S E N T E N C I A

Aguascalientes, Aguascalientes, **a tres de marzo del dos mil veintidós.-**

V I S T O S, para resolver los autos del expediente número **0122/2021** 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, según se desprende del documento base de la acción, se estableció como lugar de pago esta ciudad de Aguascalientes, de donde deriva la competencia de esta autoridad.-

IV. - El actor ********** comparece a demandar a **********, por el pago y cumplimiento de las siguientes prestaciones:

*"**A)** Que por sentencia correspondiente se decrete la ilegalidad de las transferencias realizadas de la cuenta No. ********** a nombre de la empresa ********** con código de cliente **********,** siendo esta por **$490,00.00 (Cuatrocientos noventa mil pesos*

00/100 M.N) *en fecha de 09 de noviembre del 2020, misma que nunca fue autorizada ni efectuada por mi representada.*

B) *Para que, en consecuencia, se realice la devolución y/o pago de la cantidad total de* ***$490,00.00 (Cuatrocientos noventa mil pesos 00/100 M.N)*** *derivado de la transferencia mencionada anteriormente, al no haber sido ésta autorizada, ni efectuada en ningún momento por la parte que represento.*

C) *El pago del interés legal anual que corresponda a la cantidad de* ***$490,00.00 (Cuatrocientos noventa mil pesos 00/100 M.N)*** *ello calculado desde el 09 de noviembre del 2020 – fecha en que se realizaron los cargos que ahora se reclaman – hasta el pago total del adeudo, con fundamento en el numeral 362 del Código de Comercio.*

D) *El pago de los gastos y costas que se generen con motivo del presente juicio, lo anterior de conformidad con los artículos 1082, 1083, 1084, 1085 del Código de Comercio."* (Transcripción literal visible a fojas uno y dos de los autos).

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

VI.- El actor ********** basó sus pretensiones en que:

*"**1.** En fecha 05 de diciembre de 2017, mi representada* **********, *celebró un contrato con* **********, *para lo cual la Institución Crediticia le otorgó el número de cuenta empresarial número* **********así *como el código de cliente* ********, *tal y como se desprende el Contrato referido y el cual se anexa copia simple, manifestando al efecto que el original se encuentra en poder de la parte demandada, razón por la que solicito a Su Señoría* ***se sirva a requerir a la misma para que dentro del término de ley lo exhiba en la presente causa, lo anterior bajo apercibimiento que en caso de no hacerlo se le tendrán por ciertas las manifestaciones aquí vertidas.***

2. *El día 09 de noviembre del año 2020, al ingresar al portal de Banca Electrónica de la Institución Crediticia en cuestión, con el*

*usuario y contraseñas correspondientes a la C. **********, persona autorizada por mi representada para ingresar a dicho portal, ingreso esta con la finalidad de efectuar un pago a un proveedor por diversos productos vendidos a mi representada por la cantidad de $1,375,454.81 (Un millón trescientos setenta y cinco mil cuatrocientos cincuenta y cuatro 81/!00 M.N.) para lo cual se siguió el procedimiento normal dentro de la aplicación para efectuar dicho proceso, sin embargo al momento de intentar concluir el movimiento deseado pulsando la opción de "Enviar" y antes de ingresar la clave que el dispositivo TOKEN genera para poder realizar este tipo de operaciones, en ese momento el dispositivo electrónico con el cual se ingresó a la plataforma banca electrónica de la Institución Crediticia se apagó y efectuó un proceso de reinicio, lo cual resulto de manera extremadamente extraña a la C. ****** toda vez que esto jamás había ocurrido ni se había tenido problema alguno con dicho dispositivo electrónico anteriormente, lo anterior fue percibido por la C. ********** y la C. ********** quienes laboran con mi representada.*

3. *Una vez que el dispositivo volvió a funcionar, se volvió a ingresar a la aplicación de banca electrónica con la finalidad de efectuar el movimiento que se pretendía efectuar, sin embargo, una vez que se ingresó de nuevo el usuario y contraseña correspondiente y una vez que se ingresó la cuenta de mi representada, la C. ****** se percató que el saldo de la cuenta era menor al que se tenía antes del reinicio del dispositivo, siendo la cantidad faltante $490,00.00 (Cuatrocientos noventa mil pesos 00/100 M.N) haciendo énfasis en que dicha cantidad en ningún momento se intentó transferir a diversa cuenta, eliminando el supuesto de que el pago el cual se pretendía efectuar al proveedor antes mencionado si se hubiese realizado con éxito, así mismo en el transcurso en el que el dispositivo se apagó y reinició, se recibió una alerta en el correo de mi representada así como una llamada telefónica en la cual se informaba un movimiento en la Cuenta Empresarial número **********, de mi representada por la cantidad de $490,00.00 (Cuatrocientos noventa mil pesos 00/100 M.N) misma que fue realizada de la Cuenta Empresarial número ********** perteneciente a mi representada, sin haber sido este movimiento efectuado ni autorizado por mi representada o por persona autorizada para tal efecto, es por ello que desde ese momento se desconocieron dichas transferencias, así como las cuentas o destinatarios a los que se dirigieron las*

cantidades anteriormente mencionadas en la transferencia, es así que, en consecuencia de lo anterior, la institución bancaria demandada faltó tajantemente a lo establecido por el artículo 52 de la Ley de Instituciones de crédito, el cual sostiene lo siguiente:

[…]

Así también en los artículos 46 bis y 77 de la misma Ley, disponen lo siguiente:

[…]

De igual manera resulta aplicable lo mandado por el ejecutivo federal en los artículos 316 Bis 11, 316 Bis 14 y 316 Bis 15 de las Disposiciones de Carácter General aplicables a las Instituciones de Crédito, que citan:

[…]

*Así mismo, es importante señalar que el beneficiario de dicho movimiento (transferencia indebida) fue la cuenta CLABE de numero ********** de la Institución de Crédito **** y con un nombre del beneficiario solamente señalado como "*******" movimiento con la clave de rastreo ********** mismo que se manifiesta, no se reconoce y se expresa que no se cuenta con ningún tipo de relación entre mi representante y alguien con ese nombre o similares así como que no se cuenta con ninguna cuenta con ese número de cuenta registrada en los archivos de mi representada. Me permito anexar comprobante operación emitido por la Institución Crediticia en el cual se señala la operación indebida en cuestión.*

4.** Por este motivo y con la necesidad de aclarar el movimiento efectuado a la cuenta de mi representada, en fecha 10 de noviembre del año 2020 fue presentada la solicitud de aclaración ante los ejecutivo del ******* ********** la C. ********** y el C. ********** quienes para levantar la solicitud de aclaración de dicho movimiento solicitaron una captura del comprobante de la transacción así como un correo explicando la situación y solicitando la aclaración de la transferencia anteriormente mencionada, toda vez que mi representada les hizo saber que dicha transacción fue efectuada de forma indebida, sin consentimiento ni autorización de mi representada, así mismo se me hizo mención a través de los ejecutivos mencionados, que se procedería a bloquear mi cuenta con la finalidad de evitar más intromisiones a mi cuenta. Me permito*

anexar la carta en donde se solicita la aclaración así como la captura del comprobante de la transacción en cuestión.

5. *En virtud de la reclamación antes mencionada, el banco en fecha 18 de noviembre del 2020 mediante un correo electrónico proveniente del correo electrónico* ********** *informó a mi representada que la solicitud de aclaración realizada el día 10 de noviembre de 2020 quedo registrada en el sistema de la Institución Crediticia con el Folio I20-3287572 con los siguientes datos:*

[…]

Así mismo se hizo mención que la fecha compromiso para otorgar una respuesta final sobre la aclaración en cuestión sería a más tardar el día 08 de diciembre de 2020, me permito anexar una copia del correo electrónico en mención.

6. *En el mismo orden de ideas, en fecha 7 de diciembre de 2020, la Institución Crediticia hizo del conocimiento de mi representada mediante una carta, en la cual se informaba que la solicitud de aclaración con el Folio ********** era improcedente, dicha resolución según se menciona en el cuerpo de dicha carta, se tomó en base en que las transacciones inconformadas fueron supuestamente realizadas y autorizadas por el usuario autorizado, siendo que tal y como se ha mencionado a lo largo de la presente, estos movimientos efectuados no fueron autorizados por mi representada o por persona autorizada para tal efecto.*

7. *Es así que, con la finalidad de intentar obtener una respuesta favorable de la Institución Crediticia por otros medios, se presente una denuncia ante la Fiscalía General de la Republica a la cual se le otorgo el número de Carpeta de Investigación ********** en la cual mi representada denuncia los hechos narrados en la presente demanda, así mismo se presentó ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros una queja el día 05 de marzo de 2020 a la cual se le otorgo el número de expediente ********, buscando con esto, una solución a la negativa de la Institución Crediticia de hacerse responsable sobre los cargos efectuados indebidamente a mi cuenta, toda vez que dichos cargos no fueron efectuados por mi representante ni por persona autorizada para esto. Me permito anexar copias simples de dichos documentos mismos que serán corroborados con el informe que se solicitara a dichas dependencias en el apartado de pruebas.*

8. *Es el caso, que a la fecha de la presente demanda, y pese a diversas gestiones que fueron realizadas con la hoy demandada, no se ha beneficiado el cargo no reconocido y realizado de manera ilegal en la cuenta bancaria de mi representada. Por ello es que no vemos en la imperiosa necesidad de presentar formal demanda, a efecto de acreditar antes su Señoría, que mi representada no realizó, ni autorizó el cargo indebido que se relata en el presente escrito."* (Transcripción literal visible a fojas dos a la seis de los autos).

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

*"**AL HECHO 1.-** Se afirma por ser cierto, sobre la apertura de una cuenta de la cuenta empresarial de fecha 05 de diciembre dl 2017, dentro del cual se encuentra al Contrato de Deposito de Dinero a la vista y el Contrato de Uso de Medios Electronicos, siendo esta una de la formas de disponer su dinero, utilizando la Banca Electronica, al que se le asignó el número de cuenta ********** y código de cliente ********, es de exponer para todo efecto legal como se expone en el propio escrito de demanda se dice que la persona que tiene relación con la operación no reconocida lo es la C. **********, persona que esta autorizada por parte de la moral actora para el uso de la Banca Electrónica, quien tiene el número de cliente individual ********.*

*Afirmando por igual que se pactó como medios de disposición de plástico, disposición y banca electrónica, añadiendo que desde el momento de la celebración de la cuenta se le entregaron los medios de disposición como cheques, tarjeta y claves y contraseñas como sustituidas de la firma autógrafa, tal y como se advierte de la solicitud No. **********, autorizo el uso de medios electronicos para ingresar a **********, siendo en ese momento que se le ASIGNO LA CONTRASEÑA PARA INGRESAR A ESTE SISTEMA, y mediante solicitud correspondiente en fecha 31 de Agosto del 2020, se originó el acuse de recibo del Dispositivo Electrónico Token con número de serie **********, para ingresar a ********** y todos los canales que ********* ponga a su disposición y acepto como firma autografa los medios de autentificacion y el uso de claves de acceso establecidos en el Contrato de Uso de Medios Electronicos, en terminos de lo*

dispuesto por el Articulo 316 Bis 1 de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito.

*En dichos tramites al cliente proporciono su número de celular y correo electrónico, para llevar a cabo la autentificación del uso del sistema de Banca por Internet, siendo el número dado de alta el de *********, y el correo **********.*

Cabe señalar que dentro del contrato celebrado y al que hace referencia a la parte actora, se hizo constar el Contrato de Depósito Bancario de Dinero a la vista, este se regula de conformidad con lo que establece en la Sección Primera, Clausula I.4 y I.8 del Contrato señalado que establece:

[…]

***AL HECHO 2.-** Se desconoce por n ose un hecho propio, ya que es un acto realizado por la actora.*

*Afirmamos por otro lado, que la C. ********** es autorizada para operar la banca electrónica de la actora.*

En este mismo tenor se acepta como confesión expresa, la manifestación en que la usuaria tiene las credenciales, claves, y contraseñas para operar la Banca Electrónica.

Niego el resto del hecho por no ser propio, ni tener antecedente de nuestra representada, además de que no se tiene antecedente de que el token se haya reiniciado, ni mi representada registró alguna incidencia con el dispositivo.

***AL HECHO 3.-** Con relación a hecho 3 que se contesta, se niega en la forma en que lo plantea la parte actora.*

Refiere que el dispositivo token dejo de funcionar, pero lo cierto es que, en los sistemas de nuestra representada no se encontró incidente alguno por ende se niega este hecho y lo que tenga relación con ello.

*Con relación a que una vez que ingresó las credenciales de acceso la C. ********** se percató de un faltante por transferencia por la cantidad de $490,000.00 (Cuatrocientos noventa mil pesos 00/100 M.N.), se niega por no ser un hecho propio, aunque se afirma que sí existió la transferencia pero es falso que se haya realizado sin el consentimiento de la parte actora de ilegal, ya que en los sistemas de nuestra representada se*

vincularon las claves y contraseñas con la cuenta del usuario, lo que validó el movimiento que ahora reconoce.

*En este mismo apartado, se niega que la actora esté en condiciones de negar el alta de la cuenta, pues el día 27/10/2020 a las 09:16:20 horas se dio de alta la Cuenta Interbancaria ********** se utilizó el Token*

Más como se observa de la imagen obtenida de los sistemas electrónicos de mi representada, la cuenta fue dada de alta desde el 27 de Octubre del 2020, mientras que la operación no reconocida se realizó el 09 de noviembre del 2020, esto es, 14 días previos a la transferencia no reconocida y sobre todo que se hizo desde una IP de uso frecuente del actor, entonces, son invalidas las afirmaciones de la actora en los hechos narrados, pues es una constante que la realidad de los hecho no es conforme con la narración del escrito de demanda, ya que todo lo hace desprender de un momento en que dice que el token se reinició y luego sorpresivamente se realizó una operación no reconocida, cuando lo cierto es que la cuenta destino fue dada de alta con 14 días de anticipación a la transferencia y desde una terminar IP de uso frecuente de la actora, por ende sus manifestaciones son inválidas y sujetos a prueba atento a que existe evidencia de mi representada que se contrapone a la narración de los hechos.

Por igual, son inexactas e inconducentes, las conclusiones señaladas n cuanto que mi representada faltó a las medidas de seguridad, ya que los sistemas de nuestra representada o registran incidentes en este sentido, además de que ya está afirmando la propia actora que la usuaria autorizada con claves y contraseñas accedió a la banca electrónica, luego, estando acreditado el uso y legalidad del acceso, y siendo inconveniente solo el token, le corresponde a la parte actora demostrar que sucedieron los hechos en que sustenta su acción.

Con relación al último párrafo del hecho que se contesta, se afirma solo en cuanto a la existencia de la cuenta destino, pero cabe exponer que nuestra representada por igual desconoce el beneficiario, ya que quien llena los datos en el portal de Banco de México por el cual se realiza el SPEI es el usuario o cuentahabiente y lo realiza desde el portal de la página de internet.

***AL HECHO 4.-** Mi representada solo está en condiciones de afirmar la existencia de la aclaración la cual fue debidamente atendida e investigada con el efecto de determinar la veracidad de los hechos, resultando*

improcedente la aclaración en virtud de los antecedentes y la forma de ejecución de la operación no reconocida.

AL HECHO 5.- *Se afirma por ser cierto, al registrar la aclaración en los sistemas de mi representada y a la cual se le dio el seguimiento conducente.*

AL HECHO 6.- *Se afirma por ser cierta la circunstancia de que nuestra representad dio contestación a la aclaración presentada, declarando improcedente porque se realizó con las credenciales de acceso y los elementos que constituyen la firma electrónica que son responsabilidad de la actora.*

Cabe exponer que de la investigación se obtuvieron la siguiente información:

[…]

*Intervinientes en la cuenta **********:*

[…]

Alta a Banca Electrónica

*LA empresa se dio de alta a Banca Electrónica con número de contrato ********** el 5 de diciembre de 2017, tal como se acredita en la copia de contrato enlace.*

[…]

*Se realizó comparación de firmas de la INE del cliente, así como la presentada en el contrato enlace ********** y en la cuenta ********** del señor **********, donde se observa que la firma es similar entre sí:*

[…]

*Las transferencias fueron realizadas por el ********** a nombre de **********, quien tiene facultades en el contrato enlace **********.*

*De acuerdo a Sistema Bet, la señora ********** cuenta con facultades en el contrato enlace.*

[…]

*El número de token con el cual se realizaron las operaciones es el **********, se cuenta con copia del acuse de recibo de token con fecha 31 de agosto del 2020.*

[…]

*Se realizó comparación de firmas de la INE del cliente, así como la presentada en el acuse de recibo token de la señora **********, donde se observa que la firma es similar entre sí.*

[…]

Del catálogo de conceptos, se validaron en nuestra bitácora los códigos correspondientes, sin embargo no se identificaron coincidencias.

[…]

De la revisión del log enviado por CISO en el periodo 7 de septiembre al 9 de noviembre del 2020, se identifica que el cliente utiliza su banca electrónica con frecuencia, sin embargo, no hay bloqueo y desbloqueo de token.

[…]

En sistema 390 el correo que se tiene registrado es el siguiente:

[…]

*El correo electrónica **********está registrado en sistema de 390 con fecha 1 de septiembre de 2020 ya través de la sucursal ****, como se observa:*

[…]

El cliente dio de alta el siguiente teléfono:

*Teléfono ********** está registrado en la Institución con fecha 1 de septiembre de 2020 a través de la sucursal **** y no cuenta con modificaciones.*

[…]

*El día 27/10/20 a las 09:16:20 horas se dio de alta la Cuenta Interbancaria ********** se utilizó el Token Físico* ***********

*Notificación al teléfono ********** y al correo ********** el alta de ambas cuentas.*

[…]

*La transferencia de la cuenta **********, por un porte total de $490,000.00, se realizó 13 días después de que se diera de alta la cuenta, de acuerdo al siguiente detalle:*

[…]

*Se identifica que transferencia por el importe total de $490,000.00, se realizó a través del canal ********** por el usuario 34136257 a nombre de ********** quien tiene facultades en el contrato enlace.*

[…]

Es necesario puntualizar que para llevar a cabo las transferencias de dinero, es necesario contar con el usuario, contraseña y token, el usuario y contraseña se asignaron desde la celebración del contrato y las cuales se utilizaron para solicitar y activar el token, como se dijo anteriormente, además de que se utilizo una medida de seguridad adicional, como es el envio de un codigo de autentificacion que se envió via SMS al numero celular registrado por el cliente y el cual servio para identificar que efectivamente nuestro cliente estaba solicitando la activación del OTP o TOKEN móvil.

Adicionalmente se le enviaron al cliente notificaciones de las operaciones realizadas, como fue la solicitud del OTP o TOKEN, el alta de la cuenta del tercero para transferencia y la propia transferencia, notificaciones que el cliente acepto y se obligo a las consecuencias del mismo, pues en estas se le informaba sobre las operaciones y no reporto nada irregular al banco, por lo que, conforme al principio ontologico de la prueba, las cosas ocurrieron de manera normal.

Por lo tanto que el actor como cuentahabiente era el único que estaba en condiciones de realizar las operaciones no reconocidas, puesto que nuestra representada sostiene que los movimientos se efectuaron a través de los medios electrónicos que quedaron a disposición del actor, haciendo uso de la firma electrónica digitando claves y contraseñas así como el Número de Identificación personal que estaba al alcance del actor y que sustituye la firma electrónica, vinculada con los sistemas de quien represento, así esos elementos de disposición quedaron bajo la responsabilidad del actor eximiento de toda obligación al Banco demandado.

***AL HECHO 7.-** Se niega por no ser propio, que la actora haya presentado la denuncia ante la Fiscalía General de la República, pues no se tiene antecedentes de este acto ni ha intervenido en la Carpeta correspondiente.*

Por otro lado, es cierto en cuanto a que se integró Queja que fue presentada ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros CONDUSEF; por lo que se ratifica la

contestación emitida por mi poderdante ante dicho organismo, más sin embargo, resulta menester señalar que las actuaciones llevadas ante dicha comisión no prejuzgan sobre la procedencia de la acción ni de las pretensiones de la parte actora, pues este obedece al rendido ante una autoridad administrativa (Condusef), que no tiene facultades jurisdiccionales, para determinar si está debidamente fundado o motivado, o si tiene deficiencias.

En tal sentido las actuaciones ante un órgano administrativo, en ningún momento implican que sea procedente la obligación que supuestamente pretende imputar a mi poderdante la parte actora, motivo por el cual se deduce que en ningún momento la actora con las documentales exhibidas hacen prueba de la existencia de una obligación por parte de mi representada, únicamente acredita que se inició una reclamación y nada más, por lo tanto, niego derecho alguno a la actora a pretender de mi representada las prestaciones que reclama y el rembolso de la cantidad que indica en su escrito inicial de demanda.

Lo anterior se robustece con el siguiente criterio jurisprudencial que me permito transcribir a continuación:

[…]

El sustento de la contestación a este hecho se acredita con los documentos que fueron aportados por el actor relativos a la reclamación ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), mismos que no obran al alcance de nuestra representada pero que bajo el principio de adquisición procesal de la prueba los hacemos nuestros y nos remitimos a su contenido como a las pruebas ofrecidas para justificar lo antes manifestado.

***AL HECHO 8.-** No es cierto, que exista obligación de paso alguno a favor del actor, por las razones antes expuestas. Además de que ello constituye una petición más que una imputación de un hecho, y entonces le corresponde la carga de la prueba.*

No existió cambio de claves, y en dado caso se las proporciono a un tercero.

No existió cambio de claves, y en dado caso se las proporciono a un tercero.

No existió cambio de claves, y en dado caso se las proporciono a un tercero.

Niego cualquier otro hecho al que no me hay referido implícita o explícitamente." (Transcripción literal visible a fojas ciento veintiséis a ciento treinta y dos de los autos)

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

Demanda

**********, a fin de que se le restituya la cantidad de CUATROCIENTOS NOVENTA MIL PESOS derivado de una transferencia electrónica que desconoce porque no la realizó, cantidad que fue ingresada a una cuenta de un tercero quien se encontraba dado de alta como "*******", con un número de rastreo **********.

Por su parte la demandada señala que no tiene ninguna responsabilidad, en virtud de que en ningún momento intervino en la operación y que la misma la realizó la propia actora, haciendo uso de su sistema interbancario y mediante la utilización de las contraseñas y números de token de los que sólo ella dispone señalando además que a fin de realizar la operación, es necesario ingresar el número de seguridad que proporciona el dispositivo electrónico (TOKEN) así como el número de contraseña que únicamente es conocido por la actora.

Ahora bien, en el presente caso, cabe señalar que ambas partes reconocieron la existencia de los contratos por medio de los cuales se otorgó a la parte actora el uso del token, además de que no fue motivo de controversia la realización del movimiento, es decir, la disposición de la cantidad que se es reclamada.

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.

Ahora bien, en el presente caso, la parte actora desconoció el cargo o disposición a terceros que aparecen en su cuenta, y si bien es cierto 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 FAVORDE 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 o token 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), 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 hoja de datos de Cuenta Empresaria, y la solicitud de servicio de Banca Electrónica, así como el acuse de recibo del dispositivo TOKEN, los cuales como ya se dijo, aun afirmándose la existencia de dichos documentos y su contenido, 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 original del Estado de cuenta de mes de noviembre del dos mil veinte,

sin embargo del mismo solamente se desprende que se realizó el movimiento que se desconoce más no dan la certeza de que el mismo hubiere sido realizado 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.

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 licenciada DELIA ROSA GARCÍA FLORES, quien emitió su dictamen y obra en autos a fojas de la quinientos veintisiete a la quinientos cuarenta y dos de los autos, en el cual la perito llega 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 ni analizar algún sitio del que dic ela oferente de la prueba que corresponde al sistema de banca en línea ni se 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 una transferencias bancarias por la cantidad de $490,000.00 (Cuatrocientos noventa mil pesos 00100 M.N.) todas ellas que dicen ser del nueve de noviembre del 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 nombró como perito al Ingeniero CÉSAR JAVIER LARA TRUJILLO, quien emitió su dictamen y obra en autos a fojas de la cuatrocientos sesenta y tres a la quinientos veintiséis de los autos, y quien llega a la siguiente conclusión:

"El proceso de autenticación a nivel de la validación de la contraseña es una tarea que se realiza de manera automática, en tiempo real y sin la intervención de ningún ser humano como parte inicial del proceso esta su captura en el campo determinado para tal fin, ello dentro del sistema "ENLACE" BET, su enmascaramiento otorga un nivel de seguridad adicional. Es de destacar que el sistema "ENLACE" BET sólo se ejecuta en una página HTTPS, lo cual adiciona medidas de seguridad que permiten la encriptación de los datos que viajan a través de internet. Una vez que el cliente captura su contraseña, esta se encripta y viaja de manera segura hasta el servidor y programa encargado de su validación, dicho programa compara de manera automática la información proporcionada por el cliente contra la que reside en la tabla específica, para ello lleva a cabo el proceso de desencriptación respectivo, de manera volátil y sin almacenar dato alguno en los dispositivos electrónicos del Banco. Si el proceso de comparación es exitoso se le autoriza al cliente el acceso a las facilidades de la banca electrónica, en caso contrario se le niega. Con base en lo antes descrito, y a los tiempos de respuesta establecidos, se refuerza que no existe intervención humana en este proceso."

En virtud de la contradicción de los dictámenes se nombró como perito tercero en discordia al Maestro GENARO DELGADO MONTALVO, quien emitió su dictamen y obra a fojas de la quinientos ochenta y siete a la seiscientos cinco de los autos, y quien emitió la siguiente conclusión:

"Si es técnicamente posible que el conjunto de contraseñas y claves de seguridad de los clientes de un banco permanezcan fuera del

alcance y conocimiento de los empleados de la institución Bancaria que procesa el servicio de Banca Electrónica.

Sin embargo, también es técnicamente posible que el conjunto de mecanismos de autenticación del usuario pueda estar al alcance y conocimiento de empleados (haciendo especial énfasis a los administradores, técnicos, y desarrolladores del sistema informático o aplicativo y arquitectura de base de datos que tienen los permisos necesarios para gestión de los todos los datos de los usuarios bancarios) y cualquier persona ligada o ajena a la institución bancaria. Siendo que el acceso al conjunto de mecanismos de seguridad otorgados, puedan ser sustraídos y utilizados sin consentimiento, voluntad y conocimiento del usuario bancario.

En este sentido, cabe remarcar, que la sustracción o el acceso a la vista de información contenida en bases de datos de cualquier sistema informático, por un agente malicioso, es una de las vulnerabilidades y amenazas a la ciberseguridad que poseen todos los sistemas informáticos de manea intrínseca. De acuerdo al El Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés), perteneciente a las oficinas oficiales del gobierno de Estados Unidos de América, una VULNERABILIDAD en el contexto de la informática tiene como definición: Una debilidad en la lógica computacional (por ejemplo, el código) que s encuentra en los componentes de software y hardware que, cuando se explotan, tiene como resultado un impacto negativo en la confidencialidad, integridad o disponibilidad de la información.

Bajo este contexto, todos los sistemas informáticos son susceptibles a "explotar" las vulnerabilidades intrínsecas de su diseño y que han sido detectadas por personas u otros sistemas, de tal manera que en el lapso de corrección de dichas vulnerabilidades, posibles "atacantes" o "agentes maliciosos", al conocer que existen estas "Brechas" o "agujeros" en la seguridad de los sistemas, las aprovechan para efectuar actividades ilegales o maliciosas en general.

En este orden de ideas, los sistemas informáticos bancarios no son la excepción, es decir, no son sistemas 100% seguros, y es obligación de las instituciones bancarias gestionar los riesgos asociados a las vulnerabilidades que sus sistemas informáticos puedan ser "explotados" en contra de los usuarios bancarios."

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 GENARO DELGADO MONTALVO, toda vez que se aprecia que es el dictamen más completo, 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 quinientos noventa y ocho y quinientos noventa y nueve de los autos, 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 veintidós de febrero del dos mil veintidos, 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, el perito fue bastante claro y explicativo 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

****

VIII.- 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 el actor ********** en contra de **********

****

Se condena a **********

********** a realizar la restitución de la cantidad de **CUATROCIENTOS NOVENTA MIL PESOS** por concepto de cargos no reconocidos ni autorizados, realizados en fecha nueve de noviembre del dos mil veinte.

Se condena a **********

********** al pago de los intereses legales a razón del seis por ciento anual, en términos de lo dispuesto por el artículo 362 del Código de Comercio, a partir del día nueve de noviembre del dos mil veinte, fecha en que se

realizaron las disposiciones reclamadas, y hasta el pago total de lo sentenciado, concepto que deberá regularse en ejecución de sentencia.

De conformidad con lo expuesto por el artículo 1084 del Código de Comercio, no se hace especial condena en costa, 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 **CUATROCIENTOS NOVENTA MIL PESOS** a favor de **********. por concepto de cargos no reconocidos ni autorizados, realizados en fecha nueve de noviembre del dos mil veinte.

QUINTO.- Se condena a ********** al pago de los intereses legales a razón del seis por ciento anual, en términos de lo dispuesto por el artículo 362 del Código de Comercio, a partir del día nueve de noviembre del dos mil veinte, fecha en que se realizaron las disposiciones reclamadas, y hasta el pago total de lo sentenciado, concepto que deberá regularse en ejecución de sentencia.

SEXTO.- No se hace especial condena en costas.-

SÉPTIMO. - NOTÍFIQUESE Y CÚMPLASE.-

A S I, lo sentenció y firma la C. Juez del Juzgado Quinto de lo Mercantil de esta Capital, Licenciada **VERÓNICA PADILLA GARCÍA,** por ante

su Secretaria de acuerdos Licenciada **ANA KAREN DURÁN PUENTES** que autoriza.- Doy Fe.-

Juez Secretaria

VERÓNICA PADILLA GARCÍA. **ANA KAREN DURÁN PUENTES.**

Se publica en fecha **cuatro de marzo del dos mil veintidos.-** Conste.-

L´VPG

El(La) Licenciado(a) DINA DEYANIRA REYES GUERRERO Secretario(a) de Acuerdos y/o de Estudio y Proyectos adscrito(a) al Órgano Jurisdiccional, hago constar y certifico que este documento corresponde a una versión pública de la sentencia o resolución 0122/2021 dictada en tres de marzo del dos mil veintidos por el Juez Quinto Mercantil del Estado de Aguascalientes, conste de 29 fojas útiles. Versión pública elaborada de conformidad a lo previsto por los artículos 3 fracciones XII y XXV; 69 y 70 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes y sus Municipios, 113 y 116 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.