S E N T E N C I A.

Aguascalientes, Aguascalientes, a **veinticuatro de marzo de dos mil veintidós.**

V I S T O S, para resolver los autos del expediente número **0066/2021** que en la vía **ORAL MERCANTIL** promueve ********** en contra de ********** y, siendo su estado el de dictar **Sentencia Definitiva**, se procede a dictarla bajo los siguientes:

C O N S I D E R A N D O S:

I.- Reza el artículo **1324** del Código de Comercio que: "*Toda sentencia debe ser fundada en ley, y si ni por el sentido natural ni por el espíritu de ésta se puede decidir la controversia, se atenderá a los principios generales del derecho, tomando en consideración todas las circunstancias del caso"*.

II.- La suscrita Juez es competente para conocer el presente juicio atento a lo dispuesto por el artículo **1104 fracción II** del Código de Comercio, el cual dispone que será competente para conocer del juicio el del lugar designado en el contrato para el cumplimiento de la obligación. En el presente caso, se desprende que el contrato del cual derivan las pretensiones reclamadas por la actora, fue celebrado por las partes en esta ciudad de Aguascalientes, de donde deriva la competencia de esta autoridad.

III. - La parte actora ********** comparece a demandar a **********, por el pago y cumplimiento de las siguientes prestaciones:

*"**1.** Para que por sentencia firme se tenga por acreditada la relación contractual de mi representada con la institución financiera demandada, en virtud del contrato individual de prestación de servicios bancarios y financieros múltiples celebrado por mi representada y la ahora demandada bajo el número de cliente ********* y número de cuenta **********.*

2.** Se tenga por acreditada la nulidad de las tres operaciones bancarias identificadas como SEL TRANSF. INTERBANCARIA SPEI por los siguientes montos 599,600.00 (noventa y nueve mil seiscientos pesos 00/100 M.N.); $99,600.00 (noventa y nueve mil seiscientos pesos 00/100 M.N.) y $39,000.00 (Treinta y nueve mil pesos 00/100 M.N.) efectuada supuestamente por mi parte de forma electrónica mediante el uso supuesto del usuario, contraseña y token desde la cuenta ******* que mi representada tiene con la demandada, en fecha 09 de marzo de 2020 folios de operación **********, ********** y **********respectivamente; transferencias que resalto, en ningún momento efectúe.*

3.** Como consecuencia de lo anterior me sea restituida la cantidad de $238,200.00 (Doscientos treinta y ocho mil doscientos pesos 00/100 M.N.) a la cuenta ******* que mi representada tiene con la institución bancaria demandada, toda vez que, por mi parte, insisto no realice las transferencias anteriormente señaladas, ni traspase a persona alguna los datos de usuario, contraseña y el uso del token asignado al suscrito en mi carácter de representante legal de la parte actora.*

***4.** El pago de los gastos, honorarios de abogados y costas que genere el presente juicio, mismo que se promueve por el incumplimiento injustificado de la parte demandada a sus obligaciones contraídas en el contrato con dicha parte celebrado."* (transcripción literal visible a fojas uno y dos de los autos).

IV.- La demandada **********

**********, dio contestación a la demanda, negando la procedencia de todas y cada una de las prestaciones que les son reclamadas.

V.- La parte actora **********basó sus pretensiones en que:

*"**1.** En fecha 16 de julio de 2015 el suscrito en mi carácter de representante legal de la sociedad **********celebre con la institución bancaria denominada **********, un contrato de prestación de servicios bancarios y financieros con número de cuenta ********** aperturado en la sucursal **********se adjunta a efecto de comprobar lo anterior, el correspondiente contrato y la caratula de datos como ANEXO I.*

2.** Derivado del contrato que mi representada tiene con la institución bancaria demandada, por nuestra parte se recibían en la cuenta ******* a nombre de **********, diversos depósitos en efectiva los cuales se efectuaban por mi parte o por terceras personas y a su vez por mi parte se efectuaban transferencias electrónicas como pagos a proveedores y general todos aquellos necesarios y convenientes para llevar a cabo el objeto social de mi representada, operaciones que siempre efectuaba de manera personal a excepción de las realizadas en fecha 09 de marzo de 2020 con folios de operación **********, **********y **********.*

3.** Así las cosas, el nueve de marzo de dos mil veinte, transferí $ 2,000.00 (dos mil pesos, 00/100 M.N.) a una cuenta de una tercera persona, proveedora de mi representada; posteriormente, ese mismo día, recibí tres notificaciones mediante correos electrónicos en la cuenta de la que soy titular *******, por lo que me percaté que se habían realizado*

tres transferencias más sin mi autorización, posterior a la transferencia ya referida al inicio del presente párrafo, dos de ellas por unos montos que ascienden a $99,600.00 (noventa y nueve mil seiscientos pesos, 00/100 M.N.} cada una y una tercera por $39, 000.00 (treinta y nueve mil pesos, 00/100 M.N.), con folios de operación 25070885975, 25070886497 y 25070886885 respectivamente; transferencias que resalto, en ningún momento efectúe.

Resulta relevante señalar que para poder realizar una transferencia desde la banca por internet se requiere ingresar con usuario, contraseña y un token, este último con la finalidad de autorizar dichos movimientos.

***4.** Consecuentemente, me comuniqué vía telefónica con la Institución Bancaria ya mencionada, en dónde me informaron que ese día, es decir el nueve de marzo, las sucursales bancarias no laboraron en virtud del movimiento 08M; no obstante, me recomendaron comunicarme a un número *******para bloquear la cuenta y cancelar el saldo, para posteriormente acudir a la Institución Bancaria a levantar la aclaración, razón por la que me comuniqué nuevamente a dicho número, en dónde me informaron que dicha operación no se podía realizar vía telefónica, que se debía atender directamente en una sucursal.*

5.** En ese orden de ideas, el diez de marzo de dos mil veinte, acudí a la sucursal *******., en donde ingresé la solicitud de aclaración, misma que cuenta con el número de folio **********.*

***6.** En fecha 25 de marzo de 2020 se emitió la correspondiente respuesta a mi reclamación siendo esta en sentido negativo, refiriendo la demandada lo siguiente;*

"Estimado Cliente le notificamos, se realizaron los acciones correspondientes para recuperar los recursos, sin embargo, no fue

posible la recuperación, la investigación determino que el fraude se derivó por conexión a sitio phishing desde su equipo, es importante mencionar que la guarda y custodia del usuario, contraseña y dispositivo E-Llave son responsabilidad del cliente, esto de acuerdo Cap. 2 Clausula 7 del contrato SEL; de los incisos (I) al (M)...apartado "Medidas o recomendaciones", así mismo Cap. 5, clausula 11: de los incisos (1V) al inciso (IV)... por consiguiente, el cliente asume las consecuencias que se puedan derivar por la comisión de los hechos delictivos que tengan como causa el incumplimiento a las obligaciones a su cargo señaladas. De antemano agradecemos su preferencia y nos reiteramos a sus órdenes, en nuestro centro de atención telefónica: **************, ***las 24 horas del día, los 365 días del año."***

7. *Al conocer la negativa de la respuesta de la hoy demandada, acudí ante la Comisión Nacional para la protección y defensa de los usuarios de Servicios Financieros (CONDUSEF) a presentar mi queja en fecha 14 de agosto de 2020 asignándose a la misma el número de folio ***************dentro de la cual ********** manifestó a través de sus apoderados reconocidos ante dicha instancia que;* ***"La reclamación resulta improcedente, debido a que la transacción realizada a través de*** ************ *************se efectuó de manera exitosa sin registro de falla o error. Así mismo, existió validación de usuario y contraseña para acceso al portal electrónico, desde su equipo y como es de su conocimiento la guarda, custodia, uso de la tarjeta y contraseñas de sus servicios bancarios, es responsabilidad del cliente"***

8. *En fecha 11 de diciembre de 2020 tuvo lugar la audiencia de conciliación ante la CONDUSEF en la cual la institución bancaria demandada declino someterse al arbitraje propuesto, por lo que se dejaron a salvo los derechos de las partes para que se hicieran valer ante los tribunales competentes.*

*Se adjunta al presente copias simples de las actuaciones efectuadas dentro del expediente **************seguido ante la CONDUSEF*

incluyéndose la audiencia de fecha 11 de diciembre de 2020 en donde constan los acuerdos tomados por las partes." (transcripción literal visible a fojas dos a tres de los autos).

Por su parte la demandada **********, al dar contestación a la demanda, en cuanto a los hechos señala que:

*"**HECHO NÚMERO 1.-** El correlativo es cierto.*

HECHO NÚMERO 2.-** El correlativo se contesta como falso, siendo simples manifestaciones hechas por la Actora sin sustento probatorio alguno, correspondiéndole a ésta en virtud del principio "El que afirma está obligado a probar" acreditar su dicho. Aunado a lo anterior, conviene resaltar que mi Representada actúo en todo momento conforme a Derecho y el Contrato de Banca Electrónica, ya que el Sistema de esta simplemente ejecutó las instrucciones hechas valer par el hoy Actor mediante instrumentos electrónicos válidos y suficientes para acreditar el Consentimiento de Voluntad de la sociedad *******, tal y como se acreditará a lo largo del presente procedimiento oral.*

Es importante mencionar que el uso del portal del Banco únicamente se realiza por el titular de la cuenta, porque es dicha persona que puede con el acceso de clave o número confidencial tener acceso a dicho sistema y, a través del uso de la E-Llave, realizar las transferencias correspondientes.

Así pues, es que con dichas instrucciones electrónicas se tiene por plenamente probado el consentimiento de la voluntad del ordenante de realizar una transferencia electrónica, siendo que en el caso que nos ocupa mi Representada simplemente recibió las instrucciones electrónicas de manera válida y suficiente que ordenó el hoy Actor, a través de un sistema confiable y seguro según se acreditará con la pericial correspondiente, por lo

que al tener plenamente demostrado la Voluntad del referido Actor en los términos pactados es que procedió a le ejecución de las referidas transferencias y, por ende, en tal sentido las operaciones no pueden ser desconocidas por la Actora, siendo que incluso mi Representada goza de la presunción legal contenida en el artículo 90 bis del Código de Comercio.

De acuerdo al Banco de México, la firma electrónica se define de manera dogmática como:

[...]

*Aunado a lo anterior, conviene destacar la cláusula vigésimo primera del Contrato múltiple de productos bancarios y financieros y las cláusulas vigésima primera, vigésima segunda, trigésima sexta y trigésima octava del ********** ********, celebrados entre mi Representada y el hoy actor.*

De las cláusulas descritas, se desprende que los movimientos realizados por la hoy actora en su cuenta a través de Banca Electrónica son única y exclusivamente responsabilidad del titular responsable, siendo que por voluntad de ambas partes, el hoy Actor ***libró de toda Responsabilidad a mi Representada,*** *por lo que deviene total y absolutamente improcedente su acción, en primer término por la autenticidad y veracidad de la firma electrónica del Cuentahabiente que mi Representada tomó por cierta para ejecutar las instrucciones recibidas y, en segundo término, en virtud de que fue el propio Actor quien asumió el riesgo respectivo y acordó eximir a mi Representada de* ***toda responsabilidad,*** *al darse específicamente por enterado que dichas comunicaciones pudieran estar expuestas a intromisiones ilícitas.*

HECHO NÚMERO 3.- *El correlativo se contesta como falso, siendo simples manifestaciones hechas por la Actora sin sustento probatorio alguno, correspondiéndole a ésta en virtud del principio "El que afirma está obligado a probar" acreditar su dicho. Aunado a lo anterior, conviene resaltar que mi Representada actúo en todo momento conforme a*

*Derecho y el Contrato de Banca Electrónica, ya que el Sistema de esta simplemente ejecutó las instrucciones hechas valer por el hoy Actor mediante instrumentos electrónicos válidos y suficientes para acreditar el Consentimiento de Voluntad de la sociedad **********, tal y como se acreditará a lo largo del presente procedimiento oral.*

Es importante mencionar que el uso del portal del Banco únicamente se realiza por el titular de la cuenta, porque es dicha persona que puede con el acceso de clave o número confidencial tener acceso a dicho sistema y, a través del uso de la E-Llave, realizar las transferencias correspondientes. Así pues, es que con dichas instrucciones electrónicas se tiene por plenamente probado el consentimiento de la voluntad del ordenarte de realizar una transferencia electrónica, siendo que en el caso que nos ocupa mi Representada simplemente recibió las instrucciones electrónicas de manera válida y suficiente que ordenó el hoy Actor, por lo que al tener plenamente demostrado la Voluntad del referido Actor en los términos pactados es que procedió a le ejecución de las referidas transferencias y, por ende, en tal sentido las operaciones no pueden ser desconocidas.

*Aunado a lo anterior, conviene destacar la cláusula vigésimo primera del Contrato múltiple de productos bancarios y financieros y las cláusulas vigésima primera, vigésima segunda, trigésima sexta y trigésima octava del ********** **********, celebrados entre mi Representada y el hoy actor.*

De dichas cláusulas, Su Señoría llegará a la conclusión de que los movimientos realizados por la hoy actora en su cuenta a través de Banca Electrónica son única y exclusivamente responsabilidad del titular responsable, siendo que por voluntad de ambas partes, el hoy Actor ***libró de toda Responsabilidad a mi Representada,*** *por lo que deviene total y absolutamente improcedente su acción, en primer término por la autenticidad y veracidad de la firma electrónica del Cuentahabiente que mi Representada*

tomó por cierta para ejecutar las instrucciones recibidas y, en segundo término, en virtud de que fue el propio Actor quien asumió el riesgo respectivo y acordó eximir a mi Representada de ***toda responsabilidad,*** *al darse específicamente por enterado que dichas comunicaciones pudieran estar expuestas a intromisiones ilícitas.*

HECHO NÚMERO 4.- *El correlativo que se contesta es FALSO tal y como lo plantea la actora, ya que se circunscribe a meras manifestaciones sin fundamento probatorio alguno, aunado a que como ya se ha reiterado en los hechos que anteceden y se hará en las excepciones que prosiguen, mi Representada actuó de manera legal y conforme a lo pactado en el referido Acuerdo de Voluntades, aunado a que fue el propio Actor quien expresamente eximió a mi Poderdante de cualquier instrucción responsabilidad derivada del uso de los medios electrónicos.*

HECHO NÚMERO 5: *El correlativo se contesta como cierto, tal y como se desprende de la solicitud de aclaración y su respuesta, que adjunto a la presente contestación.*

HECHO NÚMERO 6: *El correlativo se contesta como cierto, tal y como se desprende de la solicitud de aclaración y su respuesta, que adjunto a la presente contestación. Cabe destacar a Su Señoría que mi Representada, al recibir las instrucciones con clave, clave dinámica, usuario y contraseña a través de la E-llave, efectúo las transferencias que le fueran ordenadas, siendo que éstas se generan con un factor de autenticación categoría 3 - el más seguro que prevé la regulación bancaria - en términos de los artículos 310, 312 y 313 de las disposiciones de carácter general aplicables a las instituciones de crédito, publicadas por la Comisión Nacional Bancaria y de Valores en el Diario oficial de la Federación el 2 de diciembre del 2005, cuya última modificación lo fue el 25 de noviembre del 2019.*

Luego entonces, si tal y como se acreditará dentro del presente juicio, si los procedimientos de identificación que fueron utilizados durante las transacciones cumplen con las disposiciones referidas y que per

se cumplen con los requisitos previstos para la verificación de la fiabilidad de las firmas electrónicas, de lo que se colige que el mensaje de datos provenían única y exclusivamente de la persona autorizada para operar vía internet la cuenta de la Actora, es que ésta carece de acción y derecho para ejercer la acción que pretende, por lo que mi Representada actuó de manera legal y conforme a lo pactado en el referido Acuerdo de Voluntades, aunado a que fue el propio Actor quien expresamente eximió a mi Poderdante de cualquier instrucción responsabilidad derivada del uso de los medios electrónicos.

HECHO NÚMERO 7: *El correlativo que se contesta es cierto. A su vez, cabe destacar que su reclamación en efecto, no es procedente ya que las transacciones realizadas cuentan con su firma electrónica, lo que se presume como la aceptación y deseo de la titular de la cuenta para realizar dichos movimientos, presunción que confirma el Código de Comercio en sus artículos 90 y 90 bis, mismos que a la letra dicen:*

[...]

De la fracción segunda del primer precepto que se cita, se deprende una presunción para considerar que un mensaje ha sido enviado por el emisor, siendo el emisor en el presente caso la parte actora, cuando se usen medios de identificación, tales como claves o contraseñas del emisor (situación que ocurrió ya que la transferencia fue realizada mediante la utilización del número y clave confidencial que se otorgó a la parte actora bajo su más estricta responsabilidad) por lo que efectivamente existe la certeza a favor de mi representada de que la transferencia fue ordenada por el emisor (la parte actora).

Es importante mencionar que el uso del portal del Banco únicamente se realiza por el titular de la cuenta, porque es dicha persona que puede con el acceso de clave o número confidencial tener acceso a dicho sistema y, a través del uso de la E-Llave, realizar las transferencias correspondientes. Así pues, es que con dichas instrucciones electrónicas se tiene por plenamente probado el consentimiento de la voluntad del ordenante

de realizar una transferencia electrónica, siendo que en el caso que nos ocupa mi Representada simplemente recibió las instrucciones electrónicas de manera válida y suficiente que ordenó el hoy Actor, por lo que al tener plenamente demostrado la Voluntad del referido Actor en los términos pactados es que procedió a le ejecución de las referidas transferencias y, por ende, en tal sentido las operaciones no pueden ser desconocidas.

HECHO NÚMERO 8: *El correlativo que se contesta es cierto."* (transcripción literal visible a fojas ochenta y seis a la noventa y dos de los autos)

En los anteriores términos queda fijada la litis.

VI.- Procediendo con el estudio de la acción intentada, resulta lo siguiente:

Demanda **********, a fin de que se le restituya la cantidad de **DOSCIENTOS TREINTA Y OCHO MIL DOSCIENTOS PESOS** derivado de diversas transferencias electrónicas que desconoce, las cuales fueron realizadas en el mes de marzo de dos mil veinte, a su cuenta con número ********** .

Por su parte, la demandada señala que no tiene responsabilidad alguna, en virtud de que en ningún momento intervino en las operaciones reclamadas, y que las mismas las realizó la propia actora, haciendo uso de su sistema interbancario y mediante la utilización de las contraseñas y el uso del dispositivo E-Llave de los que sólo ella dispone, señalando además que a fin de realizar las operaciones, es necesario ingresar el número de seguridad que proporciona el dispositivo electrónico E-Llave así como el número de contraseña que únicamente es conocido por la actora.

Los artículos **46 Bis**, **52** y **77** de la Ley de Instituciones de Crédito, disponen:

ARTÍCULO 46 Bis.- La Comisión Nacional Bancaria y de Valores autorizará a las instituciones de banca múltiple el inicio de operaciones o la

realización de otras adicionales a las que le hayan sido autorizadas, de entre las señaladas en el artículo 46 de esta Ley, cuando acrediten el cumplimiento de lo siguiente:

I. Que las operaciones de que se trate se encuentren expresamente señaladas en sus estatutos sociales;

II. Que cuenten con el capital mínimo que les corresponda conforme a lo establecido en el artículo 19 de esta Ley, en función de las operaciones que pretendan realizar;

III. Que cuenten con los órganos de gobierno y la estructura corporativa adecuados para realizar las operaciones que pretendan llevar a cabo, de acuerdo con lo establecido en esta Ley y en las disposiciones técnicas u operativas de carácter general emitidas por la Comisión Nacional Bancaria y de Valores tendientes a procurar el buen funcionamiento de las instituciones;

IV. Que cuenten con la infraestructura y los controles internos necesarios para realizar las operaciones que pretendan llevar a cabo, tales como sistemas operativos, contables y de seguridad, oficinas, así como los manuales respectivos, conforme a las disposiciones aplicables, y

V. Que se encuentren al corriente en el pago de las sanciones impuestas por incumplimiento a esta Ley que hayan quedado firmes, así como en el cumplimiento de las observaciones y acciones correctivas que, en ejercicio de sus funciones, hubieren dictado la citada Comisión y el Banco de México.

La Comisión Nacional Bancaria y de Valores practicará las visitas de inspección que considere necesarias a efecto de verificar el cumplimiento de los requisitos a que se refieren las fracciones I a IV de este artículo.

La Comisión consultará con el Banco de México el cumplimiento de las medidas y sanciones que éste hubiere impuestos en el ámbito de su competencia. La institución de que se trate deberá inscribir en el Registro Público de Comercio, para efectos declarativos, la autorización que se le haya otorgado para el inicio de operaciones en términos del presente artículo, a más tardar a los treinta días posteriores a que le haya sido notificada.

ARTÍCULO 52.- Las instituciones de crédito podrán permitir el uso de la firma electrónica avanzada o cualquier otra forma de autenticación para pactar la celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, y establecerán en los contratos respectivos las bases para determinar lo siguiente:

I. Las operaciones y servicios cuya prestación se pacte; II. Los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y

III. Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate. Cuando así lo acuerden con su clientela, las instituciones podrán suspender o cancelar el trámite de operaciones que aquélla pretenda realizar mediante el uso de equipos o medios a que se refiere el primer párrafo de este artículo, siempre que cuenten con elementos suficientes para presumir

que los medios de identificación pactados para tal efecto han sido utilizados en forma indebida.

Lo anterior también resultará aplicable cuando las instituciones detecten algún error en la instrucción respectiva.

Asimismo, las instituciones podrán acordar con su clientela que, cuando ésta haya recibido recursos mediante alguno de los equipos o medios señalados en el párrafo anterior y aquéllas cuenten con elementos suficientes para presumir que los medios de identificación pactados para tal efecto han sido utilizados en forma indebida, podrán restringir hasta por quince días hábiles la disposición de tales recursos, a fin de llevar a cabo las investigaciones y las consultas que sean necesarias con otras instituciones de crédito relacionadas con la operación de que se trate.

La institución de crédito podrá prorrogar el plazo antes referido hasta por diez días hábiles más, siempre que se haya dado vista a la autoridad competente sobre probables hechos ilícitos cometidos en virtud de la operación respectiva.

No obstante lo dispuesto en el párrafo anterior, cuando las instituciones así lo hayan acordado con su clientela, en los casos en que, por motivo de las investigaciones antes referidas, tengan evidencia de que la cuenta respectiva fue abierta con información o documentación falsa, o bien, que los medios de identificación pactados para la realización de la operación de que se trate fueron utilizados en forma indebida, podrán, bajo su responsabilidad, cargar el importe respectivo con el propósito de que se abone en la cuenta de la que procedieron los recursos correspondientes.

Las instituciones que por error hayan abonado recursos en alguna de las cuentas que lleven a su clientela, podrán cargar el importe respectivo a la cuenta de que se trate con el propósito de corregir el error, siempre que así lo hayan pactado con ella.

En los casos señalados en los cuatro párrafos anteriores, las instituciones deberán notificar al cliente respectivo la realización de cualquiera de las acciones que hayan llevado a cabo de conformidad con lo previsto en los mismos.

El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

La instalación y el uso de los equipos, medios y formas de autenticación señalados en el primer párrafo de este artículo se sujetarán a las reglas de carácter general que emita la Comisión Nacional Bancaria y de Valores, sin perjuicio de las facultades con que cuenta el Banco de México para regular las operaciones que efectúen las instituciones de crédito relacionadas con los sistemas de pagos y las de transferencias de fondos en términos de su ley.

Las instituciones de crédito podrán intercambiar información en términos de las disposiciones de carácter general a que se refiere el artículo 115 de esta Ley, con el fin de fortalecer las medidas para prevenir y detectar actos, omisiones u operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión de los delitos en contra de su clientela o de la

propia institución. El intercambio de información a que se refiere el párrafo anterior no implicará trasgresión alguna a lo establecido en el artículo 142 de esta Ley.

ARTÍCULO 77.- Las instituciones de crédito prestarán los servicios previstos en el artículo 46 de esta Ley, de conformidad con las disposiciones legales y administrativas aplicables, y con apego a las sanas prácticas que propicien la seguridad de esas operaciones y procuren la adecuada atención a los usuarios de tales servicios.

Así mismo los artículos **316 Bis 10**, **11**, **14** y **16** de las Disposiciones de Carácter General aplicables a las Instituciones de Crédito, disponen:

Artículo 316 Bis 10.- Las Instituciones que utilicen Medios Electrónicos para la celebración de operaciones y prestación de servicios, deberán implementar medidas o mecanismos de seguridad en la transmisión, almacenamiento y procesamiento de la información a través de dichos Medios Electrónicos, a fin de evitar que sea conocida por terceros.

Para tales efectos, las Instituciones deberán cumplir con lo siguiente:

I. Cifrar los mensajes o utilizar medios de comunicación Cifrada, en la transmisión de la Información Sensible del Usuario procesada a través de Medios Electrónicos, desde el Dispositivo de Acceso hasta la recepción para su ejecución por parte de las Instituciones, a fin de proteger la información a que se refiere el Artículo 117 de la Ley, incluyendo la relativa a la identificación y Autenticación de Usuarios tales como Contraseñas, Números de Identificación Personal (NIP), cualquier otro Factor de Autenticación, así como la información de las respuestas a las preguntas secretas a que se refiere el penúltimo párrafo del Artículo 316 Bis 3 de estas disposiciones.

Para efectos de lo anterior, las Instituciones deberán utilizar tecnologías que manejen Cifrado y que requieran el uso de llaves criptográficas para asegurar que terceros no puedan conocer los datos transmitidos.

Las Instituciones serán responsables de la administración de las llaves criptográficas, así como de cualquier otro componente utilizado para el Cifrado, considerando procedimientos que aseguren su integridad y confidencialidad, protegiendo la información de Autenticación de sus Usuarios.

Tratándose de Pago Móvil, Banca Telefónica Voz a Voz y Banca Telefónica Audio Respuesta, podrán implementar controles compensatorios al Cifrado en la transmisión de información a fin de protegerla.

II. Las Instituciones deberán Cifrar o truncar la información de las cuentas u operaciones de sus Usuarios y Cifrar las Contraseñas, Números de Identificación Personal (NIP), respuestas secretas, o cualquier otro Factor de Autenticación, en caso de que se almacene en cualquier componente de los Medios Electrónicos.

III. En ningún caso, las Instituciones podrán transmitir las Contraseñas y Números de Identificación Personal (NIP), a través de correo

electrónico, servicios de mensajería instantánea, Mensajes de Texto SMS o cualquier otra tecnología, que no cuente con mecanismos de Cifrado.

Se exceptúa de lo previsto en esta fracción a las Contraseñas y Números de Identificación Personal (NIP) utilizados para acceder al servicio de Pago Móvil, siempre y cuando las Instituciones mantengan controles para que no se pongan en riesgo los recursos y la información de sus Usuarios. Las Instituciones que pretendan utilizar los controles a que se refiere el presente párrafo deberán obtener la previa autorización de la Comisión, para tales efectos.

Asimismo, la información de los Factores de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, utilizados para acceder a la información de los estados de cuenta, podrá ser comunicada al Usuario mediante dispositivos de audio respuesta automática, así como por correo, siempre y cuando esta sea enviada utilizando mecanismos de seguridad, previa solicitud del Usuario y se hayan llevado a cabo los procesos de Autenticación correspondientes.

IV. Las Instituciones deberán asegurarse de que las llaves criptográficas y el proceso de Cifrado y descifrado se encuentren instalados en dispositivos de alta seguridad, tales como los denominados HSM (Hardware Security Module), los cuales deberán contar con prácticas de administración que eviten el acceso no autorizado y la divulgación de la información que contienen.

V. Tratándose del servicio de Banca Electrónica en el que se utilicen tarjetas de débito y de crédito, con las certificaciones que se indican a continuación: (260) a) Certificaciones de normas de seguridad de la industria de tarjetas, incluyendo entre otras: la norma de seguridad de datos (PCI-DSS), la norma de seguridad de datos para las aplicaciones de pago (PA-DSS) y los requisitos de seguridad y transacciones con NIP (PTS) o sus equivalentes o aquellos que, a criterio de la Comisión, permitan la debida protección de la información almacenada, transmitida o procesada. (260) b) Certificación conforme al estándar de interoperabilidad de tarjetas de débito y de crédito conocido como EMV, niveles 1 (interfaces, físico, eléctrico y de transporte) y 2 (selección de aplicaciones de pago y procesamiento de transacciones), en su caso, aquellos otros estándares que, a criterio de la Comisión, satisfagan este requerimiento y permitan la adecuada interoperabilidad. Lo anterior solo aplicará en aquellos Dispositivos de Acceso para operaciones con Tarjeta Bancaria con Circuito Integrado en que la información para realizar operaciones se toma directamente del circuito integrado de esta."

ARTÍCULO 316 Bis 11.- Las Instituciones deberán contar con controles para el acceso a las bases de datos y archivos correspondientes a las operaciones y servicios efectuados a través de Medios Electrónicos, aun cuando dichas bases de datos y archivos residan en medios de almacenamiento de respaldo.

Para efectos de lo anterior, las Instituciones deberán ajustarse a lo siguiente:

I. El acceso a las bases de datos y archivos estará permitido exclusivamente a las personas expresamente autorizadas por la Institución en función de las actividades que realizan. Al otorgarse dichos accesos, deberá dejarse constancia de tal circunstancia y señalar los propósitos y el periodo al que se limitan los accesos.

II. Tratándose de accesos que se realicen en forma remota, deberán utilizarse mecanismos de Cifrado en las comunicaciones.

III. Deberán contar con procedimientos seguros de destrucción de los medios de almacenamiento de las bases de datos y archivos que contengan Información Sensible de sus Usuarios, que prevengan su restauración a través de cualquier mecanismo o dispositivo.

IV. Deberán desarrollar políticas relacionadas con el uso y almacenamiento de información que se transmita y reciba por los Medios Electrónicos, estando obligadas a verificar el cumplimiento de sus políticas por parte de sus proveedores y afiliados.

La obtención de información almacenada en las bases de datos y archivos a que se refiere el presente artículo, sin contar con la autorización correspondiente, o el uso indebido de dicha información, será sancionada en términos de lo previsto en la Ley, inclusive tratándose de terceros contratados al amparo de lo establecido en el Artículo 46 Bis 1 de dicho ordenamiento legal.

ARTÍCULO 316 Bis 14.- Las Instituciones deberán mantener en bases de datos todas las operaciones efectuadas a través del servicio de Banca Electrónica que no sean reconocidas por sus Usuarios y que, al menos, incluya la información relacionada con operaciones no reconocidas por los Usuarios y el trámite que, en su caso, haya promovido el Usuario, tales como folio de reclamación, fecha de reclamación, causa o motivo de la reclamación, fecha de la operación, cuenta origen, tipo de producto, servicio de Banca Electrónica en el que se realizó la operación, importe, estado de la reclamación, resolución, fecha de resolución, monto abonado, monto recuperado y monto quebrantado.

La información anterior deberá mantenerse en la Institución durante un periodo no menor a cinco años contado a partir de su registro, sin perjuicio de otras disposiciones que resulten aplicables.

ARTÍCULO 316 Bis 15.- Las Instituciones deberán generar registros, bitácoras, huellas de auditoría de las operaciones y servicios bancarios realizados a través de Medios Electrónicos y, en el caso de Banca Telefónica Voz a Voz, adicionalmente grabaciones de los procesos de contratación, activación, desactivación, modificación de condiciones y suspensión del uso del servicio de Banca Electrónica, debiendo observar lo siguiente:

I. Las bitácoras deberán registrar cuando menos la información siguiente:

a) Los accesos a los Medios Electrónicos y las operaciones o servicios realizados por sus Usuarios, así como el acceso a dicha información por las personas expresamente autorizadas por la Institución, incluyendo las consultas efectuadas.

b) La fecha y hora, número de cuenta origen y Cuenta Destino y demás información que permita identificar el mayor número de elementos involucrados en el acceso y operación en los Medios Electrónicos.

c) Los datos de identificación del Dispositivo de Acceso utilizado por el Usuario para realizar la operación de que se trate.

d) En el caso de Banca por Internet, deberán registrarse las direcciones de los protocolos de Internet o similares, y para los servicios de Banca Electrónica en los que se utilicen Teléfonos Móviles o fijos, deberá registrarse el número de la línea del teléfono en el caso de que esté disponible.

Las bitácoras, incluyendo las grabaciones de llamadas de Banca Telefónica Voz a Voz, deberán ser almacenadas de forma segura por un periodo mínimo de ciento ochenta días naturales y contemplar mecanismos para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

Las bitácoras a que se refiere la presente fracción, deberán ser revisadas por las Instituciones en forma periódica y en caso de detectarse algún evento inusual, deberá reportarse a los Comités de Auditoría y de Riesgos, conforme se establece en el último párrafo del Artículo 316 Bis 19 de las presentes disposiciones.

II. Deberán contar con mecanismos para que la información de los registros de las bitácoras en los diferentes equipos críticos de cómputo y telecomunicaciones utilizados en las operaciones de Banca Electrónica sea consistente.

La información a que se refiere el presente Artículo deberá ser proporcionada a los Usuarios que así lo requieran expresamente a la Institución mediante sus canales de atención al cliente, en un plazo que no exceda de diez días hábiles, siempre que se trate de operaciones realizadas en las propias cuentas de los Usuarios durante los ciento ochenta días naturales previos al requerimiento de la información de que se trate. En caso de grabaciones de voz no se entregará copia de la grabación, solo se permitirá su audición, debiendo proporcionar una transcripción de la misma si es requerida por el Usuario.

En el presente caso, la parte actora desconoció los cargos o disposiciones a terceros que aparecen en su cuenta, y si bien es cierto que las instituciones de crédito pueden pactar con sus cuentahabientes que determinadas operaciones bancarias se realicen vía internet por computadora; mediante teléfono celular inteligente (Smartphone); o cajeros automáticos, para lo cual deben proporcionar datos únicos y exclusivos que pueden consistir en usuarios, claves, contraseñas (como el NIP) e, incluso contraseñas dinámicas (como el token), a efecto de arrojarle la carga de la prueba al usuario, el banco primeramente debe demostrar que la plataforma donde se ejecutó la operación es fiable y segura, y que existe certeza de que una transacción sólo se realizará si se ingresan los datos correctos, y no pueda tratarse de un fraude electrónico.

Pues sólo de ese modo, es posible revertir la carga de la prueba al usuario bancario para que acredite que los mensajes de datos de la

operación que se controvierta no fueron realizados por él; por su autorizado o por un sistema de información que programó para actuar en su nombre automáticamente.

Sirve de apoyo a lo anterior el siguiente criterio jurisprudencial:

Época: Décima Época Registro: 2017826 Instancia: Tribunales Colegiados de Circuito Tipo de Tesis: Jurisprudencia Fuente: Gaceta del Semanario Judicial de la Federación Libro 58, Septiembre de 2018, Tomo III Materia(s): Civil Tesis: (IV Región)1o. J/13 (10a.) Página: 2222

PRESUNCIONES LEGALES PREVISTAS EN LOS ARTÍCULOS 90, 90 BIS Y 95 DEL CÓDIGO DE COMERCIO. PARA QUE OPEREN A FAVOR DE LAS INSTITUCIONES BANCARIAS Y SE ARROJE LA CARGA DE LA PRUEBA A LOS USUARIOS, DEBEN ACREDITAR PREVIAMENTE QUE LA PLATAFORMA DONDE SE EJECUTÓ LA OPERACIÓN ES FIABLE Y SEGURA. *Las instituciones de crédito pueden pactar con sus cuentahabientes que determinadas operaciones bancarias se realicen vía Internet por computadora; mediante teléfono celular inteligente (smartphone); o en cajeros automáticos, para lo cual deben proporcionar datos únicos y exclusivos que pueden consistir en usuarios, claves, contraseñas (como el NIP) e, incluso, contraseñas dinámicas (token). Entonces, cuando una transacción electrónica se ejecuta con éxito, de conformidad con los artículos 90, 90 Bis y 95 del Código de Comercio surge la presunción de que se realizó, porque el cuentahabiente ingresó la información correcta para ese efecto, sea que lo haya efectuado personalmente, por conducto de su autorizado o mediante un sistema de información programado para actuar en su nombre automáticamente; sin embargo, para que esta presunción opere a favor de la institución de crédito, de conformidad con el artículo 90 Bis citado, debe acreditar previamente que la plataforma donde se ejecutó la operación es fiable y segura, y que existe*

certeza de que una transacción sólo se realizará si se ingresan los datos correctos, y no pueda tratarse de un fraude electrónico, de ese modo se revertirá la carga de la prueba al usuario bancario para que acredite que los mensajes de datos de la operación que se controvierta no fueron realizados por él; por su autorizado o por un sistema de información que programó para actuar en su nombre automáticamente. Lo anterior, puede demostrarse, por ejemplo, con el dictamen de un experto en materia informática que dirima si la plataforma donde se realizó la operación bancaria es fiable y segura por contar con un procedimiento que única e invariablemente autorizará una transacción cuando se ingresen los datos correctos requeridos (usuarios, claves, NIP, contraseñas dinámicas, etcétera), y no por diversas intervenciones informáticas.

PRIMER TRIBUNAL COLEGIADO DE CIRCUITO DEL CENTRO AUXILIAR DE LA CUARTA REGIÓN.

Aunado a lo anterior, es la institución de crédito la que tiene a su alcance mayores elementos para acreditar la realización de las operaciones de transferencias bancarias y disposiciones en efectivo y, en su caso, la existencia de las autorizaciones correspondientes, así como la fiabilidad del proceso informático.

Entonces, no basta la simple afirmación acerca de que las operaciones se llevaron a cabo con el uso de las claves y contraseñas del titular de la cuenta, sino que es menester demostrar, primero, que aquellas operaciones se llevaron a cabo empleando las claves, nips, contraseñas, token o E-Llave, y, segundo, que el sistema en el que se ingresaron tales datos, es confiable.

Al efecto, para que la parte demandada agote la carga de la prueba que le asiste, de probar que la transferencia impugnada fue autorizadas por la actora, debe exhibir los certificados digitales que avalen el uso de la firma electrónica, claves, contraseñas (como el NIP), e incluso, contraseñas dinámicas (token, E-Llave), siendo insuficientes para ese efecto

las impresiones de pantallas o alguna otra, de las cuales se advierta la información general de las operaciones y sus número de autorización respectivos, pues estas documentales carecen de los elementos necesarios para autentificar los mensajes de datos comunicados e identificar a las partes en la utilización de medios electrónicos.

Ahora bien, la parte demandada ofreció como prueba de su parte las documentales, consistentes en la copia del contrato del cual derivan las prestaciones reclamadas por la actora, así como el acuse de recibo del dispositivo TOKEN, y el documento denominado auto-registro a ********** los cuales, como ya se dijo, no resultan ser elementos de prueba suficientes a fin de demostrar la fiabilidad de las plataformas que se utilizan vía electrónica o por internet.

Se ofrecieron también las documentales consistentes en la impresión del Estado de cuenta de mes de marzo de dos mil veinte, de la cuenta de la actora, así como los datos de las transferencias realizadas, sin embargo, de dichas documentales solamente se desprende que se realizaron los movimientos desconocidos, más no dan la certeza de que los mismos hayan sido efectivamente realizados por la actora, ni mucho menos hacen prueba de la confiabilidad del uso del sistema, mismo efecto que tiene la impresión del comprobante electrónico de pagos que se generó con motivo de la transferencia no reconocida y la bitácora de operaciones.

De igual manera, las partes ofrecieron como prueba de su parte la pericial en informática, para lo cual la parte actora nombró como perito de su parte a la licenciada **********, quien emitió su dictamen y obra en autos a fojas de la *quinientos treinta y cinco* a la *quinientos cuarenta y cuatro* de los autos, llegando a la conclusión de que no se observaron las debidas medidas de seguridad en la plataforma de la institución, señalando además lo siguiente:

“No es posible advertir que el sitio del que dice la oferente de la prueba que corresponde a su sistema de banca en línea cuenta

con mecanismos de seguridad, ni tradicionales como el uso de la contraseña o token, ni biométricos, porque no se pudo establecer si cuenta con certificado de seguridad SSL por la ausencia de la dirección URL al momento de ofrecer la prueba. Las bitácoras registran la realización de tres transferencias bancarias con número de folio 25070885975, 25070886497 y 25070886885, todas ellas que dicen ser del nueve de marzo de dos mil veinte; no obstante dentro de dichas bitácoras no se advierte que haya sido el actor quien haya dado las instrucciones para elaborar las transferencias bancarias ni existe un campo relacional entre la tabla que registró las transferencias y las que registró el uso de la llave token por lo que no se puede concluir que con determinado inicio de sesión se hicieron las transferencias o inclusive si había una sesión abierta al momento en que fueron elaboradas. Se advierte que el oferente de la prueba reconoce que el personal del banco tiene conocimiento de la contraseña y datos sensibles que deberían pertenecer únicamente a la actora porque incluso pidió que el análisis de los registros fuera en su sede, lo que representa una situación de riesgo y vulnerabilidad que no permite asegurar la confiabilidad de los registros; además de los documentos adjuntos y según me fue indicado, se aprecia que existen más mecanismos informáticos inclusive distintos a la interacción del actor para efectuar disposiciones electrónicas, dichos mecanismos ya han quedado indicados en el cuerpo del presente dictamen como lo es a través de los cajeros automáticos, disposiciones por ventanillas, banca por teléfono y banca en línea, por lo que las operaciones de la banca en línea no son exclusivas para la elaboración de las transferencias. En ese sentido, se concluye final y toralmente que de los registros y de la información que tuve a la visa dentro del expediente en que actúo no se advierte situación alguna que dentro de la técnica informática permita concluir que la actora fue quien realizó las operaciones de transferencia bancaria al no tener registro las bitácoras de la contraseña ingresada ni su cotejo para determinar la

autenticación del inicio de sesión con el que supuestamente se efectuaron las transferencias."

Por su parte, la demandada nombró como perito al Ingeniero **********, quien emitió su dictamen y obra en autos a fojas de la *quinientos doce* a la *quinientos treinta y cuatro* de los autos, y quien llega a la siguiente conclusión:

*"La criptografía de seguridad y claves de seguridad empleadas por ********** cumple los parámetros normativos y contractuales para prestar el servicio de banca electrónica por Internet, por lo que los datos se mantienen confidenciales para el cliente durante la transmisión de datos dentro del sitio web del servicio de banca electrónica. Las medidas de seguridad visibles en el sitio web **********cumple con las medidas de seguridad necesarias e indispensables para que sus usuarios de banca electrónica puedan ingresar su firma electrónica de forma segura. La realización del alta de cuenta destino y transferencias de banca electrónica se habilita mediante el uso de la firma electrónica del cliente, misma que es de carácter confidencial, y por ende son ejecutadas por el banco demandado conforme al instructivo que recibe el cliente al efecto. Todas las operaciones fueron confirmadas con el token con número de serie **********que fue asignado al usuario administrador de nombre **********. Existe constancia electrónica que confirma las razones por las que el sistema bancario obedeció la orden de alta de cuenta y transferencias, conforme al pacto entre las partes, y por ende, en lo que a la interpretación informática que me corresponde, son responsabilidad de la parte actora, quien tras digitar su firma electrónica ya sea de propia mano o por su instrucción a un tercero, ingresó al sistema para realizar los movimientos objeto de la litis."*

En virtud de la contradicción de los dictámenes rendidos por los peritos de las partes, se nombró como perito tercero en discordia al Maestro **********, quien emitió su dictamen y obra a fojas

de la *seiscientos treinta y dos* a la *seiscientos cincuenta* de los autos, quien llegó a la siguiente conclusión:

*"No advertí de algún registro que generé certeza para determinar la atribución y así emitir cabalmente mi dictamen de que el C. **********, administrador único de la sociedad denominada **********., haya expresado su consentimiento, voluntad y autorización de ejecución respecto de todas y cada una de las operaciones electrónicas ahora en controversia.*

*Esto porque al analizar cada uno de los documentos que forma parte del expediente de esta litis, solo puedo advertir, con la revisión y análisis de estados de cuenta, "logs" o registros de operaciones y movimientos supuestamente extraídos de los sistemas "**********", de la existencia de operaciones de transferencia de fondos bancarios efectuadas a través de la cuenta asociada a la empresa **********., a través de los procedimientos previstos por parte de "**********", sin embargo en ninguno de los documentos abalizados me ofrece los elementos suficientes para determinar que **********, administrador único de la parte actora, haya sido quien efectuó, consintió y autorizó todas y cada una de las operaciones registradas: inicio de sesión, alta de cuentas y las transferencias bancarias, exhibidos en los "logs" supuestamente extraídos del sistema de información de "**********", pues se insiste que es necesario tener a la vista al servidor que contiene los sistemas electrónicos originales del banco para poder determinar lo relativo.*

Por otro lado, los peritos emitieron la reproducción verbal de sus dictámenes en audiencia de juicio, además de someterse al interrogatorio que les formularon las partes.

Ahora bien, procediendo a valorar los dictámenes emitidos, esta autoridad le otorga pleno valor probatorio al realizado por el

perito tercero en discordia, Maestro **********, toda vez que se aprecia que es el dictamen más completo, pues desde un inicio indicó los elementos que tomaría como base y con lo que contaba para emitir sus conclusiones, señaló los estudios e investigaciones que tuvo que realizar, plasmó el estudio de campo que realizó señalando que hizo pruebas a fin de verificar el funcionamiento del sistema de banca en línea proporcionado por la demandada. Es un dictamen explicado en términos técnicos pero además en terminología sencilla accesible a cualquier persona que no tenga conocimientos de la materia, lo anterior convierte su dictamen en un documento práctico y de fácil discernimiento. Además, de ser un dictamen ilustrativo con esquemas fotografías y diagramas de flujo, con lo que conducen a un mejor entendimiento del problema y la forma en que se desarrolla el uso de una banca en línea.

Así, en cada uno de los planteamientos que va realizando el perito de alguna y otra foja lo va explicando, esquematizando o ilustrando, siendo de especial relevancia la forma en que aporta el conocimiento para evidenciar cómo en el caso concreto se materializó una vulneración al sistema informático en el cual la parte actora fue perjudicada, lo que queda claramente esquematizado sobre todo a fojas *seiscientos treinta y tres* a *seiscientos treinta y cuatro,* mediante la reproducción de diseños o esquemas, donde se va indicado, dentro del proceso de utilización del servicio en línea, cada uno de los movimientos que se hacen.

Además de lo anterior, el perito, al emitir su exposición verbal en audiencia de juicio de fecha once de marzo de dos mil veintidós, expuso la forma en que se presentaba la vulnerabilidad, cómo el ciberataque se actualizó en el presente caso, pues concluyó que no existen elementos que lleven a la convicción de que fue la propia parte actora, quien haya realizado los movimientos, dado que existe la posibilidad de que el portal fue ingresado por dos IP distintas, dos usuarios distintos y que el propio sistema electrónico

del banco en cuanto a su estructura permitió la intromisión indebida en la cual se realizó un movimiento bancario ilegal.

Por lo anterior y con fundamento en lo dispuesto por el artículo **1301** del Código de Comercio, se le otorga pleno valor probatorio al peritaje emitido por el perito tercero en discordia.

Cabe señalar que no se le otorga el mismo valor al dictamen emitido por el perito de la demandada pues su dictamen aunque es ilustrativo y elaborado con técnica, es poco claro, resulta ser muy dogmático, sus conclusiones no tienen sustento habiendo sido formuladas en forma muy concreta, de modo que ofreciera alguna convicción en esta juzgadora.

Por lo que respecta al dictamen emitido por el perito de la actora, es un dictamen poco esquematizado, poco ilustrativo, aunque sí muestra una explicación clara, en términos entendibles, y que además al realizar su exposición en audiencia de juicio, la perito fue bastante clara y explicativa en su emisión, habiendo aportado conclusiones muy bien soportadas en razones y elementos objetivos, sin embargo a juicio de quien hoy resuelve, encuentra que el dictamen mejor elaborado y más convincente es el del perito tercero en discordia.

Con lo anterior queda de manifiesto que existió una vulnerabilidad en la seguridad del uso del portal en línea, pues es claro un movimiento anormal y en el cual la seguridad bancaria no se activó para verificar la autenticidad del usuario y sus movimientos.

Ahora bien, la parte actora ofreció como prueba de su parte la documental en vía de informe a cargo de la Comisión Nacional Bancaria y de Valores, documento que merece pleno valor probatorio en términos de lo dispuesto por el artículo **1292** del Código de Comercio, y en el cual se señala que los artículos **316 Bis 10** y **Bis 11**, son vinculantes para las instituciones bancarias y les establece las obligaciones que deben asumir para garantizar la seguridad a los usuarios en el servicio de Banca Electrónica.

Entonces, de dichos artículos deviene la obligación de las instituciones bancarias de garantizar a los usuarios de servicios financieros la seguridad del uso de servicio de banca electrónica, por lo tanto, cualquier irregularidad o vulnerabilidad del servicios debe ser resarcido por la propia institución.

Sirve de apoyo además, el siguiente criterio jurisprudencial:

TESIS JURISPRUDENCIAL 17/2021 (10a.)

TRANSFERENCIAS ELECTRÓNICAS BANCARIAS. CUANDO SE RECLAME SU NULIDAD, CORRESPONDE A LA INSTITUCIÓN BANCARIA DEMOSTRAR QUE SE SIGUIERON LOS PROCEDIMIENTOS ESTABLECIDOS NORMATIVAMENTE PARA ACREDITAR SU FIABILIDAD.-

HECHOS: Los Tribunales Colegiados de Circuito contendientes sostuvieron posturas distintas respecto a quién correspondía demostrar, en un juicio de naturaleza mercantil, la fiabilidad del mecanismo por el cual se efectuaron transferencias electrónicas de recursos mediante la utilización de plataformas digitales; así, uno estimó que cuando el cuentahabiente niega haber dado su autorización al banco para realizar la transferencia y la institución de crédito afirma que sí recibió la instrucción, corresponde al primero demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad y, por tanto, que su cuenta saboteada electrónicamente; mientras que el otro sostuvo lo contrario, es decir, que corresponde a la institución bancaria soportar la carga probatoria de acreditar que las mismas se realizaron mediante el uso de los elementos de seguridad empleados para garantizar la certeza de las operaciones.

CRITERIO JURÍDICO: La Primera Sala de la Suprema Corte de Justicia de la Nación determina que no puede presumirse la fiabilidad de la banca electrónica a partir de la mera acreditación de que una transferencia se llevó a cabo utilizando un determinado mecanismo de autenticación por parte del usuario.- Al respecto, se establece que dicha presunción solamente se puede obtener una vez que la institución bancaria demuestre haber seguido el procedimiento exigido por las Disposiciones de Carácter General, aplicables a las Instituciones de Crédito, emitidas por la Comisión Nacional Bancaria y Valores.- En ese sentido, una vez acreditado que se siguió debidamente el procedimiento normativamente exigido de la institución financiera para la operación impugnada y que no se tuvo conocimiento de incidentes que comprometieran los

datos del cuentahabiente, sólo entonces la carga de la prueba se le revertirá al usuario quien tendrá el deber de desvirtuar lo aportado por aquélla.

JUSTIFICACIÓN: Las disposiciones aludidas establecen la previsión de contenidos mínimos para el funcionamiento de la banca electrónica tratándose de las transferencias de recursos, dentro de los que destacan: a) la introducción de mecanismos complejos de autenticación del usuario divididas en cuatro categorías; b) el establecimiento de operaciones con las cantidades dinerarias máximas que pueden llevarse a cabo bajo determinado medio de autenticación; c) la necesidad de registrar previamente las cuentas de destino, así como el periodo mínimo que debe transcurrir antes de poder realizar la transferencia, según sea el caso; y, d) la obligación de generar comprobantes y notificar al usuario de las transacciones.- Sin embargo, a partir de que actualmente se conocen diversas maneras de poder obtener fraudulentamente datos de los clientes o vulnerarse contenido electrónico para realizar operaciones sin el consentimiento de los usuarios, la presunción en el sentido de que las transferencias mediante mecanismos electrónicos son infalibles no puede prosperar, por lo que no es posible trasladar, en un primer momento, la carga de la prueba al usuario del servicio; máxime si se considera la tecnicidad de los sistemas digitales por medio de los cuales se presta el servicio de la banca electrónica lo que representa un obstáculo excesivo a efecto de que el usuario del servicio pudiera demostrar su pretensión, además de que el banco es quien cuenta con la infraestructura necesaria para generar la evidencia presentada ante los órganos jurisdiccionales. De manera tal que la institución financiera es quien debe acreditar que los procedimientos de identificación que fueron utilizados durante la transacción y que fueron acordados con el usuario se emitieron correctamente, además de la fiabilidad del procedimiento que se utilizó para autorizar la transacción.- Consecuentemente, una vez acreditado que se siguió el procedimiento normativamente exigido de la institución financiera para la operación impugnada y que no se tuvo conocimiento de incidentes que comprometieran los datos del cuentahabiente, sólo entonces la carga de la prueba se revertirá al usuario quien tendrá el deber de desvirtuar lo aportado por aquélla, sin que lo anterior implique la imposición a los bancos de una carga imposible consistente en la demostración de la fiabilidad abstracta de todo su sistema ante cualquier tipo de riesgo, sino sólo de aquellos que se pudieran llegar a materializar.

Contradicción de tesis 206/2020. Entre las sustentadas por el Primer Tribunal Colegiado en Materia Civil del Décimo Sexto Circuito y el Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito.17 de marzo de 2021. Cinco votos de las Ministras Norma Lucía Piña Hernández, Ana Margarita Ríos Farjat, y los Ministros Juan Luis González Alcántara Carrancá, Jorge Mario Pardo Rebolledo y Alfredo Gutiérrez

Ortiz Mena. Ponente: Jorge Mario Pardo Rebolledo. Secretario: Jorge Arriaga Chan Temblador. Tesis y/o criterio.

En tal orden de ideas, y con las pruebas que han sido valoradas, la demandada no acreditó la confiabilidad del sistema de uso de los servicios y, por lo tanto, que los movimientos objetados en forma cierta hubieren sido autorizados por la actora, razón por la cual resulta procedente la acción que ejercitó **********.

VII.- Por lo anterior, se declara procedente la Vía Oral Mercantil en que promovió **********, en contra de **********.

En este orden de ideas, se concluye que quedó probada la acción ejercitada por la parte actora ********** en contra de **********.

Se condena a ********** a realizar la restitución de la cantidad de **DOSCIENTOS TREINTA Y OCHO MIL DOSCIENTOS PESOS** por concepto de cargos no reconocidos ni autorizados, realizados en fecha *nueve de marzo de dos mil veinte* **.**

De conformidad con lo expuesto por el artículo **1084** del Código de Comercio, no se hace especial condena en costas, toda vez que del sumario no se advierte que la parte demandada se hubiera conducido con temeridad o mala fe, por lo que cada una de las partes deberá absolver sus propios gastos y costas.

Por lo anteriormente expuesto y con fundamento en lo que disponen los artículos **1390 Bis y correlativos** del Código de Comercio, es de resolverse y se resuelve:

PRIMERO.- La suscrita Juez es competente para conocer de este asunto.

SEGUNDO. - Se declara procedente la vía **ORAL MERCANTIL.**

TERCERO. - Se declara que **********, probó la acción ejercitada en el presente juicio.

CUARTO.- Se condena a ********** ********** a restituir a **********, la cantidad de **DOSCIENTOS TREINTA Y OCHO MIL DOSCIENTOS PESOS** por concepto de cargos no reconocidos ni autorizados, realizados en fecha nueve de marzo del dos mil veinte.

QUINTO.- No se hace especial condena en costas.

SEXTO.- En términos de lo previsto en el artículo 73 fracción II, de la Ley General de Transparencia y Acceso a la Información Pública, misma que fue publicada en el Diario Oficial de la Federación el día trece de agosto de dos mil veinte, se ordena se proceda a la elaboración y publicación de la versión pública de la presente sentencia siguiendo lo establecido en los Lineamientos para la Elaboración de Versiones Públicas de Sentencias y Resoluciones dictadas por los Juzgados y Salas del Poder Judicial del Estado de Aguascalientes.

SÉPTIMO. - Notifíquese y cúmplase.

A S Í, lo sentenció y firma la Juez del Juzgado Quinto de lo Mercantil de esta Capital, Maestra **VERÓNICA PADILLA GARCÍA,** por ante

su Secretario de acuerdos, Licenciado **ÓSCAR REYES LEOS** que autoriza.- Doy Fe.

La sentencia que antecede se publica en fecha **veinticinco de marzo de dos mil veintidos.-** Conste.

L'VPG*Alex

de la Ley General de Transparencia y Acceso a la Información Pública, así como del trigésimo octavo de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, se suprimió: nombre de las partes, representantes legales, domicilios y demás datos generales, seguir el listado de datos suprimidos, información que se considera legalmente como confidencial o reservada por actualizarse lo señalado en los supuestos normativos en cita. Conste.