígitos, con la consecuente y lógica cantidad de tiempo que puede llegar a insumir transcribirlos a todos e ingresarlos en un sitio de internet. Lo que en algún punto, (de haberlo acreditado) hubiere revelado la circunstancia de la urgencia o la necesidad en la que suelen estar inmersos los sujetos que son víctimas de este tipo de delitos informáticos. Cuestión que a veces justifica que algunos detalles de apariencia en los sitios web no sean tenidos en cuenta por los usuarios que son víctimas de este tipo de fraudes.

Como fuere, el punto dirimente para resolver el presente conflicto, no es si la actora fue diligente o no en la custodia de sus datos confidenciales, o en el uso de las herramientas digitales (que correspondería expedirse en un análisis posterior para el caso de acogimiento de la demanda), sino que la misma no ha acreditado por ningún medio el antecedente fáctico de la supuesta estafa digital.

Se repite, nada de ello ha sido probado en la causa por ningún elemento probatorio, que amerite poder seguir avanzando sobre la responsabilidad endilgada al banco demandado.

En este punto, debe recordarse, que es la parte actora quien tenía la carga de probar y acreditar los extremos que hacen a su derecho y no lo hizo (art. 1744 del CCC). No se trata de una imposibilidad no imputable de prueba, sino que se podía haber acreditado los extremos necesarios, por cualquier medio de prueba (pericial, informativa, testimonial, etc.). En este sentido, autorizada doctrina ha sostenido que *"la desidia del interesado, omisión de la prueba del quantum, a pesar de contar con los medios necesarios, que razonablemente le permitían la acreditación de ese extremo, lleva al rechazo de la pretensión, aunque estuviera demostrada la responsabilidad del contrario y la existencia del daño"* (Conf. Vénica, Oscar H., Conclusión del juicio, en Código Procesal Civil y Comercial, ley 8465, varios autores, Cba, Foro de Cba, p. 127; citado en autos: "Risso,

Paola Adriana c/ MET Córdoba S.A. – Ordinario" – exp. n.° 2 374 189, sentencia n.° 97 de la Excma. Cámara Civ. y Com. de 1.° Nom.).

Es preciso puntualizar, que en casos como estos, existen dos maniobras, por un lado el antecedente fáctico, esto es, la llamada telefónica, el envío del mail, la existencia de una página falsa, etc., que suele constituirse en el "anzuelo" por el que los estafadores logran hacerse de los datos de los usuarios. Y luego, existe una maniobra posterior, que es la estafa propiamente dicha, en la que el tercero realiza las transferencias o pedidos de créditos etc. Es necesario, que ambas maniobras se encuentren debidamente acreditadas, no solo las operaciones fraudulentas. En este caso, como se viene desarrollando, no se ha probado por ningún elemento probatorio el elemento fundante de la maniobra o el antecedente fáctico de la estafa digital, lo que lleva derechamente a no tener otra alternativa que el rechazo de la pretensión resarcitoria de la actora.

Vinculado al punto, en un caso semejante se ha establecido: "*Pero también es real que la única prueba obrante en autos a los fines de acreditar que terceros operaron sobre tales cuentas sin su consentimiento, es la versión que da ella misma, sin prueba objetiva alguna que la avale".*(Excma. Cámara de Apelaciones en lo C. y C. de 4° Nominación, Sentencia n.° 121 del 24/07/2023 en autos: "Ulloque Olivetto, Noelia Aldana c/ Banco de la Provincia de Córdoba Bancor – Abreviado – Daños y Pejuicios – Otras formas de responsabilidad extracontractual – Trámite Oral"- Expte. N.° 10493294). Además, en otro precedente muy similar, se ha establecido: **"***El actor no logró acreditar la ocurrencia de los hechos que fundamentan la estafa, lo que incluye: La inexistencia de prueba concluyente de que haya ingresado a una página falsa que simulara ser la oficial del Banco. La falta de peritaje informático sobre los dispositivos del actor (computadora o celular) para verificar si accedió a un sitio apócrifo o si recibió comunicaciones*

fraudulentas. Ausencia de pruebas sobre la supuesta llamada o contacto posterior que habría utilizado ingeniería social para solicitar sus datos. Sin esta base fáctica, no se puede determinar que el Banco haya incumplido el deber de seguridad" (Excma. Cámara de Apelaciones en lo C. y C. de 7° Nominación, Sentencia n.° 228 del 18/12/2024 en autos: "Soppe Ingeniería S.R.L. y otro c/ Banco Macro S.A - Abreviado – Otros. Trámite Oral"- Expte. N° 11 352 534).

Por otra parte, atendiendo al argumento de la actora que manifiesta que el banco incumplió con el deber de seguridad a su cargo por haber actuado con falta de diligencia luego de los hechos sucedidos, tampoco ha merecido respaldo probatorio alguno. Así, a la luz de los elementos de prueba colectados en la causa, se observa que la misma actora reconoce que recibió dos llamadas telefónicas de distintos empleados para alertarla de las transferencias realizadas, que los mismos empleados le solicitaron que se apersonara en el banco inmediatamente para formular el reclamo correspondiente. Además, reconoce que personal del banco le dio un ticket donde figuraba el n.° de su reclamo y le imprimieron la constancia de C.B.U. de la cuenta a la cual habían sido girados los fondos, a fin de que sin dilaciones formulara la denuncia penal correspondiente. Estas actitudes, reveladas por el personal del Banco inmediatamente de sucedido los hechos, no hacen sino revelar una conducta diligente conforme las circunstancias fácticas que rodearon el caso, lo que repele por completo el argumento intentado por la actora acerca de la falta de seguridad del banco.

Finalmente, cabe recordar que no ha surgido de la causa que los sistemas del banco hubieran sufrido vulnerabilidad alguna el día de los hechos, puesto que de constancias de la pericia oficial, en el cuestionario de la demandada en sus punto n.° 2, 3 y 4 se le pide al perito que detalle la protección de los sistemas del banco, si posee antivirus y el grado

de vulnerabilidad de los mismos, a lo que responde: *"[…] Se cuenta con un mecanismo de protección ante conexiones no autorizadas (Antispoofing) identificando el sentido donde las mismas se originan. Todos los servidores del banco cuentan con antivirus. El Banco Macro realiza en forma trimestral el chequeo de la seguridad de sus servicios (Pentest) de Banca Virtual, para detectar en forma temprana cualquier falla de seguridad que se presente o que el mismo presente vulnerabilidades a nuevas técnicas de ataque. Como resultado de los mismos se evalúa si existe exposición o riesgos que comprometan todo el sistema o cada una de las partes, y si en algún caso pueden comprometerse las credenciales de los usuarios […]".* De lo que se desprende, que ha quedado acreditado que no hubo fallas en los sistemas de seguridad del banco el día de los hechos.

En definitiva, de todas las consideraciones expuestas se colige que la actora no probó el presupuesto de viabilidad de la acción intentada, cual es, el antecedente fáctico de la estafa digital, no quedando otra alternativa que el rechazo de la demanda.

III) Las costas, en atención al resultado del juicio y en virtud del principio objetivo de la derrota establecido por el art. 130 del C.P.C.C., se imponen a la actora, debiendo regularse los honorarios del letrado de la contraria a la condenada en costas, esto es al Dr. Martín Cortes Olmedo (art. 26 de la ley 9459) a cuyo fin se debe tomar como base el monto demandado (art. 31 inc. 2° del C.A.) y adicionarle sus intereses, conforme a lo solicitado en la demanda. De ese modo, el rubro daño emergente por el que se reclama la suma de pesos treinta y ocho mil trescientos ($ 38 300) y daño moral por el que se reclama la suma de pesos quince mil ($ 15 000), serán actualizados desde la fecha del hecho (12/10/2012) y el rubro pérdida de chance por el que se reclama la suma de pesos veinte mil ($ 20 000) no llevará intereses, atento a tratarse de un rubro futuro. Teniendo en cuenta la cuantía del asunto, conjugados con las demás reglas de evaluación cualitativas

establecidas por el art. 39 de la ley 9459, se estima adecuado a la justicia del caso aplicar medio punto sobre el punto medio de la escala del art. 36, esto es el 23%. Realizadas las operaciones correspondientes y resultando exiguo el monto resultante, corresponde regular al letrado el mínimo legal correspondiente según el tipo de juicio, esto es 20 jus. Asimismo, corresponde regular los honorarios en forma definitiva al perito informático oficial ingeniero Iván J. Garro en el valor de 12 jus atento a las reglas de evaluación cualitativas establecidas por el art. 39 de la ley 9459. Se deja constancia de que todos los honorarios aquí regulados, tienen el carácter de definitivos y generarán intereses desde la fecha de la presente resolución, según la tasa pasiva promedio mensual que publica el BCRA con más el 3% nominal mensual hasta su efectivo pago.

Por las consideraciones expuestas y normas legales citadas.

SE RESUELVE:

1.º) Rechazar la demanda entablada por la Sra. Ana Valeria Machado en contra del Banco Macro S.A.

2.º) Imponer las costas a cargo de la parte actora, a cuyo fin se regulan, en forma definitiva los honorarios del Dr. Martín Cortes Olmedo en la suma de pesos seiscientos treinta y cinco mil quinientos veintiocho con cuarenta centavos ($ 635 528,40) con más el IVA en caso de corresponder; esto es, si al tiempo del pago dicho profesional reviste la calidad de inscripto ante la AFIP. Regular los honorarios en forma definitiva del perito oficial ingeniero Iván J. Garro, en la suma de pesos trescientos ochenta y un mil trescientos diecisiete con cuatro centavos ($ 381 317,04) con más el IVA en caso de corresponder; esto es, si al tiempo del pago dicho profesional reviste la calidad de inscripto ante la AFIP.

Protocolícese e incorpórese copia.-

Texto Firmado digitalmente por: **MAYDA Alberto Julio**
JUEZ/A DE 1RA. INSTANCIA
Fecha: 2025.03.14