

REPUBLICA DE COLOMBIA
RAMA JUDICIAL DEL PODER PÚBLICO



JUZGADO CUARENTA Y UNO CIVIL DEL CIRCUITO
BOGOTA D.C. Treinta y uno (31) de octubre de dos mil veintidós (2022)

REF: : VERBAL No. 11001-0800-008-2020-01727-01

Demandante: **CONJUNTO RESIDENCIAL MARQUES DE PONTEVEDRA**

Demandado: **BANCO COMERCIAL AV VILLAS S.A.**

SENTENCIA DE SEGUNDA INSTANCIA

Se procede a dictar sentencia que dirimirá el recurso de apelación formulado por ambos extremos procesales contra la sentencia proferida por la Delegatura para Funciones Jurisdiccionales de la Superintendencia Financiera de Colombia, el día 2 de julio 2021 que accedió parcialmente a las pretensiones de la demanda.

ANTECEDENTES

El **CONJUNTO RESIDENCIAL MARQUES DE PONTEVEDRA**, a través de apoderado, formuló demanda en contra del **BANCO AV VILLAS**, a fin de obtener sentencia que acceda a las siguientes **PRETENSIONES**:

1.- Declarar el incumplimiento del BANCO AV VILLAS del contrato del depósito en cuenta corriente por parte de ésta al permitir la realización de transferencias fraudulentas desde la Cuenta Corriente N° 067036007 del CONJUNTO el 22 de noviembre de 2019 por la suma \$62.760.700; retiro realizado de forma maliciosa en 3 transacciones diferentes el referido día,

2.- Condenar al banco demandado al pago de la mencionada suma de dinero, más los intereses corrientes liquidados desde el 22 de noviembre de 2019 hasta la fecha de pago de la obligación.

HECHOS

Las pretensiones que se formulan se sustentan en los hechos que se compendian de la siguiente manera:

El 25 de noviembre de 2019, bajo el radicado N° CUR 9942316, el CONJUNTO demandante presentó reclamación ante el BANCO AV VILLAS C.C. TITAL PLAZA,

por haber permitido y autorizado el débito de la cuenta corriente No. 067036007 de la demandante (\$62.760.700), en 3 retiros relacionados en la demanda; que las transacciones mencionadas NO fueron EFECTUADAS ni AUTORIZADAS por EL CONJUNTO, correspondiendo a operaciones distintas y anormales a cualquiera de las que ORDINARIAMENTE realiza éste, pero fueron autorizadas por el BANCO AV VILLAS sin haber implementado con la debida diligencia los protocolos y controles internos de seguridad que ha debido usar, como por ejemplo el perfil del usuario, la activación de alertas, el vigilar las cuentas autorizadas de pago; la existencia de instrucciones precisas por parte del CONJUNTO para la realización de los pagos por transferencias, autorizando únicamente el pago a proveedores una vez al mes, indicando claramente que: “(...) cualquier modificación debe estar autorizada por las firmas registradas y de acuerdo a las condiciones pactadas por el banco”, por lo cual el banco emitió 5 formatos de asociación de cuenta para transferencia, dentro de los proveedores autorizados por EL CONJUNTO en el citado documento del 20 de mayo de 2019 no se encuentra relacionado Electricaribe a quien se le autorizaron tres transferencias por valor de \$62.760.700 no autorizados por el titular de la cuenta. El CONJUNTO no realiza ni ha realizado transacciones con ELECTRICARIBE.

TRAMITE

La demanda fue admitida por la Delegatura de Funciones Jurisdiccionales de la Superintendencia financiera el 7 de julio de 2020, Notificada la entidad demandada BANCO AV VILLAS, quien a través de apoderado contestó en tiempo la demanda oponiéndose a las pretensiones. Propuso como medios de defensa las excepciones que estimó pertinentes para enervar las aspiraciones de la demandante y rotuló “DESATENCIÓN DE LAS PRACTICAS DE PROTECCIÓN PROPIA POR PARTE DEL CONSUMIDOR FINANCIERO”; “INCUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES Y DE LOS REGLAMENTOS QUE INCLUYEN TÉRMINOS Y CONDICIONES DE USO PARA EL CORRECTO FUNCIONAMIENTO DE LOS SERVICIOS OFRECIDOS POR EL BANCO”; “EL BANCO AV VILLAS CUMPLIÓ SUS OBLIGACIONES CONTRACTUALES Y POR TANTO NO CAUSÓ NINGÚN PERJUICIO”; INEXISTENCIA DE LOS ELEMENTOS PROPIOS DE LA RESPONSABILIDAD CONTRACTUAL PARA ATRIBUIR RESPONSABILIDAD AL BANCO AV VILLAS”; “EL DEMANDANTE PRETENDE ALEGAR A SU FAVOR SU PROPIA CULPA” , “CULPA EXCLUSIVA DE LA VICTIMA”, sustentadas en síntesis en que el banco dio cumplimiento a los requisitos contractuales para autorizar los pagos ordenados por la demandante a través del portal empresarial.

Surtido el traslado de las excepciones, se convocó a las partes para la audiencia de que trata el artículo 372 del Código General del Proceso y ante el fracaso de la etapa de conciliación se practicaron las pruebas solicitadas.

LA SENTENCIA APELADA

Historiado el litigio la Delegatura con Funciones Jurisdiccionales de la Superintendencia Financiera, encontró probado el contrato de cuenta corriente celebrado entre las partes; consideró que la actividad financiera es una actividad de interés público que le impone cumplir las obligaciones inherentes a su actividad y los parámetros necesarios en los canales a través de los cuales presta sus servicios ofrecidos; que se trata de responsabilidad objetiva, por lo que no le basta para exonerarse haber sido diligente, sino que debe demostrar una causa que no le es imputable o que ambos contratantes contribuyeron al hecho dañino; que el banco debe cumplir los requerimientos de seguridad establecidos por la ley; que ello no implica que el consumidor financiero debe desatender sus obligaciones de seguridad; que conforme al material probatorio se acredita que la demandante utilizaba frecuentemente el portal del banco para el pago de proveedores y servicios públicos; que para su uso se requería el usuario y clave y código adicional de seguridad o Token que arroja una clave de un solo uso, el cual era de cuidado de la demandante; que conforme al dictamen pericial aportado por la parte demandada, el equipo de la parte demandante fue víctima de un ataque el día en que se efectuaron las transferencias objeto del proceso, pues se encontró un virus o troyano bancario que incidió en las realización de las operaciones; que la amenaza estaba relacionada con el hurto de las claves de acceso del portal transaccional del banco, incluida la clave temporal generada por el token, que se estableció la fecha de instalación de la amenaza y el modus operandi para hurtar las claves del usuario; que en el historial encontró el perito una serie de intentos fallidos de inicio en el portal por el usuario, intentos necesarios para que los atacantes obtuvieran las claves generadas por el token para la autenticación y posterior autorización de las transacciones; que el perito concluye que se abrió un correo electrónico en ese computador y se descargó un archivo indicado por el perito, apertura que comprometió el equipo donde se generaron las transacciones y que hizo nugatoria la seguridad del equipo; que se encontraron inactivas y abiertas sesiones por largo tiempo; que conforme a los documentos aportados, el importe de las 3 transferencias se encuentran dentro del todo establecido para el pago a proveedores y servicios públicos; que solo tenía un solo usuario; que el cliente contaba con un solo token suministrado por el banco; que se hizo una correcta autenticación mediante clave o los números generados por el token; que, entonces, dichas transacciones se hicieron desde el canal entregado al usuario, con el medio asignado y dentro de los topes autorizados, lo cual no releva al

banco de cumplir sus obligaciones a su cargo, particularmente de construir un perfil del cliente; que si bien no es de recibo el argumento del demandante de haber limitado sus transferencias a 5 clientes, dicha limitación se circunscribía a transferencias y no a servicios públicos, tipo de operación que hacía la demandante de manera habitual; que a pesar de ello no se puede exonerar al banco, dado que no elaboró un perfil del usuario conforme a las orientaciones de la Superintendencia Financiera traídas a colación, para identificar operaciones que no correspondan al mismo; que al concluirse que hubo presencia de un software malicioso en el equipo de la demandante en la fecha de las operaciones, lo cual compromete su esfera de responsabilidad, lo cual no acredita una conducta totalmente negligente de la demandante, pero ese software se instaló por una conducta imprudente del usuario al abrir un archivo desconocido, práctica general que debe aplicar el consumidor financiero; que tampoco resulta admisible que dicha irregularidad se haya hecho hasta el día lunes. Con base en lo considerado concluyó que hubo concurrencia de culpas, pero no en igual grado por lo que se condenará al banco al pago del 40% de las obligaciones reclamadas y deberá la demandante soportar el valor restante; con base en lo considerado declaró no probadas las excepciones propuestas por el demandado y condenó al banco demandado al pago de la suma de \$25.104.280. Sin costas.

LOS RECURSOS INTERPUESTOS

En tiempo la sentencia de primera instancia fue apelada por las partes así:

Apelación parte demandante

Que no existe ningún sistema autónomo que bloquee este tipo de amenazas, por lo que el archivo descargado por el usuario es de tipo común, frente al cual, una persona no experta no tendría la prevención de descargar, más cuando no se trata de los recomendados no descargar por el banco; que conforme a la jurisprudencia si es un tercero el que burla esos protocolos de autenticación, y -haciéndose pasar por el cuentahabiente - dispone por cualquier medio de los recursos depositados en cuentas de ahorros o corrientes, la obligación de verificación se incumple, pues la carga de que se viene hablando no puede entenderse satisfecha simplemente con los buenos oficios del banco, sino con la efectiva confirmación de la identidad de su cliente (SC5176-2020); que ante esos compromisos, el banco debe mantener las precauciones, diligencias y cuidados indispensables para que los actos de movimiento de la cuenta del usuario se alcancen con plena normalidad; por eso, cualquier desviación constituye un factor de desatención del contrato; que es responsable por el reembolso de sumas depositadas que haga a personas distintas del titular de cuenta o de su mandatario (art. 1398 C. Co.); que los testimonios recaudados a instancias del demandado no restan credibilidad a las

demás probanzas, puesto que solo se limitaron a realizar un recuento general del modo en que se realizaban los procesos de recepción y visado de las transferencias una vez las mismas eran radicadas por (Findeter); que en el caso sub judice, el demandante en el interrogatorio de parte indicó, que no es un experto informático, que su conocimiento se limita al común para usuarios de medios electrónicos, que no se le dio información detallada de este tipo de amenazas por parte del banco; que la razón por la que ese tipo de correos titulados “PROCESO JUDICIAL” se abren y se revisan junto con un promedio de cien correos diarios que ingresan al correo electrónico del conjunto. Si bien el a quo señala que la responsabilidad resulta para el presente caso compartida, no resulta viable aceptar esta teoría toda vez que la jurisprudencia en repetidas ocasiones ha insistido en la posición que hace responsable al banco en los casos que, como el presente, el usuario ha sido prudente y diligente pero que por ataques fraudulentos adquieren su información bancaria. En este sentido, y en un caso similar y del que hacía parte la misma entidad financiera aquí demandada La Corte Suprema de Justicia Dijo: “5. La responsabilidad en este tipo de fraudes: De la exposición que precede, queda claro que en el caso de defraudación por transacciones electrónicas, dado que tal contingencia o riesgo es inherente a la actividad bancaria la cual es profesional, habitual y lucrativa, cuya realización requiere de altos estándares de diligencia, seguridad, control, confiabilidad y profesionalismo, que también tienen que ser atendidos en materia de seguridad de la información que sea transmitida por esa vía, siendo innegable e ineludible su obligación de garantizar la seguridad de las transacciones que autoriza por cualquiera de los medios ofrecidos al público y con independencia de si los dineros sustraídos provienen de cuentas de ahorro o de cuentas corrientes. De ahí que atendiendo la naturaleza de la actividad y de los riesgos que involucra o genera su ejercicio y el funcionamiento de los servicios que ofrece; el interés público que en ella existe; el profesionalismo exigido a la entidad y el provecho que de sus operaciones obtiene, los riesgos de pérdida por transacciones electrónicas corren por su cuenta, y por lo tanto, deben asumir las consecuencias derivadas de la materialización de esos riesgos a través de reparar los perjuicios causados, y no los usuarios que han confiado en la seguridad que les ofrecen los establecimientos bancarios en la custodia de sus dineros, cuya obligación es apenas la de mantener en reserva sus claves de acceso al portal transaccional. Desde luego que consumada la defraudación, el Banco para exonerarse de responsabilidad, debe probar que esta ocurrió por culpa del cuentahabiente o de sus dependientes, que con su actuar dieron lugar al retiro de dinero de la cuenta, transferencias u otras operaciones que comprometieron sus recursos, pues amén de que es este quien tiene el control de mecanismo que le permiten hacer seguimiento informático a las operaciones a través de controles implantados en los software especializados con los que cuentan, la culpa incumbe demostrarla a

quien la alegue (art. 835 C.Co.), pues se presume la buena fe «aún la exenta de culpa».”¹ Y aquí, así como en el caso correspondiente a la jurisprudencia citada, el demandado no probó la conducta imprudente del demandante, máxime cuando lo alegado y tomado como argumento por la primera instancia es que el demandante realizó la descarga del archivo que permitió el ataque, se desconoce que el mismo no tenía un conocimiento experto que le permitiese suplir el deber de la entidad financiera y prever el riesgo de ese acto. Aunado a lo anterior, es menester resaltar que tampoco se tuvo en cuenta por parte del fallador al analizar la prudencia y diligencia del demandante, el cual realizó transacciones durante más de nueve meses, en un espacio que consideraba seguro, siguiendo todas las instrucciones de la entidad financiera y al instante de percatarse de la baja en el saldo de su cuenta procedió a informar al banco inmediatamente. 1 corte Suprema de Justicia. Sala de casación Civil. Sentencia de Casación. Magistrado Ponente: ARIEL SALAZAR RAMÍREZ. SC18614-2016. Radicación n° 05001-31-03-001-2008-00312-01. 19 de diciembre del año 2016. Frente a lo anteriormente mencionado, también hay que insistir en que el banco no emitió ninguna comunicación electrónica al usuario, ni por medio de mensaje de texto, ni por medio de correo electrónico y durante el interrogatorio de parte, el representante legal, informa que esa comunicación debía entenderse como la confirmatoria de transacción dentro de la plataforma bancaria, lo cual, para el caso concreto era imposible de verificar por el usuario, toda vez que como se probó, no fue la persona que se encontraba con un inicio de sesión abierto en la plataforma del banco. Y en soporte de lo anterior el mismo defensor del consumidor financiero en la prueba N° 6 C01-049-2020-03-17-5, apartado 3.4 del sustento jurídico, indicó: “3.4. Notificar operaciones realizadas, en línea. De conformidad con lo previsto en la Circular Externa 052 de 2007 –Modificada por la Circular 029 de 2014- las entidades deben “3.4.3 Establecer las condiciones bajo las cuales los clientes podrán ser informados en línea acerca de las operaciones realizadas con sus productos.” C.E. (no incluido en P1 T° II Cap. I- (C.E. 029 DE 2014/CBJ), este hecho se contrapone al P2 T°I Cap. 3 - (C.E. 029 DE 2014/CBJ) 7.2. Instrucciones especiales en materia de seguridad y calidad para la realización de operaciones. Las entidades vigiladas deben observar las disposiciones generales previstas en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones previstas en numeral 2. del Capítulo I, Título II de la Parte I de esta Circular, con excepción de los siguientes:(...)7.2.6. El establecimiento de las condiciones sobre las cuales los clientes van a ser informados en línea acerca de las operaciones realizadas con sus productos. En todo caso, la entidad financiera es quien tiene la carga de la prueba debiendo demostrar que dio cumplimiento al deber transcrito en el párrafo anterior y en el evento que la entidad no demuestre el cumplimiento de esta obligación, debe el DCF dar aplicación a lo expuesto en el artículo 4 de Ley 1480 de 2011, norma que establece lo siguiente: “Las normas de

esta ley deberán interpretarse en la forma más favorable al consumidor. En caso de duda se resolverá en favor del consumidor”, y, por lo tanto, de resolverse en favor del consumidor.” Para el presente caso y conforme con lo expuesto anteriormente, la responsabilidad no solo debe recaer en la entidad financiera en los casos donde por una vulneración de un tercero se realizan transacciones maliciosas, así mismo, en los casos en los que existe duda sobre la responsabilidad, también es la entidad financiera la que debe hacerse responsable de la totalidad del perjuicio. Para finalizar, se solicita al superior que tenga conocimiento del recurso que revoque en su totalidad la sentencia de primera instancia decretada por la SUPERINTENDENCIA FINANCIERA DE COLOMBIA, y en consecuencia se acceda a las pretensiones de la demanda.

Apelación parte demandada

LAS OPERACIONES OBJETADAS SE EMARCAN DENTRO DEL PERFIL DEL CLIENTE Y NO DEBEN GENERAR ALERTAS AL INTERIOR DEL BANCO; señalando que el portal transaccional es utilizado de forma ininterrumpida desde 29/03/2019, habilitado para adelantar operaciones monetarias y no monetarias, la realización de pagos de servicios públicos, transferencias, pagos PSE, pago a proveedores, pagos de nómina entre otros, sin que exista algún tipo de estipulación entre las partes, orientado a restringir el pago a determinados proveedores, o a limitar montos o cuantías de las transacciones, o al bloqueo del canal para la realización de operaciones en atención a su naturaleza; que a la luz de las operaciones adelantadas por la copropiedad, difiere de lo resuelto por la Delegatura al referir la inexistencia del perfil del cliente, máxime cuando se advierten transacciones monetarias por medio del canal de internet hasta por el valor de \$15.645.642 en cuyo caso el Banco, según su motor de riesgo, entiende que las operaciones ejecutadas, i) se encuentran habilitadas en el portal, ii) dentro de los topes asignados, iii) con la claves suministradas por el cliente (Usuario Contraseña), aunado a la utilización, iv) de un mecanismo fuerte de autenticación; que la Circular Básica Jurídica (C.E. 029/14) de la Superintendencia Financiera, fija las siguientes obligaciones, a las entidades financieras en tratándose de seguridad y calidad de las operaciones: 2.2. Definiciones aplicables 2.2.6. Mecanismos fuertes de autenticación: Se entienden como mecanismos fuertes de autenticación los siguientes: 2.2.6.1. Biometría. originados por medio del dispositivo token y que el mismo, vi) fue efectivamente entregado por el Banco al usuario primario, el señor Álvaro Pinilla Cortés, quien dentro del presente asunto confesó, se encontraba bajo su exclusiva custodia; que si el actor acostumbraba a realizar transacciones valiéndose del canal de servicios de internet por el valor de \$15.645.642 y si la primera transacción objetada, cursada el pasado 22 de noviembre del 2019 a las 11:33 a.m. se ordenó, por el valor de \$20.000.000; esta última operación, no puede constituir un hecho anómalo o extraño, capaz de

generar alertamientos al interior de los sistemas del Banco, como quiera que la misma encuentra soporte o correspondencia, con otras operaciones efectuadas por la copropiedad, similares en su cuantía, y llevadas a cabo con antelación a las materializadas el 22 de noviembre del 2019. De otro lado, tanto la segunda y tercera operación efectuada el 22/11/2019 a las 12:57p.m. y 12:56 p.m., dichos movimientos, no pueden entenderse anómalos, en tanto que se efectuaron dentro del tope asignado para este tipo de operaciones, al no desbordar la suma de \$70.000.0003 (Según precisó la testigo técnico LINA FERNANDA ROMERO ROMERO4); al paso que las operaciones objetadas se concretaron por el valor de \$ 40.000.000 y \$ 2.760.700 en la hora y fecha ya referida, es decir, dentro de horario y día hábil.; 2. EL BANCO NO DEBIÀ DESPLEGAR PROTOCOLO DE CONFIRMACIÓN PORQUE LAS OPERACIONES CURSARON DE ACUERDO CON LO LEGALMENTE PACTADO ENTRE LAS PARTES: Al no ser desconocidos, ni tachados de falsos, los documentos que instrumentan las relaciones jurídicas entre el Banco y la Copropiedad; dichos insumos, son ni más ni menos que ley para las partes, por lo que no puede exigírsele a mi mandante nada distinto a lo taxativamente estipulado en dichos contratos, en donde no se pactó llamada de confirmación telefónica o la detección de algún tipo de parametria previamente informada por la copropiedad al Banco, pues no existió comunicación recibida por el Banco en tal sentido; que, el Banco, no debió desplegar ningún alertamiento o llamada de confirmación, porque como ya se expresó, las operaciones se encuentran dentro de los hábitos de la persona jurídica demandante, cumplió con los topes monetarios establecidos para el tipo de transacción, además de superar con éxito los mecanismos de seguridad, comoquiera que las transacciones se surtieron con la utilización del usuario y contraseña del cliente, junto con la clave dinámica procedente del dispositivo token que se encontraba en custodia de la persona autorizada, tal y como lo expresó el representante legal de la copropiedad, según se desprende del interrogatorio de parte oportunamente practicado . 3. LA CAUSA QUE ORIGINA LA DEFRAUDACIÓN SE ENCUENTRA POR FUERA DE LA ORIBITA DEL BANCO Y OCURRE BAJO LA ESFERA DE DOMINIO DEL ACTOR. Sobre este punto refulge con total claridad, que las transacciones objeto de reclamación, se adelantaron con ocasión a las negligencias cometidas por usuario posibilitando el compromiso sobre el equipo de cómputo a través de técnicas de phishing, mediante el cual se instaló el software malicioso en el sistema del Conjunto Residencial, por la descarga del archivo denominado "Proceso Judicial.uu" identificado con el No [351575] el día 3/10/2019 16:11:07 PM., siendo este archivo, encontrado en el directorio de descargas del usuario MARQUEZ, como concluyó el perito Daniel Torres Falkonert: que la amenaza, tuvo origen en el equipo de cómputo de la copropiedad, que fue instalada de forma negligente por el consumidor financiero al abrir de forma imprudente el archivo adjunto, ejecutando

con tal proceder, la amenaza de tipo troyano que infectó la máquina, que permaneció desde el 03/10/2019, es decir, casi un (1) mes y 19 días hasta el 22 /11/2019 operando de forma permanente; sin que el representante legal del Conjunto Residencial adoptara las medidas necesarias para proteger el equipo, que por demás, únicamente contaba con un antivirus básico, según declaró el perito en desarrollo de la sustentación oral recepcionada por el Despacho Judicial; que el BANCO COMERCIAL AV VILLAS, no advirtió que sus sistemas fueran vulnerados, penetrados, accedidos, para la época de los hechos; 4. LAS TRANSACCIONES NO RECONOCIDAS SE PRODUJERON POR LA EXCLUSIVA RESPONSABILIDAD DEL CONSUMIDOR FINANCIERO AL NO GUARDAR LAS RECOMENDACIONES DE SEGURIDAD IMPARTIDAS POR EL BANCO. Sobre el particular, la ley 1328 de 2009 en su artículo 6 literal C) prevé la siguiente disposición: “PRÁCTICAS DE PROTECCIÓN PROPIA POR PARTE DE LOS CONSUMIDORES FINANCIEROS. c) Observar las instrucciones y recomendaciones que imparta la entidad vigilada sobre el manejo de productos o servicios financieros.” que el representante legal de la sociedad, no sólo manifiesta haber recibido cabalmente toda la información tocante a los productos adquiridos, sino que asume de igual modo, todas las obligaciones derivadas del contrato, especialmente aquella contenida en el numeral 2) del acápite denominado “Conocimientos informados” que le impone la obligación de consultar la página web del Banco de forma asidua dado que tal contenido, tiene por objeto informar a los clientes, respecto del uso y funcionamiento de los servicios ofrecidos por el Banco, incluidas las recomendaciones de seguridad para el manejo de sus productos.

Concedidos y tramitados los recursos es del caso resolverlos, previas las siguientes,

CONSIDERACIONES

Fluye de la demanda que la acción encausada por el CONJUNTO RESIDENCIAL MARQUES DE PONTEVEDRA, contra BANCO AV VILLAS S.A., se orienta a obtener la indemnización de perjuicios al permitir la realización de transferencias fraudulentas desde la Cuenta Corriente N° 067036007 del CONJUNTO el 22 de noviembre de 2019 por la suma \$62.760.700; retiro realizado de forma maliciosa en 3 transacciones diferentes el referido día.

DE LA RESPONSABILIDAD BANCARIA

La responsabilidad bancaria frente a sus cuentahabientes y ahorradores ha sido considerada por la jurisprudencia patria como de resultado, basada en que la actividad financiera es una actividad de alto riesgo, **“Precisamente, por ese**

riesgo social que su ejercicio lleva implícito, las entidades bancarias se hallan obligadas a observar reglas fundamentales de prudencia, control y adecuada organización, tendientes a obviar el surgimiento de daños para sí y su clientela. Cuando no proceden de tal forma, su responsabilidad se compromete, pero puede desvirtuarse o aminorarse, si se demuestra una causa extraña, tipificada en el caso fortuito o la fuerza mayor, el hecho de un tercero o de la víctima, cuando los mismos han determinado el resultado lesivo y tienen la connotación de imprevisibles e irresistibles”¹.

Es por ello que la diligencia exigible a las instituciones financieras no es apenas la que se espera de un buen padre de familia, referida por tanto a los negocios propios, sino la que corresponde a un profesional que deriva provecho económico de un servicio que compromete el ahorro privado y en el que existe un interés público, pues como tradicionalmente se ha considerado, se trata de un comerciante experto en la intermediación financiera, como que es su oficio, que maneja recursos ajenos con fines lucrativos y en el que se encuentra depositada la confianza colectiva.

A voces del artículo 335 de nuestra Constitución Política, la actividad bancaria constituye un servicio público, esencial para el desarrollo económico, de interés general, dirigida a la captación de recursos provenientes del público, a su aprovechamiento e inversión y está supeditada a la autorización, intervención y vigilancia del Estado, en cuya labor, adquieren obligaciones debido al alto riesgo social que esa actividad conlleva, obligaciones, que, en suma, se concretan en la especial diligencia que deben observar en desarrollo de las actividades mercantiles constitutivas de su objeto social y, dentro de ellos, el ejercicio de controles y adopción de procedimientos dirigidos a la debida y completa identificación de sus clientes y de quienes utilizan el servicio público para realizar operaciones financieras, tendiente a impedir o minimizar los riesgos que su omisión puede provocar.

Empero, Cuando tales instituciones desatienden sus deberes de diligencia y cuidado, comprometen su responsabilidad, pues como lo tiene decantado la jurisprudencia, la exigencia de deberes especiales de diligencia al sistema financiero, tiene fundamento en que las instituciones bancarias son depositarias de la confianza pública e implica riesgo social, dada la intermediación financiera que realiza -de gran importancia para el desarrollo económico-, su desempeño impone una indiscutible profesionalidad, idoneidad y experiencia, riesgo social que lleva implícita la obligación de observar reglas fundamentales de prudencia, control y adecuada organización, tendientes a obviar el surgimiento de daños para

¹ C.S.J., sentencia, 25 de abril de 2018, Rad. No. 08001-31-03-003-2006-00251-01

sí y su clientela, pues como lo recordó la Sala en CSJ SC 16496-2016, **«(...) la responsabilidad del banco ‘deriva del ejercicio y del beneficio que reporta de su especializada actividad financiera, como así lo tiene definido la jurisprudencia cuando asevera que una entidad crediticia es una empresa comercial que dado el movimiento masivo de operaciones, ‘asume los riesgos inherentes a la organización y ejecución del servicio de caja’ (...).»**

Respecto de la responsabilidad que tienen los bancos, como profesionales de la actividad financiera, la Corte, en sentencia SC18614-2016, concluyó:

«(...) el régimen de responsabilidad de los Bancos por la defraudación con el uso de instrumentos espurios para disponer de los fondos depositados en cuentas, se ha fundado en vertientes de la teoría del riesgo: En una primera época, la del ‘riesgo creado’ en virtud de la cual quien en desarrollo de una actividad genere un peligro o contingencia, debe indemnizar los perjuicios que de aquel deriven para terceros, con independencia de si ha actuado de manera diligente o culposa, o de si ha obtenido o un provecho; después se dio aplicación a la teoría del ‘riesgo provecho’ que carga con la obligación resarcitoria a quien ejerza la actividad que genera un riesgo o peligro y, además, saca de la misma una utilidad o percibe lucro, sin que importe que su conducta haya sido diligente o imprudente; por último, se acudió a la teoría del ‘riesgo profesional’ que es una derivación de la anterior, empleada también en otras áreas del derecho como, por ejemplo, en materia de accidentes y enfermedades laborales. En esta última, la obligación de asumir los riesgos inherentes al ejercicio de la actividad se basa en el profesionalismo que esta requiere.

(...)

Siendo la bancaria y la de intermediación financiera, actividades en las que -como atrás se dijo existe un interés público y son realizadas por expertos que asumen un deber de custodia de dineros ajenos, siéndole exigibles, según lo previsto por el Estatuto Orgánico del Sistema Financiero (Decreto 663 de 1993) y las Circulares Básica Contable y Financiera (100 de 1995) y Básica Jurídica (007 de 1996) unos altos y especiales cargas o cumplimiento de estándares de seguridad, diligencia, implementación de mecanismos de control y verificación de las transacciones e incluso de seguridad de la confiabilidad de la información y preservación de la confiabilidad, es natural que la asunción de tales riesgos no les corresponda a los clientes que han encomendado el cuidado de parte de su patrimonio

a tales profesionales, de ahí que sea ellos quienes deban asumir las consecuencias derivadas de la materialización de esos riesgos.

En ese orden de ideas, 'a la hora de apreciar la conducta de uno de tales establecimientos -ha dicho la Corte- es necesario tener presente que se trata de un comerciante experto en la intermediación financiera, como que es su oficio, que maneja recursos ajenos con fines lucrativos y en el que se encuentra depositada la confianza colectiva' (CSJ SC-076, 3 Ago. 2004, Rad. 7447) y por tales razones se le exige 'obrar de manera cuidadosa, diligente y oportuna en ejercicio de sus conocimientos profesionales y especializados en materia bancaria' para impedir que sean quebrantados los derechos patrimoniales de titulares de las cuentas de ahorro y corrientes de cuya apertura y manejo se encarga (CSJ SC, 3 Feb. 2009, Rad. 2003-00282-01). De todo lo anterior deriva, necesariamente que en la materia impera un 'modelo particular de responsabilidad profesional del banco» (CSJ SC-201, 15 Dic. 2006, Rad. 2002-00025-01).

Dicha responsabilidad se hace extensiva y se torna más rigurosa en transacciones electrónicas, dado que las entidades financieras como depositarias de la confianza de los usuarios, debe extremar medidas para prevenir y remediar el fraude electrónico, pues siendo un servicio ofrecido, regulado y manejado por las entidades bancarias, son ellas responsables de tal fraude, precisamente por ser un riesgo creado por la respectiva entidad, en el afán de establecer llamativas ofertas para la captación de clientes y recursos.

“De la exposición que precede, queda claro que en el caso de defraudación por transacciones electrónicas, dado que tal contingencia o riesgo es inherente a la actividad bancaria la cual es profesional, habitual y lucrativa, cuya realización requiere de altos estándares de diligencia, seguridad, control, confiabilidad y profesionalismo, que también tienen que ser atendidos en materia de seguridad de la información que sea transmitida por esa vía, siendo innegable e ineludible su obligación de garantizar la seguridad de las transacciones que autoriza por cualquiera de los medios ofrecidos al público y con independencia de si los dineros sustraídos provienen de cuentas de ahorro o de cuentas corrientes.

De ahí que atendiendo la naturaleza de la actividad y de los riesgos que involucra o genera su ejercicio y el funcionamiento de los

servicios que ofrece; el interés público que en ella existe; el profesionalismo exigido a la entidad y el provecho que de sus operaciones obtiene, los riesgos de pérdida por transacciones electrónicas corren por su cuenta, y por lo tanto, deben asumir las consecuencias derivadas de la materialización de esos riesgos a través de reparar los perjuicios causados, y no los usuarios que han confiado en la seguridad que les ofrecen los establecimientos bancarios en la custodia de sus dineros, cuya obligación es apenas la de mantener en reserva sus claves de acceso al portal transaccional.

Desde luego que consumada la defraudación, el Banco para exonerarse de responsabilidad, debe probar que esta ocurrió por culpa del cuentahabiente o de sus dependientes, que con su actuar dieron lugar al retiro de dinero de la cuenta, transferencias u otras operaciones que comprometieron sus recursos, pues amén de que es este quien tiene el control de mecanismo que le permiten hacer seguimiento informático a las operaciones a través de controles implantados en los software especializados con los que cuentan, la culpa incumbe demostrarla a quien la alegue (art. 835 C.Co.), pues se presume la buena fe «aún la exenta de culpa»².

Acorde con lo dicho, la culpa del cuentahabiente en la defraudación debe ser alegada y demostrada por el banco, sin que ni por asomo deba considerarse que corresponde al cliente demostrar la culpa de la entidad o su ausencia de culpa en la defraudación. No puede el operador judicial ligeramente invertir la carga de la prueba, ni admitir tímidas explicaciones del banco para exonerarlo de su obligación de vigilancia y cuidado en transacciones de tal linaje.

DEL CASO CONCRETO:

La existencia de las transferencias electrónicas génesis de esta controversia, no fue remitida a duda por la parte demandada, quien, por el contrario, admite su existencia y haberlas conocidas en su oportunidad.

También es punto pacífico de la controversia, que las transacciones fraudulentas desde la Cuenta Corriente No. 067036007 del CONJUNTO RESIDENCIAL MARQUÉS DE PONTEVEDRA el 22 de noviembre de 2019 por la suma

² C.S.J., sentencia, 19 de diciembre de 2016, Rad. No. 05001-31-03-001-2008-00312-01

\$62.760.700, tuvo como fuente la amenaza de tipo troyano que infectó la máquina, de propiedad de la parte demandante, como lo concluyó el perito Daniel Torres Falkonert, que permitió el hurto de claves y contraseñas para acceder al portal del banco demandado y que dicho ataque se produjo al darse apertura al correo electrónico relacionado por el perito.

Aspecto probatorio que le sirvió de estribo a la falladora de primer nivel para considerar que hubo culpa de la parte demandante al abrir un correo malicioso, ignorando así elementales reglas de seguridad, de no abrir correos desconocidos.

Sin embargo, con base en las consideraciones plasmadas con anterioridad y los antecedentes jurisprudenciales que vienen de memorarse, dada la actividad del banco y el lucro que percibe, se presume su responsabilidad, pues a su cargo corre adoptar los mecanismos de prevención y seguridad a fin de asegurar los recursos de sus clientes. Por tanto, no es admisible considerar como lo aconteció en la sentencia apelada, que, por el perfil transaccional de la demandante, era procedente considerar genuinas sus transacciones, pues tal pensamiento se convertiría en patente de corso para que, bajo el supuesto de continuas transacciones, se exonere a los bancos de transacciones irregulares, premiando su negligencia o descuido, incluso su complicidad en el fraude electrónico,, por lo que resulta inadmisibles deducir a cargo de la demandante culpa en el ilícito llevado a cabo. De admitir como válida tal presunción, aquellas personas naturales o jurídicas que diariamente efectúan innumerables transacciones electrónicas, quedarían expuestas a fraudes de tal linaje sin derecho a recibir indemnización alguna, lo cual no es admisible, ni por asomo patrocinar.

Se precisó en consideraciones precedentes que conforme a la jurisprudencia, “... **consumada la defraudación, el Banco para exonerarse de responsabilidad, debe probar que esta ocurrió por culpa del cuentahabiente o de sus dependientes, que con su actuar dieron lugar al retiro de dinero de la cuenta, transferencias u otras operaciones que comprometieron sus recursos, pues amén de que es este quien tiene el control de mecanismo que le permiten hacer seguimiento informático a las operaciones a través de controles implantados en los software especializados con los que cuentan, la culpa incumbe demostrarla a quien la alegue (art. 835 C.Co.), pues se presume la buena fe «aún la exenta de culpa»³.**

En consecuencia, correspondía a la parte demandada probar que las transacciones tildadas de fraudulentas ocurrieron por culpa de la demandante o

³ C.S.J., sentencia, 19 de diciembre de 2016, Rad. No. 05001-31-03-001-2008-00312-01

sus dependientes o que de manera alguna facilitó o permitió la transacción. Sin embargo, revisado el expediente, la parte demandada no aportó prueba que demuestre o al menos haga presumir que la defraudación acaeció por culpa de la demandante o que intervino en ella.

Si bien la parte demandada atribuye a la demandante culpa por dar apertura a un correo malicioso, tal conclusión resulta equivocada, pues no puede inferirse razonablemente, que cualquier correo no conocido debe ser desechado, ni mucho menos, que por ser desconocido conlleva una amenaza seria y real de ataque cibernético.

En los actuales tiempos en que se han implementado los mensajes de datos, entre ellos el correo electrónico como medio idóneo para las comunicaciones y actuaciones en todos los sectores o actividades de la sociedad, no resulta razonable considerar que la simple apertura de un correo de origen desconocido, entraña culpa del usuario frente a las obligaciones del sector financiero, como lo entendió la juez a quo y la parte demandada, quien simplemente afirmó haber cumplido los protocolos para autorizar las transferencias a través de su portal.

Sin embargo, no probó la parte demandante, que en su labor utilizó todos los mecanismos informáticos para detectar y detener el fraude informativo que sirve de estribo a la presente acción, que cuenta con herramientas que le permiten hacer seguimiento informático a las operaciones a través de controles implantados en los softwares especializados para detectar y detener los ataques entre ellos el Troyano que probó como fuente del fraude, y que, pese a sus controles, el ataque fue insuperable.

Tampoco se encuentra idóneamente probado que, frente a ataques de tal linaje, el fraude se convierte en un hecho insuperable, imposible de ser detectado por cualquier banco o entidad financiera.

El banco demandado se limita a señalar haber cumplido los protocolos de seguridad previstos por la entidad, como el uso de claves y de token, y así justifica la inexistencia de responsabilidad a su cargo. Sin embargo, la práctica bancaria enseña que adicionalmente pueden existir otros mecanismos de control o de seguridad, no aplicados por el banco, como mensajes a la línea celular registrada, claves, códigos de confirmación que se envían a través de ese medio tecnológico, etc.

Más aun, si se tiene en cuenta que si bien es cierto era o es costumbre del Conjunto demandante pagar servicios públicos a través del portal del banco, no

probó el demandado que el pago a ELECTRICARIBE era habitual por la demandante, o que se pagan servicios públicos que no correspondían a la ciudad de Bogotá, todo lo cual deja una inmensa duda sobre la labor diligente del banco en legalidad de las transacciones motivo del presente proceso.

No basta entonces, siguiendo las orientaciones jurisprudenciales ya vistas, que el banco alegue haber cumplido los protocolos de seguridad que a su juicio son suficientes, sino que debió probar que el fraude que acreditó con su dictamen pericial, se convirtió en un hecho insuperable, pues como lo tiene decantado la jurisprudencia en providencia citada con anterioridad, ***“...en el caso de defraudación por transacciones electrónicas, dado que tal contingencia o riesgo es inherente a la actividad bancaria la cual es profesional, habitual y lucrativa, cuya realización requiere de altos estándares de diligencia, seguridad, control, confiabilidad y profesionalismo, que también tienen que ser atendidos en materia de seguridad de la información que sea transmitida por esa vía, siendo innegable e ineludible su obligación de garantizar la seguridad de las transacciones que autoriza por cualquiera de los medios ofrecidos al público y con independencia de si los dineros sustraídos provienen de cuentas de ahorro o de cuentas corrientes”***.

Por tanto, no es procedente atribuir culpa a la parte demandante por el solo hecho de abrir un correo de origen desconocido, pues más allá de la veracidad de ese hecho, era obligación del banco demostrar la existencia de altos estándares de diligencia, seguridad, control, confiabilidad y profesionalismo para prevenir, detectar y evitar ataques cibernéticos, lo cual no ocurrió en el presente caso, pues se limitó a afirmar haber cumplido los parámetros de verificación usuario y claves, sin atender la tarea de prevenir el fraude electrónico analizado en el presente caso.

Así pues, a partir de la actividad de riesgo que entraña la actividad bancaria y ante la falta de prueba real y seria que conlleve a considerar que hubo culpa de la demandante, es claro que es obligación del demandado a indemnizar la totalidad del perjuicio reclamado, sin que haya lugar a considerar concurrencia de cuplas como equivocadamente se consideró en la sentencia apelada, la cual, por consiguiente, será revocada y en su lugar se accederá a las pretensiones de la demanda, ordenando la restitución de la suma de dinero motivo de fraude, junto con los intereses pedidos en la demanda, esto es, los corrientes liquidados desde el 19 de noviembre de 2019, hasta la fecha de pago de la obligación.

Se condenará al demandado al pago de costas en ambas instancias.

DECISIÓN

Acorde con lo esbozado, el JUZGADO CUARENTA Y UNO CIVIL DEL CIRCUITO DE BOGOTA D.C., administrando justicia en nombre de la República y por autoridad de la Ley,

RESUELVE

PRIMERO: REVOCAR la sentencia apelada, esto es, la proferida por la Superintendencia Financiera de Colombia, el día 2 de julio de 2021, y en su lugar, **SE DISPONE:**

SEGUNDO: DECLARAR NO PROBADAS las excepciones de mérito propuestas por el **BANCO COMERCIAL AV VILLAS S.A.**

TERCERO CONDENAR al **BANCO COMERCIAL AV VILLAS S.A.**, a pagar a la demandante **CONJUNTO RESIDENCIAL MARQUES DE PONTEVEDRA**, una vez ejecutoriada la presente sentencia, la suma de **\$62.760.700.**

CUARTO: CONDENAR al **BANCO COMERCIAL AV VILLAS S.A.**, a pagar a la demandante **CONJUNTO RESIDENCIAL MARQUES DE PONTEVEDRA**, una vez ejecutoriada la presente sentencia, los intereses corrientes sobre la anterior suma de dinero causados desde el 22 de noviembre de 2019, hasta la fecha de pago.

QUINTO: CONDENAR a la parte demandada al pago de costas de ambas instancias. Tásense las de la presente instancia con base en la suma de \$3.000.000 como agencias en derecho. Liquídense por el a quo.

Oportunamente devuélvanse las diligencias a la oficina de origen.

NOTIFÍQUESE y CUMPLASE



JANETH JAZMINA BRITTO RIVERO

JUEZ

M.A.E.