



SENTENCIA NÚMERO: (279)

En la Ciudad de Altamira, Tamaulipas, a los veintitrés días del mes de Octubre de dos mil veintitrés.

V I S T O S para resolver los autos del expediente **0571/2021**, relativo al Juicio Oral Mercantil promovido por ***** en contra de ***** , y;-

RESULTANDO

ÚNICO.- Mediante promoción recibida el veinte de septiembre del año dos mil veintiuno compareció ***** promoviendo Juicio Oral Mercantil en contra de ***** , de quien reclama las siguientes prestaciones:
A).- La nulidad absoluta, de la operación de alta de beneficiario de otro Banco, de la cuenta terminación 22950088 de Scotiabank, sin nombre de beneficiario, número de referencia 7686072, para autorizar transferencias de la cuenta 56637857857613, de la titular Karla Zanira Guerreo Rodríguez, operación realizada sin su consentimiento por ***** , a través de SuperNet, en fecha 20 de julio del 2020. B).- La nulidad absoluta, de la disposición de la cantidad de \$48,000.00 (cuarenta y ocho mil pesos 00/100 MN), que realizo ***** sin autorización de la titular ***** de la cuenta número 56637857613, por transferencia electrónica SPEI a través de Supernet, a la cuenta con terminación 2950088 de Scotiabank sin nombre de beneficiario en fecha 20 de julio del año 2020, Número de referencia 3637259, identificada con clave de rastreo terminación 451063690. C).- La nulidad absoluta, de la disposición de la cantidad de \$48,000.00 (cuarenta y ocho mil pesos 00/100 MN) que realizo ***** , sin autorización de la titular ***** de la cuenta número 56637857613, por transferencia electrónica

SPEI a través de Supernet, a la cuenta con terminación 2950088 de Scotiabank sin nombre de beneficiario en fecha 20 de julio del año 2020, Número de referencia 6213803, identificada con clave de rastreo terminación 453931420. D).- La restitución y devolución de la cantidad total de \$96,000.00 (noventa y seis mil pesos 00/100 MN) que *****, que dispuso indebidamente de la cuenta 5663757613, a través de las dos transferencias electrónicas SPEI a través de SUPERNET, descritas en los incisos B) y C) efectuadas en fecha 20 de julio del 2020, a la cuenta terminación 25950088 de Scotiabank sin nombre de beneficiario, número de referencia 7686072 y sin autorización de la titular*****. E).- En consecuencia, el pago de los intereses generados desde fecha 20 de julio del 2020 y los que se sigan generando hasta la fecha de entrega por parte de la institución de crédito, de la cantidad reclamada y de conformidad a la tasa de intereses más alta que otorga Banco de México de forma anual. F).- El pago de los gastos y costas judiciales causados por la tramitación del presente juicio. ”.- Fundándose para ello en los hechos y disposiciones legales que consideró aplicables al caso.- Por auto del veintiuno de septiembre del año dos mil veintiuno se tuvo por admitida la demanda ordenándose emplazar y correr traslado a la parte demandada para que dentro del término legal produjera su contestación si tuviere excepciones legales que hacer valer.- Mediante diligencia del veintitrés de septiembre del año dos mil veintiuno se emplazó a la parte demandada, tal y como consta en las actas que se levantaron con tal motivo.- Por auto del ocho de octubre del año dos mil veintiuno se le tuvo dando contestación a



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

la demanda instaurada en su contra.- El primero de noviembre del año dos mil veintiuno se llevó a cabo la audiencia preliminar en donde se llevó a cabo la depuración del procedimiento; la conciliación y/o mediación de las partes por conducto del juez; la fijación de acuerdos sobre hechos no controvertidos; la fijación de acuerdos probatorios; la calificación sobre la admisibilidad de las pruebas, y se citó para audiencia de juicio, la que se llevó a cabo el siete de diciembre del año dos mil veintiuno, en la que se fijo perito en discordia y se señalaron las once horas del día once de enero del año dos mil veintidós, para efecto de la reanudación de la audiencia de juicio, la que fue diferida por cuestión de que el perito tercero no acepto el cargo, por lo que fue hasta el día veintisiete de septiembre del año en curso en que se dio continuidad a la audiencia de juicio y se desahogo el dictamen del perito tercero, en los términos que aparece en la video-grabación que al efecto se realizó, citándose a las partes para el día veintitrés de octubre del año dos mil veintitrés, para la continuación de la audiencia de juicio, a fin de dictar la presente sentencia, y.-

CONSIDERANDOS

PRIMERO.- Que este tribunal es competente para conocer y decir el presente juicio conforme a lo establecido por el artículo 104 fracción I de la Constitución Política de los Estados Unidos Mexicanos que establece que corresponde a los Tribunales de la Federación conocer de todas las controversias del orden civil que se susciten sobre el cumplimiento y aplicación de leyes federales, como en el caso acontece al tramitarse el presente juicio conforme al código de comercio que es una ley federal;

amén de que cuando dichas controversias sólo afecten intereses particulares, podrán conocer también de ellas, a elección del actor, los jueces y tribunales del orden común de los Estados y del Distrito Federal.- Así como también conforme a lo dispuesto por los artículos 1090, 1091, 1092 y 1093 del código de comercio, y 38 fracción III de la Ley Orgánica del Poder Judicial del Estado, al haberse promovido la demanda ante este Juzgado Civil de Primera Instancia que por turno le correspondió conocer del juicio, ser concurrente la materia y además de haberse sometidos tácitamente.

SEGUNDO.- La vía en la que se comparece es la correcta, de conformidad con lo dispuesto por el artículo 1390 Bis del código de comercio que señala: “Se tramitarán en este juicio todas las contiendas cuya suerte principal sea inferior a la que establece el artículo 1339 para que un juicio sea apelable, sin que sean de tomarse en consideración intereses y demás accesorios reclamados a la fecha de interposición de la demanda.-

TERCERO: Legitimación activa. La ***** se encuentra legitimado en el proceso, en razón de que es la titular de las cuentas bancarias de las cuales se realizaron las transferencias bancarias, que refiere fueron realizadas sin su consentimiento.

Legitimación Pasiva.-***** se encuentra legitimado en el Proceso, al figurar como depositario, en el contrato que celebros con la actora, es decir tiene la obligación de custodiar de las cantidades depositadas a la cuenta de la actora y de las cuales se hicieron las transferencias y disposiciones que la actora no



reconoce.

CUARTO: Así tenemos que ***** promueve Juicio Oral Mercantil **en contra de *******, de quien reclama las prestaciones transcritas en el resultando único de esta sentencia, basándose para ello medularmente en que tiene aperturada una cuenta de débito con la institución bancaria demandada, en cual se registro su firma electrónica para realizar operaciones en establecimientos mercantiles o disposiciones en efectivo en sucursales o cajeros autorizados, transferencias electrónicas, que en fecha veinte de julio del año dos mil veinte se dio cuenta que sin su consentimiento se retiro de su cuenta numero 56637857613, mediante dos transferencias electrónicas SPEI, a través de SuperNet, la primera, a las 12:08:32, por la cantidad de \$48,000.00 (cuarenta y ocho mil pesos 00/100 MN) a la cuenta con terminación 2950088 de Scotiabank, sin nombre de beneficiario, identificada con clave de rastreo terminación 451063690, número de referencia 3637259 y la segunda a las 15:40:58 por la cantidad de \$48,000.00 (cuarenta y ocho mil pesos 00/100 mn) a la misma cuenta con terminación 2950088 de Scotiabank sin nombre de beneficiario, con el número de referencia de 4998658, por lo que refiere reporte vía telefónica a la unidad de aclaraciones de ***** registrándose bajo el numero de Folio 120-2025049 y le dicen que espere una respuesta dado seguimiento a su inconformidad, la que fue determinada improcedente, en razón de ello se acudió ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, en la que en fecha cinco de marzo del año dos mil veintiuno, se emitió el

Dictamen Valoración Técnica y Jurídica, en la que se declaro procedente lo reclamado, por lo cual señala que resultan procedentes las prestaciones reclamadas.

Por su parte la demandada al dar contestación a la demanda instaurada en su contra, se opuso a las prestaciones que se le reclaman, bajo los hechos que expone en su ocurso de cuenta, oponiendo las siguientes excepciones: **1.- FALTA DE ACCIÓN Y DE DERECHO**, Para ejercer una acción en juicio se requieren la existencia de un derecho y la violación de este. En la especie, la parte actora reclama la nulidad de un alta de cuenta de tercero y de dos cargos en su cuenta número 56637857613, correspondientes a transferencias electrónicas de dinero (SPEI) que dice no haber realizado por un importe total de \$96,000.00. Del contrato de prestación de servicios bancarios y la aceptación del uso de medios electrónicos, se desprende que la parte actora puede disponer de sus fondos, entre otras formas, a través de la banca electrónica, mediante las claves de acceso confidenciales que obran en su poder y los filtros de seguridad dispuestos por el Banco, tanto para ingresar al sistema, como para dar de alta cuentas de destino y realizar transferencias de recursos. En este caso los medios de acceso a la banca electrónica y FACTORES DE AUTENTIFICACIÓN asignados a la parte actora son los siguientes: 1.- El código de cliente. 2.- El número de identificación personal (NIP) generado por la propia usuaria y que solo ella conoce. 3.- La contraseña dinámica de un solo uso (OTP) generada por el dispositivo en poder de la usuaria. Para utilizar la banca



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

electrónica hay que acceder al portal Supernet de banco [www. santander.com,mx,](http://www.santander.com.mx) a través de la red mundial de datos conocida como Internet. El acceso a dicho portal solo es posible tecleando el código del cliente con el que se identifica al titular de la cuenta y el Número de Identificación Personal que éste haya creado para tal efecto y que solo es de su conocimiento. Adicionalmente, tanto para dar de alta cuentas de destino, como para ejecutar transferencias SPEI, es indispensable teclear la contraseña dinámica de un solo uso (Super Token) que obra en poder del cliente. Estos elementos constituyen la firma electrónica del cliente, lo que genera un vínculo jurídico que torna incuestionable la sutoria del titular inclusive , de acuerdo con el contrato, el Banco se encuentra obligado a realizar las operaciones que el cuentahabiente le ordene mediante el uso de su firma electrónica. En el presente caso, tal y como se indico al contestar el hecho 2 de la demanda, esta registrado el ingreso a la banca electrónica del cliente para dar de alta la cuenta destino, espero mas de una hora para que esta quedará activa, después volvió a ingresar a la banca electrónica y efectuó una transferencia. Todas estas operaciones utilizando una contraseña dinámica de un solo uso diferente, generadas por el Super Token en poder del cuentahabiente. Por lo tanto, se trata de operaciones ordenadas por el cliente, llevadas a cabo a través de banca electrónica con su firma electrónica, que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio, conforme a lo previsto en los artículos 52 de la Ley de Instituciones de Crédito y 89 del Código de Comercio, en

L'MDG / L'MGM / NGE

consecuencia, se puede concluir que no se ha lesionado derecho alguno en perjuicio de la parte actora. **2.- CONSENTIMIENTO /EXCLUSIÓN DE RESPONSABILIDAD.** Conforme a lo pactado en el contrato de prestación de servicios bancarios, transcrito parcialmente al contestar el hecho 1 de la demanda, el uso de las CLAVES DE ACCESO es exclusiva responsabilidad del CLIENTE, quien reconoce y acepta como suyas todas las operaciones que se celebren con el BANCO utilizando dichas claves de Acceso, y para todos los efectos legales a que haya lugar, expresamente también reconoce y acepta el carácter personal e intransferible del Código de Cliente y Nips, así como su absoluta confidencialidad, . Asimismo de conformidad a lo señalado en el Título Segundo, Libro Segundo, del Código de Comercio, denominado “Del comercio electrónico”, según el cual el uso de los medios de identificación que se establezcan en sustitución de la firma autógrafa, producirían los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio, en virtud de ello, las Claves de Acceso establecida para el uso de medios electrónicos, sustituyen a la firma autógrafa por una de carácter electrónico, y las constancias documentales o técnicas derivadas del uso de los medios en donde aparezca dicha firma electrónica, producirían los mismos efectos que las leyes otorgan a los documentos suscritos por las partes y tendrían igual valor probatorio. Asimismo se libero de responsabilidad al banco al ejecutar instrucciones recibidas mediante las claves de acceso a la banca electrónica del cliente. En el presente caso la parte actora reclama un alta de cuenta de tercero y dos r



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

transferencias de dinero a cuenta de tercero que, para poderse llevar a cabo, implicó el uso de la banca electrónica, Siendo que, para poder ingresar a banca electrónica se requiere forzosamente utilizar el código del cliente y la contraseña o número de identificación personal que el cliente genera y solo el reconoce y para dar de alta cuentas de terceros y transferir dinero a las mismas, se utiliza la contraseña dinámica de un solo uso generada por el dispositivo electrónico Super Token en poder del cliente. Por lo tanto al ser elementos confidenciales y en poder del cliente se presupone que fueron llevados a cabo por el mismo. Es decir, existe una expresión de su voluntad captando este tipo de cargos, por lo tanto no hay vicio que afecte la validez de los mismos. Hay que mencionar también que no existe evidencia alguna de que el sistema de banco haya sido vulnerado o intervenido ilícitamente como lo supone el actor. Siendo aplicable al caso concreto, el artículo 1803 del Código Civil Federal, que a la letra dice: Art. 1803: El consentimiento puede ser expreso o tacito, para ello se estará a lo siguiente: I.- Será expreso cuando la voluntad se expresa verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y II.- El tacito resultara de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente. Por lo tanto opera a favor del Banco la cláusula señalada, que lo libera de cualquier responsabilidad por ejecutar instrucciones a través de los medios electrónicos puestos a disposición del cliente, mediante el uso de las claves de acceso en

poder del cliente, aún y cuando estas hubiesen sido robadas. **3. VICIOS DEL DICTAMEN VALORACIÓN TÉCNICA Y JURÍDICA**, conforme a lo mencionado al contestar los hechos 3, 4 y 5 de la demanda y que pido se tengan por aquí mencionado a l contestar los hechos 3, 4, y 5 de la demanda y que pido se tengan por aquí reproducidos debiéndose considerar dicho instrumento como infundado e inmotivado y que no sirve para producir convicción sobre la procedencia de la acción intentada por la parte actora.

QUINTO: El artículo 1194 del código de comercio dispone: “El que afirma está obligado a probar. En consecuencia, el actor debe probar su acción y el reo sus excepciones.”.- Así tenemos que la parte actora desahogó los siguientes medios de convicción mismos que fueron admitidos en la audiencia preliminar: **1.- DOCUMENTAL PUBLICA.** Consistente en copias certificadas del expediente 2020/280/4384 radicado ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, Delegación Estatal Tampico, que deriva de la reclamación interpuesta por la ***** en contra de ***** , en el que consta el Dictamen Valoración Técnica y Jurídica.- A la cual se le concede valor probatorio de conformidad a lo dispuesto en el numeral 1292 del Código de Comercio. **II.- PRESUNCIONAL LEGAL Y HUMANA e INSTRUMENTAL DE ACTUACIONES.** Que se desahogan atendiendo a su propia y especial naturaleza.- A las cuales se les concede



valor probatorio de conformidad a lo dispuesto por los numerales 1294, 1305 y 1306 del Código de Comercio.

Por su parte la demandada a fin de acreditar sus excepciones, ofreció el siguiente material probatorio: .- 1.-

DOCUMENTAL PUBLICA Consistente en copia certificada de la escritura pública número ochenta y nueve mil ochocientos noventa y dos, de fecha catorce de febrero del año dos mil diecinueve, pasada ante la fe publica del licenciado Antonio Ruiz Aguirre, titular de la notaría número doscientos veintinueve de la Ciudad de México, en la cual consta el Poder General para Pleitos y Cobranzas que otorga ***** en favor de los licenciados o *****.- A

la cual se le concede valor probatorio de conformidad a lo dispuesto en el numeral 1292 del Código de Comercio. **2.-**

DOCUMENTAL PUBLICA. Consistente en copia simple de la cédula de inscripción del RFC de ***** , con RFC BSM970519DU8, de fecha once de febrero del año dos mil diecinueve, expedido por el Servicio de Administración Tributaria.- A la cual se le concede valor probatorio de conformidad a lo dispuesto por el numeral 1292 del Código de Comercio. **3.- DOCUMENTAL PUBLICA.** Consistente

en copias de las cédulas profesionales expedida por la Secretaria de Educación Pública a favor de ***** , así como copia de su clave única de registro de población.- A la cuales se les concede valor probatorio de conformidad a lo dispuesto por el numeral 1292 del Código de Comercio.

5.- DOCUMENTAL PRIVADA.- Consistente en el clausulado del contrato de prestación de servicios bancarios y financieros múltiples celebrado entre las partes, el que se encuentra certificado en términos del artículo 100 de la Ley de Instituciones de Crédito, inscrito

en el Registro de Contratos de Adhesión de la CONDUCEF 0307-4378-005677/04-13900-1011 de fecha 07-10-2011.-

A la cual se le concede valor probatorio de conformidad a lo dispuesto en el numeral 1296 del Código de Comercio.

6- DOCUMENTAL PRIVADA. Consistente en la bitácora de operaciones de la cuenta número 5663785613 a nombre de *****.- A la cual se le concede valor probatorio de conformidad a lo dispuesto por el numeral 1296 del Código de Comercio. **7.- DOCUMENTAL**

PRIVADA. Consistente en los comprobantes de transferencias SPEI, correspondiente a los cargos no reconocidos de la cuenta número 56637857613 a la cuenta numero 044180256022950088 a nombre de Jacqueline Cazares Bautista con RFC CABJ820723SP8 de Scotiabank Inverlat S.A. Institución de Banca Múltiple Grupo Financiero Scotiabank Inverlat.- A la cual se le concede valor probatorio de conformidad a lo dispuesto por el numeral 1296 del Código de Comercio. **8.-**

DOCUMENTAL PUBLICA. Consistente en el folleto ¿Que es y cómo funcional el SPEI, emitido por Banco de México en mayo 2018, publicado en la pagina electrónica de dicho organismo.- A la cual se le concede valor probatorio de conformidad a lo dispuesto por el numeral 1292 del Código de Comercio. **9.- DOCUMENTAL PRIVADA.**

Consistente en los Informes Técnicos elaborados los días 26 de noviembre del 2020, 30 de septiembre y 30 de octubre del 2021 por las áreas internas de prevención y seguridad y reclamaciones de *****.- A la cual se le concede valor probatorio de conformidad a lo dispuesto en el numeral 1296 del Código de Comercio. **10.-**

DOCUMENTAL PUBLICA. Consistente en la copia



certificada de la escritura pública número ochenta y un mil novecientos noventa y nueve, de fecha tres de diciembre del año dos mil ocho, pasada ante la fe publica del licenciado Alfonso González Alonso, Notario Público número 31 en la Ciudad de México, en la cual consta el poder que otorga ***** en favor del funcionario bancario Reynaldo Daniel Maldonado Almanza.- A la cual se le concede valor probatorio de conformidad a lo dispuesto en el numeral 1292 del Código de Comercio.

11.- CONFESIONAL.- A cargo de la parte actora, desahogada en la Audiencia de juicio de fecha siete de diciembre del año dos mil veintiuno en los términos en los que consta en la video-grabación que con tal motivo se levantó.- A la cual se le concede valor probatorio de conformidad a lo dispuesto por el numeral 1286 del Código de Comercio.

9.- INSPECCIÓN JUDICIAL.- Desahogada el día seis de diciembre del año dos mil veintiuno en las instalaciones de este Juzgado, por conducto de la Secretaria de Acuerdos e este Juzgado, que se practico sobre el portal del Banco ***** , en los términos en los que consta en el acta que con tal motivo se levantó.- A la cual se le concede valor probatorio de conformidad a lo dispuesto por el numeral 1299 del Código de Comercio

10.- PERICIAL EN INFORMÁTICA.- A cargo del Ingeniero ***** , dictamen que corre agregado a fojas 371 a 388 del expediente principal, que fue expuesto en la Audiencia de Juicio, quien dio respuesta a las interrogantes planteadas por las partes, de la siguiente forma.

CUESTIONARIO DE LA DEMANDADA

a).- Que diga el perito, según su leal saber y entender, si existe el portal ***** en la red mundial de datos conocida como internet.

Respuesta.- Al teclear la dirección www. ***** en un buscador de internet y oprimir la tecla “enter” se puede constatar que automáticamente se abre el sitio web antes mencionado como se aprecia en la imagen.

2.- Que diga el perito, según su leal saber y entender, cual es el procedimiento y/o requisitos para iniciar una sesión de Banca Electrónica (Supernet) en dicho portal.

Respuesta.- Ser cliente: Debe de contar con un código de cliente, cuenta de cheques o número de tarjeta de crédito o débito.

3.- Que diga el perito, según su leal saber y entender, si es posible ingresar a la Banca Electrónica (Supernet) solamente con el código del cliente asignando a la parte actora

Respuesta: Si se intenta ingresar a una cuenta Supernet utilizando el código de cliente asignado, se podrá observar que esto no es posible debido a que se requiere tener conocimiento de la contraseña de usuario, misma que es propiedad del cliente.

4.- Que diga el perito, según su leal saber y entender, si es posible ingresar a la Banca Electrónica (Super Net) sin teclear el NIP o contraseña de acceso.

Respuesta: Se puede apreciar que no es posible ingresar a la Supernet sin teclear el NIP o contraseña de acceso, ya que para obtener acceso a ella se requiere rotundamente ingresar sus datos para poder ingresar al SuperNet, ya sea código de cliente, tarjeta de crédito o débito o número de cuenta, como se puede apreciar en la siguiente imagen.



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

5.- Que diga el perito, según su leal saber y entender, si es posible ingresar a la Banca Electrónica (Supernet) sin teclear un código de cliente y/o NIP de acceso aleatorio, que no corresponda al usuario interesado en ingresar a la Banca Electrónica.

Respuesta.- Si se teclea un código de cliente y/o NIP de acceso que no corresponda al usuario interesado en ingresar a la Supernet, en la pantalla aparecerán los datos de acceso designados por el usuario de dicha cuenta (nombre e imagen), por lo que de inmediato se tendrá que reconocer que no estas ingresando a la cuenta interesad, así mismo al introducir una contraseña incorrecta mandará un aviso, como se muestra en el siguiente ejemplo. NOTA. Se tecleo al azar el numero 20802124 solo se uso para ejemplificar.

6.-Que diga el perito, según su leal saber y entender, cual es el resultado de teclear un código de cliente y la contraseña que el usuario haya generado para ingresar a la Banca Electrónica (Supernet)

Respuesta: El resultado de teclear el código de cliente y la contraseña que el usuario haya generado para ingresar a la Banca Electrónica (Supernet) Permitirá el total acceso a la aplicación para consultar su saldo, movimientos, realizar transacciones etc.

7.- Que diga el perito, según su leal saber y entender , cuales son los datos que requiere la Banca Electrónica (Supernet) para dar de alta una cuenta de otro Banco para poder transferir dinero a la misma.

Respuesta:.-Los datos que se requiere el sistema Supernet para dar de alta una cuenta de otro banco para poder transferir dinero a la misma son los siguientes:

Numero de cuenta, Banco, Tipo de cuenta, Nombre del titular de la cuenta.

8.- Que diga el perito, según su leal saber y entender , si es posible realizar el alta de cuenta de tercero destino de transferencias, sin utilizar la contraseña dinámica de un solo uso en poder del usuario de banca electrónica.

Respuesta.- Porque se puede ver en el punto anterior no es posible realizar el alta de una cuenta de otro banco destino de transferencias, sin utilizar la contraseña dinámica de un solo uso en poder de la parte actora.

9.- Que diga el perito según su leal saber y entender, cuales son los datos que requiere el sistema de Banca Electrónica (Supernet) para realizar una transferencia a una cuenta de tercero.

Respuesta. Los datos que requiere el sistema de Banca Electrónica (Supernet) para realizar una transferencia a una cuenta de tercero, son los siguientes: Numero de cuenta. Banco, Tipo de Cuenta, Nombre del titular de la cuenta. Altas.

10.- Si es posible realizar una transferencia a una cuenta de tercero, sin utilizar la contraseña dinámica de un solo uso en poder del usuario de banca electrónica (Supernet)

Respuesta.- Como ya se vio en los puntos anteriores no es posible realizar una transferencia a un tercero, sin antes ingresar la contraseña tanto para acceder a su sesión en la aplicación y para dar de alta la nueva cuenta a quien se le realizara la transferencia. Ya que para realizar cualquier operación es necesario contar con una contraseña dinámica que se genera en la aplicación de Santander movil.



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

11.- Que diga el perito, según su leal saber y entender, que es una contraseña, como y quien la genera.

Respuesta:.- En informática una contraseña es un conjunto de caracteres, no obligatoriamente formado únicamente de cifras y letras, con o sin significado, y son utilizadas para verificar la identidad de los usuarios.- Las contraseñas son generadas para propósitos de seguridad y de salvaguardar información de cuentas determinadas son generadas aleatoriamente por los usuarios utilizando frase, palabras, o conjunto de número y letras que más a ellos convengan .

12.- Que diga el perito según su leal saber y entender que es la contraseña dinámica.

Respuesta.- Una contraseña de un solo uso OTP (por sus reglas en ingles one-time password), también conocida como contraseña dinámica es una contraseña que solo se puede usar una vez, generalmente durante una breve periodo de unos segundos o minutos después de que se haya emitido la contraseña. Este tipo de contraseñas son emitidas en tiempo real por un autenticador de software o hardware que un usuario tiene en su poder. El autenticador que tiene el usuario comparte una clave criptográfica con el verificador, que es el software que intenta verificar la identidad del usuario. De cualquier forma, que se genere, cada OTP solo se puede usar una vez. El verificador que examina la contraseña como un medio para comprobar la identidad de un usuario rechazaría los usos repetidos de una contraseña.

CUESTIONARIO DE LA ACTORA.

1.- Que diga el perito que es y para que sirve una IP.

Respuesta.- La IP o Protocolo de internet (Por sus siglas en ingles "Internet Protocol") es una dirección única que sirve para identificar a un dispositivo en internet o en una red local.

2.- Que diga el perito , si logra identificar la dirección IP, fecha y hora, de beneficiario de las transacciones reclamadas.

Respuesta.- Se logra identificar lo que aparentemente es la dirección IP, fecha y hora, de las transferencias reclamadas, dichos datos aparecen en los documentos con nombre "Informe Técnico Anexo 9" "Informe Técnico Anexo 10" e" informe Técnico Anexo 11"

3.- Por los estudios encomendado, que diga el perito si logra identificar desde que numero de IP se realizaron las transacciones reclamadas y geolocalizar la IP.

Respuesta: En los documento con nombre "Informe Técnico Anexo 9" "Informe Técnico Anexo 10" e" informe Técnico Anexo 11" que se me pusieron a la vista se visualizan aparentemente las direcciones IP donde se realizaron las transacciones reclamadas y a continuación expongo su geolocalización.

Y al geolocalizar la longitud y latitud que aparecen en ambas direcciones IP nos arroja la siguiente dirección: "Colonia del Valle, Benito Juárez, 03100 Ciudad de México, CDMX" . Para ser mas específicos en un parque llamado arboledas.



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

4.-. Que diga el perito, si por su estudio encomendado, logra determinar si la IP con la que se realizó las transacciones reclamadas, se ha usado en más de 2.

Respuesta. En los documentos con nombre "Informe técnico Anexo 9" "Informe Técnico anexo 10", "Informe Técnico anexo 11", que se me pusieron a la vista se visualizaron aparentemente las dos direcciones IP donde se realizaron las dos transacciones reclamadas.

5.-Que diga el perito, cuáles son los mecanismos de seguridad con que debe de contar una institución bancaria.

Respuestas:- Los mecanismos de seguridad con que debe de contar una institución bancaria podrían ser: Firma electrónica, claves únicas de acceso o Nip dinámico, autenticación en dos pasos, por un número generado en un token personal.

6.- Que diga el perito, en que consiste el protocolo de seguridad de firma electrónica.

Respuesta.- La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son: Identificar al firmante de manera inequívoca. Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación. Asegurar el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos, y, por tanto, posteriormente, ni puede decir que no ha firmado el documento. Proceso básico que se sigue para la firma electrónica es el siguiente:

El usuario dispone de un documento electrónico (una hoja de cálculo, un pdf, una imagen, incluso un formulario en una página web) y de un certificado que le pertenece y le identifica.

La aplicación o dispositivo digital utilizados para la firma realiza un resumen del documento. El resumen de un documento de gran tamaño puede llegar a ser tan solo de unas líneas, Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.

La aplicación utiliza la clave privada para codificar el resumen.

La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este nuevo documento es la firma electrónica.

El resultado de todo este proceso es un documento electrónico obtenido a partir del documento original y de las claves del firmante. La firma electrónica, por tanto, es el mismo documento electrónico resultante.

7.- Que diga el perito, si en las bitácoras mostradas y operaciones reclamadas logra identificar, que se haya usuario el protocolo de seguridad de firma electrónica

Respuesta. En las bitácoras mostradas se identifican las operaciones y movimientos realizados los cuales aparecen con un folio de identificación que en este caso sería la referencia, ip de origen y id de inicio de sesión, en los informes técnicos 9, 10 y 11 se puede visualizar el id de token en las operaciones en las tablas que se presentan en dichos documentos



8.- Que diga el perito como se relaciona el sistema de pagos electrónicos interbancarios SPEI y banco ***** , así como la herramienta empalada para intercomunicarse.

Respuesta: El Sistema de Pagos Electrónicos Interbancarios (SPEI) es la infraestructura de pagos del Banco de México que permite a sus participantes, (bancos, casas de bolsa, y otras entidades financieras reguladas) enviar y recibir pagos entre sí para poder brindar a sus clientes finales el servicio de transferencias electrónicas en tiempo real. Este sistema esta relacionado con cualquier banco al utilizar la banca electrónica, y la herramienta empleada para llevar a cabo dichas operaciones es la banca digital del banco ya sea en la computadora o en la aplicación móvil en el celular.

9.- Que diga el perito, quien desarrolla y da mantenimiento a la aplicación informática de banca electrónica del ***** .

Respuesta :

10.- Que diga el perito, que medios de almacenamiento utiliza el ***** , para almacenar la información sensible del cliente

11.- Que diga el perito, quien es el encargado de administrar la información de los clientes almacenada en el *****

Respuestas: La respuesta a las incógnitas anteriores i,j y k es que se desconoce dicha información ya que pertenece a un protocolo interno o medida de seguridad propia del banco Santander.

13.- Que diga el perito, por su experiencia en sistemas de información si los sistemas pueden ser vulnerados, violados por ciberdelincuentes o cibercriminales ?

Respuesta:- Los sistemas pueden ser vulnerados, violados por ciberdelincuentes o cibercriminales? Todo medio digital puede ser vulnerado, pero para eso existen las medidas de seguridad informática y de la información las cuales ayudan a proteger los datos, por lo mismo hoy en día las aplicaciones ya sean móviles o en la computadora presentan constantes actualizaciones para prevenir dichos ataques.

14.- Que diga el perito, si por su estudio encomendado logra determinar, que la propiedad de un token, una dirección IP, contraseñas y claves de seguridad, evitan que se realicen operaciones electrónicas, sin su consentimiento del propietario en la banca electrónica supernet

Respuesta:- Mientras un usuario mantenga en privado su token, una dirección IP, contraseñas y claves de seguridad, evitara que se realicen operaciones electrónicas, sin su consentimiento la banca electrónica supernet.

15.- Que diga el perito, si por su estudio encomendado, logra determinar, que las operaciones no reconocidas, fueron efectuadas físicamente por la C. *****.

Respuesta. No se puede asegurar si físicamente las operaciones no reconocidas fueron efectuadas por la C. ***** pero cibernéticamente todas sus credenciales de autenticación de su propiedad se utilizaron para entrar a su cuenta de SuperNet.

16.- Que diga el perito, si por su estudio encomendado, logra determinar, que la información que tiene registrada el banco bitácoras, informes técnicos de movimiento y



hechos de la banca móvil supernet, acreditan que físicamente la***** , realizo las operaciones que desconoció

Respuesta Según la información que tiene registrada el banco de bitácoras, informes técnicos de movimiento y hechos de la banca móvil supernet, acreditan que cibernéticamente la C. ***** realizo las operaciones que desconoció, ya que sus credenciales de autenticación privadas fueron utilizadas para entrar a su cuenta, y físicamente no es comprobable ya que únicamente se requieren las credenciales de autenticación.

17.- Que diga el perito si ´por su estudio encomendado, logra determinar, la existencia de inconsistencias en la realización de las operaciones no reconocidas, como lo son, la falde notificaciones de autorización de dichas operaciones a la C. *****y que esta se realizaron de IPS no usados previamente por el usuario, tal como se precisa el informe técnico del banco (anexo 9, 10, y 11)

Respuestas: No se puede constatar que presuntamente no existieron notificaciones, ya que las notificaciones en un dispositivo movil pueden ser desactivadas por el usuario, y si es en un correo electrónico, al no tener a la vista dicho correo se desconoce dicha información. En cuanto a las direcciones IP, estas cambian dependiendo el dispositivo que se utilice.

18.- Que diga el perito, si por su estudio encomendado, la información que exhibió el banco, en su contestación de demanda, de contrato, bitácoras, informes técnicos de

movimiento y hechos de la banca móvil supernet, son ilegibles en su mayoría o que presentan alteraciones.

Respuesta.- La información que exhibió el banco, en su contestación de demanda, de contrato, bitácoras, informes técnicos de movimiento y hechos de la banca móvil supernet que se me puso a la vista, es legible y al ser un documento formato PDF se desconoce si supuestamente existiera una alteración ya que no son imágenes si no un documento.

Prueba pericial a la cual no se le otorga valor probatorio en atención a que la perito omitió contestar las preguntas señaladas con los incisos i, j y k es que se desconoce dicha información señalando que pertenecen a un protocolo interno o medida de seguridad propia del banco Santander, puntos importantes para determinar la seguridad con la que cuenta el Banco.

Por su parte la actora designo como perito de su intención a ***** cuyo dictamen se encuentra agregado a fojas 332 a 367 del principal, del cual se transcribe de manera medular lo siguiente:

“ CUESTIONARIO DE LA DEMANDADA

a).- Que diga el perito, según su leal saber y entender, si existe el portal ***** en la red mundial de datos conocida como internet.

Respuesta.- Al teclear la dirección www. ***** en un buscador de internet y oprimir la tecla “enter” se puede constar que automáticamente se abre el sitio web antes , mencionado como se aprecia en la imagen.



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

2.- Que diga el perito, según su leal saber y entender, cual es el procedimiento y/o requisitos para iniciar una sesión de Banca Electrónica (Supernet) en dicho portal.

Respuesta.- Ser cliente: Debe de contar con un código de cliente, cuenta de cheques o número de tarjeta de crédito o débito.

3.- Que diga el perito, según su leal saber y entender, si es posible ingresar a la Banca Electrónica (Supernet) solamente con el código del cliente asignando a la parte actora

Respuesta: Si se intenta ingresar a una cuenta Supernet utilizando el código de cliente asignado, se podrá observar que esto no es posible debido a que se requiere tener conocimiento de la contraseña de usuario, misma que es propiedad del cliente.

4.- Que diga el perito, según su leal saber y entender, si es posible ingresar a la Banca Electrónica (Super Net) sin teclear el NIP o contraseña de acceso.

Respuesta: Se puede apreciar que no es posible ingresar a la Supernet sin teclear el NIP o contraseña de acceso, ya que para obtener acceso a ella se requiere rotundamente ingresar sus datos para poder ingresar al SuperNet, ya sea código de cliente, tarjeta de crédito o débito o número de cuenta, como se puede apreciar en la siguiente imagen.

5.- Que diga el perito, según su leal saber y entender, si es posible ingresar a la Banca Electrónica (Supernet) sin teclear un código de cliente y/o NIP de acceso aleatorio, que no corresponda al usuario interesado en ingresar a la Banca Electrónica.

Respuesta.- Si se teclea un código de cliente y/o NIP de acceso que no corresponda al usuario interesado en ingresar a la Supernet, en la pantalla aparecerán los datos de acceso designados por el usuario de dicha cuenta (nombre e imagen), por lo que de inmediato se tendrá que reconocer que no estas ingresando a la cuenta interesad, así mismo al introducir una contraseña incorrecta mandará un aviso, como se muestra en el siguiente ejemplo. NOTA. Se tecleo al azar el numero 20802124 solo se uso para ejemplificar.

6.-Que diga el perito, según su leal saber y entender, cual es el resultado de teclear un código de cliente y la contraseña que el usuario haya generado para ingresar a la Banca Electrónica (Supernet)

Respuesta: El resultado de teclear el código de cliente y la contraseña que el usuario haya generado para ingresar a la Banca Electrónica (Supernet) Permitirá el total acceso a la aplicación para consultar su saldo, movimientos, realizar transacciones etc.

7.- Que diga el perito, según su leal saber y entender , cuales son los datos que requiere la Banca Electrónica (Supernet) para dar de alta una cuenta de otro Banco para poder transferir dinero a la misma.

Respuesta:.-Los datos que se requiere el sistema Supernet para dar de alta una cuenta de otro banco para poder transferir dinero a la misma son los siguientes: Numero de cuenta, Banco, Tipo de cuenta, Nombre del titular de la cuenta.

8.- Que diga el perito, según su leal saber y entender , si es posible realizar el alta de cuenta de tercero destino de



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

transferencias, sin utilizar la contraseña dinámica de un solo uso en poder del usuario de banca electrónica.

Respuesta.- Porque se puede ver en el punto anterior no es posible realizar el alta de una cuenta de otro banco destino de transferencias, sin utilizar la contraseña dinámica de un solo uso en poder de la parte actora.

9.- Que diga el perito según su leal saber y entender, cuales son los datos que requiere el sistema de Banca Electrónica (Supernet) para realizar una transferencia a una cuenta de tercero.

Respuesta. Los datos que requiere el sistema de Banca Electrónica (Supernet) para realizar una transferencia a una cuenta de tercero, son los siguientes: Numero de cuenta. Banco, Tipo de Cuenta, Nombre del titular de la cuenta. Altas.

10.- Si es posible realizar una transferencia a una cuenta de tercero, sin utilizar la contraseña dinámica de un solo uso en poder del usuario de banca electrónica (Supernet)

Respuesta.- Como ya se vio en los puntos anteriores no es posible realizar una transferencia a un tercero, sin antes ingresar la contraseña tanto para acceder a su sesión en la aplicación y para dar de alta la nueva cuenta a quien se le realizara la transferencia. Ya que para realizar cualquier operación es necesario contar con una contraseña dinámica que se genera en la aplicación de Santander móvil.

11.- Que diga el perito, según su leal saber y entender, que es una contraseña, como y quien la genera.

Respuesta:.- En informática una contraseña es un conjunto de caracteres, no obligatoriamente formado únicamente de cifras y letras, con o sin significado, y son

utilizadas para verificar la identidad de los usuarios.- Las contraseñas son generadas para propósitos de seguridad y de salvaguardar información de cuentas determinadas son generadas aleatoriamente por los usuarios utilizando frase, palabras, o conjunto de número y letras que más a ellos convengan .

12.- Que diga el perito, según su leal saber y entender, que es la contraseña dinámica de un solo uso, como y quien la genera.

Respuesta.- Una contraseña de un solo uso OTP (por sus reglas en inglés one-time password), también conocida como contraseña dinámica es una contraseña que solo se puede usar una vez, generalmente durante un breve periodo de unos segundos o minutos después de que se haya emitido la contraseña. Este tipo de contraseñas son emitidas en tiempo real por un autenticador de software o hardware que un usuario tiene en su poder. El autenticador que tiene el usuario comparte una clave criptográfica con el verificador, que es el software que intenta verificar la identidad del usuario. De cualquier forma, que se genere, cada OTP solo se puede usar una vez. El verificador que examina la contraseña como un medio para comprobar la identidad de un usuario rechazaría los usos repetidos de una contraseña.

CUESTIONARIO DE LA ACTORA.

1.- Que diga el perito que es y para que sirve una IP.

Respuesta.- En el inciso 4.2 basado en el Manual sobre redes basadas en el Protocolo Internet (IP) y asuntos conexos publicado por Unión Internacional de Telecomunicaciones. Los números denominados



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

“direcciones IP” son necesarios para el funcionamiento de las redes IP. Tales redes se definen comúnmente con el término “Internet”. El formato de direcciones IP se define en las normas publicadas por el Grupo Especial sobre Ingeniería de Internet (IETF). Véanse, en particular, las peticiones de comentarios RFC) 791 Y 2460.

Con fundamento en lo señalado el que suscribe concluye que una dirección IP es un protocolo o conjunto de reglas usado para la comunicación en internet, una dirección IP es un conjunto de números que identifica a un dispositivo en internet.

2.- Que diga el perito , si logra identificar la dirección IP, fecha y hora, de beneficiario de las transacciones reclamadas.

Respuesta.- De acuerdo a la bitácora de “Resumen de movimientos” proporcionado se puede observar:

IP: 201.175.135.175 y 201.175.135.81

Fecha: 20/07/2020 para los dos movimientos

Hora: NO ES VISIBLE PARA NINGUNO DE LOS DOS MOVIMIENTOS

3.- Por los estudios encomendado, que diga el perito si logra identificar desde que numero de IP se realizaron las transacciones reclamadas y geolocalizar la IP.

Respuesta: De acuerdo a la bitácora “Resumen de movimientos” se visualizan los siguientes números de IP: 201. 175.135.175 Y 201.175.135.81

Se procede a geolocalizar los números de IP antes mencionados con la herramienta de whatismyipaddres:

Geolocalización del número de IP: 201.175.135.175, dando los siguientes resultados:

Arroja encontrarse en la Ciudad de México, con nombre de dispositivo apn3g.mm6.175.x.attmex.mx, con proveedor de internet AT&T México

Geolocalización del número de IP: 201.175.135.81, dando los siguientes resultados:

Arroja encontrarse en la Ciudad de México, con nombre de dispositivo apn3g.mm6.175.x.attmex.mx, con proveedor de internet AT&T México, Código Postal número 03730

4.- Que diga el perito, si por su estudio encomendado, logra determinar si la IP con la que se realizó las transacciones reclamadas, se ha usado en mas de 2.

Respuesta. De acuerdo a la información proporcionada no se puede visualizar más movimientos. La bitácora de movimiento solo muestra las 2 transacciones reclamadas. Por lo tanto el que suscribe determina que no se usó más de dos veces el número de IP.

5.-Que diga el perito, cuales son los mecanismos de seguridad con que debe de contar una institución bancaria.

Respuestas: Con fundamento circular única de bancos, los mecanismos de seguridad que las instituciones bancarias están obligadas a implementar previo a la liberación al público del servicio de banca electrónica es este país para dar fiabilidad a las transacciones interbancarias que se realizan por vía electrónica, es decir por internet, son las estipuladas en el capítulo X “Del Uso de Servicios de Banca Electrónica”, las cuales a continuación se enlistan de manera resumida:



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

Los mecanismos y procedimientos de Identificación del Usuario y Autenticación.

Los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados por las Instituciones, a través del servicio de Banca Electrónica.

Comuniquen a sus Usuarios los riesgos inherentes a la utilización del servicio de Banca Electrónica, así como que hagan de su conocimiento sugerencias para prevenir la realización de operaciones irregulares o ilegales que vayan en detrimento del patrimonio de los clientes y de las Instituciones.

6.- Que diga el perito, en que consiste el protocolo de seguridad de firma electrónica.

Respuesta.- De acuerdo a lo señalado en el artículo 89 del código de comercio señala: Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos , o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

De acuerdo a lo anterior el que suscribe concluye que la firma electrónica es un procedimiento acordado entre las partes interesadas para garantizar al emisor, al receptor la integridad del mensaje de datos cuyos procedimientos pueden ser admisibles en juicio.

7.- Que diga el perito, si en las bitácoras mostradas y operaciones reclamadas logra identificar, que se haya usuario el protocolo de seguridad de firma electrónica

Respuesta. De acuerdo a las bitácoras mostradas, no se puede observar el mensaje de datos enviado donde se le informa al cliente de que se realizaron las transacciones reclamadas.

De haberse enviado debería mostrarse la fecha, número de teléfono celular al que fue enviado.

8.- Que diga el perito como se relaciona el sistema de pagos electrónicos interbancarios (SPEI) y Banco Scotiabank, S.A., Institución de Banca Múltiple Grupo Financiero Scotiabank Inverlat, así como la herramienta empalada para intercomunicarse.

Respuesta: ¿Qué es el SPEI? De acuerdo a banco de México, el Sistema de Pagos Electrónicos Interbancarios (SPEI) es la infraestructura de pagos del Banco de México, que permite a sus participantes, (bancos, casas de bolsa, sofipos y otras entidades financieras reguladas) enviar y recibir pagos entre si para poder brindar a sus clientes finales el servicio de transferencias electrónicas en tiempo real.

El SPEI puede conceptualizarse como una tubería central a la que se conectan los participantes, sobre la cual, de manera eficiente y segura se cargan y abonan las cuentas de los participantes (e.g. Bancos) con el Banco de México para poder liquidar las operaciones entre participantes, ya sea que hayan sido enviadas por cuenta propia o por cuenta de sus clientes.



Para realizar esa conexión con el SPEI los participantes realizan desarrollos propios o contratan a terceros para que les brinden ese servicio.

De acuerdo a lo anterior el que suscribe concluye la relación existe mediante una aplicación desarrollada (Banca Móvil) por Banco Scotiabank que se conecta al sistema SPEI, el banco es el encargado de dar mantenimiento a Banca Móvil así como implementar los mecanismos de seguridad.

9.- Que diga el perito, quien desarrolla y da mantenimiento a la aplicación informática de banca electrónica del banco Scotiabank, S.A. INSTITUCIÓN DE BANCA MÚLTIPLE GRUPO FINANCIERO, SCOTIABANK INVERLAT.

Respuesta :De acuerdo a Banco de México: Los participantes tienen las especificaciones completas del protocolo, lo cual los habilita para desarrollar las aplicaciones con las que se conectan al sistema de acuerdo a sus necesidades particulares.

En base al párrafo anterior el que suscribe concluye que la institución bancaria en el caso que actual banco Scotiabank, S.A., Institución de Banca Múltiple, Grupo Financiero Scotiabank Inverlat es la encargada de desarrollar, dar mantenimiento e implementar los protocolos de seguridad de la Banca Electrónica.

10.- Que diga el perito, que medios de almacenamiento utiliza el banco Scotiabank, S.A. institución de banca múltiple grupo financiero, Scotiabank Inverlat, para almacenar la información sensible del cliente

Respuesta: De acuerdo al 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, aún cuando dichas bases de datos y archivos residan en medios de almacenamiento de respaldo.

Por lo anterior el que suscribe concluye que la información de los usuarios es almacenada en las infraestructuras de BANCO SCOTIABANK, específicamente en bases de datos administradas por su propio personal autorizado

11.- Que diga el perito, quien es el encargado de administrar la información de los clientes almacenada en el BANCO SCOTIABANK, S.A. INSTITUCION DE BANCA MULTIPLE, GRUPO FINANCIERO SCOTIABANK INVERLAT.

Respuestas: El Banco Scotiabank mediante su personal autorizado será el encargado de administrar la información sensible/delicada para garantizar la integridad de información de sus clientes para que esta no sea alterada, dañada, extraviada o robada.

12.- Que diga el perito, por su experiencia en sistemas de información si ¿ los sistemas pueden ser vulnerados, violados por ciberdelincuentes o cibercriminales ?

Respuesta: Ningún sistema es totalmente 100% seguro, aunque cada día se está investigando e incrementando los mecanismos de seguridad pero también las técnicas para generar ataques a los sistemas informáticos han aumentado más sofisticadamente y están en constante evolución.



13.- Que diga el perito, si por su estudio encomendado logra determinar, que la propiedad de un token, una dirección IP, contraseñas y claves de seguridad, evitan que se realicen operaciones electrónicas, sin su consentimiento del propietario en la banca electrónica supernet.

Respuesta:- Un token, una dirección IP, contraseñas y claves de seguridad es solo un mecanismo de seguridad que puede ser manipulado o vulnerado por personas o grupos de personas expertas en computación.

14.- Que diga el perito, si por su estudio encomendado, logra determinar, que las operaciones no reconocidas, fueron efectuadas físicamente por la C. *****.

Respuesta. No se puede asegurar si físicamente las operaciones no reconocidas fueron efectuadas por la C. ***** pero cibernéticamente todas sus credenciales de autenticación de su propiedad se utilizaron para entrar a su cuenta de SuperNet.

15.- Que diga el perito, si por su estudio encomendado, logra determinar, que la información que tiene registrada el banco bitácoras, informes técnicos de movimiento y hechos de la banca móvil supernet, acreditan que físicamente la ***** , realizo las operaciones que desconoció

Respuesta Según la información que tiene registrada el banco de bitácoras, informes técnicos de movimiento y hechos de la banca móvil supernet, acreditan que cibernéticamente la C.***** , realizo las operaciones que desconoció, ya que sus credenciales de autenticación privadas fueron utilizadas para entrar a su cuenta, y

físicamente no es comprobable ya que únicamente se requieren las credenciales de autenticación.

16.- Que diga el perito si ´por su estudio encomendado, logra determinar, la existencia de inconsistencias en la realización de las operaciones no reconocidas, como lo son, la falde notificaciones de autorización de dichas operaciones a la C.***** y que esta se realizaron de IPS no usados previamente por el usuario, tal como se precisa el informe técnico del banco (anexo 9, 10, y 11)

Respuestas: No se puede constatar que presuntamente no existieron notificaciones, ya que las notificaciones en un dispositivo móvil pueden ser desactivadas por el usuario, y si es en un correo electrónico, al no tener a la vista dicho correo se desconoce dicha información. En cuanto a las direcciones IP, estas cambian dependiendo el dispositivo que se utilice.

17.- Que diga el perito, si por su estudio encomendado, la información que exhibió el banco, en su contestación de demanda, de contrato, bitácoras, informes técnicos de movimiento y hechos de la banca móvil supernet, son ilegibles en su mayoría o que presentan alteraciones.

Respuesta.- La información que exhibió el banco, en su contestación de demanda, de contrato, bitácoras, informes técnicos de movimiento y hechos de la banca móvil supernet que se me puso a la vista, es legible y al ser un documento formato PDF se desconoce si supuestamente existiera una alteración ya que no son imágenes si no un documento.



CUESTIONARIO OFRECIDO POR LA DEMANDADA

a. Si existe el portal ***** en la red mundial de datos conocida como como Internet

Respuesta: Sí existe.

b. Cuál es el procedimiento y/o requisitos para iniciar una sesión de Banca Electrónica (Supernet) en dicho portal.

Respuesta: 1. Ir al navegador de internet. 2. Teclar la dirección ***** 3. De la página web que se abre seleccionar la opción “ingresar a SuperNet”, se encuentra de lado derecho de la pantalla. 4. Se abrirá otra pantalla donde se pedirá el código de cliente/Nº Tarjeta/Nº Cuenta. 5. Valida que tu imagen y frase correspondan a las que ya tenías establecidas, si son correctas, teclea tu contraseña de acceso y da clic en el botón “Continuar”. 6. Una vez dentro de tu banca se mostraran tus saldos y un resumen de tus ingresos y egresos de los últimos tres meses. 7. Se muestran las siguientes imágenes alusivas

c. Si es posible ingresar a la Banca Electrónica (Supernet) solamente con el código del cliente asignando a la parte actora

Respuesta: No es posible de acuerdo al manual de la institución bancaria se necesita validar que tu imagen y frase correspondan a las que ya tenías establecidas, si son correctas, se pide teclear la contraseña de acceso y dar clic en el botón “Continuar”

d. Si es posible ingresar a la Banca Electrónica (Super Net) sin teclear el NIP o contraseña de acceso.

Respuesta: No es posible ingresar con la pura clave. Se necesita código de cliente o N° Tarjeta o N° Cuenta, en seguida se pide validar una imagen y una frase, eso se valida poniendo la contraseña.

e. Cuál es el resultado de si es posible teclear un código de cliente y/o NIP de acceso aleatorio, que no corresponda al usuario interesado en ingresar a la Banca Electrónica (Supernet)

Respuesta: El sistema valida un código de cliente aleatorio.

f. Cuál es el resultado de teclear un código de cliente y la contraseña que el usuario haya generado para ingresar a la Banca Electrónica (Supernet)

Respuesta: Una vez dentro de banca se mostrarán tus saldos y un resumen de tus ingresos y egresos de los últimos tres.

Además, tendrás atajos a tus operaciones favoritas y a las más usadas.

g. Cuáles son los datos que requiere la Banca Electrónica (Supernet) para dar de alta una cuenta de otro Banco para poder transferir dinero a la misma.

Respuesta: **Dar de alta cuenta otro banco:** A. En el carrusel superior da clic en la opción "Cuenta tercero mismo banco" B. Captura los 11 dígitos de la cuenta. C. Captura el nombre del titular de la cuenta. D. Captura un alias para la cuenta. E. Da clic en "Aceptar". A. Valida que los datos sean correctos B. Da clic en "Confirmar". Esta operación requiere NIP dinámico, captúralo y da clic en "Aceptar". El proceso de alta de cuenta ha concluido, da



clic en “Finalizar.” **Dar de alta cuenta mismo banco.** A. Ingresa a tu banca digital. B. Desde la pantalla “Mis saldos”, da clic en la opción “Alta de Cuentas”. A. En el carrusel superior da clic en la opción “Tarjeta de crédito tercero mismo banco”. B. Captura los 16 dígitos de la tarjeta a dar de alta. C. Captura el nombre del titular de la tarjeta. D. Captura un alias para la tarjeta. E. Da clic en “Aceptar”. A. Valida que los datos sean correctos. B. Da clic en “Confirmar”. Esta operación requiere un Nip dinámico, captúralo y da clic en “Aceptar”. El proceso de alta de servicio ha concluido, da clic en “Finalizar.”

h. Si es posible realizar el alta de cuenta de tercero destino de transferencias, sin utilizar la contraseña dinámica de un solo uso en poder del usuario de banca electrónica.

Respuesta: No es posible dar de alta una cuenta sin la clave dinámica.

i. Cuáles son los datos que requiere el sistema de Banca Electrónica (Supernet) para realizar una transferencia a una cuenta de tercero.

Respuesta:

j. Si es posible realizar una transferencia a una cuenta de tercero, sin utilizar la contraseña dinámica de un solo uso en poder del usuario de banca electrónica (Supernet)

Respuesta: No es posible hacer una transferencia una cuenta de tercero sin contraseña dinámica.

k. Qué es una contraseña, como y quien la genera.

Respuesta: Es una cadena de caracteres (palabra) secreta que solo conoce quien la genera, se usa para accionar ciertos mecanismos o para acceder ciertas funciones de un sistema.

De acuerdo al manual de la misma institución bancaria define que la Clave***** es una clave numérica de 4 dígitos que usas para ingresar a Online Banking y la App*****, usar la banca telefónica y para realizar extracciones en las cajas de sucursales. El usuario la puede generar totalmente online, App***** o desde cajero Banelco.

I. Qué es la contraseña dinámica de un solo uso, como y quien la genera.

Respuesta: El código OTP es una password o contraseña de un único también conocida como password o contraseña dinámica. Se utiliza como segundo factor de autenticación. Se utiliza en entornos que requieren un alto nivel de seguridad que las contraseñas estáticas por sí solas no consiguen. Algunos ejemplos de entornos de este tipo son las conocidas bancas electrónicas.

Los tokens es un dispositivo físico, el usuario acciona para que al momento se genere la contraseña dinámica...

CONCLUSIONES: "... Habiendo realizado los estudios técnicos y análisis de la información proporcionada se establece que banca movil de ***** cuenta con mecanismos de seguridad estandarizados como por ejemplo usuario y contraseña dispositivo o APP, token , pero no puede garantizar el cien por ciento de la seguridad ya que los sistemas pueden ser vulnerados por personas expertas en tecnología de información... la información mostrada en la bitácora gran parte de ella son muy confusas y difíciles de interpretar debido a la manera de ser extraídas o al tratamiento o la manera de manipulación que se le pudo haber dado... Las transacciones reclamadas si fueran identificadas en las bitácoras mas sin embargo no se pueden identificar que se hallan ejecutado



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

los mecanismos de seguridad por cada transacción realizada.. Las bitácoras son información de transacciones u operaciones registradas y administradas por sistemas de información de la institución bancaria de manera automática... Una medida de seguridad de acuerdo con el artículo 316 bis 13 de la circular de bancos señala lo siguiente: Las Instituciones deberán mantener mecanismos de control para la detención y prevención de eventos que se aparten de los parámetros de uso habitual de sus usuarios a través de medios electrónicos... El sistema de Banco debió de haber detectado dos transacciones realizadas en el mismo día como inusual por lo tanto no llevarlas a cabo... Por lo tanto concluyo que la información del cliente es almacenada y administrada en base de datos de la propia institución bancaria y por personal autorizado por la propia institución para garantizar su integridad .. Los número del IP de donde se llevo a cabo las transacciones no reconocidas nunca antes fueron usadas por la cliente los números de IP 201.175.135.175 y 201.175.135.81 y solo se usaron una vez para realizar dichas transacciones reclamadas por lo tanto se procede a su geolocalización de las mismas y como resultado nos muestran que esas IPS su ubicación pertenece a la Ciudad de México y nos da referencia de la zona donde posiblemente puede encontrarse el equipo o aparato donde se realizaron las transacciones, también nos muestra que el proveedor de internet es la empresa AT&T México... “

Prueba pericial a la cual se le concede valor probatorio de conformidad a lo dispuesto en el numeral 1301 del Código de Comercio.

Y toda vez que los peritajes fueron contradictorios este Juzgado designo como perito tercero en discordia al M*****, cuyo dictamen se encuentra glosado a fojas 572 a 594 del principal.

a).- Que diga el perito, según su leal saber y entender, si existe el portal ***** en la red mundial de datos conocida como internet.

Respuesta.- Se hace una investigación de campo sobre la sitio WEB de***** en el link http://. Www.*****.com.mx Lo cual podemos verificar que su acceso principal cuenta con un certificado de seguridad valido y vigente. El cual cuenta con un algoritmo de encoiación sha

2.- Que diga el perito, según su leal saber y entender, cual es el procedimiento y/o requisitos para iniciar una sesión de Banca Electrónica (Supernet) en dicho portal.

Respuesta.- Para utilizar la banca electrónica de Supernet a través del sitio Web, *****, es importante seguir una serie de pasos y recomendaciones para garantizar la seguridad de tus transacciones en linea. A continuación, se detalla la información relavante que se pudo analizar.

1.- Acceso al Sitio Web. Abre tu navegador y escribe la dirección *****en la barra de direcciones

2.- Pagina de inicio de sesión: Una vez en el sitio web, serán redirigido a la pagina de inicio de sesión de Supernet, es importante que verifiques que estas en la pagina oficial de***** y que la conexión sea segura (Deberías ver un candado en la barra de direcciones “https. Al principio de la URL)



3.- Credenciales de Acceso: Ingresa tus credenciales de acceso, que generalmente consisten en un nombre de usuario y contraseña.

3.- Que diga el perito, según su leal saber entender, si es posible ingresar a la Banca Electrónica (Supernet) solamente con el código del cliente asignando a la parte actora

Respuesta: No es posible acceder a la banca electrónica de Supernet solamente utilizando el código de cliente. El código de cliente es una parte fundamental de tu identificación.

4.- Que diga el perito, según su leal saber y entender, si es posible ingresar a la Banca Electrónica (Super Net) sin teclear el NIP o contraseña de acceso.

Respuesta: No es posible acceder a la banca electrónica de Supernet, sin saber la contraseña de la banca electrotécnica, una medida de seguridad en todas las plataformas de banca en línea.

5.- Que diga el perito, según su leal saber y entender, si es posible ingresar a la Banca Electrónica (Supernet) sin teclear un código de cliente y/o NIP de acceso aleatorio, que no corresponda al usuario interesado en ingresar a la Banca Electrónica.

Respuesta.- Si alguien intenta ingresar a la banca electrónica (Supernte) de otra persona utilizando un código de cliente y/o Nio de acceso aleatorio que no corresponda al usuario legítimo, el sistema de banca electrónica verificara la información proporcionada durante

el proceso de inicio de sesión. En el caso de que el código de cliente y/o NIP ingresados no coincidan con la información almacenada en el servidor, la autenticación será fallida.

7.-según su leal saber y entender cual es el resultado de teclear el código de cliente y la contraseña que el usuario haya generado para ingresar a la Banca Electrónica.

Respuesta.- Si el código de cliente y la contraseña ingresados coinciden con la información almacenada en el sistema del banco y son correctos, el usuario obtendrá acceso autorizado a su cuenta de banca en línea .

8.- Que diga el perito, según su leal saber y entender , cuales son los datos que requiere la Banca Electrónica (Supernet) para dar de alta una cuenta de otro Banco para poder transferir dinero a la misma.

Respuesta:.-Los detalles necesarios para dar de alta una cuenta de otro banco y habilitar transferencias de dinero a través de Banca Electrónica (Supernet) los datos a requerirse incluyen:

Numero de cuenta: Deberás proporcionar el número de cuenta completo de la cuenta en el otro banco a la que deseas realizar las transferencias de dinero. Este número de cuenta es único y se encuentra en los estados de cuenta de banco receptor. Nombre del Titular de la cuenta. Clave Interbancaria o Clabe. Nombre del Banco Receptor. Alias o Descripción. Confirmación de Datos. para garantizar la precisión de la información, es posible que se le solicite ingreso alguno de estos datos nuevamente para su confirmación.



8.- Que diga el perito, según su leal saber y entender, si es posible realizar el alta de cuenta de tercero destino de transferencias, sin utilizar la contraseña dinámica de un solo uso en poder del usuario de banca electrónica.

Respuesta.- No es posible dar de alta una cuenta de tercero destino de transferencias sin utilizar una contraseña dinámica e un solo uso, depende de las políticas de seguridad y los procedimientos específicos implementados por el banco y la plataforma de banca electrónica.

9.- Que diga el perito según su leal saber y entender, cuales son los datos que requiere el sistema de Banca Electrónica (Supernet) para realizar una transferencia a una cuenta de tercero.

Respuesta. Los detalles necesarios para dar de alta una cuenta de tercero y habilitar transferencias de dinero a través de la Banca Electrónica, (Supernet) los datos a requerirse incluyen: Numero de cuenta. Nombre de la titular de la cuenta, clave interbancaria, Nombre el Banco Receptor, Alias o Descripción. Confirmación de Datos

10.- Si es posible realizar una transferencia a una cuenta de tercero, sin utilizar la contraseña dinámica de un solo uso en poder del usuario de banca electrónica (Supernet)

Respuesta.- No es posible realizar una transferencia a una cuenta de tercero sin utilizar una contraseña dinámica de un solo uso (OTP)

11.- Que diga el perito, según su leal saber y entender, que es una contraseña, como y quien la genera.

Respuesta:.- Una contraseña es una combinación secreta de caracteres, como letras, números, símbolos o una

combinación de estos, que se utiliza para autenticar la identidad de un usuario.

12.- Que diga el perito su leal y saber entender que es la contraseña dinámica de un solo uso como y quien la genera.

Respuesta.- Una contraseña de un solo uso OTP (por sus reglas en ingles one-time password), es una contraseña temporal que se genera para un solo uso o para un periodo limitado de tiempo, su principal propósito es mejorar la seguridad al proporcionar una forma de autenticación adicional mas alla de la contraseña tradicional.

CUESTIONARIO DE LA ACTORA.

1.- Que diga el perito que es y para que sirve una IP.

Respuesta.- La IP significa Protocolo de internet Se puede definir como la matricula de un dispositivo, también permite saber como se conecta ademas sirve para identificar y localizar un equipo.

2.- Que diga el perito , si logra identificar la dirección IP, fecha y hora, de beneficiario de las transacciones reclamadas.

Respuesta.- Si se puede identificar dos Ips ,que son utilizadas en la misma fecha para las transacciones reclamadas por la parte actora.

3.- Por los estudios encomendado, que diga el perito si logra identificar desde que numero de IP se realizaron las transacciones reclamadas y geolocalizar la IP.



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

Respuesta: Si se puede identificar, que son utilizadas en la misma fecha para las transacciones realizadas por la parte actora.

4.- Que diga el perito, si por su estudio encomendado, logra determinar si la IP con la que se realizo las transacciones reclamadas, se ha usado en mas de 2.

Respuesta. De acuerdo a la bitácora de transacciones que existe en el expediente, en cuestión de transferencias solo aparece el día 20/07 2020 y no se pude visualizar mas transacciones con dichas IPS

5.-Que diga el perito, cuales son los mecanismos de seguridad con que debe de contar una institución bancaria.

Respuestas: De acuerdo a la Comisión Nacional Bancaria y de Valores en sus disposiciones generales menciona lo siguiente:

Los mecanismos y procedimientos de Identificación del Usuario y Autenticación para que sus Usuarios del servicio de Banca por internet puedan autenticar a las propias instituciones al inicio de una sesión.

Los mecanismos y procedimientos para la notificación de las operaciones realizadas.

Factor de Autenticación categoria 3.

Deberán mantener procedimientos de seguridad.

6.- Que diga el perito, en que consiste el protocolo de seguridad de firma electrónica.

Respuesta.-El protocolo de seguridad de firma electrónica consiste en un conjunto de procedimientos y estandares diseñados para garantizar la autenticidad integridad y confidencialidad de los documentos y transacciones electrónicas.

7.- Que diga el perito, si en las bitácoras mostradas y operaciones reclamadas logra identificar, que se haya usuario el protocolo de seguridad de firma electrónica

Respuesta. No existe información en la imagen siguiente donde se pueda apreciar la solicitud de autenticación por ningún tipo de factor, Además de no se hace mención sobre la utilización del Token.

En las bitácoras mostradas se identifican las operaciones y movimientos realizados los cuales aparecen con un folio de identificación que en este caso sería la referencia, ip de origen y id de inicio de sesión, en los informes técnicos 9, 10 y 11 se puede visualizar el id de token en las operaciones en las tablas que se presentan en dichos documentos

8.- Que diga el perito como se relaciona el sistema de pagos electrónicos interbancarios SPEI y banco ***** así como la herramienta empalada para intercomunicarse.

Respuesta: El Sistema de Pagos Electrónicos Interbancarios (SPEI) es un sistema de transferencias electrónicas utilizado en México para realizar pagos y transferencias de fondos entre cuentas bancarias de diferentes instituciones financieras enviar y recibir dinero de manera electrónica.

9.- Que diga el perito, quien desarrolla y da mantenimiento a la aplicación informática de banca electrónica del *****.

Respuesta: Es un detalle interno de la operación del banco.



10.- Que diga el perito, que medios de almacenamiento utiliza el ***** , para almacenar la información sensible del cliente.

Respuesta: Generalmente se almacena utilizando una combinación de medios de almacenamiento y tecnologías de seguridad diseñadas para garantizar la confidencialidad, integridad y disponibilidad de los datos.

La administración y protección de la información de los clientes en ***** recae en la responsabilidad de la propia institución financiera.

11.- Que diga el perito, quien es el encargado de administrar la información de los clientes almacenada en el *****

Respuesta: La administración y protección de la información de los clientes en ***** recae en la responsabilidad de la propia institución financiera.

12.- Que diga el perito si los sistemas pueden ser vulnerados.

Respuesta.- Ningún sistema es cien por ciento confiable-

13.- Que diga el perito, si por su estudio encomendado logra determinar que la propiedad de un token, una dirección IP, contraseñas y claves de seguridad evitan que se realicen operaciones electrónicas sin consentimiento del propietario en la banca electrónica supernet.

Respuesta.- En conjunto, estos elementos contribuyen a la seguridad de la banca electrónica al requerir múltiples capas de autenticación y protección de datos.

14.- Que diga el perito, si por su estudio encomendado logra determinar que las operaciones no reconocidas fueron efectuadas físicamente por la C. ***** .

Respuesta No existe información en la imagen siguiente donde se pueda apreciar la solicitud de autenticación por ningún tipo de factor.- Prueba pericial a la cual se le concede valor probatorio en términos de lo dispuesto por el artículo 1301 del Código de Comercio.

11.- PRESUNCIONAL LEGAL y HUMANA e INSTRUMENTAL DE ACTUACIONES.- Que se desahogan atendiendo a su propia y especial naturaleza.- A las cuales se les concede valor probatorio de conformidad a lo dispuesto por los numerales 1294. 1305 y 1306 del Código de Comercio.

QUINTO. En el presente caso tenemos que ********* promueve Juicio Oral Mercantil en contra de ********* de quien reclama la nulidad de dos transferencias bancarias electrónicas no reconocidas.

Por lo que una vez que fueron analizadas las constancias procesales que integran el presente juicio, se declara **procedente** la acción ejercitada.

Así, previo al análisis de fondo del asunto se estima necesario precisar lo siguiente. Sobre el tema de la nulidad del acto jurídico, los artículos 2224, 2225, 2226, 2227 y 2239 del Código Civil Federal, de aplicación supletoria al Código de Comercio, establecen:

“Artículo 2224. El acto jurídico inexistente por la falta de consentimiento o de objeto que pueda ser materia de él, no producirá efecto legal alguno. No es susceptible de valer por confirmación, ni por prescripción; su inexistencia puede invocarse por todo interesado.



Artículo 2224.- El acto jurídico inexistente por la falta de consentimiento o de objeto que pueda ser materia de él, no producirá efecto legal alguno. No es susceptible de valer por confirmación, ni por prescripción; su inexistencia puede invocarse por todo interesado

Artículo 2226. La nulidad absoluta por regla general no impide que el acto produzca provisionalmente sus efectos, los cuales serán destruidos retroactivamente cuando se pronuncie por el juez la nulidad. De ella puede prevalecerse En mérito de lo anterior, es de concluir que los elementos de la acción de nulidad aquí promovida son los siguientes:

1. La existencia del contrato de prestación de servicios bancarios y financieros múltiples

2. La existencia de los actos cuya nulidad se pretende; y,

3.- Que exista la falta de consentimiento en dicho actos.

Por cuanto al primer elemento este se acredita, con el contrato de Prestación Servicios Bancarios y Financieros Múltiples, celebrado entre ***** y la ***** , anexado a la solicitud multioferta de de fecha 21 de septiembre del año 2012.

Así también se acredita la alta de un tercero con cuenta de Scotiabank y las dos transferencias bancarias no reconocidas, la primera por la cantidad de \$48,00.00 (cuarenta y ocho mil pesos 00/100 MN) de fecha veinte de julio del año dos mil veinte, a las 12:08:34 y la segunda por la cantidad de \$48,00.00 (cuarenta y ocho mil pesos 00/100 MN) de fecha veinte de julio del año dos mil veinte a las 15:41:03 horas, que dan un total de \$96,000.00

(noventa y seis mil pesos 00/100 mn) desde la cuenta numero 56637857613 a la cuenta con terminación 2950088 de Scotiabank, ambas por la cantidad de \$48,000.00 (cuarenta y ocho mil pesos 00/100 MN) las cuales se hicieron el día veinte de julio del año dos mil veinte, estas se acreditaron con los comprobantes de transferencias bancarias, exhibidos por el Banco, así como con los informes técnicos elaborados los días 26 de noviembre de 2020, 30 de septiembre y 30 de octubre del 2021, por las áreas internas de prevención y seguridad y de reclamaciones del Banco, en el que se desprenden, el alta de la cuenta de tercero y las dos transferencias bancarias no reconocidas por la actora.

Y por ultimo por cuanto a la falta de consentimiento, es decir si fue o no la actora quien realizo las transferencias bancarias de su cuenta de débito, tenemos que de conformidad a lo dispuesto por los artículos 1194, 1195 y 1196 del Código de Comercio, la carga de la prueba de los hechos controvertidos se impone a la parte que tenga mayor facilidad para aportar los medios conducentes y a quien desconoce una presunción legal que tiene a su favor el colitigante, de ahí que en el presente caso al tratarse de transferencias no reconocidas por el actor, sea el Banco al que le corresponda acreditar que dichos movimientos se hicieron siguiendo los protocolos establecidos, pues es este quien tiene mayor facilidad para aportar los medios de convicción que justifiquen que dichos movimientos fueron realizados por la parte actora, lo anterior es así porque de conformidad con las Disposiciones de carácter general



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

aplicables a las Instituciones de Crédito, emitidas por la Comisión Nacional Bancaria y de Valores publicadas en el Diario Oficial de la Federación el dos de diciembre del año dos mil cinco, las Instituciones Bancarias pueden acordar con los usuarios el servicio de Banca por Internet, para lo cual se deben asegurar que las operaciones estén consentidas por los cuentahabientes, a través del uso de identificadores de usuarios, contraseñas y factores de autenticación de las categorías 2, 3, 4 señalados en el artículo 310 de esas disposiciones, y tienen la obligación de generar y preservar registros, bitácoras, huellas de auditoría, de las operaciones y servicios que contengan por lo menos, los accesos realizados por los usuarios, la fecha, hora, número de cuenta origen, cuenta destino y demás información que permita el mayor número de elementos involucrados en el acceso u operación de los medios electrónicos, los datos del dispositivo de acceso utilizado, los protocolos de internet; de ahí que sea el Banco quien posea la información para acreditar la fiabilidad de su sistema electrónico y el empleo de las claves de seguridad, por lo que es al Banco al que le corresponda acreditar que las disposiciones se hicieron conforme al contrato que fue la actora quien realizó las transacciones, que el sistema para realizar dichas transferencias es fiable y que no fue vulnerado, para lo cual requiere de que se exhiba el peritaje en la materia.

Tiene sustento legal el siguiente criterio Tesis
Registro digital: 2023157 **Instancia:** Primera Sala **Undécima**
Época **Materia(s):** Civil **Tesis:** 1a./J. 17/2021 (10a.) **Fuente:**
Gaceta del Semanario Judicial de la Federación. Libro 1, Mayo de

2021, Tomo II, página 1752 **Tipo:** Jurisprudencia

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 fue sabotada 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



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

procedimiento exigido por las disposiciones de carácter general, aplicables a las instituciones de crédito, emitidas por la Comisión Nacional Bancaria y de 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.

Luego entonces tenemos que el Banco a efecto de acreditar que las transferencias bancarias fueron realizadas por el cliente y que se cumplió con la normatividad aplicable, exhibe los Informes Técnicos elaborados por su representada en donde constan las las operaciones que se tachan de nulas , en donde se desprende que se especifican las operaciones no



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

reconocidas, la fecha y hora el tipo de movimiento, la cantidad, cuenta de cargo cuenta de abono e importe; empero no especifica la identificación del dispositivo utilizado en dichas transacciones, ni se advierte que consten las notificaciones al usuario de las transacciones; de ahí que dichas bitácoras no cumplan con los requisitos establecidos por el artículo 316 de las disposiciones emitidas por la Comisión Nacional Bancaria y de Valores

Por otro lado el Banco a efecto de acreditar que el sistema es fiable y que las transacciones las hizo el cliente mediante los medios de autenticación otorgados, desahogo la prueba pericial que estuvo a cargo la Ingeniero en Sistemas computacionales ***** , más sin embargo a dicho peritaje no se le otorgo valor probatorio en atención a que la perito no dio respuesta a la totalidad de las interrogantes planteadas por las partes., específicamente no dio respuesta a las interrogantes propuestas por la parte actora, en los siguientes incisos i).- Que diga el perito, quien desarrolla y da mantenimiento a la aplicación informática de banca electrónica del ***** . j).- Que medios de almacenamiento utiliza el ***** para almacenar la información del cliente. K).- Que diga el perito quien es el encargado de administrar la información de los clientes almacenada en el *****; dado que respondió que desconoce dicha información ya que pertenece a un protocolo interno o medida de seguridad propia del Banco ***** , interrogantes que eran determinantes para establecer la seguridad con la que cuenta el sistema de internet con el que cuenta el Banco.

De ahí que el Banco no haya acreditado que su sistema no fue vulnerado, y que las transferencias fueron realizadas por la parte actora.

Lo anterior además porque dentro de los peritajes exhibidos se aborda de que para dar e alta la cuenta de un tercero de otro banco es necesario el Token, y que el mismo fue utilizado en las operaciones realizadas, más sin embargo la parte actora en la prueba confesional refirió que no cuenta con dicho dispositivo, y el banco no acreditó, la entrega del mismo, por otro lado el perito de la parte actora expuso un dato relevante en su pericial consistente en que las direcciones de los protocolos de internet desde los cuales se hicieron dichas transferencias, refiere que corresponden a 201175135.175, más sin embargo, del propio dictamen observa que se inserta una tabla de las transacciones realizados por el cliente del periodo 28/04/2020 al 20/07/2020,, advirtiéndose que en dicha tabla no aparece la IP desde las cuales se hicieron las transferencias bancarias que en este juicio se reclaman, por lo que se presume que dicha IP al momento de su realización era inusual, en razón de que en las bitácoras exhibidas no existe antecedente de la misma; de ahí que se presuma si dichas transacciones se realizaron desde una IP inusual,

En esta tesitura y atendiendo a que las mismas eran por cantidades considerables, el Banco por precaución debió de dar por terminada la sesión automáticamente y suspender la utilización del servicio de banca electrónica o rechazar la operación, con base en la interpretación de



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

lo dispuesto por los artículos 316 Bis 2, fracción I, Inciso b), 316 bis 15, fracción I, Inciso d), de las Disposiciones de carácter General aplicables a las Instituciones de Crédito, emitidas por la Comisión Nacional Bancaria y de Valores, publicadas en el Diario Oficial de la Federación el 2 de Diciembre del 2005 y modificadas mediante resolución publicada el veintisiete de enero del año dos mil diez, en donde se establece que los Bancos deberán proveer lo necesario para que una vez autenticado el usuario en el servicio de Banca electrónica de que se trate, la sesión no pueda ser utilizada por un tercero y que, las instituciones deberán establecer, al menos, los mecanismos de seguridad del sistema de banca electrónica siguientes: dar por terminada la sesión en forma automática e informar al usuario cuando en el curso de una sesión del servicio de banca por internet, la institución identifique cambios relevantes en los parámetros de comunicación del medio electrónico, tales como la identificación del dispositivo de acceso “rango de direcciones de los protocolos de comunicación, ubicación geográfica, entre otros”, así mismo las Instituciones financieras están facultadas para detectar y prevenir eventos apartados de los parámetros de uso habitual de los usuarios, como suspender la utilización del servicio de banca electrónica, o en su caso, de la operación que se pretenda realizar, en el evento de que cuenten con elementos que hagan presumir que el identificador de usuario o los factores de autenticación no están siendo utilizados por el usuario.

Tiene sustento legal a lo anterior el siguiente criterio :

Tesis Instancia: Tribunales Colegiados de Circuito
Undécima Época Materia(s): Civil Tesis: III.2o.C.5 C

(11a.) **Fuente:** Gaceta del Semanario Judicial de la Federación. Libro 16, Agosto de 2022, Tomo V, página 4610 **Tipo:** Aislada **Registro digital:** 2025074

TRANSFERENCIAS ELECTRÓNICAS BANCARIAS. CUANDO LA DIRECCIÓN DE PROTOCOLO DE INTERNET (IP) TIENE UN LUGAR DE ORIGEN INUSUAL Y A PESAR DE ELLO EL BANCO AUTORIZA LA OPERACIÓN SIN ANTES SUSPENDER EL SERVICIO DE BANCA ELECTRÓNICA O RECHAZAR LA TRANSACCIÓN PRECAUTORIAMENTE, DEBE CONSIDERARSE QUE EL CLIENTE NO OTORGÓ SU CONSENTIMIENTO, AUN CUANDO SE HAYAN UTILIZADO TODOS LOS FACTORES DE AUTENTICACIÓN NECESARIOS PARA APROBARLA.

Hechos: En un juicio oral mercantil el cuentahabiente demandó a la institución de crédito por la nulidad de una transferencia electrónica bancaria; seguida la controversia en todas sus etapas, el Juez responsable emitió sentencia definitiva en la cual declaró la nulidad absoluta de la operación, principalmente, por considerar que no existía certeza de que el cuentahabiente otorgó su consentimiento en la transacción, pues el lugar de origen de la dirección de protocolo de Internet desde donde se realizó no era usual para la actora, al corresponder al área geográfica de otro país. Criterio jurídico: Este Tribunal Colegiado de Circuito determina que cuando la dirección de protocolo de Internet (IP) tiene un lugar de origen inusual de operaciones del cuentahabiente y a pesar de ello el banco la autoriza sin suspender el servicio de banca electrónica o rechazar la transacción precautoriamente, debe considerarse que el cliente no otorgó su consentimiento, aun cuando se hayan



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

utilizado todos los factores de autenticación necesarios para aprobar la transferencia electrónica bancaria. Justificación: Lo anterior, porque de los artículos 316 Bis 2, fracción I, inciso b), 316 Bis 13 y 316 Bis 15, fracción I, inciso d), de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores, publicadas en el Diario Oficial de la Federación el 2 de diciembre de 2005 y modificadas mediante resolución publicada en el mismo medio de difusión el 27 de enero de 2010, se advierte que los bancos deberán proveer lo necesario para que una vez autenticado el usuario en el servicio de banca electrónica de que se trate, la sesión no pueda ser utilizada por un tercero y que, para efectos de lo anterior, las instituciones deberán establecer, al menos, los mecanismos de seguridad del sistema de banca electrónica siguientes: dar por terminada la sesión en forma automática e informar al usuario cuando en el curso de una sesión del servicio de banca por Internet, la institución identifique cambios relevantes en los parámetros de comunicación del medio electrónico, tales como la identificación del dispositivo de acceso "rango de direcciones de los protocolos de comunicación, ubicación geográfica, entretros"; asimismo, las instituciones están facultadas para detectar y prevenir eventos apartados de los parámetros de "uso habitual" de los usuarios, como suspender la utilización del servicio de banca electrónica o, en su caso, de la operación que se pretenda realizar (lo que implica rechazarla), en el evento de que cuenten con elementos que hagan presumir que el identificador de usuario o los factores de autenticación no están siendo utilizados por el propio usuario; igualmente,

que en las bitácoras generadas de su parte, las instituciones de crédito deberán registrar las direcciones de los protocolos de Internet o similares. Con base en lo anterior, el hecho de que el protocolo o dirección de protocolo de Internet desde la cual se originó la operación cuya nulidad se pretende, corresponda a una área geográfica de otro país, cuando el domicilio principal del cliente registrado en el contrato bancario está ubicado en México, y el objeto de dicha operación haya sido la transferencia de miles de pesos, ante los ojos de cualquier observador racional, constituye una actividad inusual que amerita, por precaución básica, dar por terminada la sesión automáticamente y suspender la utilización del servicio de banca electrónica o rechazar la operación, con base en la interpretación armónica y aplicación de los preceptos 316 Bis 2, fracción I, inciso b) y 316 Bis 13 citados. Así, el hecho de que la operación impugnada se haya originado desde esa dirección de protocolo de Internet inusual (de Israel, sea porque quien robó la identidad haya estado verdaderamente en ese país o haya utilizado un programa para disfrazar su ubicación real a través de ese protocolo), y aun así la institución de crédito haya autorizado la transferencia, revela que el banco omitió seguir los procedimientos establecidos normativamente para la fiabilidad de la operación y, por el contrario, ello demuestra la falta de seguridad de sus sistemas electrónicos, pues un dato tan grave y evidente como lo es lo inusual de la ubicación geográfica de la dirección de protocolo de Internet de donde procedió la operación, no fue detectado por sus mecanismos de seguridad. De ahí que ante la apuntada deficiencia en los filtros de seguridad de la



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

institución de crédito en la prestación del servicio de banca electrónica, no puede considerarse que el cuentahabiente otorgó su consentimiento en la operación impugnada, a pesar de que se pudieran o no haber utilizado todos los datos de autenticación del cliente, como lo pueden ser nombres de usuarios, claves, claves dinámicas derivadas de tokens, o cualquier otro factor de autenticación, pues es sabido que los grupos delictivos obtienen los datos confidenciales de los clientes a través de engaños, que luego pueden usarse para autenticar transacciones fraudulentas

Establecido lo anterior resulta procedente entrar al estudio de las excepciones opuestas por el demandado consistentes en: **1.- FALTA DE ACCIÓN Y DE DERECHO**, Para ejercer una acción en juicio se requieren la existencia de un derecho y la violación de este. En la especie, la parte actora reclama la nulidad de un alta de cuenta de tercero y de dos cargos en su cuenta número 56637857613, correspondientes a transferencias electrónicas de dinero (SPEI) que dice no haber realizado por un importe total de \$96,000.00. Del contrato de prestación de servicios bancarios y la aceptación del uso de medios electrónicos, se desprende que la parte actora puede disponer de sus fondos, entre otras formas, a través de la banca electrónica, mediante las claves de acceso confidenciales que obran en su poder y los filtros de seguridad dispuesto por el Banco, tanto para ingresar al sistema, como para dar de alta cuentas de destino y

L'MDG / L'MGM / NGE

realizar transferencias de recursos, En este caso los medios de acceso a la banca electrónica y FACTORES DE AUTENTIFICACIÓN asignados a la parte actora son los siguientes: 1.- El código de cliente.2.- El número de identificación personal (NIP) generado por la propia usuaria y que solo ella conoce. 3.- La contraseña dinámica de un solo uso (OTP) generada por el dispositivo en poder de la usuaria. Para utilizar la banca electrónica hay que acceder al portal Supernet de banco www.*****.com,mx, a través de la red mundial de datos conocida como Internet. El acceso a dicho portal solo es posible tecleando el código del cliente con el que se identifica al titular de la cuenta y el Número de Identificación Personal que éste haya creado para tal efecto y que solo es de su conocimiento. Adicionalmente, tanto para dar de alta cuentas de destino, como para ejecutar transferencias SPEI, es indispensable teclear la contraseña dinámica de un solo uso (Super Token) que obra en poder del cliente. Estos elementos constituyen la firma electrónica del cliente, lo que genera un vínculo jurídico que torna incuestionable la sutoria del titular inclusive, de acuerdo con el contrato, el Banco se encuentra obligado a realizar las operaciones que el cuentahabiente le ordene mediante el uso de su firma electrónica. En el presente caso, tal y como se indico al contestar el hecho 2 de la demanda, esta registrado el ingreso a la banca electrónica del cliente para dar de alta la cuenta destino, espero mas de una hora para que esta quedará activa, después volvió a ingresar a la banca electrónica y efectuó una transferencia. Todas estas operaciones utilizando una contraseña dinámica de un



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

solo uso diferente, generadas por el Super Token en poder del cuentahabiente. Por lo tanto, se trata de operaciones ordenadas por el cliente, llevadas a cabo a través de banca electrónica con su firma electrónica, que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio, conforme a lo previsto en los artículos 52 de la Ley de Instituciones de Crédito y 89 del Código de Comercio, en consecuencia, se puede concluir que no se ha lesionado derecho alguno en perjuicio de la parte actora. **Excepción que una vez analizada se declara improcedente**, en atención, a que si bien ha quedado de manifiesto todos los mecanismos de autenticación y seguridad que se utilizan para realizar una transferencia bancaria, también lo es que como ha quedado expuesto líneas arriba, era necesario que el Banco acreditara que su sistema cumple con la normatividad aplicable y que su sistema no fue vulnerado, lo cual no acredito, en atención a que como se expuso las bitácoras no contienen todos los datos que deben quedar registrados, y la prueba pericial no le fue otorgado valor probatorio. **2.- CONSENTIMIENTO /EXCLUSIÓN DE RESPONSABILIDAD.** Conforme a lo pactado en el contrato de prestación de servicios bancarios, transcrito parcialmente al contestar el hecho 1 de la demanda, el uso de las CLAVES DE ACCESO es exclusiva responsabilidad del CLIENTE, quien reconoce y acepta como suyas todas las operaciones que se celebren con el BANCO utilizando dichas claves de Acceso, y para todos los efectos legales a que haya lugar, expresamente también reconoce y acepta el carácter personal e intransferible del Código de Cliente y Nips, así como su

absoluta confidencialidad, . Asimismo de conformidad a lo señalado en el Título Segundo, Libro Segundo, del Código de Comercio, denominado “Del comercio electrónico”, según el cual el uso de los medios de identificación que se establezcan en sustitución de la firma autógrafa, producirían los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio, en virtud de ello, las Claves de Acceso establecida para el uso de medios electrónicos, sustituyen a la firma autógrafa por una de carácter electrónico, y las constancias documentales o técnicas derivadas del uso de los medios en donde aparezca dicha firma electrónica, producirían los mismos efectos que las leyes otorgan a los documentos suscritos por las partes y tendrían igual valor probatorio. Asimismo se libero de responsabilidad al banco al ejecutar instrucciones recibidas mediante las claves de acceso a la banca electrónica del cliente. En el presente caso la parte actora reclama un alta de cuenta de tercero y dos transferencias de dinero a cuenta de tercero que, para poderse llevar a cabo, implico el uso de la banca electrónica, Siendo que, para poder ingresar a banca electrónica se requiere forzosamente utilizar el código del cliente y la contraseña o número de identificación personal que el cliente genera y solo el reconoce y para dar de alta cuentas de terceros y transferir dinero a las mismas, se utiliza la contraseña dinámica de un solo uso generada por el dispositivo electrónico Super Token en poder del cliente. Por lo tanto al ser elementos confidenciales y en poder del cliente se presupone que fueron llevados a cabo por el mismo. Es decir, existe una expresión de su voluntad captando este



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

tipo de cargos, por lo tanto no hay vicio que afecte la validez de los mismos. Hay que mencionar también que no existe evidencia alguna de que el sistema de banco haya sido vulnerado o intervenido ilícitamente como lo supone el actor. Siendo aplicable al caso concreto, el artículo 1803 del Código Civil Federal, que a la letra dice: Art. 1803: El consentimiento puede ser expreso o tacito, para ello se estará a lo siguiente: I.- Será expreso cuando la voluntad se expresa verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y II.- El tacito resultara de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente. Por lo tanto opera a favor del Banco la cláusula señalada, que lo libera de cualquier responsabilidad por ejecutar instrucciones a través de los medios electrónicos puestos a disposición del cliente, mediante el uso de las claves de acceso en poder del cliente, aún y cuando estas hubiesen sido robadas. **3 Excepción que una vez analizada se declara improcedente**, en atención a que dicha clausula a que hace referencia no libera al banco de acreditar que su sistema no fue vulnerado, lo que consta de autos no acreditado, en razón de que la prueba pericial ofrecida no se le concedió valor probatorio. **3. VICIOS DEL DICTAMEN VALORACIÓN TÉCNICA Y JURÍDICA**, conforme a lo mencionado al contestar los hechos 3, 4 y 5 de la demanda y que pido se tengan por aquí mencionado a l contestar los hechos 3, 4, y 5 de la demanda y que pido se tengan por aquí reproducidos debiéndose considerar dicho instrumento como infundado e inmotivado y que no

sirve para producir convicción sobre la procedencia de la acción intentada por la parte actora. **Excepción que una vez analizada se declara improcedente**, en razón de que dicho dictamen se trata meramente de una opinión, el que sirve como una prueba mas, empero el mismo no tiene fuerza vinculatoria ni obliga a ninguna de las partes,

Atento a lo anterior se declara **procedente** el presente **Juicio Oral Mercantil** promovido por *********, en contra de ********* en consecuencia, se declara la nulidad absoluta de la operación de alta de beneficiario de otro banco de la cuenta terminación 22950088 de Scotiabank, numero de referencia 7686072 para autorizar transferencias de la cuenta 56637857613, de la titular *********, a través de SuperNet, en fecha 20 de julio del 2020, así como la nulidad absoluta de la disposición de la cantidad de \$48,000.00 (cuarenta y ocho mil pesos 00/100 MN), sin autorización de la titular *********, de la cuenta número 56637857613, por transferencia electrónica SPEI a través de SUPERNET, a la cuenta con terminación 2950088 de Scotiabank de fecha 20 de julio del 2020, numero de referencia 3637259, que se identifica con clave rastreo terminación 451063690., así como la nulidad absoluta de la disposición de la cantidad de \$48,000.00 (CUARENTA Y OCHO MIL PESOS 00/100 M.N.) sin autorización de la titular *********, de la cuenta número 56637857613, por transferencia electrónica SPEI a través de SUPERNET, a la cuenta con terminación 2950088 de Scotiabank de fecha 20 de julio del 2020, numero de referencia 6213803, identificada con clave de rastreo terminación



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

453931420, por lo que se le condena a la parte demandada a la restitución y devolución de la cantidad total de \$96,000.00 (noventa y seis mil pesos 00 /100 MN) en favor de la actora que se dispuso indebidamente de la cuenta 56637857613, a través de dos transferencias electrónicas SPEI a través de Supernet, descritas líneas arriba, efectuadas el día veinte de julio del año dos mil veinte, a la cuenta termina 2950088 de Scotiabank, sin autorización de la titular *****

Así mismo y con fundamento en lo dispuesto por el artículo 362 del Código de Comercio, se condena a la demandada al pago del interés legal a razón del 6% anual, generados desde la fecha en que se efectuaron las transferencias bancarias no reconocidas hasta la total liquidación del adeudo.

Lo cual tiene sustento en la siguiente jurisprudencia: Primera Sala Undécima Época Materia(s): Civil Tesis: 1a./J. 93/2023 (11a.) Fuente: Semanario Judicial de la Federación. Tipo: Jurisprudencia Tesis Registro digital: 2026917 **CARGOS NO RECONOCIDOS A TARJETA DE DÉBITO. PROCEDE EL PAGO DE INTERESES MORATORIOS POR LA DISPOSICIÓN DE DINERO SIN AUTORIZACIÓN DEL CUENTAHABIENTE A PARTIR DE QUE ÉSTE HACE EL AVISO CORRESPONDIENTE Y LA INSTITUCIÓN BANCARIA NO REEMBOLSA LAS CANTIDADES SUSTRÁIDAS.** Hechos: Un Tribunal Colegiado de Circuito y un Pleno de Circuito sostuvieron un criterio distinto al analizar a partir de qué momento deben

computarse los intereses moratorios con base en el artículo 362 del Código de Comercio por cargos indebidos realizados a cuentahabientes de una institución bancaria, a los que obliga la jurisprudencia 1a./J. 61/2020 (10a.), de rubro: "CARGOS NO RECONOCIDOS A TARJETA DE DÉBITO. PROCEDE EL PAGO DE INTERESES MORATORIOS POR LA FALTA O RETRASO EN LA RETRIBUCIÓN DE LAS CANTIDADES SUSTRÁIDAS, EN TÉRMINOS DEL ARTÍCULO 362 DEL CÓDIGO DE COMERCIO." Criterio jurídico: La Primera Sala de la Suprema Corte de Justicia de la Nación considera que el pago de intereses moratorios reclamados con base en el artículo 362 del Código de Comercio, **debe contabilizarse a partir del aviso que hace la persona tarjetahabiente a la institución bancaria** sobre los cargos no reconocidos y no a partir de la sentencia que declara la nulidad de los actos que originaron esta situación. Justificación: Se afirma lo anterior, pues en términos de la jurisprudencia 1a./J. 61/2020 (10a.) citada y del análisis sistemático a los artículos 267, 271, 272 y 273 de la Ley General de Títulos y Operaciones de Crédito; 332, 333, 334, 335 y 338 del Código de Comercio; 46, 48, fracción I, y 48 Bis 2 de la Ley de Instituciones de Crédito y demás aplicables en materia bancaria, tratándose de cargos no reconocidos efectuados con tarjeta de débito, la institución financiera depositaria tiene la obligación de conservación y restitución del dinero cuya propiedad le transfirió la persona cuentahabiente y, por ende, cuando ocurre esta situación tendrá el deber de responder por los montos sustraídos y, si la institución bancaria depositaria del dinero no restituye el monto del



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

cargo no reconocido a la titular de la tarjeta de débito vinculada a la cuenta de depósito que contrató, deberá pagar los intereses moratorios en razón del 6% (seis por ciento) anual, en términos del artículo 362 del Código de Comercio. Esto se debe a que la responsabilidad que provoca el descuido del dinero surge desde que se detecta su indebida disposición y no hasta la resolución favorable que se dicte en el proceso o procedimiento al que se obliga a la persona cuentahabiente a accionar para recuperar el dinero que la institución bancaria se niega a devolver, a pesar de tener que reembolsarlo; por tanto, no es adecuado acudir a la regla de que el acto produce sus efectos hasta en tanto no se declare su nulidad, como lo disponen los artículos 2226 y 2229 del Código Civil Federal, puesto que ésta se produce cuando es necesario acudir a juicio para demostrar un punto de derecho y, en este caso, la institución bancaria no debe obligar a sus clientes a reclamar lo que es suyo mediante un proceso o procedimiento, ya que la devolución de lo descuidado debe efectuarse con el solo aviso que realiza el cuentahabiente

Sin que se condene al demandado al pago de gastos y costas, en virtud de que no se advierte temeridad o mala fe de su parte, al no situarse en ninguno de los supuestos que establece el numeral 1084 del Código de Comercio

Por lo expuesto y con fundamento en los artículos 1049, 1054, 1321, 1322, 1324, 1325, 1327, 1390 Bis 39 y demás relativos del Código de Comercio; es de resolverse y se:

RESUELVE:

L'MDG / L'MGM / NGE

PRIMERO. La parte actora acreditó su acción, y la demandada no acreditó sus excepciones, por lo tanto.-

SEGUNDO. Ha procedido el presente juicio Oral Mercantil, promovido por ***** , en contra de*****

TERCERO. Se declara la nulidad absoluta de la operación de alta de beneficiario de otro banco de la cuenta terminación 22950088 de Scotiabank, número de referencia 7686072 para autorizar transferencias de la cuenta 56637857613, de la titular***** , a través de SuperNet, en fecha 20 de julio del 2020.

SEGUNDO: Se declara la nulidad absoluta de la disposición de la cantidad de \$48,000.00 (cuarenta y ocho mil pesos 00/100 MN), sin autorización de la titular***** , de la cuenta número 56637857613, por transferencia electrónica SPEI a través de SUPERNET, a la cuenta con terminación 2950088 de Scotiabank de fecha 20 de julio del 2020, a las 12:08:34 horas, número de referencia 3637259, identificada con clave rastreo terminación 451063690.

TERCERO.- Se declara la nulidad absoluta de la disposición de la cantidad de \$48,000.00 (CUARENTA Y OCHO MIL PESOS 00/100 M.N.) sin autorización de la titular***** , de la cuenta número 56637857613, por transferencia electrónica SPEI a través de SUPERNET, a la cuenta con terminación 2950088 de Scotiabank de fecha 20 de julio del 2020, hora 15:41:10 número de referencia 6213803, identificada con clave de rastreo terminación 453931420,



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

CUARTO.- Por lo que se le condena a la parte demandada a la restitución y devolución de la cantidad total de \$96,000.00 (noventa y seis mil pesos 00 /100 MN), que se dispuso indebidamente de la cuenta 56637857613, a través de dos transferencias electrónicas SPEI a través de Supernete, descritas líneas arriba,

QUINTO .- Así mismo y con fundamento en lo dispuesto por el artículo 362 del Código de Comercio, se condena a la demandada al pago del interés legal a razón del 6% anual, desde la fecha en que se efectuaron las transferencias bancarias no reconocidas hasta la total liquidación del adeudo.

SEXTO.. Sin que se condena a la demandada al pago de las costas del juicio, por las razones expuestas en la parte considerativa de la presente resolución.

NOTIFÍQUESE PERSONALMENTE.- Así lo resolvió y firman electrónicamente la Licenciada María de Lourdes Domínguez Gómez, Jueza Primero de Primera Instancia de lo Civil del Segundo Distrito Judicial del Estado, actuando con la Licenciada Ma. Ignacia Galicia Martínez, Secretaria de Acuerdos que autoriza. Doy fe.-

Licenciada María de Lourdes Domínguez Gómez
Jueza Primero Civil

Licenciada Ma. Ignacia Galicia Martínez
Secretaria de Acuerdos

Enseguida se publicó en lista de acuerdos.- Conste.-

L'MDG/L'nege

L'MDG / L'MGM / NGE

Notifíquese a las partes que, de conformidad con el Acuerdo 40/2018 del Consejo de la Judicatura de fecha doce de diciembre de dos mil dieciocho, una vez concluido el presente asunto contarán con 90 (noventa) días para retirar los documentos exhibidos, apercibidos de que en caso de no hacerlo, dichos documentos serán destruidos junto con el expediente.

La licenciada NORMA EDITH GUZMAN ENRIQUEZ, Secretario Proyectista, adscrito al JUZGADO PRIMERO CIVIL DEL SEGUNDO DISTRITO, hago constar y certifico que este documento corresponde a una versión pública de la resolución número 279 dictada el LUNES, 23 DE OCTUBRE DE 2023 por la JUEZ PRIMERO CIVIL DEL SEGUNDO DISTRITO, constante de 74 fojas útiles. Versión pública a la que de conformidad con lo previsto en los artículos 3 fracciones XVIII, XXII, y XXXVI; 102, 110 fracción III; 113, 115, 117, 120 y 126 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas, y trigésimo octavo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas; se suprimieron: el nombre de las partes, el de sus representantes legales, sus domicilios, y sus demás datos generales, información que se considera legalmente como confidencial, sensible o



GOBIERNO DE TAMAULIPAS
PODER JUDICIAL

reservada por actualizarse lo señalado en los supuestos normativos en cita. Conste.

Documento en el que de conformidad con lo previsto en los artículos 3 fracciones XXIV; 90, 91 fracción III; 97, 98, 100, 103, 108 Y 109 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas, se suprimió la información considerada legalmente como reservada o confidencial que encuadra en el ordenamiento mencionado.

Versión pública aprobada en la Sesión de Instalación del nuevo Comité de Transparencia del Poder Judicial del Estado, celebrada el 29 de abril de 2026.