Santiago, veintisiete de agosto de dos mil veintiséis.

Vistos:

Se reproduce la sentencia en alzada, con excepción de sus fundamentos octavo, noveno y décimo segundo a décimo cuarto, que se eliminan.

Y se tiene en su lugar y, además, presente:

1° Que las operaciones discutidas en autos son 2, por un monto total de $3.000.000, realizadas desde la tarjeta de crédito del cliente, a través de la plataforma Kushki y efectuadas con código QR, haciéndose descripción por el actor de todos los pasos que se deben seguir para efectos de poder hacer uso de esa forma de pago y explicando que todos los datos que se deben ingresar al sistema para poder emplearlo son de uso y custodia exclusiva del cliente. Añade que, al hacerse uso de este sistema de pago, se genera de modo inmediato un comprobante de pago que llega al correo registrado por el usuario, de modo que discute el desconocimiento que alega de no haber advertido lo sucedido sino hasta 2 días después.

2° Que, como ya se asentó en el fallo que se revisa y, en lo relevante, el cliente declaró sospechar que pudo ser víctima de phishing, ya que no se afectó saldos de cuentas ni avances ni otras tarjetas del mismo banco. Admitió que luego de estos hechos, formateó su teléfono e instaló un antivirus con detección de phishing, porque habría advertido que no solo las entidades financieras pueden ser objeto de ataques cibernéticos, sino que también a los clientes. En su comunicación al banco, cuando el cliente hizo una breve descripción de los hechos, señaló que el fraude también se intentó en sus otros bancos, pero que no se habría logrado; sin embargo, en su contestación, indica que existe al menos otra causa seguida ante el mismo tribunal, pero iniciada por BCI, también por operaciones en la misma fecha y en horas aproximadas.

Luego, se deja constancia del pago a través de terminal QR, expresándose que para concretarlo se requieren todos los datos de la tarjeta del cliente: número completo, nombre impreso, fecha de vencimiento, CVV, verificación SMS y aviso al correo electrónico; y, se deja constancia de que, por tratarse de compras

seguras, no es posible efectuar contra cargo u obtener información del proceso de intercambio.

3° Que, con el objeto de establecer un mejor contexto legal para la resolución de este asunto, resulta útil considerar lo establecido en el artículo 5 ter de la Ley 20.009, con la precisión de que esta disposición fue incorporada a la ley, con posterioridad a los hechos conocidos en autos. Esa disposición establece situaciones en que se debe presumir el dolo o la culpa grave del usuario, indicando en su literal **g)**, la existencia de indicios suficientes de haber sido el mismo usuario quien realizó la operación reclamada en canales físicos previo a la solicitud de restitución y/o cancelación de cargos; y, en su literal **h)** aquellos casos en que la operación desconocida hubiere sido realizada con autenticación reforzada, en los términos del artículo 4 de esa ley, siendo al menos uno de los factores de autenticación el de inherencia.

Para comprender esta última situación, el citado artículo 4 dice, en lo pertinente, que *"La Comisión para el Mercado Financiero, mediante norma de carácter general, establecerá estándares mínimos de seguridad, registro y autenticación. A través de la referida norma de carácter general, la Comisión determinará los supuestos de uso y transacciones en que resulte obligatorio por parte del emisor el uso de autenticación reforzada."* Añadiendo a continuación, en esa misma disposición, que *"…se entenderá por autenticación el procedimiento que permita al emisor comprobar la identidad del usuario o la validez de la utilización de un medio de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario, y por autenticación reforzada, la utilización de al menos dos factores de autenticación, sea de conocimiento, posesión o inherencia, diferentes e independientes entre sí, para el acceso o utilización de los medios de pago, cuentas o sistemas similares que permitan efectuar pagos o transacciones electrónicas."*

4° Que, sobre este tópico, la referida comisión, dictó la norma de carácter general N°538, de 17 de junio de 2025, donde se reitera lo mismo acerca del concepto de autenticación y se agrega que por "Conocimiento" se comprende algo que solo el usuario conoce, así como las contraseñas o números de identificación

personal o PIN; por “Posesión”, algo que solo el usuario posee, tal como un dispositivo token o hardware criptográfico portátil, un mensaje tipo OTP, la tarjeta de pago o un smartphone; y, por “Inherencia” algo que el usuario es, explicando que, *“…usualmente para este factor se utiliza la verificación biométrica, tal como huella dactilar, rostro, voz o datos conductuales. El uso de este factor debe tener como objetivo permitir distinguir inequívocamente al usuario y* ***mitigar el riesgo*** *de suplantación de identidad.* Por último, se identificó como “Dispositivo de Confianza”, aquel dispositivo electrónico reconocido por el propio usuario ante el emisor como tal y debe haber cumplido con un proceso de enrolamiento a través de ARC.

Cuando se explican los “Supuestos de Uso de Autenticación Reforzada”, se establecen como casos de aplicación obligatoria: 1) En la gestión y realización de transferencias electrónicas de fondos, con la excepción que se detalla; y, 2) En el proceso de incorporación del cliente en las plataformas digitales del emisor, incorporación y modificación de datos personales, modificación de claves de autenticación, incorporación de dispositivo de confianza y su reemplazo o eliminación.

5° Que, en la especie, las operaciones que se describen fueron cumplidas con código QR que, como antes se explicó, exige datos de la tarjeta del cliente: número completo, nombre impreso, fecha de vencimiento, CVV, verificación SMS y aviso al correo electrónico, esto es, existió el procedimiento para comprobar la identidad del usuario o la validez del uso del medio de pago señalado, incluyendo la utilización de credenciales de seguridad personalizadas del usuario.

Y, si de autenticación reforzada se trata, la disposición exige el uso de al menos 2 factores de autenticación, sea de conocimiento, posesión o inherencia, diferentes e independientes entre sí, lo que en la especie también se cumplió, ya que, tal como se informó por el banco y se reconoció por el propio cliente, tuvo aplicación el factor *conocimiento*, porque se empleó las contraseñas o números de identificación personal del cliente; y también tuvo aplicación el factor *posesión*, porque la operación se cumplió a través del smartphone del cliente quien optó por hacer uso de este medio, al que accedía a través de sus claves personales, con la

clave secreta para transferencias Itaú Pass y habiéndose contemplado la comunicación vía SMS o correo electrónico, Por último, se presume que pudo concurrir el factor *inherencia,* ya que el usuario usó su teléfono inteligente, pero se desconoce si en aquél tiene habilitada solo clave, o además cuenta con huella y/o reconocimiento facial.

6° Que la cita de una norma vigente con posterioridad al hecho de autos, se cumple para evidenciar que el legislador ha tratado de actualizar y precisar las exigencias de cuidado y seguridad que impone a las instituciones financieras para mejorar sus medidas de seguridad respecto de las operaciones que realizan sus clientes, precisamente a consecuencia de los avances tecnológicos; y, del modo señalado se procura explicar la afirmación del banco en el sentido de haberse operado sobre una plataforma segura.

Aquí se reitera que el hecho ocurrió en el año 2022, en tanto la norma general de la CMF inició su vigencia a partir del 1 de agosto de 2025, *"excepto los casos de ARC obligatoria… cuya vigencia comenzará el 1 de agosto de 2026."*

Esto es, se está midiendo el caso con la mayor exigencia que entró en vigor con posterioridad, advirtiéndose que para el año 2022 el banco demandante ya mantenía en uso algunas de las medidas de seguridad que se hicieron exigibles después.

7° Que, por otra parte, dos cosas llaman la atención en el hecho que se analiza: primero, que el cliente dijo creer que fue víctima de phishing, lo que le movió a resetear su teléfono y, además, a instalar -recién entonces- un antivirus especialmente diseñado para ese tipo de estafa; y, en segundo lugar, informó haber sufrido el mismo fraude, en la misma fecha y hora similar, respecto de otras tres instituciones financieras, pidiendo incluso que se tuviera a la vista la causa iniciada por el BCI en su contra, por aquella situación.

En el escenario descrito, resulta posible concluir la existencia de indicios suficientes de haber sido el usuario quien actuó en algún momento con grave descuido o negligencia en el cuidado de aquellas medidas de seguridad que son de su cuidado exclusivo y en las cuales ninguna injerencia tiene el banco, especialmente si él mismo califica la situación como un fraude cometido por

terceros (Phishing), si también declara que después de estos hechos decidió adoptar mejores medidas de resguardo de su smartphone y, si asimismo, si reconoce que hubo otros fraudes o intentos de fraude en sus otras cuentas bancarias. No aparece muy razonable, conocido su relato, concluir que los otros 3 bancos sufrieron también brechas en sus sistemas de seguridad, sino que más bien, se identifica como elemento común, al cliente y el aparato tecnológico que emplea para sus operaciones bancarias y/o financieras. Aquí resulta oportuno considerar que, en parte, el demandado atribuyó responsabilidad al banco porque, según sus palabras, el fraude no se habría podido materializar en los otros bancos lo que en su opinión, pondría en evidencia que el desempeño deficiente fue del actor, sin embargo, consta de los antecedentes del proceso que el banco demandante frenó otras dos operaciones incluso antes de que el cliente lo advirtiera, a consecuencia de haberse levantado una de las alertas que mantiene en funcionamiento; y, por otra parte, el mismo demandado reconoció que el BCI también lo demandó, de modo que subsiste la conclusión de que el problema no fue de la banca, sino que de las medidas de cuidado cuya adopción recae en el cliente.

Y, también existe como indicio para concluir la responsabilidad del usuario, el hecho que las operaciones desconocidas fueron realizadas con autenticación reforzada, como ya antes se explicó, por haber concurrido al menos dos de los factores pertinentes: conocimiento y posesión. En lo que cabe a la inherencia, se presume que aquel concurría, pero faltan elementos de prueba para así tenerlo por cierto, a lo que se suma el hecho de que tal exigencia recién empezó a aplicarse a partir del mes en curso. No obstante, en cuanto al factor inherencia, no debe perderse de vista que la autoridad señala el uso de este factor para *"permitir distinguir inequívocamente al usuario y mitigar el riesgo de suplantación de identidad"*, énfasis en el verbo **mitigar**, esto es, no se puede dar una seguridad absoluta, sino tan solo, disminuir o reducir el riesgo o el daño, que es precisamente lo que se aprecia cumplido en el proceso cuando se informa -por ambas partes-, que el banco pudo frenar otras dos operaciones.

Por estas consideraciones y de acuerdo también a lo establecido en el artículo 32 de la Ley 18.287, **se revoca** la sentencia apelada de treinta de marzo de dos mil veintitrés, pronunciada por el Segundo Juzgado de Policía Local de Ñuñoa, por la cual se rechazó la acción deducida y, en cambio, **se declara que aquella queda acogida**, debiendo procederse por el cliente a la restitución del abono normativo, en la forma que señala la ley; y, se autoriza al banco a dejar sin efecto la cancelación de los cargos o demás medidas que haya adoptado en su oportunidad.

Se dispone que cada parte pague sus costas, por haberse litigado con motivo plausible.

Redactó la ministra Carolina Vásquez Acevedo.

Regístrese y devuélvase.

Rol N°2951-2023 Policía Local

Pronunciada por la Décima Tercera Sala de la Corte de Apelaciones de Santiago integrada con los ministros Carolina Vásquez Acevedo, Claudia Lazen Manzur y Fiscal Judicial Carla Troncoso Bustamante.

Carolina Soledad Vásquez Acevedo
Ministro
Corte de Apelaciones
Veintisiete de agosto de dos mil veintiséis
09:07 UTC-4

Claudia Andrea Lazen Manzur
Ministro
Corte de Apelaciones
Veintisiete de agosto de dos mil veintiséis
12:51 UTC-4

Carla Paz Troncoso Bustamante
Fiscal
Corte de Apelaciones
Veintisiete de agosto de dos mil veintiséis
12:52 UTC-4

María Laura Gjurovic Manríquez
Secretario(a)
Corte de Apelaciones
Veintisiete de agosto de dos mil veintiséis
13:21 UTC-4

Pronunciado por la Decimotercera (zoom) Sala de la C.A. de Santiago integrada por los Ministros (as) Carolina Soledad Vasquez A., Claudia Lazen M. y Fiscal Judicial Carla Paz Troncoso B. Santiago, veintisiete de agosto de dos mil veintiseis.

En Santiago, a veintisiete de agosto de dos mil veintiseis, notifiqué en Secretaría por el Estado Diario la resolución precedente.