the answer company™
THOMSON REUTERS®

Vouchers de cargos bancarios con firma electrónica fraudulenta: Carga de la prueba

MIRAMONTES
CONTADORES PUBLICOS Y CONSULTORES

C.P.C. Héctor Manuel Miramontes Soto, Socio de Miramontes Soto y Asociados, S.C.

Socio fundador y Director de la firma
Actividades: Experiencia en asuntos tributarios, medios de defensa fiscal y consultoría corporativa
Tiene 31 años en la firma

INTRODUCCIÓN

Recientemente se publicaron dos tesis aisladas dictadas por el Tercer Tribunal Colegiado en Materia Civil del Primer Circuito, con motivo del juicio de amparo directo 499/2016, promovido contra BBVA Bancomer, S.A., I.B.M., Grupo Financiero BBVA Bancomer, resuelto con fecha 10 de agosto de 2016, bajo los rubros **VOUCHERS. *CARGA DE LA PRUEBA DE CARGOS EFECTUADOS MEDIANTE EL USO DE LA FIRMA ELECTRÓNICA, y FIRMA ELECTRÓNICA. REQUISITOS PARA CONSIDERARLA AVANZADA O FIABLE***, identificadas bajo los números de registro 2014564 y 2014545, respectivamente, mediante las cuales, de manera medular, se establecen las siguientes cuestiones a considerar.

En la primera de ellas, se analiza si en el caso de cargos efectuados mediante el uso de firma electrónica relacionados con una tarjeta de crédito en la que el tarjetahabiente asumió el uso de la firma electrónica como fuente de obligaciones, que sólo él conoce y que lo único que está a discusión es si el tarjetahabiente efectuó la operación, debe de estimarse que su cuestionamiento compete a quien lo pone en tela de juicio, bajo el principio ontológico de la carga de la prueba, según el cual: *Lo ordinario se presume y lo extraordinario se prueba*, siendo lo ordinario, que las terminales punto de venta (TPV) y el sistema operativo, *no sean vulnerables*, por lo que corresponde la carga de la prueba a quien alega lo contrario.

En la segunda de las tesis en cita, se señala que, de conformidad con los artículos 89 y 97 del Código de Comercio (CCom); las reglas 2, 6 y 7 de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre las firmas electrónicas, así como la Guía para su Incorporación al Derecho Interno, *el uso de la firma electrónica en las operaciones bancarias constituye*

una fuente válida de obligaciones para los tarjetahabientes que se vinculan a dicho mecanismo de seguridad, para las transacciones comerciales, debido a que los medios electrónicos han permitido realizar operaciones comerciales entre personas que se encuentran en distintos lugares, cuestión que obstaculiza el perfeccionamiento del acto jurídico mediante la firma autógrafa.

La primera tesis en comento, es del tenor siguiente:

VOUCHERS. ***CARGA DE LA PRUEBA DE CARGOS EFECTUADOS MEDIANTE EL USO DE LA FIRMA ELECTRÓNICA.*** *Cuando en la contestación a la demanda, la institución bancaria demandada expone que las operaciones reclamadas fueron realizadas a través de medios electrónicos, mediante el uso de la firma electrónica del cuentahabiente que generó folios que demuestran la existencia, así como la validez de cada operación y exhibe copia certificada del* voucher *que contiene la manifestación de que el cargo fue autorizado con firma electrónica, debe señalarse que el banco emisor asume la carga probatoria de la validez de los cargos realizados y arroja al tarjetahabiente la carga de desvirtuar la fiabilidad de la firma, por lo que debe probar que las operaciones se hicieron a través de una mecánica distinta a la prevista contractualmente, es decir, sin la utilización de la firma electrónica o mediante ésta, por persona distinta al cliente, sin su autorización y que dio aviso a la demandada del robo, pérdida, extravío o mal uso de cualquiera de los dispositivos de seguridad, incluyendo la firma electrónica, ya que el cargo genera la presunción legal del consentimiento en la operación. Así, la distribución de la carga de la prueba en el caso de cargos efectuados mediante el uso de firma electrónica deberá tomar en consideración que el uso de la tarjeta de crédito tiene su origen en un contrato en el que el tarjetahabiente asumió el uso de la firma electrónica como fuente de obligaciones, que sólo él conoce y que lo único que está a discusión es si el tarjetahabiente efectuó la operación,* ***por lo que su cuestionamiento compete a quien lo pone en tela de juicio bajo el principio ontológico de la carga de la prueba, según el cual, lo ordinario se presume y lo extraordinario se prueba, siendo lo ordinario que las terminales punto de venta (TPV) y el sistema operativo no sean vulnerables, por lo que corresponde la carga de la prueba a quien alega lo contrario***.

TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.

Amparo directo 499/2016. BBVA Bancomer, S.A., I. de B.M., Grupo Financiero BBVA Bancomer. 10 de agosto de 2016. Unanimidad de votos. Ponente: Víctor Francisco Mota Cienfuegos. Secretaria: María Estela España García.

Esta tesis se publicó el viernes 16 de junio de 2017 a las 10:22 horas en el Semanario Judicial de la Federación.

No. de Registro 2014564. Semanario Judicial de la Federación. *Décima Época. Tribunales Colegiados de Circuito. Materia civil. Tesis aislada. Tesis I.3o.C.265 C (10a.). Publicación: viernes 16 de junio de 2017, 10:22 h.*

(Énfasis añadido.)

La segunda tesis que se menciona es del literal siguiente:

FIRMA ELECTRÓNICA. REQUISITOS PARA CONSIDERARLA AVANZADA O FIABLE. *De conformidad con los artículos 89 y 97 del Código de Comercio; las reglas 2, 6 y 7 de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre las firmas electrónicas, así como la Guía para su Incorporación al Derecho Interno, el uso de la firma electrónica en las operaciones bancarias constituye una fuente válida de obligaciones para los tarjetahabientes que se vinculan a dicho mecanismo de seguridad para las transacciones comerciales, ya que los medios electrónicos han permitido realizar operaciones comerciales entre personas que se encuentran en distintos lugares y que obstaculiza el perfeccionamiento del acto jurídico mediante la firma autógrafa. La Ley Modelo establece las reglas para crear una firma electrónica que al ser utilizada vincule a quien la emite, por lo que el eje rector de ésta lo constituye la fiabilidad en su creación; de modo que otorgue certeza a quien la posee, que sólo él o ella puede utilizarla para constituir fuente de obligaciones. En consecuencia, para considerar fiable una firma electrónica debe reunir los requisitos siguientes, que:* ***a)*** *Los datos de creación de la firma corresponden exclusivamente al firmante;* ***b)*** *Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;* ***c)*** *Sea posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y,* ***d)*** *Respecto de la integridad de la información*

de un mensaje de datos sea posible detectar cualquier alteración de ésta hecha después del momento de la firma.

TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO.

Amparo directo 499/2016. BBVA Bancomer, S.A., I.B.M., Grupo Financiero BBVA Bancomer. 10 de agosto de 2016. Unanimidad de votos. Ponente: Víctor Francisco Mota Cienfuegos. Secretaria: María Estela España García.

Esta tesis se publicó el viernes 16 de junio de 2017 a las 10:22 horas en el Semanario Judicial de la Federación.

No. de Registro 2014545. Semanario Judicial de la Federación. *Décima Época. Tribunales Colegiados de Circuito. Materia civil. Tesis aislada. Tesis I.3o.C.264 C (10a.). Publicación: viernes 16 de junio de 2017, 10:22 h.*

ANÁLISIS DE LOS FALLOS

Es cierto que de conformidad con los artículos 89 y 97 del CCom, las reglas 2, 6 y 7 de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre las firmas electrónicas, así como la Guía para su Incorporación al Derecho Interno, el uso de la firma electrónica en las operaciones bancarias constituye una fuente válida de obligaciones para los tarjetahabientes que se vinculan a dicho mecanismo.

Esto, siempre que la firma electrónica reúna los requisitos siguientes: **(i)** los datos de creación de la firma corresponden exclusivamente al firmante; **(ii)** los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante; **(iii)** sea posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma, y **(iv)** respecto de la integridad de la información de un mensaje de datos sea posible detectar cualquier alteración de ésta, hecha después del momento de la firma.

También es cierto que, en los casos de un conflicto en el que un cuentahabiente desconozca ciertos cargos bancarios realizados a su cuenta mediante el uso de medios digitales con firma electrónica, debe señalarse que el banco emisor asume la carga probatoria de la validez de los cargos realizados, y arroja al tarjetahabiente la carga de desvirtuar la fiabilidad de la firma, por lo que debe probar que las operaciones se hicieron a través de una mecánica distinta a la prevista contractualmente; es decir, sin la utilización de la firma electrónica o mediante ésta, por persona distinta al cliente, sin su autorización y que dio aviso a la demandada del robo, pérdida, extravío o mal uso de cualquiera de los dispositivos de seguridad, incluyendo la firma electrónica, dado que el cargo genera la presunción legal del consentimiento en la operación.

Sin embargo, lo cierto es que la misma tecnología utilizada como base del comercio electrónico ha sido y sigue siendo "blanco" cotidiano del crimen cibernético, mediante múltiples formas de fraude electrónico, entre las que se encuentran las denominadas *phishing*, *pharming* y *Key Logger.*

Como es bien sabido, el denominado *phishing* es una forma de fraude electrónico que se da a través del Internet, mediante la cual se obtienen los datos del usuario, claves, cuentas bancarias, números de tarjetas de crédito, entre otros, para usarlos posteriormente en operaciones fraudulentas de comercio electrónico.

En cuanto al denominado *pharming,* se trata de otra forma de fraude electrónico, la cual consiste en reproducir páginas *web* que son visitadas por los usuarios, que no son auténticas sino reproducciones ficticias, mismas que son utilizadas para recabar datos confidenciales, especialmente relacionados con la banca en línea, y otras operaciones de comercio electrónico.

Por su parte, el programa denominado *Key Logger,* o capturas de teclado, es un *software* que se instala en un computador sin que el usuario sea consciente de ello, para grabar lo que escribe y utilizar sus datos, claves y contraseñas de sus tarjetas de crédito o cuentas bancarias, para cometer fraudes electrónicos.

Dichas modalidades de fraude electrónico se encuentran reconocidas en cuanto a su existencia no sólo por las instituciones que componen el sistema financiero nacional e internacional, sino también por las propias autoridades reguladoras del mismo, como es el caso, a nivel nacional, del Banco de México (Banxico) y de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), que de manera expresa, en múltiples boletines, informes y estudios han dado cuenta de la gravedad del problema que afecta a la banca electrónica y al desarrollo del comercio electrónico a nivel mundial.

De las múltiples formas de fraude electrónico se destaca como elemento común el hecho de que las herramientas utilizadas para ello aprovechan en todos los casos la

vulnerabilidad de los sistemas operativos y desarrollos informáticos utilizados por los distintos actores del comercio electrónico, entre ellos, el sistema financiero nacional y las múltiples empresas que participan diariamente en las operaciones propias del comercio electrónico.

Por esta razón, resulta muy difícil sostener la premisa utilizada como argumento de la primera de las tesis en comento, en el sentido de que tratándose de la carga de la prueba en procesos judiciales en los cuales se reclamen cargos bancarios fraudulentos, que *lo ordinario es que las terminales punto de venta (TPV) y el sistema operativo* ***no sean vulnerables****, por lo que corresponde la carga de la prueba a quien alega lo contrario.* La realidad del mundo cibernético diariamente nos demuestra lo contrario.

CONCLUSIONES

Es innegable que los medios electrónicos han permitido realizar operaciones comerciales entre personas que se encuentran en distintos lugares, y que la distancia geográfica que los separa obstaculiza –en muchas ocasiones– el perfeccionamiento del acto jurídico mediante la firma autógrafa.

Es precisamente por esa situación, que tanto el desarrollo de los medios digitales como el uso de la firma electrónica constituyen en sí una herramienta poderosa para el desarrollo del comercio electrónico.

Sin embargo, esto al mismo tiempo exige no sólo mayores niveles de seguridad cibernética capaces de combatir eficazmente el fraude electrónico, sino también la correspondiente asunción de la responsabilidad civil inherente, a cargo de las instituciones financieras al ofrecer dichos medios digitales a sus clientes, en la prestación de sus servicios, para la realización de las múltiples operaciones financieras que hoy en día se realizan a través de la *web*.

Por ello, aun cuando efectivamente el uso de la firma electrónica en las operaciones bancarias es cierto que constituye una fuente válida de obligaciones para los tarjetahabientes que se vinculan a dicho mecanismo de seguridad, no menos cierto es que quien ofrezca a los usuarios el uso de herramientas digitales para la prestación de sus servicios financieros, no puede excluirse de las consecuencias derivadas de los riesgos que le son propios, ante la posible vulnerabilidad de dichas herramientas. •