Monitor Semanal

Noticias tributarias y legales

No. 1116
21 de julio de 2025

En esta edición:

Ciberseguridad: reciente condena a un banco ante un caso de Phishing a un cliente

Damos noticia de algunos de los principales puntos considerados por el fallo

Ciberseguridad: reciente condena a un banco ante un caso de Phishing a un cliente

Damos noticia de algunos de los principales puntos considerados por el fallo

En una reciente sentencia, un Tribunal de Apelaciones en lo Civil condenó a un banco de plaza a pagar 9 mil dólares a uno de sus clientes que fue víctima de un fraude cibernético conocido como "phishing" (entendiéndose éste como suplantación de identidad, técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de su identidad)[1]

Este fallo, que destaca la importancia del tema ciberseguridad en las instituciones financieras, subraya la responsabilidad de los bancos en la protección de los fondos de sus clientes y en su deber de monitorear cualquier actividad inusual como forma de prevenir y evitar los fraudes.

El caso

El caso se originó cuando un cliente del banco “XX”, titular de una cuenta de ahorro en dólares, descubrió el 19 de noviembre de 2021, que su cuenta había sido vaciada mediante dos transferencias no autorizadas constatando que se habían realizado dos débitos por un total de 9 mil dólares a una cuenta a nombre de un tercero, “BB”.

BB recibió mensajes de alguien que dijo ser AA solicitándole la transferencia de esas sumas a una tercera cuenta, a nombre de “CC” quien, una vez acreditadas las transferencias, procedió al retiro total de la suma que mantenía en la cuenta. CC ya ha sido vinculado previamente a otras situaciones similares por lo que se confirmó rápidamente la existencia de un fraude.

El banco argumentó al apelar la sentencia de primera instancia, que no hubo falla en sus sistemas de seguridad y que el fraude se debió a la negligencia del cliente (hecho de la víctima), quien habría

[1] Artículo 9 literal K) numeral 1) de la Ley Nº 20.327.

proporcionado sus credenciales de acceso al defraudador. Esgrimió que, en el contrato de depósito de dinero, regulado por el Código de Comercio, el banco asume una obligación de medios y no de resultados (restituir los fondos). Sin embargo, aún bajo la posición de que se trate de una obligación de medios, el Tribunal determinó que el banco no actuó con la diligencia debida para detectar y prevenir la actividad fraudulenta del tercero que ingresó indebidamente y realizó las transferencias inusuales.

La sentencia: ciberseguridad y responsabilidad bancaria

La sentencia que comentamos confirma la condena al banco a pagar la suma de 9 mil dólares a AA, con intereses legales desde la demanda. El Tribunal consideró que, si bien existieron indicios de suplantación de identidad, no comparte que se haya dado por probado que la obtención de la información necesaria para efectuar la maniobra fraudulenta fuese por negligencia del cliente, víctima del fraude. Apalanca su razonamiento en una sentencia reciente de la Sala Primera de lo Civil del Tribunal Supremo Español (Sentencia Nro. 571/2025, de fecha 9 de abril de 2025) que dejó asentado: "... el que un tercero hubiera podido acceder a las claves de acceso a la banca digital del demandante no supone per se que haya incurrido en negligencia alguna, pudiendo existir múltiples explicaciones, muchas de las cuales resultan difícilmente atribuibles a título de negligencia, y menos aún, de negligencia grave".

El Tribunal destacó que la relación contractual entre el banco y el cliente está regulada por las Condiciones Generales y Particulares de las Cajas de Ahorro, así como por un Contrato de Servicios Banca Digital Personas. Según estos contratos, el banco tiene la obligación de proteger los fondos de sus clientes y de actuar con diligencia para prevenir fraudes y para ello cuenta con atribuciones que le concede el cliente que acepta contractualmente que, con la finalidad de protegerlo de accesos indebidos, el banco pueda unilateralmente bloquear total o parcialmente su acceso a los servicios durante el tiempo que lo estime necesario, sin necesidad de notificación previa.

Para el Tribunal, entonces, el banco no acreditó haber cumplido con su deber de seguridad, ya que no detectó la actividad inusual en la cuenta del cliente, a pesar de que los sistemas funcionaron normalmente ese día.

La sentencia del Tribunal oficia de buen recordatorio para los operadores de la plaza financiera y sus usuarios de la responsabilidad que tienen los bancos en la protección de los fondos de sus clientes, pero también de la obligación de los usuarios de mantenerse alerta frente a estos ataques. En un mundo cada vez más digitalizado, la ciberseguridad es esencial para prevenir fraudes y garantizar la confianza en los servicios bancarios en línea. Es claro que los bancos deben estar preparados para detectar y responder a actividades sospechosas de manera proactiva, protegiendo así los intereses de sus clientes y manteniendo la integridad de sus sistemas financieros, pero también que los usuarios deben conocer los riesgos, cuáles son los indicios de phishing manteniendo una conducta diligente en el uso de sus datos personales, así como en la trasmisión de éstos a terceros.

Medidas de ciberseguridad recomendadas

Más allá de este caso que comentamos en esta breve reseña de la sentencia del Tribunal, basta recordar las numerosas situaciones que han trascendido tanto a nivel nacional como internacional de ataques de piratas informáticos que lograron acceder a sistemas sensibles y sustraer en forma indebida datos confidenciales, así como las constantes noticias que nos llegan sobre ataques de ciberseguridad tanto a consumidores como a empresas, para dimensionar que estamos ante un tema al que resulta crítico darle trascendencia tanto a nivel regulatorio como de recaudos de seguridad a tomar por las entidades y también por los usuarios de servicios en línea.

En el caso puntual de las instituciones financieras, para prevenir fraudes como el phishing (vía el cual los delincuentes obtienen información confidencial haciéndose pasar por el banco), éstas deben implementar medidas de seguridad robustas para detectarlas a tiempo. En efecto, existen buenas prácticas que pasan por adoptar las medidas de seguridad necesarias para garantizar el correcto funcionamiento del sistema tales como las orientadas a detectar de forma automática los indicios de que puede tratarse de una operación inusual o rara y generar una alerta o un bloqueo temporal. Tales indicios pueden ser, por ejemplo, la reiteración de transferencias, la geolocalización de las operaciones, el horario en que se producen, importe de las transacciones, destinatarios, antecedentes en el uso de la cuenta, etc.

A nivel normativo, para operaciones realizadas a través de instrumentos electrónicos, en la Recopilación de Normas de Regulación y Control del Sistema Financiero (RNRCSF) se exige a las instituciones de intermediación financiera que establezcan medidas que garanticen la seguridad del sistema. Entre otras, quedan comprendidas las operaciones con los cajeros automáticos, por Internet o por vía telefónica, las transferencias electrónicas de fondos o información, y las tarjetas de crédito y débito.

Así, específicamente el artículo 364 de la RNRCSF, dispone la obligación de incluir metodologías de autenticación asociadas a los riesgos de los distintos tipos de transacciones y niveles de acceso, debiendo requerir como mínimo un doble factor de autenticación para las transferencias o pagos a terceros realizados desde una cuenta bancaria y las solicitudes de préstamos que fueran realizadas en forma no presencial.

También los bancos y demás instituciones financieras deben monitorear y controlar las operaciones de tal modo que puedan detectar hechos irregulares vinculados con el uso del instrumento o el sistema en el que opera, incluyendo los cambios e intentos de cambios de clave, número de identificación personal, dirección, teléfono y correo electrónico de contacto, medios establecidos para recibir comunicaciones, entre otros. Dicho sistema deberá resguardar fechas y horas de las operaciones; contenidos de los mensajes; identificación de operadores, emisores y receptores; cuentas y montos involucrados; mecanismo de autenticación del usuario utilizado en la operación; identificación de la terminal desde la cual se operó; y si la operación fue realizada en forma presencial o remota.

Todo ello sin perjuicio de informar al cliente sobre los principales riesgos a que está expuesto al utilizar el instrumento electrónico para realizar transacciones financieras, y proporcionarle recomendaciones

sobre cómo debe protegerse adecuadamente para mitigar dichos riesgos. Por ejemplo, dejar saber a los clientes cuáles son los indicios de que está siendo víctima de phishing (v.g. urgencia de los pedidos, errores ortográficos, enlaces sospechosos, solicitud de información confidencial, etc.)

En la normativa dictada por el regulador (BCU)[2] también se establece que son las instituciones las que deben demostrar, en caso de un reclamo del usuario en relación con alguna transacción efectuada, y sin perjuicio de cualquier prueba en contrario que el usuario pueda producir, que la transacción:

- Fue efectuada de acuerdo con los procedimientos acordados con el cliente.
- Fue registrada y contabilizada correctamente.
- No se ha visto afectada por un fallo técnico o por cualquier otra anomalía.
- Ha sido correctamente autenticada de acuerdo con la metodología establecida para la misma, debiendo además poner a su disposición - independientemente si el instrumento fue utilizado en el país o en el exterior - la información resguardada señalada previamente, así como cualquier otro elemento que permita demostrar que dicha transacción fue realizada por el cliente o por terceros con conocimiento del cliente. En caso de no poder demostrarlo, el emisor será responsable de la transacción reclamada, siempre que no sea atribuible a incumplimientos de las obligaciones del usuario.

Por último, cabe resaltar que fuera de los aspectos normativos y de las soluciones que se adopten ante los variados y disímiles casos que se presentan diariamente, los expertos en la temática coinciden en que en temas de ciberseguridad es clave la educación y concientización de los usuarios de los servicios en línea, sobre las técnicas de phishing y como reconocerlas siendo esta la forma más eficiente y efectiva de reducir la probabilidad de que los usuarios caigan en trampas de phishing.

[2] Art. 364 de la RNRCSF literal h)

Breves

- Según lo informado por la Dirección General Impositiva en su página Web, desde el 1° de agosto de 2025 los contribuyentes con actividades de transporte terrestre profesional de carga deberán incluir mensualmente en el formulario 2181: 1) en la línea 13 (IVA compras combustible), el importe del IVA compras deducido por gasoil; y 2) en la línea 505 (IVA Compras Plaza Tasa Básica), el importe informado en la línea 13.

- De acuerdo con lo dispuesto en el Decreto Nro. 144/025, del 4 de julio de 2025, se actualiza el valor del Timbre del Registro de Testamentos y Legalizaciones creado por la Ley Nro. 17.707, de 10 de noviembre de 2003. El nuevo valor, vigente entre el 1º de julio y el 31 de diciembre de 2025, es de $ 2.656.

Contacto

Invitamos a nuestros lectores a enviarnos sus inquietudes sobre la temática de esta sección a: **UY-FMLegal@kpmg.com**

home.kpmg/uy/es