FACULTAD DE DERECHO

INFORME JURÍDICO DE EXPEDIENTE ADMINISTRATIVO N° 0409-2021/CC1

PRESENTADO POR
CESAR GERMAN SALAZAR DÍAZ

TRABAJO DE SUFICIENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

CHICLAYO – PERÚ
2023

Trabajo de Suficiencia Profesional para optar el Título de Abogado

Informe Jurídico sobre Expediente N° 0409-2021/CC1

Materia	:	**Protección al Consumidor**
Entidad	:	**INDECOPI**
Bachiller	:	**Cesar German Salazar Díaz**
Código	:	**2011514826**

CHICLAYO – PERÚ

2023

En el presente informe se analizará un procedimiento administrativo ante la Comisión de Protección al Consumidor N° 1 (en adelante CPC) de INDECOPI, comienza con la interposición de la denuncia de la persona iniciales J.A.Y.C. (en adelante denunciante) contra el banco de iniciales SP S.A.A. (en adelante denunciado) el 22.02.2021 por haber permitido retiros de la cuenta de ahorros por los montos de S/3,196.30 y S/5,900.00 de fecha 25.05.2020 y S/9,597.00 de fecha 24.06.2020, solicitando como medida correctiva la devolución de los mencionados montos.

Ante ello, el banco contesta y señala que los montos han sido debitados correctamente y de acuerdo a sus filtros de seguridad, ingresando el denunciante la clave dinámica y digital correspondiente, además de cumplir el banco con enviarle mensaje y correo electrónicos a los consignados por el propio denunciante, adjuntando captura pantalla de su sistema denominado SPLUNK.

La secretaria técnica de la CPC, elabora informe respecto del caso, señalando que de los medios probatorios adjuntados por el banco se evidencia que este no ha cumplido con acreditar el ingreso de la clave digital para la autorización de las operaciones de fecha 25.05.2020, ni cumplió con presentar los reportes remitidos por su propio sistema, que den cuenta del momento del inicio de sesión a la aplicación los días 25 de mayo y 24 de junio de 2020, antes de las operaciones cuestionadas, ni tampoco que estas se hayan realizado con las validaciones que correspondían, además de incumplir con presentar medios probatorios que acrediten el registro de las operaciones a través de sus sistemas. Por último señala que tampoco cumplió con presentar los reportes emitidos por su propio sistema respecto de la operación del 24.06.2020, que den cuenta del envío de la clave SMS al teléfono celular del denunciante.

En primera instancia tomando en cuenta los argumentos señalados por la secretaria técnica, se declara fundada la denuncia por infracción a los artículos 18° y 19° de la Ley N°29571- Código de Protección y Defensa del Consumidor (en adelante El Código), toda vez, que no ha quedado acreditado que el banco adoptó las medidas de seguridad pertinentes, al permitir que se efectuaran tres operaciones no reconocidas con cargo a la cuenta de ahorro del denunciante, además como medida correctiva la devolución de los montos e intereses legales, sanción con una multa de 4,25 UIT, el pago de costas y costos, y la inscripción en el Registro de Infracciones y Sanciones.

El banco presenta su recurso de apelación reiterando lo señalado en su contestación a la denuncia agregando además otros medios probatorios y detallando el significado de cada medio probatorio.

En segunda instancia se resuelve declarar infundada la denuncia argumentando que en las operaciones de fecha 25.05.2020 se acreditó el correcto ingreso a la banca móvil y que habían sido autorizadas mediante el ingreso de su clave secreta y la clave digital correspondiente, y que fueron efectuadas mediante dos mecanismos de autenticación distintos (una clave secreta y una digital); y que la clave digital de cada operación había sido remitida al celular y correo afiliados por el denunciante (lo cual evidencia que este mecanismo constituida una clave dinámica). Respecto de la operación de fecha 24.06.2020 se acreditó el registro de la operación y los datos correspondiente como son número de operación, número de tarjeta, código de autorización, monto de la operación, establecimiento comercial y canal donde se realizó la operación, además de la comunicación del Banco (vía SMS al celular del denunciante), posterior a la realización del consumo objetado, mediante la cual se procedió a alertar al cliente sobre la compra realizada en el establecimiento.

NOMBRE DEL TRABAJO

INFORME JURIDICO - SALAZAR DIAZ.docx

RECUENTO DE PALABRAS

15557 Words

RECUENTO DE CARACTERES

82965 Characters

RECUENTO DE PÁGINAS

29 Pages

TAMAÑO DEL ARCHIVO

95.4KB

FECHA DE ENTREGA

Jul 21, 2023 6:18 PM GMT-5

FECHA DEL INFORME

Jul 21, 2023 6:18 PM GMT-5

20% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

- 19% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr
- 13% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 10 palabras)

USMP UNIVERSIDAD DE SAN MARTÍN DE PORRES | Filial Norte

Mtro. MARCO ANTONIO FERNANDINI DIAZ
COORDINADOR PROGRAMA DE DERECHO

INDICE

I. RELACIÓN DE LOS PRINCIPALES HECHOS EXPUESTOS POR LAS PARTES INTERVINIENTES EN EL PROCEDIMIENTO.

1. DENUNCIA

Interpuesta en INDECOPI por la persona iniciales J.A.Y.C. (en adelante denunciante) contra el banco de iniciales SP S.A.A. (en adelante denunciado) el 22.02.2021 por haber permitido retiros de la cuenta de ahorros FREE, los cuales no reconoce haber autorizados.

Petitorio

Solicita declare fundada la denuncia y se ordene al banco, como medida correctiva la devolución de los fondos indebidamente retirados de sus cuenta por el monto total de S/18,693.00, por los siguientes retiros:

- S/3,196.30 de fecha 25.05.2020 (debito compras)
- S/5,900.00 de fecha 25.05.2020 (pago efectivo) de la tarjeta debito MasterCard
- S/9,597.00 de fecha 24.06.2020 (pago efectivo) de la tarjeta debido VISA

Fundamentos de hecho

1. El 24.05.2020 se realizaron dos retiros de su cuenta de ahorros por el monto de S/9,096.30, los cuales no reconoce, al percatarse inmediatamente llamó al Banco, el cual anuló su tarjeta de débito MasterCard y cerró cualquier nueva operación, con código de bloqueo N°843586.
2. El 25.05.2020 se acercó al Banco y presentó el reclamo N°2020067952, informándole que tenía un plazo de atención de 30 días.
3. El 12.06.2020 el banco le envía un cuestionario con las siguientes preguntas:
    - ¿En algún momento (fecha cercana a la operación no reconocida) perdió el control del celular o chip, indicar fecha y hora aproximada?:
      Respuesta: No.
    - ¿Cambio de operador?
      Respuesta: No, no cambie de operador.
    - ¿Ha habido alguna llamada solicitando la clave digital o información de sus cuentas?
      Respuesta: No, no se ha recibido ninguna comunicación de ese tipo.

    Después de contestar las preguntas, le informaron que tenía registrado el reclamo N°SCI-A-2020005872, teniendo el banco 30 días más para solucionar el fraude de su cuenta.
4. El 24.06.2020 se percata que no podía hacer operaciones en la aplicación del banco, realizando inmediatamente el cambio de usuario y clave, dándose cuenta que realizaron un nuevo retiro no reconocido por el monto de S/9,597.00, acudió al banco y bloqueo la tarjeta y la cuenta con numero de bloqueo N°383817 y reclamo N°2020084006.
5. El 24.10.2020 al querer recargar su celular, no pudo acceder a su cuenta mediante el aplicativo del banco, procediendo a cambiar de usuario y clave inmediatamente, reportando el hecho al banco, asignándole el reclamo N°SCI-R-2020168843, en esta oportunidad no retiraron dinero, debido a que solo contaba con S/15.00; dejando constancia que nuevamente entraron a su cuenta y la bloquearon.

Medios Probatorios

1. Estados de cuenta
2. Correos de reclamo y bloqueos
3. Mensajes de teléfono bloqueando los accesos a compras a nivel nacional e internacional.
4. Denuncias policiales

Mediante carta N°264-2021/PS2 se le informa al denunciante que su caso por razón de cuantía será derivado a la Comisión de Protección al Consumidor N°1 (en adelante CPS), la cual a través de la resolución N°01 admite a trámite la denuncia y requiere información al banco, para que en un plazo de 05 d.h. presente copia legible de los contratos y/o documentos suscritos a nombre del denunciante y los documentos que acrediten la validez de las operaciones no reconocidas, cuestionadas por el denunciante.

El denunciado solicita plazo adicional por motivo que los documentos solicitados requieren un plazo mayor para su atención. Y mediante resolución N°2, se tiene por apersonado al denunciado y se le concede un plazo adicional de 05 d.h. para presentar la información requerida.

2. CONTESTACIÓN DE DENUNCIA

Solicita se declare INFUNDADA la denuncia, en tanto se ha acreditado que las operaciones se han registrado correctamente en su sistema. Niega y contradice los hechos denunciados bajo los siguientes fundamentos:

Respecto de las operaciones no reconocidas:

Tal como se señala en el escrito de denuncia, se cuestiona tres operaciones, las cuales se realizaron a través de la banca móvil por APP (aplicación) la cual requiere el ingreso de contraseña creada por el denunciante, y de la cual él tiene únicamente conocimiento, dado que es creada por él mismo; y clave digital es enviada a donde el cliente solicita (SMS o correo electrónico).

A fin de acreditar que las operaciones cuestionadas se realizaron válidamente, adjuntan los prints de pantallas, donde se advierte que las referidas operaciones se registraron exitosamente.

Según los prints de pantalla, las operaciones se efectuaron sin anomalías ya que se realizaron ingresando la clave digital y se envió al medio que el denunciante predeterminó para la recepción de la clave digital, no habiendo modificado el número o correo distinto al que registró.

Las operaciones de la banca móvil cuentan con medidas de seguridad suficientes para asegurar que los titulares realicen operaciones, ya que solo requieren claves de conocimiento exclusivo del cliente. Sin embargo, se debe tener en cuenta que la medida de seguridad más importante es el cuidado que debe tener el propio cliente con la información de su tarjeta de débito, por ello, reciben una serie de indicaciones y recomendaciones en temas de seguridad a través de vides, folletos, e información que aparece en la página web del banco, y que se encuentra disponible en la red de agencias, con el fin que los consumidores tomen medidas para evitar fraudes, robos de identidad y/o tarjetas, entre otros.

De acuerdo al artículo 14 de la Resolución SBS N°6523-2013 "Reglamento de tarjetas de Crédito y Débito (en adelante Reglamento) las entidades financieras cargaran a cuenta de los clientes las órdenes de pago que podrían ser sustituidas a través de medios electrónicos y/o firmas electrónicas. Siendo responsabilidad de los clientes custodiar dicha información, datos que son exclusivos y propios, teniendo la responsabilidad y cuidado de las claves solicitadas por la banca móvil el denunciante, por lo que se exime de responsabilidad al banco.

En el caso materia de análisis, se realizó el ingreso de las claves, por lo que, las operaciones fueron debitadas con normalidad. No es posible para el banco determinar si fue el denunciante o fue otra persona, puesto que el sistema únicamente valida que claves ingresadas sean las correctas. En cualquier caso, el denunciante sería responsable puesto que el solo tiene conocimiento de la información y tiene el deber de bloquear el aplicativo inmediatamente ya sea por extravió o robo del móvil.

El banco ha acreditado que las operaciones cuestionadas se encontraban debidamente autorizadas con el ingreso de la clave secreta como se puede observar en los printers, y que esta clave es de conocimiento exclusivo del denunciante, la única persona en poder de la tarjeta y la clave secreta.

Medidas de seguridad adoptadas

Entre las obligaciones del denunciante, está la de custodiar adecuadamente su tarjeta, mantener en confidencialidad su clave secreta, comunicar el robo, hurto o extravió de la tarjeta, entre otros.

Parte del servicio prestado por el banco, implica la confianza que el consumidor deposita sus sistemas de seguridad para la realización y comprobación de cualquier transacción comercial realizada mediante la tarjeta de crédito o debido que afecte su patrimonio. Evitando a través de los mecanismos de seguridad el uso indebido o fraudulento de las tarjeta.

De acuerdo al artículo 9 del Reglamento, en cualquiera de los escenarios que se realice un consumo, este se debe efectuar en observancia de las medidas de seguridad correspondientes, por lo que, se exige a las

entidades financieras contar con un sustento indubitable de la autorización realizada por el cliente, sea a través de una orden de pago, código, firma electrónica y/o virtual (clave secreta, clave digita, CVV, etc.).

El artículo 14° del Reglamento señala que para cargar válidamente el importe en las tarjetas de débito sus clientes, se debe acreditar lo siguiente:

(i) En los consumos con tarjeta no presente, debe haber autorización del usuario a través de medios electrónicos, firmas electrónicas o vía telefónica,
(ii) Consumos con tarjeta presente, las órdenes de pago deben estar suscritas por el cliente o acreditarse el ingreso de la clave secreta para entenderse autorizados, según corresponda.

Esto quiere decir que, ante el cuestionamiento de un consumidor, el banco debe estar en la posibilidad de acreditar de manera fehaciente que las operaciones cargadas han sido debidamente autorizadas por el cliente en las tarjetas de crédito y débito.

Habiendo cumplido con las medidas de seguridad señaladas, adicionalmente, se debe cumplir con las medidas de seguridad establecidas en el artículo 17 del Reglamento, con respecto a las operaciones con tarjeta:

(i) Contar con un sistema de monitoreo de operaciones, que detecte operaciones que no corresponden al comportamiento habitual de consumo del usuario.
(ii) Implementar procesos complementarios para gestionar las alertar generadas por el sistema de monitoreo de operaciones.
(iii) Identificar patrones de fraudes, mediante el sistema analítico de la información histórica de las operaciones, los que deberán incorporarse al sistema de monitoreo de operaciones
(iv) Establecer límites y controles en los diversos canales de atención, que permitan mitigar las perdidas por fraude.
(v) Requerir al usuario la presentación de un documento oficial de identidad.
(vi) En el caso de operaciones de retiro o disposición de efectivo, u otras con finalidad informativa sobre operaciones realizadas u otra información similar, deberá requerirse la clave secreta del usuario, en cada oportunidad, sin importar el canal utilizado para tal efecto.

Se aprecia de la citada norma, que entre las medidas de seguridad exigidas a las entidades financieras se encuentra la de contar con un sistema de monitoreo de operaciones que permita : i) detectar aquellas transacciones que no corresponden al comportamiento habitual de los consumidores e (ii) identificar patrones de fraude.

El banco alertó al denunciante sobre el bloqueo de la tarjeta de débito, solicitando se comunique de inmediato, así también los mensajes remitidos por el banco fueron adjuntados por el propio denunciante.

Asimismo, se adjunta los printers de pantalla que muestran que se realizó el envío y validación correcta de OTP para una transacción realizada el 24 de mayo y 26 de junio de 2020, que acredita que la clave digital fue enviada al número de teléfono del denunciante.

Sobre el comportamiento habitual de los consumidores, el artículo 2° del reglamento refiere que en aquellos casos que se cuestione que las operaciones de consumo no corresponden al comportamiento habitual de consumo o son compatibles con patrones de fraude, se requiere analizar, primero, si se contó con la autorización del titular para la realización de las operaciones cuestionadas, y , finalmente, si, en efecto estas no se encontraban acorde con el comportamiento habitual del consumidor o presentaban características de fraude, para poder concluir si funcionó correctamente el sistema de monitoreo del Banco.

En el presente caso el banco acreditó que las operaciones cuestionadas se encontraban debidamente autorizadas a través del ingreso de la clave alfanumérica, clave digital y el código de autorización generado por cada operación. Por lo tanto, habiendo el banco acreditado la validez de las operaciones materia de reclamo, no corresponde que el Banco asuma la responsabilidad por la conducta materia de denuncia.

Adjunta: Vigencia de poder, Printers de pantalla del sistema, Mecanismo de seguridad

3. INFORME FINAL DE INSTRUCCIÓN

La secretaria técnica de la CPC N°1 en el informe de instrucción, concluye que el banco ha vulnerado los artículos 18° y 19° de la Ley N°29571- Código de Protección y Defensa del Consumidor (en adelante El Código), toda vez, que no ha quedado acreditado que adoptó las medidas de seguridad pertinentes, al permitir que se efectuaran tres operaciones no reconocidas con cargo a la cuenta de ahorro del denunciante por el importe total de S/18,693.00, recomendando se sancione con una multa de 4,25 UIT, bajo los siguientes fundamentos relevantes:

Análisis

Sobre la presunta infracción al deber de idoneidad

El artículo 18° del código establece que la idoneidad es la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, el artículo 19° establece que los proveedores son responsables por la calidad e idoneidad de los productos que ofrecen en el mercado.

Sobre las operaciones no reconocidas

Parte del servicio prestado por el banco, implica la confianza que el consumidor deposita en los sistemas de seguridad con los que cuenta el banco, al cual se le exige la implementación de mecanismos de seguridad destinados a proteger las transacciones que realizan sus clientes, evitando el uso indebido o fraudulento de las tarjetas que crédito o débito.

Del análisis de los artículos 9 y 14 del Reglamento, se desprende que los bancos en cualquiera de los escenarios en que se realice una operación, esta se debe efectuar en observancia de las medidas de seguridad correspondientes, por lo cual, se exige a los bancos contar con el sustento que acredite de manera indubitable la autorización realizada por el cliente, sea a través de la suscripción de una orden de pago, el ingreso de un código o la firma de manera electrónica y/o virtual (clave secreta, clave dinámica, CVV, etc.).

En la dinámica común del mercado existen diversos tipos de operaciones que pueden realizarse con tarjetas de crédito o débito, siendo que para algunas se requiere la presencia física del medio de pago (plástico) y en otros casos no, por lo que pueden realizarse operaciones "con tarjeta presente" y con tarjeta "no presente", para garantizar que este tipo de operaciones se realicen válidamente, con la autorización del cliente, las entidades financieras deben adoptar medidas de seguridad específicas.

Conforme a lo establecido en el Reglamento, las empresas del sistema financiero para cargar válidamente en la cuenta de tarjeta de crédito o débito de sus clientes el importe de las operaciones realizadas con sus tarjetas, deben acreditar que:

(i) En las operaciones realizadas con "tarjeta no presente" hubo autorización del usuario a través de medios electrónicos y/o firmas electrónicas,
(ii) Para los casos de operaciones con "tarjeta presente" las órdenes de pago deben estar suscritas por el cliente para entenderse autorizado o el ingreso de la clave secreta, según corresponda.

Ante el cuestionamiento de un consumidor, la entidad financiera debe estar en la posibilidad de acreditar de manera fehaciente que la operación cargada ha sido autorizada por el cliente.

Sobre las operaciones con transferencia de fondos a terceros

El parámetro de idoneidad en este tipo de casos está constituido por los mecanismos de seguridad implementados para realizar operaciones vía internet, por ello, es necesario que, dentro de un procedimiento de este tipo, se verifique si las operaciones realizadas a través de internet se efectuaron de acuerdo a parámetro de seguridad mínimos implementados por el proveedor, como es el ingreso de las respectivas claves que otorguen validez a dichas transacciones.

Respecto del sistema de seguridad implementado por las entidades se ha emitido la circular N°6-140-2009, Gestión de seguridad de la información (en adelante Circular), la cual en el artículo 6° establece que para transferencia de fondos a terceros por canales electrónicos se deben de contar con dos factores de autenticación, siendo que uno de ellos deber ser de generación o asignación dinámica – claves dinámicas-

u otro factor de nivel de seguridad equivalente o superior a fin de autorizar dichas transferencias a través de banca telefónica.

Por lo expuesto, a fin de determinar la responsabilidad de la entidad financiera, se deberá verificar si las operaciones cuestionadas realizadas a través de internet se efectuaron de acuerdo con los parámetros de seguridad implementado por el proveedor; esto es, con el ingreso de clave secreta de internet y la clave dinámica (token).

(i) Sobre las operaciones de "Pago Efectivo" por los importes de S/5,900.00 y S/9,597.00

En el presente caso, de conformidad con la normativa previamente desarrollada y lo expuesto por las partes, corresponde analizar los reportes de los sistemas del banco que permitan acreditar: (i) el acceso a la aplicación del banco a través del ingreso de la contraseña alfanumérica del cliente, (ii) el ingreso de la clave digital y el registro de las operaciones cuestionadas.

Respecto del reporte de acceso a la aplicación, el banco no ha cumplido con presentar medios probatorios que acrediten el acceso del denunciante al aplicativo, de forma previa a la realización de las operaciones cuestionadas. Sin perjuicio a ello, se analizaron los posteriores filtros de seguridad.

Al respecto para acreditar el ingreso de la clave digital para la autorización de ambas operaciones el banco presentó impresiones de pantallas, en las cuales se verifica la consignación de la glosa "SUCCESFULL", y solo se aprecia coincidencia en la fecha respecto de la operación realizada el 24 de junio de 2020 a las 1:43, por el importe de S/9,597.00; ya que, en el caso de la operación realizada el 25 de mayo de 2020 a las 12:41 por el importe de S/5,900.00, figura una fecha (24.05.2020) que no coincide con la señalada en los estados de cuenta(25.05.2020); por lo que, no habría quedado acreditada la validez de la transacción en cuestión.

El banco además no cumplió con presentar los reportes remitidos por su propio sistema, que den cuenta del momento del inicio de sesión a la aplicación los días 25 de mayo y 24 de junio de 2020, antes de las operaciones cuestionadas, y que estas se hayan realizado con las validaciones que correspondían. Así, la entidad bancaria pudo presentar, por ejemplo, el reporte detallado de inicio de sesión, generación de clave digital e ingreso de la misma plataforma para autorizar las transacciones cuestionadas.

Tampoco cumplió con presentar medios probatorios que acrediten el registro de las operaciones a través de sus sistemas.

De ahí que, atendiendo a la dinámica probatoria, consideran que encontrándose el banco en mejor posición para acreditar que no le era atribuible la infracción denunciada en su contra, le correspondía proporcionar toda la documentación e información necesaria a fin de eximirse de responsabilidad, sin embargo, no ocurrió.

Por las consideraciones previamente expuestas, no queda acreditado que el denunciado adoptó las medidas de seguridad pertinentes al permitir que se efectuaran dos operaciones no reconocidas con cargo a la cuenta de ahorro del denunciante.

(ii) Sobre el consumo por el importe de S/3,196.30

De acuerdo al banco, la primera y segunda impresión de pantalla, demuestra que la operación cuestionada fue autorizada a través del ingreso de un código enviado como mensaje de texto al celular del denunciante, mientras que la tercera impresión de pantalla acreditaría el registro de la operación cuestionada, en el que se detallan elementos como el número de operación, número de tarjeta, código de autorización, moto de la operación, establecimiento comercial y el canal donde se realizó la operación.

De la revisión de los reportes, si bien se observan los datos descritos por el banco, en las imágenes N°3 y 4 no se acredita el envió de la clave SMS sino tan solo la comunicación y registro de la realización de la operación cuestionada.

En ese sentido, el banco no cumplió con presentar los reportes emitidos por su propio sistema, que den cuenta del envío de la clave SMS al teléfono celular del denunciante, lo que resulta indispensable para analizar el ingreso satisfactorio de dicha clave.

No verificándose que el denunciante haya autorizado la operación, a través de algún elemento de seguridad como los descritos en el numeral 18 del presente informe, no ha quedado acreditado que el banco haya adoptado las medidas de seguridad pertinentes al permitir que se efectuara una operación no reconocida con cargo a la cuenta de ahorros del denunciante por el importe de S/3,196.30.

Por todo lo señalado, recomiendan, declarar fundada la denuncia interpuesta.

Sobre la graduación de la sanción

Habiendo verificado la existencia de una infracción administrativa, señala que se debe aplicar los criterios previstos en el código y de manera supletoria los criterios contemplados en el TUO de la LPAG. Conforme al principio de razonabilidad, la autoridad administrativa debe asegurar que la magnitud de la sanción sea mayor o igual al beneficio esperado por la comisión de la infracción.

El artículo 112° del Código, establece que, para determinar la gravedad de la infracción, se consideran diversos criterios como: (i) el beneficio ilícito esperado, (ii) la probabilidad de detección de la infracción, (iii) el daño resultante de la infracción, (iv) los efectos que se pudiesen generar en el mercado, entre otros.

Al respecto, en la resolución final N° 1283-2010/CPC del 31 de mayo de 2010 la comisión estableció la metodología a emplear a efectos de determinar la sanción final a imponer.

Beneficio ilícito, esperado por el denunciado referido al ahorro que representa el no haber adoptado los mecanismos para validar los cargos correspondientes.

No se cuenta con la información que permita cuantificar el beneficio ilícito, y en el expediente tampoco obra documentación que permita establecer parámetro objetivo, razón por la cual, la graduación de la sanción se realiza a partir de los criterios señalados en los artículos 112 del Código.

Daño resultante, en la medida que se autorizó indebidamente 03 operaciones, afectando su patrimonio y vulnerando además las expectativas del consumidor, en tanto no esperaba, que el banco cargara operaciones en su cuenta sin autorización.

Por ello, a efectos de determinar el daño, se utilizará como referencia el importe total de dichas operaciones, debido a que represente la suma de tres operaciones no realizadas válidamente, el cual, equivale a 4,25 UIT.

Efectos en el mercado, se configura una afectación al mercado, al existir una defraudación de expectativa por pate de las empresas del sistema financiero a los consumidores, quienes podrían verse perjudicados al efectuarse el cargo de transacciones que no han realizado.

Consideran que el daño ocasionado al consumidor, así como los efectos generados en el mercado ocasionados por la presente información, y, en aplicación de los principios de predictibilidad (numeral 1.15 del artículo IV del TUO de la LPAG) y razonabilidad (el número 3 del artículo 248° del TUO de la LPAG) corresponde sancionar al banco con una multa de 4,25 UIT.

Mediante resolución N°4 se agrega al expediente el informe final y se le concede al denunciado un plazo de 5 d.h. para presentar descargos al informe.

4. CONTESTACION AL INFORME FINAL

Solicitan desestimar la recomendación efectuada, reiterando lo señalado en la contestación de la denuncia y agregando los siguiente argumentos:

Respecto a las operaciones no reconocidas

a) Las operaciones de "pago efectivo" por los importes de S/5,900.00 y S/9,597.00

Al respecto conforme al escrito de descargos, las operaciones se realizaron a través de la App, la cual requiere el ingreso de contraseña creada por el cliente.

Adjuntan printers de pantalla que muestran que se realizó el envío y validación correcta del OTP para una transacción (SELSIGNING) realizada el 24.05.2020 y 24.06.2020, es decir, que acredita que la clave digital fue enviada al número de teléfono del cliente

En ese sentido, contrariamente a lo señalado por la Secretaria Técnica, mediante los reportes denominados splunk, se acredita la correcta autorización de las operaciones cuestionadas.

Asimismo las claves dinámicas fueron enviadas al cliente al medio que predeterminó, en este caso el denunciante afilia en una agencia bancaria, utilizando biométrico: teléfono el 13.08.2019 y con fecha 09.04.2020 afilia al correo; finalmente se desafilia teléfono y correo el 27.05.2020 y vuelve a afiliar los mismos, las claves digitales fueron enviadas al medio que el propio denunciante estableció.

b) Sobre el consumo por el importe de S/3,196.30

Se ha realizado siguiendo el circuito operativo normal para este tipo de operaciones, de acuerdo al siguiente detalle:

1. El establecimiento comercial (página web) ordena el cargo por el monto de consumo a la TC.
2. Visa procesa el cargo
3. El cargo se registra en la TC operada por el banco.

Las transacciones con una tarjeta de crédito a través de internet requieren el número de tarjeta, el nombre del titular, la fecha de vencimiento, el código CVV2(que se muestra al reverso de la tarjeta)

En el presente caso, la transacción cuestionada por la denunciante se registró con total normalidad en sus sistemas, puesto que se efectuó con el ingreso de los datos necesarios y exigidos por la SBS, para luego ser procesados por VISA exitosamente generándose el código de autorización.

Adjuntan impresión de pantalla del registro de consumo en los sistemas de manera exitosa, en el cual se observa el código de autorización generado, así como el monto consumido y el número de la tarjeta utilizada.

Asimismo, señalan que de acuerdo con el sustento (contracargo) remitido por la empresa procesadora se aprecian datos como la fecha, el número de tarjeta utilizada y otros datos generados por el consumo, y que coinciden con los datos contenidos en el print insertos en párrafos precedentes.

Se han resuelto denuncias versadas en consumos no reconocidos por internet recaído en la Resolución Final 1117.2019/CC1, la cual declara INFUNDADA la denuncia, toda vez que, en los printers de pantalla insertos se visualiza el código de autorización que se genera como consecuencia del proceso de verificación de los datos de la tarjeta de crédito, como el ingreso del código CVV, fecha de vencimiento, etc., que son solicitados para las compras por internet, y que generan certeza de que se realizó el ingreso de los datos de la tarjeta de crédito, siendo suficiente para verificar la correcta autorización del consumo.

Por lo tanto, conforme acreditadon con los documentos presentados, el establecimiento comercial en el que se efectuaron los consumos cuestionamos aceptaba como medio de pago la tarjeta visa, por lo que, debe entenderse que la tarjeta de crédito entregada se encontraba facultada a efectuar las operaciones materia de denuncia.

Asimismo, debe de tenerse en cuenta el criterio recogido por la autoridad administrativa a cargo de resolver conflictos referidos a los derechos del consumidor publicados en la página web de INDECOPI, que señala lo siguiente:

3.2.7 ¿El titular de la tarjeta de crédito es responsable por su uso?

Sí, se considera que el titular de la tarjeta de crédito será responsable de la conservación de su tarjeta y de su clave de identificación personal. El consumidor debe comunicar al banco respecto de cualquier potencial riesgo de uso ilícito de su tarjeta, tales como la pérdida o sustracción, que podría posibilitar su uso por un tercero no autorizado, Una vez efectuada dicha comunicación, la entidad financiera bloqueará la tarjeta, de modo que los titulares y usuarios no asumirán el pago de las transacciones no autorizadas que se hayan realizado con posterioridad al mencionado bloqueo.

Jurisprudencia: El denunciante señaló que bloqueó su tarjeta de crédito el 14.04.2012 a las 13:19:43 horas, pero la entidad financiera permitió que posteriormente a dicho bloqueo se efectuará un consumo por el importe de S/2,012.00. La comisión declaró infundada la denuncia,

en tanto quedó acreditado que el consumo cuestionado se realizó a las 11:11 horas, es decir, con anterioridad al bloqueo de la tarjeta de crédito"

Las operaciones realizadas por la banca móvil cuentan con medias de seguridad suficientes para asegurar que solo los titulares puedan realizar operaciones con ellas, ya que solo se requiere las claves que son de conocimiento exclusivo del denunciante.

Conforme a lo señalado, corresponde en cumplimiento al principio de presunción de veracidad, presumir la legalidad los printers que acrediten los correctos registros de las operaciones materia de denuncia.

Solicitan se consideren que las operaciones realizadas por banca móvil se realizaron de manera correcta y sin presentar anomalías en el proceso de transacción, por lo que corresponde declarar infundada la denuncia interpuesta.

5. RESOLUCIÓ FINAL

Resuelve lo siguiente:

- Declarar fundada la denuncia interpuesta por infracción a los artículos 18° y 19° del Código, toda vez que no quedó acreditado que el banco adoptó las medidas de seguridad pertinentes al permitir que se efectuaran 03 operaciones no reconocidas en la cuenta de ahorros del denunciante por el importe total de S/18,693.30.
- En calidad de medida correctiva el banco en un plazo no mayor de 15 d.h., tiene que devolver el monto de las tres operaciones no reconocidas, más los intereses legales correspondientes.
- Se le sanciona al banco con una multa de 4.25 UIT.
- Se le requiere al banco que en un plazo no mayor de 15 d.h., pague las costas del procedimiento S/36.00 al denunciante.
- Dispone la inscripción del banco en el Registro de Infracciones y Sanciones (en adelante RIF) de INDECOPI, una vez que la resolución quede firme en sede administrativa.

Bajo los siguientes fundamentos relevantes:

Sobre la presunta infracción al deber de idoneidad

El artículo 18° del Código establece que la idoneidad es la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe. El artículo 19° del Código establece que los proveedores son responsables por la calidad e idoneidad de sus productos y servicios que ofrecen en el mercado.

En aplicación a esta norma, los proveedores tienen el deber de entregar los productos y prestar los servicios al consumidor en las condiciones ofertadas o previsibles, atendiendo a la naturaleza de estos, la regulación sobre el particular se haya establecido y, en general, a la información brindada por el proveedor o puesta a disposición.

Sobre las operaciones no reconocidas

Parte del servicio prestado por el banco, implica la confianza que el consumidor deposita en los sistemas de seguridad con los que cuenta la institución financiera para la realización y aprobación de cualquier transacción comercial realizada a través de tarjetas de crédito o débito que afecte su patrimonio.

Por ello, se exige la implementación de mecanismos de seguridad para proteger las transacciones, evitando el uso indebido o fraudulento de las tarjetas de crédito o débito.

Del articulo 9 y 14 del Reglamento, se desprende que lo que se busca garantizar, es que en cualquiera de los escenarios en que se realice la operación, esta se haya efectuado en observancia de las medidas de seguridad correspondientes, por lo cual, se exige contar con sustento que acredite la autorización realizada por el cliente, se a través de una orden de pago, código o firma electrónica y/o virtual (clave secreta, clave dinámica, CVV, etc.).

Pudiendo realizarse operaciones con tarjeta presente o con tarjeta no presente. Conforme a lo establecido en el reglamento, para cargar válidamente los importes a las tarjetas de crédito o débito, deben acreditar que:

(i) En las operaciones realizada con "tarjeta no presente", hubo autorización del usuario a través de medios electrónicos y/o firmas electrónicas,
(ii) Operaciones con "tarjeta no presente", las órdenes de pago deben estar suscritas por el cliente para entenderse autorizado o el ingreso de la clave secreta, según corresponda.

Esto quiere decir, que ante el cuestionamiento de un consumidor, la entidad financiera debe estar en la posibilidad de acreditar de manera fehaciente que la operación cargada ha sido autorizada por el cliente.

Sobre las operaciones con transferencias de fondos a terceros

En efecto para este tipo de operaciones de SBS y AFP ha emitido la Circular N°G-140-2009 – Gestión de seguridad de la información (en adelante Circular), en el artículo 6° establece que para la transferencia de fondos a terceros por canales electrónicos se deben de contar con dos factores de autenticación, siendo que uno de ellos debe ser de generación o asignación dinámica – claves dinámicas- u otro factor de nivel de seguridad equivalente o superior a fin de autorizar dichas transferencias a través de la banca electrónica.

Por lo señalado, se deberá verificar si las operaciones cuestionadas realizadas a través de internet se efectuaron de acuerdo con los parámetros de seguridad implementados por el proveedor; esto es, con el ingreso de clave secreta de internet y la clave dinámica (token).

Por ello, para que la entidad financiera sea exonerada de responsabilidad, deberá presentar los medios probatorios que acrediten que las operaciones cuestionadas fueron efectuadas válidamente.

Sobre las operaciones de "pago efectivo" por los importes de S/5,900.00 y S/9,597.00

De conformidad con la normativa previamente desarrollada y lo expuesto por las partes, corresponde analizar los reportes de los sistemas de banco que permita acreditar: (i) el acceso a la aplicación del banco a través del ingreso de la contraseña del cliente, (ii) ingreso de la clave digital y el registro de las operaciones cuestionadas.

Respecto al reporte del acceso a la aplicación, el banco no ha cumplido con presentar medios probatorios que acrediten el acceso del denunciante al aplicativo, de forma previa a la realización de las operaciones cuestionadas.

Es importante que el banco acredite el ingreso a la aplicación por el consumidor, de manera previa a la realización de las operaciones cuestionadas, siendo que ello permitirá analizar la validez de las transacciones no reconocidas; sin embargo, ello no sucedió en el presente caso.

Sin perjuicio de lo expuesto, se analizan los posteriores filtros de seguridad.

Al respecto, para acreditar el ingreso de la clave digital para la autorización de ambas operaciones, el banco presentó impresiones de pantalla.

De la verificación de los medios probatorios adjuntados, se verifica la consignación de la glosa "SUCCESFULL", solo se aprecia coincidencia en la fecha respecto de la operación realizada el 24.06.2020 a la 01:43 por el importe de S/9,597.00; ya que en el caso de la operación realizada el 25.05.2020 a las 12:41 por el importe de S/5,900.00 figura una fecha que no coincide con la señalada en los estados de cuenta (24.05.2020), por lo que, no habría quedado acreditada a la validez de la transacción en cuestión.

Constituye obligación de las partes la presentación de medios probatorios que permitan acreditar su posición, siendo que estos deben contar con el detalle y la información necesaria que permitan su comprensión y análisis.

El banco no cumplió con presentar los reportes emitidos por su propio sistema, que den cuenta del momento del inicio de sesión a la aplicación los días 25 de mayo y 24 de junio de 2020, antes de las operaciones cuestionadas, y que estas se hayan realizado con las validaciones que correspondían. El banco pudo presentar, por ejemplo, el reporte detallado de inicio de sesión, generación de clave digital e ingreso de la misma en la plataforma para autorizar las transacciones cuestionadas. Cabe indicar que el banco tampoco ha cumplido con presentar medios probatorios que acrediten el registro de las operaciones a través de sus sistemas.

Atendiendo a la dinámica probatoria, consideran que encontrándose el banco en mejor posición para acreditar que no le era atribuible la infracción denunciada en su contra, le correspondía proporcionar toda la documentación e información necesaria a fin de eximirse de responsabilidad; sin embargo, ello no ocurrió.

Por lo que no ha quedado acreditado que el denunciado adoptó las medidas de seguridad pertinentes al permitir que se efectuaran dos operaciones no reconocidas con cargo a la cuenta de ahorros del denunciante por los importes de S/9,597.00 y S/5,900.00.

Sobre el Consumo por el importe de S/3,196.30

El banco presento tres impresiones de pantalla de sus sistemas para acreditar la validez de la operación cuestionada, señalando que la operación fue autorizada a través del ingreso de un código enviado como mensaje de texto al celular del denunciante, mientras que otra de las imágenes adjuntadas acreditaría el registro de la operación cuestionada, en el que se detallan elementos como el número de operación, número de tarjeta, código de autorización, monto de la operación, establecimiento comercial y el canal donde se realizó la operación.

Al respecto, de la revisión de los reportes, si bien en la imagen N° 5, se observan los datos descritos por la entidad bancaria, las imágenes N° 3 y 4 no acreditan el envió de la clave SMS sino tan solo la comunicación y registro de la realización de la operación cuestionada, por lo tanto, posterior a la transacción en cuestión.

No cumpliendo el banco con presentar los reportes emitidos por su propio sistema, que den cuenta del envío de la clave SMS al teléfono celular del denunciante, lo que resulta indispensable para analizar el ingreso satisfactorio de dicha clave.

Si bien el banco, en el escrito del 14.09.2021, señaló que la operación fue válidamente realizada a través del ingreso de datos como el número de tarjeta, el nombre del denunciante, fecha de vencimiento y el código CVV2, lo cierto es que en el presente caso no se ha acreditado el ingreso del código CVV2 al cual hace referencia.

No se ha verificado que el denunciante haya autorizado la operación, a través de algún elemento de seguridad como los descritos en el numeral 16 y 17 de la presente resolución, no ha quedado acreditado que el banco haya adoptado las medidas de seguridad pertinentes al permitir que se efectuara una operación no reconocida en la cuenta de ahorros del denunciante por el importe de S/3,196.30.

Por lo expuesto, acogiendo la recomendación efectuada en el informe final, se declara fundada la denuncia interpuesta por la infracción de los articulo 18 y 19 del Código, toda vez que no ha quedado acreditado que el proveedor denunciado adoptó las medidas de seguridad pertinentes al permitir que se efectuaran 03 operaciones no reconocidas en la cuenta de ahorros del denunciante por el importe de S/18,693.30.

Sobre las medidas correctivas

Ha quedado acreditada la infracción consistente en no acreditar la adopción de medidas de seguridad pertinentes al permitir que se efectuaran tres operaciones no reconocidas en la cuenta de ahorros del denunciante por el importe total de S/18,693.30.

A efetos de revertir la conducta infractora, corresponde ordenar al Banco, en calidad de medida correctiva que, en un plazo no mayor de 15 d.h., devuelva el importe de las tres operaciones S/18,693.30, en la cuenta de ahorros del denunciante, más los intereses legales correspondientes hasta la fecha de cumplimiento de la medida correctiva.

Sobre la graduación de la sanción

El artículo 112° del Código , establece que para determinar la gravedad de la infracción, se debe tomar en cuenta diversos criterios tales como: (i) beneficio ilícito esperado, (ii) probabilidad de detección de la infracción. (iii)daño resultante de la infracción, (iv) efectos que pudiese generar en el mercado, entre otros.

Bien ilícito, estaría referido al ahorro que representa el no haber adoptado los mecanismos para validar los cargos correspondientes.

No se cuenta con la información que permita cuantificar dicho beneficio o ahorro ilícito, sino que en el expediente tampoco obra documentación que permita establece un parámetro objetivo para dicho fin, razón por la cual, la graduación de la sanción se realizara a partir de los otros criterios previstos en el art. 112 del Código.

Efectos en el mercado, se afecta el mercado al existir una defraudación de las expectativas de los consumidores, quienes podrían verse perjudicados al efectuarse el cargo de las transacciones que no han realizado.

La sanción a imponer deberá guardar correspondencia, razonabilidad y proporcionalidad con la conducta infractora del denunciados y los efectos de esta, por lo que acogen la recomendación del informe final de sancionar al banco con una multa de 4,25 UIT.

Sobre las costas y costos, se deberá pagar al denunciante las costas por el monto de S/36.00 en u plazo de 15 d.h. de notificado.

Sobre la inscripción en el registro de infracciones y sanciones, los proveedores sancionados con resolución firme quedan automáticamente registrado por el lapso de 04 años.

6. RECURSO DE APELACIÓN

Solicita se declare fundado el recurso interpuesto, se deje sin efecto la multa interpuesta, medidas correctivas, pago de costas y costos, así como la inscripción en el Registro de Infracciones y Sanciones. Se declare la nulidad de la resolución de primera instancia o en su defecto se revoque , en virtud de lo siguientes:

Respecto de los consumos de S/5,900.00 y S/9,597.00

Se adjuntan printers, que acreditan el ingreso a la banca móvil, para la realización de los consumos y correcto registro de las operaciones.

Con relación a las claves dinámicas, estas fueron remitidas al cliente al medio que predeterminó. En el presente caso afilió su número de teléfono el 13.08.2019, posteriormente el 09.04.2020 afilia el correo.

Evidenciándose que desde agosto de 2019, el denunciante tenía afiliado su correo y celular como medios válidos para recibir claves digitales.

El 27.05.2020 (posterior al consumo del 24.05.2020 por S/5,900.00) a horas 13:18, el cliente desafilia el correo y su número; sin embargo, lo vuelve a afiliar a las 15:35 horas, adjuntando printers de ello.

De los medios probatorios adjuntados, se desprende que al momento de la realización en mayo y junio el denunciante tenía afiliado su teléfono y correo, como medio valido para recibir la clave digital.

Al no existir variación del medio predeterminado para la recepción de la clave digital, siendo que fueron enviada al cliente al medio que eligió (y que no es materia de cuestionamiento), se aprueba el correcto envió de estas. Asimismo el correo y número telefónico consignado en el escrito de denuncia coinciden con los registrados en el sistema del banco.

Habiendo quedado acreditado el ingreso a la banca digital en mayo y junio de 2020, en su sistema denominado splunk, se acredita el envío e ingreso exitoso de la clave digital, adjuntan printers.

De los medios probatorios se aprecia la consignación de la glosa SUCCESFULL, que se genera cuando existe un correcto registro y validación de claves en el sistema, quedando acreditado la validez de las transacciones efectuadas en mayo y junio de 2020.

El denunciante el 27.05.2020 tenía afiliado un ID a su cuenta corriente al servicio de banca móvil, que luego fue modificado hasta el 08.07.2020, dicho ID coinciden con las pantallas splunk de las operaciones adjuntas precedentemente.

En ese sentido, con los medios probatorios presentados se aprecia que ha quedado acreditado que: (i) existió un correcto ingreso a la banca móvil en mayo y junio de 2020, (ii) las operaciones fueron válidamente

cargadas y registradas pues se confirmó y validó la operación (en tanto se ingresaron las claves remitidas al denunciante).

En el numeral 34 de la resolución se señala que la operación realizada el 25.05.2022 por el importe de S/5,900.00 figura una fecha que no coincide con la señalada en los estados de cuenta. La comisión señala que debido a que en el estado de cuenta no coincide la fecha con las pantallas splunk (por diferencia de un día) respecto a la operación por S/5,900.00, no queda acreditado la validez de la operación; sin embargo, cabe indicar que el desface se debe al registro de la operación en el sistema, que nada tiene que ver con la realización y validez de la operación.

En el presente caso se ha cumplido con presentar todos los medios probatorios que sustentan que la operación realizada el 25.05.20202 es la misma que la cargada el 24.05.2020.

el denunciante no ha señalado que se le cargó una operación el 24.05.2020 y otra el 25.05.2020 por el importe de S/5,900.00, así como tampoco ha manifestado su oposición respecto a que se trataría de distintas operaciones (o que se trataría de un doble cargo).

En ese sentido, en aplicación del principio de presunción de veracidad, solicitamos se considere y valores los argumentos respecto a la operación del 25.05.2020 es la misma que la del 24.05.2020.

Respecto a las operaciones por S/3,196.00

El mencionado consumo ha sido realizado siguiendo el circuito operativo normal previsto para este tipo de operaciones, de acuerdo a lo siguiente:

1. Establecimiento comercial (página web) ordena el cargo por el monto del consumo a la TC.
2. Visa procesa el cargo.
3. El cargo se registra en la TC operada por el banco.

Las transacciones efectuadas con una tarjeta de crédito a través de internet requieren el numero de la tarjeta, el nombre del denunciante, fecha de vencimiento, código CVV2 (que se encuentra al reverso de la tarjeta).

En el presente caso la transacción cuestionada por la denunciante se registró con total normalidad en sus sistemas, puesto que se efectuó con el ingreso de los datos necesarios y exigidos por la SBS, para luego ser procesados por Visa exitosamente generándose el código de autorización.

Adjuntan la impresión de pantalla del registro de consumo en sus sistemas de manera exitosa, en la cual se observa el código de autorización generado, así como el monto consumido y el numero de la tarjeta utilizada.

Contrariamente a lo señalado en el numeral 46 de la resolución materia de apelación, la impresión de pantalla adjunta acredita el ingreso del código CVV, toda vez que se aprecia el código TRACE (código de autorización) que únicamente es generada al ingresar el código CVV de manera valida.

De acuerdo con las impresiones de pantalla remitido por la empresa procesadora Visa, se aprecian datos como el envío del OTP por mensaje de texto (así como la correcta autenticación del ingreso de la clave).

El Banco, al efectuarse el primer consumo procedió con alertar al cliente, informándole a través de un mensaje de texto de la compra realizada en un establecimiento comercial, dicho mensaje fue recibido al número de teléfono del cliente.

Es así que en el presente caso, es posible concluir que para la operación se concrete válidamente tuvo que contar con todas las medidas de seguridad, las cuales han sido desarrolladas de manera precedente.

Por lo tanto, solicitamos tener el presente el artículo 1.7 del artículo V y el artículo 51 del TUO de la LPAG, que hablan del principio de presunción de veracidad. Correspondiendo en cumplimiento del mencionado principio, presumir la legalidad de las impresiones de pantalla que acreditan el correcto registro de las operaciones materia de denuncia.

Respecto a la sanción impuesta

Respecto de la sanción impuesta por 4,25 UIT, aún en el supuesto negado que el banco mereciera ser sancionado, se puede advertir que aún en ese supuesto no se ha realizado un análisis adecuado sobre la graduación de la multa, vulnerando el principio de razonabilidad. A través del mencionado principio se busca que el administrado puede anticiparse con mejor grado de aproximación en las decisiones administrativas.

En el presenta caso se ha graduado la sanción tomando en cuenta el ahorro de no haber adoptado los mecanismos para validad los cargos. Sin embargo, no se ha cumplido con indicar cual sería el daño generado, limitándose únicamente a indicar que el daño está asociado a la afectación del patrimonio y vulnerando las expectativas del consumidor.

No pudiendo tener la sanción impuesta como fundamento hechos subjetivos como los indicado. Para gravar la sanción, se utilizó como fundamento que la sanción aplicable tenga un efecto real disuasivo, sin embargo, dicha consideración no le otorga la posibilidad de sancionar sin el debido sustento y motivación conforme a lo dispuesto por la normativa aplicable.

concluyen que de ningún modo puede imponerse multas de manera arbitraria con la presente, en la que no existen criterios factico que respalden la misma. Existiendo elementos suficientes para demostrar que la multa no debió imponerse.

Mediante Resolución N°6 se concede el recurso de apelación, y mediante el proveído N°1, la sala especializada en protección al Consumidor, le otorga un plazo de (5) d.h. al denunciante para que haga conocer sus argumentos respecto del recurso presentado.

7. INFORMACIÓN COMPLEMENTARIA A LA APELACIOÓN

El banco adjunta las siguiente información complementaria:

Pantallas correspondiente al detalle de transacción por la operación de fecha 25.06.2021 por el monto de S/5,900.00:

Si bien se registra como fecha de proceso el 25.05.2022, esta fue realizada con fecha real el 24.05.2020 conforme a la captura pantalla que adjunta.

Para el presente caso la operación se ubicó con ID, aparece lo siguiente: Login Satisfactorio a las 12:30 am con envío otp a Huawei p9 lite.

A las 12:30 pm se realizó un envío exitosos de clave digital vía SMS para autorizar un login a la aplicación (account: SEL). Se validó correctamente la clave digital enviada en el registro anterior (account: SEL).

A las 12:41:12 pm se realizó un envío exitoso de clave digital vía SMS para autorizar la transacción (account: SELSIGNING).

Se validó correctamente la clave digital enviada previamente para autorizar la transacción (account: SELSIGNING).

Pantallas correspondiente al detalle de transacción por la operación de fecha 24.06.2020 por el monto de S/9,597.00:

La operación se ubicó con ID, Login Satisfactorio a las 01:38 am con envío otp a Huawei p9 lite.

A las 01:38 pm se realizó un envío exitosos de clave digital vía SMS para autorizar un login a la aplicación (account: SEL). Se validó correctamente la clave digital enviada en el registro anterior (account: SEL).

A las 12:43:52 pm se realizó un envío exitoso de clave digital vía SMS para autorizar la transacción (account: SELSIGNING).

Se validó correctamente la clave digital enviada previamente para autorizar la transacción (account: SELSIGNING).

Pantallas correspondiente al detalle de transacción por el monto de S/3,196.30:

Esta operación fue realizada a través de la página del establecimiento, asimismo se valida el envío de la clave la cual se observa en la pantalla VCAS:

1- Authentication Type: OTP-SMS (se envió mensaje)
2- Authentication Status: Y-Fully Authenticated (autenticado)
3- Account Number

Reiteran las pantallas SPLUNK, que acreditan el ingreso al aplicativo para realizar las operaciones. Reportes emitidos por su propio sistema, que den cuenta del envío de la clave SMS al teléfono del denunciante de las 03 operaciones.

La sala teniendo en cuenta el caso le realiza el requerimiento al denunciante y al banco para que en un plazo de 02 d.h. presenten los estados de movimientos de su cuenta de ahorros, correspondiente a los periodos entre los meses de noviembre de 2019 y abril de 2020.

8. PRESENTA INFORMACIÓN REQUERIDA – DENUNCIANTE

El denunciante cumple con adjuntar los movimientos de los meses de enero a abril de 2020, asimismo, menciona que el banco todavía no entrega la copia de los estados de cuenta de los meses de noviembre, diciembre de 2019 (adjunta correo solicitándolo) y el banco tienen 3 d.h. para la entrega.

9. PRESENTA INFORMACIÓN REQUERIDA – BANCO

El banco adjunta, los estados de cuenta de noviembre de 2019 a abril de 2020.

10. RESOLUCIÓN FINAL

Resuelve revocar la resolución recurrida, y en consecuencia se declara infundada por la presunta infracción de los articulo 18 y 19 del Código de Protección y defensa del consumidor, al haber quedado acreditado que el banco adoptó las medidas de seguridad respectivas en las tres operaciones de la cuenta de ahorros del denunciante, en tanto se verificó que fueron válidamente autorizadas. En consecuencia se deja sin efecto la resolución venida en grado en los extremos que ordena el cumplimiento de una medida correctiva, sanción por 4,25 UIT, pago de costas y costos, y la inscripción en el registro de infracción y sanciones.

Bajo los siguientes fundamentos relevantes:

Sobre el comportamiento habitual de consumo del cliente

De lo señalado por las partes en el procedimiento y de los medios probatorios, se tiene que las operaciones cuestionadas fueron cargadas a la cuenta de ahorros del denunciante el 24 de mayo y 25 de junio de 2020.

En este punto corresponde determinar si las operaciones cuestionadas coincidían con un patrón de consumo del cliente. Para ello, dichas transacciones deben ser evaluadas de acuerdo con el comportamiento habitual del denunciante.

De la revisión de los estados de movimiento, se verificó lo siguiente:

a) Noviembre de 2019, se registró un cargo total de S/340.00
b) Enero de 2020, cargo total por S/1,048.00
c) Febrero de 2020, cargo total por S/23,590.00
d) Marzo de 2020, cargo total por S/25,725.00
e) Abril de 2020, cargo total por S/1,387.36

Se verifica que en el estado de movimientos se registró el reporte total más elevado de consumos y/o operaciones en el mes de marzo de 2020, apreciándose un total de operaciones que ascienden a S/25,725.00.

Corresponde evaluar si el banco se encontraba obligado a alertar por uso irregular o sospechoso en la tarjeta de débito del denunciante, que implique el bloqueo preventivo de la misma por las operaciones no reconocidas, en atención a la comparación de estas con el comportamiento de consumo previo registrado por el titular.

Las dos operaciones discutidas del 25.05.2020 por S/9,096.30, sumándole importe el total de las operaciones realizadas hasta antes del 25.05.2020 por el monto de S/9,991.61, no superaba dicha suma el máximo total registrado por denunciante en el mes de marzo por S/25,725.00.

De la misma forma se tiene que la suma comprendida por el importe correspondiente a la operación objetada del 24.06.2020, ascendente a S/9,597.00 BAJO LA GLOSA DE PAGO EFECTIVO-BI, y el total de las operaciones realizadas hasta antes del 24.06.2020 en dicho mes, se obtiene como monto resultante el importe de S/10,842.00, el mismo que no superaba el máximo total registrado por el denunciante en el mes de marzo de 2020 por la suma de S/25,725.00, por lo que, se concluye que la transacción referida, también materia de denuncia, se encontraba dentro del patrón de consumo del consumidor (según su historial de operaciones).

En ese sentido, en mayoría advierte que ante la realización de las tres operaciones objetadas el banco no se encontraba obligado a generar alerta alguna por operación inusual o fraudulenta, en tanto tales transacciones se encontraban dentro del patrón de consumo evidenciado en el historio de operaciones del denunciante.

Sobre la validez de las operaciones cuestionadas por el denunciante

Sobre las operaciones "pago efectivo -bi" por los importes de S/5,900.00 y S/9,597.00

Previamente a analizar si las transacciones cuestionadas fueron o no autorizadas de acuerdo con las medidas de seguridad, es menester verificar si el denunciante accedió a la banca móvil del banco para efectos de realizar las operaciones registradas el 25.05.2020 y 24.06.2020.

Para ello, se aportó el reporte de su sistema denominado "Pantallas Splunk" el mismo que registral el ingreso a la banca móvil para cada una de las operaciones analizadas en este punto.

El reporte del banco denominado "Log de Consultas tarjetas virtuales", del cual se desprenden los códigos de identificación "ID CAMS" asignados al denunciante, y que son consignados al momento del registro de cada una de las operaciones materia de análisis, se adjunta imagen.

Del medio probatorio observado, se evidencia este guarda concordancia con el argumento del banco, referente al hecho de que hasta el 27.05.2020, el denunciante tenía afiliada a su cuenta el servicio de banca móvil bajo un código de identificación ID, y que, posteriormente, fue modificado por otro código ID, hasta el 08.07.2020, siendo estos códigos los mismos que coincidían con aquellos que se encontraban consignados en la pantallas SPLUNK que acreditaban el ingreso a la banca móvil para la realización de las operaciones en cuestión, visualizadas en el punto 41 de la presente resolución, acreditando así el correcto acceso del denunciante a dicho aplicativo para la realización de ambas transacciones.

De la revisión de tales medios probatorios se aprecian los siguientes datos: (i) fecha y hora: 24.05.2020 a las 12:30:10 horas (en referencia a la operación registrada el 25.05.2020, y 24.06.2020 a las 01:38:47 horas); (ii) código de identificación del denunciante (un código ID respectivamente para cada operación); (iii) nota "OTPVIASMSM.VERIFY-OTP-SUCCESFUL"-glosa que significa el correcto registro y validación de las claves en el sistema, conforme lo explicado por el banco en su apelación, (iv) glosas: account=SEL soucetype=log4 (que significaban login satisfactorio) los cuales son conducentes a acreditar el correcto acceso del denunciante a la banca móvil del banco.

Habiéndose determinado ello, correspondía dilucidar si, dicho acceso se realizó mediante el ingreso de la clave secreta y la clave digital correspondiente.

De acuerdo al banco ambas operaciones habían sido autorizadas mediante el ingreso de su clave secreta y la clave digital correspondiente, se denota que las dos operaciones materia de análisis fueron efectuadas mediante dos mecanismos de autenticación distintos (una clave secreta y una digital); y que la clave digital de cada operación había sido remitida al celular y correo afiliados por el denunciante (lo cual evidencia que este mecanismo constituida una clave dinámica). De acuerdo a las imágenes adjuntadas se permitió identificar el registro y aprobación de las claves secretas y las claves digitales empleadas con tal fin, adjunta imagen.

De la revisión de las imágenes adjuntadas, se advierte que los sistemas del banco registran dos fechas para hacer referencia a cada una de las operaciones discutidas, siendo estas las siguientes: fecha contable y fecha real. Así se desprende lo siguiente:

(i) La operación que en el estado de movimientos figura registrada el 25.05.2020 (fecha contable), ha sido realizada el 24.05.2020, identificando tal fecha como real.
(ii) La operación que en el estado de movimiento figura registrada el 24.06.2020 (fecha contable) ha sido realizada el mismo día- esto es el 24.06.2020, identificando tal fecha como real.

Se concluye que no existe una contradicción entre las fechas consignadas en los estados de movimiento de la cuenta del denunciante y los medios probatorios adoptados por el banco, sino que esta diferencia encuentra su sustento en el detalle presentado previamente.

Si bien en la resolución recurrida la operación ascendente a S/5,900.00 no había sido acreditada como valida, por cuanto existían reportes de diferían en cuanto a la fecha de registro, lo cierto es, que ello obedece a un desfase en el registro de operación en el sistema del banco, lo cual era independiente y no tenía incidencia en su realización y validez (efectuada en fecha real el 24.05.2020).

Quedando acreditado las fechas consignadas en tales reportes, no han sido ejecutadas indebidamente, es pertinente continuar con el análisis de los medios probatorios presentados y acotar que los mismos recogen la siguiente información:

(i) Fecha y hora de las operaciones (24.05.2020, a las 12:41:12 horas – fecha real – y 24.05.2020 a las 01:47:52 horas).
(ii) Fecha contable de la operación.
(iii) Código de identificación por cada operación.
(iv) Nota "OTPVIASMSM.VERIFY-OTP-SUCCESFUL" - glosa que significa el correcto registro y validación de las claves en el sistema, conforme lo explicado por el banco en su apelación.

El banco sustentó que el envío de las claves digitales para autorizar las transacciones controvertidas al celular del denunciante, vía SMS, se acreditaba bajo la consignación de la nota [OTPVIASMSM-VERIFY-OTP]_ID" en sus sistemas. Código que se encuentra registrado en los medios probatorios citados previamente, tal como ha sido corroborado en la presente resolución.

Conforme a los prints de pantalla de los sistemas del banco denominado "Status Clave Digital" que se adjuntan, se encontraba acreditado que el denunciante mantuvo afiliados al servicio de banca móvil a su correo y celular, al momento en que se llevaron a cabo las operaciones cuestionadas y analizadas en este punto, siendo tales datos los mismos que el denunciante consignó en su escrito de denuncia evidenciándose de esa forma que las claves que autorizaron las operaciones controvertidas fueron remitidas al denunciante, sin que este haya presentado documento alguno que desvirtúe tal afirmación.

La mayoría de este colegiado es de la opinión que de la valoración conjunta de los medios probatorios ofrecidos por el banco y la explicación brindada por del significado de cada uno de los términos contenidos en tales documentos, es posible colegir que las transacciones analizadas fueron procesadas en cumplimiento de los requisitos de validez exigidos para su ejecución, no existiendo en el procedimiento indicio alguno que controvierta la veracidad de los mismos.

En ese sentido, dado que quedó acreditado que los dos transacciones cuestionadas fueron aprobadas atendiendo a los requisitos de valides contemplados para ello.

Sobre el consumo por el importe de S/3,196.00

Con relación a las operaciones con tarjeta no presente, se solicita que la autorización se realice a través de medios electrónicos, como por ejemplo vía internet en el que requiere el ingreso de datos del medio de pago como fecha de vencimiento y código CVV2 o clave dinámica, con lo que se verifica la autorización del cliente.

Respecto de la operación en cuestión, el banco señaló que el referido consumo había sido realizado siguiendo el circuito operativo normal previsto para este tipo de operaciones.

El banco presento 03 prints de pantalla de sus sistemas para acreditar la validez de la operación cuestionada, tal y como se observa en las imágenes adjuntas.

De acuerdo con lo informado con el banco, la primera imagen daba cuenta del registro de la operación cuestionada, en el que se detallan elementos como el número de operación, número de tarjeta, código de autorización, monto de la operación, establecimiento comercial y canal donde se realizó la operación (por internet en tanto se consignó la glosa "on line").

De la revisión de la segunda imagen corresponde a Visa, se observa la glosa "Authentication Type: OTP-SMS que deja constancia del envío de la clave SMS, así como su correcta autentificación bajo la glosa: Authentication Status: Y-Fully Authenticated, ello, conforme fue explicado por el banco en su escrito de apelación.

La tercera imagen da cuenta de la comunicación del Banco (vía SMS al celular del denunciante), posterior a la realización del consumo objetado, mediante la cual se procedió a alertar al cliente sobre la compra realizada en el establecimiento.

Si bien en la resolución recurrida se concluyó que no se habría acreditado el ingreso del código CVV de la operación en cuestión, lo cierto es que, ante esta instancia el banco brindó una explicación sobre tal ingreso, al alegar que tal punto se encontraba acreditado bajo el código denominado "Trace" (constituyendo este el código de autorización) el mismo que era generado, únicamente, al ingresar el código CVV en forma valida.

La parte denunciante no ha presentado ningún argumento o medio de prueba que cuestione lo dicho (argumentos) o aportados (medios probatorios) por el banco, a fin de controvertir la veracidad de los mismos; por lo que, en aplicación del principio de presunción de veracidad, debe considerarse la validez de los medios probatorios aportados por el banco, los cuales fueron debidamente puestos al conocimiento del denunciante.

En consecuencia, dado que quedó acreditado que la operación analizada en este punto fue válidamente autorizada, mediante el debido cumplimiento de requisitos de validez contemplados para tal fin, es preciso exonerar de responsabilidad administrativa al banco, por la comisión de la conducta infractora atribuida en su contra.

De la consideraciones expuestas, corresponde revocar la resolución recurrida, en el extremo que declaró fundada la denuncia interpuesta, al haber quedado acreditado que el banco adopto las medidas de seguridad respectivas al procesar las tres operaciones en la cuenta de ahorros del denunciante, en tanto, se verificó que fueron válidamente autorizadas. Correspondiendo dejar sin efecto la medida correctiva ordenada, la sanción, costas y costos, inscripción en el RIS, por lo que, carece de objeto emitir un pronunciamiento sobre los alegatos destinados a cuestionar los referidos puntos.

II. Identificación y análisis de los principales problemas jurídicos del expediente.

1. Deber de idoneidad

El artículo 18° del Código de Protección y Defensa del Consumidor, establece que la idoneidad es la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, y el artículo 19° establece que los proveedores son responsables por la calidad e idoneidad de los productos que ofrecen en el mercado.

En el presente caso se denunció tres operaciones bancarias que no se reconocían (S/5,900.00, S/9,597.00 y S/3,196.30), el banco acreditó que las operaciones bancarias se efectuaron correctamente, de acuerdo al deber de idoneidad.

Correspondiendo la aplicación del mencionado deber analizar las mencionadas operaciones, de acuerdo a lo siguiente**:**

- **"Pago Efectivo" por los importes de S/5,900.00 (25.05.2020) y S/9,597.00 (24.06.2020)**

De acuerdo a su sistema denominado "Pantallas Splunk" se da cuenta del ingreso a la banca móvil para cada una de las operaciones y del reporte del banco denominado "Log de Consultas tarjetas virtuales", se evidencia los códigos de identificación "ID CAMS" asignados al denunciante, y que son consignados al momento del registro de cada una de las operaciones material de análisis.

Siendo las operaciones efectuadas mediante dos mecanismos de autenticación distintos (una clave secreta y una digital); y la clave digital respectiva a cada operación había sido remitida al celular y correo afiliados por el denunciante (lo cual evidencia que este mecanismo constituida una clave dinámica), las pruebas de la aplicación de los mencionados mecanismos fueron adjuntadas, al presente proceso, evidenciándose de las transacciones fueron realizadas validamente.

- **Consumo por el importe de S/3,196.30 del 25.05.2020**

Se solicita que la autorización se realice a través de medios electrónicos, como por ejemplo vía internet en el que requiere el ingreso de datos del medio de pago como fecha de vencimiento y código CVV2 o clave dinámica. El banco presento 03 prints de pantalla de sus sistemas, acreditando que la operación fue válidamente autorizada, mediante el debido cumplimiento de requisitos de validez contemplados para tal fin, cumpliendo con el deber de idoneidad el banco.

2. Comportamiento habitual

Sobre el comportamiento habitual de los consumidores, el artículo 2° del reglamento señala que esta referido al tipo de operaciones que usualmente realiza un consumidor con su tarjeta de crédito y/o débito, considerando diversos factores; como, por ejemplo, país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales se determinan a partir de la comparación de la información histórica de operaciones.

En el presente caso se analizaron las tres operaciones cuestionadas, de acuerdo al estado de movimientos desde los meses de noviembre de 2019 a abril de 2020, del mencionado período se aprecia que el consumo más elevado es en el mes de marzo de 2020 por el monto de S/25,725.00.

Pues teniendo en cuenta, las operaciones discutidas del 25.05.2020 (S/5,900.00 y S/3,196.30), y las operaciones realizadas hasta esa fecha, se tiene el monto resultante de S/9,991.61, el mismo que no superaba el máximo total de consumo registrado por denunciante en el mes de marzo por S/25,725.00.

En ese sentidos, en las tres operaciones objetadas, el banco no se encontraba obligado a generar alerta alguna por operación inusual o fraudulenta, en tanto tales transacciones se encontraban dentro del patrón de consumo evidenciado en el historio de operaciones del denunciante.

III. Posición fundamentada sobre los problemas jurídicos identificados.

1. Deber de idoneidad

Respecto del artículo 18° del Código de Protección y Defensa del Consumidor, el parámetro de idoneidad en el presente caso son los mecanismos de seguridad implementados por el banco para realizar operaciones (vía internet, presencial), en casos como este, en el que se cuestiona el servicio brindado, el banco es responsable de presentar los medios probatorios suficientes para desvirtuar el hecho denunciado y corroborar que autorizó válidamente la operación.

Correspondiendo en caso de vulneración del mencionado artículo 18° y 19°, que se verifique si las operaciones (a través de internet y físicas) se efectuaron de acuerdo a parámetros de seguridad mínimos, como es el ingreso de las claves que otorguen validez a dichas transacciones. Que de acuerdo a la Circular N°6-140-2009- Gestión de seguridad de la información (en adelante Circular)- en su artículo 6°, refiere que en transacciones electrónicas se requiere el ingreso de claves dinámicas (token, clave de coordenadas o clave SMS, entre otros) y claves secreta.

En el presente caso se denunció tres operaciones bancarias que no se reconocían (S/5,900.00, S/9,597.00 y S/3,196.30), el banco acreditó que las operaciones bancarias se efectuaron correctamente, de acuerdo al deber de idoneidad, de acuerdo a lo siguiente**:**

- **"Pago Efectivo" por los importes de S/5,900.00 (25.05.2020) y S/9,597.00 (24.06.2020)**

De acuerdo a su sistema denominado "Pantallas Splunk" se da cuenta del ingreso a la banca móvil para cada una de las operaciones y del reporte del banco denominado "Log de Consultas tarjetas virtuales", se evidencia los códigos de identificación "ID CAMS" asignados al denunciante, y que son consignados al momento del registro de cada una de las operaciones material de análisis.

Y se tiene que de la revisión de tales medios probatorios se aprecian los siguientes datos: (i) fecha y hora: 24.05.2020 a las 12:30:10 horas (en referencia a la operación registrada el 25.05.2020 , y 24.06.2020 a las 01:38:47 horas); (ii) código de identificación del denunciante (un código ID respectivamente para cada operación); (iii) nota "OTPVIASMSM.VERIFY-OTP-SUCCESFUL"-glosa que significa el correcto registro y validación de las claves en el sistema, conforme lo explicado por el banco en su apelación, (iv) glosas: account=SEL soucetype=log4 (que significaban login satisfactorio) los cuales son conducentes a acreditar el correcto acceso del denunciante a la banca móvil del banco.

Siendo las operaciones efectuadas mediante dos mecanismos de autenticación distintos (una clave secreta y una digital); y la clave digital respectiva a cada operación había sido remitida al celular y correo afiliados por el denunciante (lo cual evidencia que este mecanismo constituida una clave dinámica).

Y se advierte de la revisión de las imágenes adjuntadas, que los sistemas del banco registran dos fechas para hacer referencia a cada una de las operaciones discutidas, siendo estas las siguientes: fecha contable y fecha real. Así se desprende lo siguiente:

(iii) La operación que en el estado de movimientos figura registrada el 25.05.2020 por S/5,900.00 (fecha contable), ha sido realizada el 24.05.2020, identificando tal fecha como real.

(iv) La operación que en el estado de movimiento figura registrada el 24.06.2020 por S/9,597.00 (fecha contable) ha sido realizada el mismo día- esto es el 24.06.2020, identificando tal fecha como real.

Si bien en la operación por S/5,900.00, existen reportes de diferían en cuanto a la fecha de registro, ello se debe a un desfase en el registro de operación en el sistema del banco, lo cual era independiente y no tenía incidencia en su realización y validez (efectuada en fecha real el 24.05.2020).

De la valoración conjunta de los medios probatorios se colige que las transacciones analizadas fueron procesadas en cumplimiento de los requisitos de validez exigidos para su ejecución, toda vez que se ha acreditado el ingreso a la banca móvil y la introducción de las claves correspondientes.

- **Consumo por el importe de S/3,196.30 del 25.05.2020**

Con relación a las operaciones con tarjeta no presente, se solicita que la autorización se realice a través de medios electrónicos, como por ejemplo vía internet en el que requiere el ingreso de datos del medio de pago como fecha de vencimiento y código CVV2 o clave dinámica.

El banco presento 03 prints de pantalla de sus sistemas, en la primera imagen detalla el registro de la operación cuestionada, como el número de operación, número de tarjeta, código de autorización, monto de la operación, establecimiento comercial y canal donde se realizó la operación (por internet en tanto se consignó la glosa "on line").

En la segunda imagen se observa la glosa "Authentication Type: OTP-SMS que deja constancia del envío de la clave SMS, así como su correcta autentificación bajo la glosa: Authentication Status: Y-Fully Authenticated.

En la tercera imagen da cuenta de la comunicación del Banco (vía SMS al celular del denunciante), posterior a la realización del consumo objetado, mediante la cual se procedió a alertar al cliente sobre la compra realizada en el establecimiento.

Acreditando con las imágenes analizadas que la operación fue válidamente autorizada, mediante el debido cumplimiento de requisitos de validez contemplados para tal fin, cumpliendo con el deber de idoneidad el banco.

2. Comportamiento habitual

Sobre el comportamiento habitual de los consumidores, el artículo 2° del reglamento señala que esta referido al tipo de operaciones que usualmente realiza un consumidor con su tarjeta de crédito y/o débito, considerando diversos factores; como, por ejemplo, país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales se determinan a partir de la comparación de la información histórica de operaciones.

Por lo que, en aquellos casos como el presente, en que se cuestione que las operaciones de consumo no corresponden al comportamiento habitual, se requiere analizar si las operaciones de consumo coinciden con un patrón de consumo del cliente. Para ello, dichas transacciones deben ser evaluadas de acuerdo al histórico de consumo, través de los estados de cuenta.

En el presente caso se analizaron las tres operaciones cuestionadas, de acuerdo al estado de movimientos desde los meses de noviembre de 2019 a abril de 2020, del mencionado período se aprecia que el consumo más elevado es en el mes de marzo de 2020 por el monto de S/25,725.00.

Este monto en comparación con las operaciones del mes de mayo por S/5,900.00 y S/3,196.30 ; y en junio por S/9,597.00, no superaban el máximo de operaciones total registrados por el denunciante, entrando los mencionados montos dentro del comportamiento habitual de su consumo.

Pues teniendo en cuenta, las operaciones discutidas del 25.05.2020 (S/5,900.00 y S/3,196.30), y las operaciones realizadas hasta esa fecha, se tiene el monto resultante de S/9,991.61, el mismo que no superaba el máximo total de consumo registrado por denunciante en el mes de marzo por S/25,725.00.

De la misma forma se tiene que la suma comprendida por el importe correspondiente a la operación objetada del 24.06.2020, ascendente a S/9,597.00 y el total de las operaciones realizadas hasta antes de esa fecha, se obtiene como monto resultante el importe de S/10,842.00, el mismo que no superaba el máximo total registrado por el denunciante en el mes de marzo de 2020 por la suma de S/25,725.00, por lo que, se concluye que la transacción referida, también materia de denuncia, se encontraba dentro del patrón de consumo del consumidor (según su historial de operaciones).

En ese sentidos, en las tres operaciones objetadas, el banco no se encontraba obligado a generar alerta alguna por operación inusual o fraudulenta, en tanto tales transacciones se encontraban dentro del patrón de consumo evidenciado en el historio de operaciones del denunciante.

IV. Posición fundamentada sobre las resoluciones emitidas

RESOLUCIÓN DE PRIMERA INSTANCIA

Se analizarán los fundamentos relevantes por los cuales la primera instancia resuelve declarar fundada la denuncia:

Sobre las operaciones de "pago efectivo" por los importes de S/5,900.00 y S/9,597.00

- Correspondía analizar los reportes de los sistemas de banco que permita acreditar: (i) el acceso a la aplicación del banco a través del ingreso de la contraseña del cliente, (ii) ingreso de la clave digital y el registro de las operaciones cuestionadas.
- Respecto al reporte del acceso a la aplicación, el banco no ha cumplido con presentar medios probatorios que acrediten el acceso del denunciante al aplicativo, de forma previa a la realización de las operaciones cuestionadas.
- Pese a ello, se analizan los posteriores filtros de seguridad del banco, señalan que de los medios probatorios adjuntados, se verifica la consignación de la glosa "SUCCESFULL", y solo se aprecia coincidencia en la fecha respecto de la operación realizada el 24.06.2020 a la 01:43 por el importe de S/9,597.00; ya que en el caso de la operación realizada el 25.05.2020 a las 12:41 por el importe de S/5,900.00 figura una fecha (24.05.2020) que no coincide con la señalada en los estados de cuenta, por lo que, el banco, no habría quedado acreditada a la validez de la transacción en cuestión.
- Por lo que consideran que no ha quedado acreditado que el denunciado adoptó las medidas de seguridad pertinentes al permitir que se efectuaran dos operaciones no reconocidas con cargo a la cuenta de ahorros del denunciante por los importes de S/9,597.00 y S/5,900.00.

Respecto a la conclusión del análisis medios probatorios tenemos discordancia, toda vez, que en primera instancia se refiere que el banco no ha cumplido con presentar medios probatorios que acrediten el acceso del denunciante al aplicativo, de forma previa a la realización de las operaciones cuestionadas, no teniéndose en cuenta que el banco adjunto el reporte de su sistema denominado "Pantallas Splunk" el mismo que acredita el ingreso a la banca móvil para cada una de las operaciones analizadas.

Además que de los medios probatorios se evidencia que hasta el 27.05.2020, el denunciante tenía afiliado a su cuenta el servicio de banca móvil bajo un código de identificación ID que son los mismos que coincidían con aquellos que se encontraban consignados en la pantallas SPLUNK, que acreditan el ingreso a la banca móvil para la realización de las operaciones en cuestión, lo que evidencia el acceso del denunciante a dicho aplicativo para la realización de ambas transacciones.

Y además se aprecian los siguientes datos: (i) fecha y hora, (ii) código de identificación del denunciante (un código ID respectivamente para cada operación); (iii) nota "OTPVIASMSM.VERIFY-OTP-SUCCESFUL"-glosa que significa el correcto registro y validación de las claves en el sistema, conforme lo explicado por el banco en su apelación, (iv) glosas: account=SEL soucetype=log4 (que significaban login satisfactorio) los cuales acreditan el correcto acceso del denunciante a la banca móvil del banco.

Posteriormente señala que de los medios probatorios adjuntados, se verifica la consignación de la glosa "SUCCESFULL", y solo se aprecia coincidencia en la fecha respecto de la operación realizada el 24.06.2020 a la 01:43 por el importe de S/9,597.00; ya que en el caso de la operación realizada el 25.05.2020 a las 12:41 por el importe de S/5,900.00 figura una fecha (24.05.2020) que no coincide con la señalada en los estados de cuenta, por lo que, el banco, no habría quedado acreditada a la validez de la transacción en cuestión.

Sin tener en cuenta el reporte denominado "Log de Consultas tarjetas virtuales", del cual se desprenden los códigos de identificación "ID CAMS" asignados al denunciante, y que son consignados al momento del registro de cada una de las operaciones materia de análisis. Ni tampoco se observó que las operaciones materia de análisis fueron efectuadas mediante dos mecanismos de autenticación distintos (una clave secreta y una digital); es más la clave digital respectiva a cada operación había sido remitida al celular y correo afiliados por el denunciante (lo cual evidencia que este mecanismo constituida una clave dinámica).

Siendo que las operaciones materia de análisis fueron efectuadas de acuerdo con los requisitos de validez invocados por el propio denunciado para validad la comprar como es el correo y celular que el mismo afilió.

Tampoco se tuvo en cuenta que los sistemas del banco registran dos fechas para hacer referencia a cada una de las operaciones discutidas (fecha contable y fecha real) como se detalla a continuación:

(i) La operación que figura registrada el 25.05.2020 (fecha contable), ha sido realizada el 24.05.2020, identificando tal fecha como real.
(ii) La operación que figura registrada el 24.06.2020 (fecha contable) ha sido realizada el mismo día- esto es el 24.06.2020, identificando tal fecha como real.

No existiendo una contradicción en la fecha de las operaciones y las registradas, en relación operación ascendente a S/5,900.00 que según la primera instancia no había sido acreditada como valida, por cuanto existían reportes de diferían en cuanto a la fecha de registro, la mencionada diferencia de fechas se debe a un desfase en el registro de operación en el sistema del banco, lo cual era independiente y no tenía incidencia en su realización y validez (efectuada en fecha real el 24.05.2020).

Es más del análisis de los medios probatorios, se evidencia que registra como Fecha y hora de las operaciones (24.05.2020, a las 12:41:12 horas – fecha real – y 24.05.2020 a las 01:47:52 horas), fecha contable de la operación, código de identificación por cada operación, nota "OTPVIASMSM.VERIFY-OTP-SUCCESFUL" - que significa el correcto registro y validación de las claves en el sistema.

Además el banco sustentó el envío de las claves digitales para autorizar las transacciones al celular del denunciante, vía SMS, se acreditaba bajo la consignación de la nota [OTPVIASMSM-VERIFY-OTP]_ID" en sus sistemas. Código que se encuentra registrado en los medios probatorios citados previamente, tal como ha sido corroborado en la presente resolución.

Sobre el Consumo por el importe de S/3,196.30

- De las imágenes adjuntadas, el banco señala que se observa que la operación cuestionada fue autorizada a través del ingreso de un código enviado como mensaje de texto al celular del denunciante, mientras que otra de las imágenes adjuntadas acreditaría el registro de la operación cuestionada, en el que se detallan elementos como el número de operación, número de tarjeta, código de autorización, monto de la operación, establecimiento comercial y el canal donde se realizó la operación.
- De la revisión de los reportes, si bien en la imagen N°5, se observan los datos descritos por la entidad bancaria, las imágenes N°3 y 4 no acreditan el envió de la clave SMS sino tan solo la comunicación y registro de la realización de la operación cuestionada, por lo tanto, posterior a la transacción en cuestión.
- No cumpliendo el banco, con presentar los reportes emitidos por su propio sistema, que den cuenta del envío de la clave SMS al teléfono celular del denunciante, lo que resulta indispensable para analizar el ingreso satisfactorio de dicha clave.
- Cabe reiterar que, si bien el banco, en su escrito del 14.09.2021, señaló que la operación del consumo materia de cuestionamiento fue válidamente realizada a través del ingrese de datos como el número de tarjeta, el nombre del denunciante, fecha de vencimiento y el código CVV2, sin embargo, caso no se ha acreditado el ingreso del código CVV2 al cual hace referencia.
- No verificándose que el denunciante haya autorizado la operación, a través de algún elemento de seguridad como los descritos en el numeral.

En la presente operación en discusión también tenemos discordancia respecto a la conclusión del análisis medios probatorios, toda vez, que la primera instancias refiere que de la revisión de los reportes, si bien en la imagen N°5, se observan los datos descritos por la entidad bancaria (número de operación y de tarjeta, código de autorización, monto de la operación, establecimiento comercial y el canal donde se realizó la operación), las imágenes N°3 y 4 no acreditan el envió de la clave SMS sino tan solo la comunicación y registro de la realización de la operación cuestionada, por lo tanto, posterior a la transacción en cuestión. No cumpliéndose con adjuntar los reportes emitidos que respalden el envío de la clave SMS al teléfono celular del denunciante.

Sin tener en cuenta, las tres imágenes adjuntadas por el banco, de las cuales la segunda imagen de Visa, se observa la glosa "Authentication Type: OTP-SMS que deja constancia del envío de la clave SMS, así como su correcta autentificación bajo la glosa: Authentication Status: Y-Fully Authenticated, lo cual fue explicado por el banco en su escrito de apelación.

Tampoco se tuvo en cuenta la tercera imagen, que acredita la comunicación del Banco (vía sms al celular del denunciante), posterior a la realización del consumo objetado, mediante la cual se procedió a alertar al cliente sobre la compra realizada en el establecimiento.

Y respecto a lo señalado en primer instancia que no se verificó que en la operación en cuestionamiento se haya acreditado el ingreso del código CVV2 al cual hace referencia el banco, esta instancia no tuvo en cuenta lo señalado por el banco respecto a que se quedaba acreditado con el código denominado "Trace" (constituyendo este el código de autorización) el cual se genera, únicamente, al ingresar el código CVV en forma valida, el correcto registro de la transacción materia de análisis.

Por lo argumentos antes mencionados, se evidencia que en primera instancia no se cumplió con analizar correctamente los medios probatorios aportados en el procedimiento, correspondiendo de acuerdo al análisis realizado declarar la denuncia interpuesta, toda vez, que el banco cumplió con comprobar que las operaciones cuestionadas se efectuaron de acuerdo a los mecanismos de seguridad implementados por el banco, siendo por ello, operaciones validas.

RESOLUCIÓN DE SEGUNDA INSTANCIA

Estamos de acuerdo con la segunda instancia al declarar infundada la denuncia interpuesta, bajos los siguientes fundamentos:

Sobre las operaciones de "pago efectivo" por los importes de S/5,900.00 y S/9,597.00

Respecto a los mencionados importes la segunda instancia, cumplió con analizar el reporte del sistema del banco denominado "Pantallas Splunk" que acredita el ingreso a la banca móvil para cada una de las operaciones analizadas.

Además analizó, los medios probatorios conjuntamente, dándose cuenta que el denunciante tenía afiliado a su cuenta el servicio de banca móvil bajo un código de identificación ID que es el mismo consignado en la pantallas SPLUNK, acreditando el ingreso a la banca móvil para la realización de las operaciones en cuestión.

Del análisis realizado también observó los siguientes datos: (i) fecha y hora, (ii) código de identificación del denunciante (un código ID respectivamente para cada operación); (iii) nota "OTPVIASMSM.VERIFY-OTP-SUCCESFUL"-glosa que significa el correcto registro y validación de las claves en el sistema, conforme lo explicado por el banco en su apelación, (iv) glosas: account=SEL soucetype=log4 (que significaban login satisfactorio) acreditando el correcto acceso del denunciante a la banca móvil del banco.

Y verificó el reporte denominado "Log de Consultas tarjetas virtuales", del cual evidencian los códigos de identificación "ID CAMS" asignados al denunciante, y que son consignados al momento del registro de cada una de las operaciones materia de análisis. También tuvo en cuenta los dos mecanismos de autenticación distintos (una clave secreta y una digital); de los cuales evidenció que habían sido remitidos al celular y correo afiliados por el denunciante

Además de las dos fechas registradas para cada una de las operaciones discutidas (fecha contable y fecha real) como se detalla a continuación:

(iii) La operación que figura registrada el 25.05.2020 (fecha contable), ha sido realizada el 24.05.2020, identificando tal fecha como real.
(iv) La operación que figura registrada el 24.06.2020 (fecha contable) ha sido realizada el mismo día- esto es el 24.06.2020, identificando tal fecha como real.

Señalando que respecto a la operación ascendente a S/5,900.00 la mencionada diferencia de fechas se debe a un desfase en el registro de operación en el sistema del banco, lo cual era independiente y no tenía incidencia en su realización y validez (efectuada en fecha real el 24.05.2020).

Y que en cada una de las operaciones cuestionadas cuenta con un código de identificación con la nota "OTPVIASMSM.VERIFY-OTP-SUCCESFUL" - que significa el correcto registro y validación de las claves en el sistema.

Por último, verificó el envío de las claves digitales para autorizar las transacciones al celular del denunciante, vía SMS, a través de la consignación de la nota [OTPVIASMSM-VERIFY-OTP]_ID" en el sistema del banco.

Cumpliendo la segunda instancia con analizar conjuntamente todos los medios probatorios aportados al procedimiento y el significado de estos.

Sobre el Consumo por el importe de S/3,196.30

La segunda instancia cumplió con analizar las imágenes adjuntadas por el banco, en la imagen de Visa, observa la glosa "Authentication Type: OTP-SMS que deja constancia del envío de la clave SMS, así como su correcta autentificación bajo la glosa: Authentication Status: Y-Fully Authenticated, lo cual fue explicado por el banco en su escrito de apelación.

Además analizó la tercera imagen, que acredita la comunicación del Banco (vía sms al celular del denunciante), posterior a la realización del consumo objetado, alertando al cliente sobre la compra realizada en el establecimiento.

Tuvo en cuenta lo señalado por el banco respecto a que quedaba acreditado con el código denominado "Trace" (constituyendo este el código de autorización) el cual se genera, únicamente, al ingresar el código CVV en forma valida, el correcto registro de la transacción materia de análisis.

De lo señalado se evidencia que cumplió con analizar la segunda instancia los medios probatorios señalados, a fin de comprobar si la operación cuestionada se había realizado válidamente, teniendo en cuenta también los argumentos señalados por las partes.

Por lo que, estamos de acuerdo con la segunda instancia al declarar infundada la denuncia interpuesta, pues cumplió con analizar conjuntamente todos los medios probatorios aportados al procedimiento y el significado de estos, determinando que se ingresó a la banca móvil de la revisión de las imágenes del sistema denominado Splunk, observó los dos mecanismos de autenticación distintos (una clave secreta y una digital); de los cuales evidenció que habían sido remitidos al celular y correo afiliados por el denunciante. Por último, verificó el envío de las claves digitales para autorizar las transacciones al celular del denunciante, vía SMS, de lo cual advirtió que las operaciones fueron debitadas correctamente y de acuerdo a su sistema de seguridad implementado.

V. Conclusiones.

1. El artículo 18° del Código de Protección y Defensa del Consumidor, establece que la idoneidad es la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, y el artículo 19° establece que los proveedores son responsables por la calidad e idoneidad de los productos que ofrecen en el mercado.

2. Siendo el parámetro de idoneidad en el presente caso los mecanismos de seguridad implementados por el banco para realizar operaciones (vía internet, presencial), en casos como este, en el que se cuestiona el servicio brindado, el banco es responsable de presentar los medios probatorios suficientes para desvirtuar el hecho denunciado y corroborar que autorizó válidamente la operación.

3. Respecto a lo resuelto en primera instancia tenemos discordancia, toda vez, que en primera instancia se refiere que el banco no ha cumplido con presentar medios probatorios que acrediten el acceso del denunciante al aplicativo, de forma previa a la realización de las operaciones cuestionadas, no teniéndose en cuenta que el banco adjunto el reporte de su sistema denominado "Pantallas Splunk" el mismo que acredita el ingreso a la banca móvil, el envío del mensaje y correo, y las claves correspondiente para cada una de las operaciones analizadas.

4. Estamos de acuerdo con la segunda instancia al declarar infundada la denuncia interpuesta, pues cumplió con analizar conjuntamente todos los medios probatorios aportados al procedimiento y el significado de estos, determinando que se ingresó a la banca móvil de la revisión de las imágenes del sistema denominado Splunk, observó los dos mecanismos de autenticación distintos (una clave secreta y una digital); de los cuales evidenció que habían sido remitidos al celular y correo afiliados por el denunciante. Por último, verificó el envío de las claves digitales para autorizar las transacciones al celular del denunciante, vía SMS, de lo cual advirtió que las operaciones fueron debitadas correctamente y de acuerdo a su sistema de seguridad implementado.

VI. Bibliografía.

1. Decreto Supremo N°004-2019-JUS, Texto Único ordenado de la ley N°27444-Ley de procedimiento Administrativo general, promulgado el 25 de enero de 2019.
2. Ley 29571, Código de protección y defensa del consumidor, publicado el 2 de setiembre de 2020 y modificado por Decreto Legislativo N°1308.
3. Resolución SBS N°6523-2013, Reglamento de tarjetas de crédito y débito, publicada el 02 de noviembre de 2013 y vigente desde el 01 de abril de 2014.

VII. Anexos

Resolución de segunda instancia

PROCEDENCIA	:	COMISIÓN DE PROTECCIÓN AL CONSUMIDOR – SEDE LIMA SUR N°1
PROCEDIMIENTO	:	DE PARTE
DENUNCIANTE	:	[redacted]
DENUNCIADO	:	[redacted]
MATERIAS	:	DEBER DE IDONEIDAD SERVICIOS FINANCIEROS
ACTIVIDAD	:	OTROS TIPOS DE INTERMEDIACIÓN MONETARIA

SUMILLA:** Se revoca la resolución recurrida, en el extremo que declaró fundada la denuncia interpuesta por el señor J[redacted] contra S[redacted] n consecuencia, se declara infundada la misma, por presunta infracción de los artículos 18° y 19° de la Ley 29571, Código de Protección y Defensa del Consumidor, al haber quedado acreditado que la entidad bancaria adoptó las medidas de seguridad respectivas, a fin de procesar tres (3) operaciones ascendentes a S/ 3 196,30, S/ 5 900,00 y S/ 9 597,00, con cargo a la Cuenta de Ahorros 679-*500 del denunciante, en tanto se verificó que fueron válidamente autorizadas.*

En consecuencia, se deja sin efecto la resolución venida en grado, en los extremos que ordenó a S[redacted] cumplimiento de una medida correctiva, le impuso una sanción de 4,25 UIT, lo condenó al pago de costas y costos del procedimiento, y dispuso su inscripción en el Registro de Infracciones y Sanciones del Indecopi.

Lima, 20 de junio de 2022

ANTECEDENTES

1. El 21 de febrero de 2021, el señor J[redacted] adelante, el señor Yataco) denunció a S[redacted] elante, el Banco), por presuntas infracciones de la Ley 29571, Código de Protección y Defensa del Consumidor (en adelante, el Código), atendiendo a las siguientes consideraciones:

   (i) Era cliente del Banco a razón de la contratación de la Cuenta de Ahorros 679-****500, vinculada a la Tarjeta de Débito 5118-****-****-2432 originalmente, y luego a la Tarjeta de Débito 4285-****-****-4502;

   (ii) el 24 de mayo de 2020, advirtió que se efectuaron dos (2) operaciones no reconocidas con cargo a su cuenta de ahorros, de acuerdo al siguiente detalle:

Tarjetas de Débito N° 5118-****-****-2432			
HORA	**FECHA**	**CONCEPTO**	**IMPORTE**
12:41	25/05/2020	Pago efectivo-bi	S/ 5 900,00
Tarjetas de Débito N° 4285-**-****-4502**			
01:43	24/05/2020	Pago efectivo-bi	S/ 9 597,00
TOTAL		**S/ 15 497,00**	

(iii) posterior a ello, se comunicó con el Banco a fin de solicitar una explicación sobre lo sucedido, ante lo cual la entidad financiera procedió con anular y bloquear la Tarjeta de Débito 5118-****-****- 2432 con el Código 843586;

(iv) el 25 de mayo de 2020, se presentó en las oficinas del Banco a fin de presentar el Reclamo 2020067952, el mismo que sería atendido en un plazo de treinta (30) días, oportunidad en la cual se le precisó que, si deseaba realizar alguna operación con cargo a su cuenta, debía sacar una nueva tarjeta de débito –concepto por el cual pagó el importe de S/ 18,00-;

(v) mediante correo electrónico del 12 de junio de 2020, el Banco le envió un cuestionario de tres (3) preguntas, las mismas que respondió mediante una comunicación hecha vía Banca Telefónica en fecha 17 de junio del mismo año;

(vi) las preguntas detalladas en dicho cuestionario fueron las siguientes: ¿en algún momento (fechas cercanas a las operaciones no reconocidas) perdió el control de su celular o chip, indicar fecha y hora aproximada?; ¿cambió de operador?; ¿ha recibido alguna llamada solicitando la clave digital del SBP o información de sus cuentas?, interrogantes que fueron contestadas en forma negativa por su parte;

(vii) después de contestado el cuestionario, la operadora del Banco le confirmó que su reclamo había sido registrado y que el plazo de atención del mismo era de treinta (30) días para efectos de dar solución al fraude del cual habría sido víctima;

(viii) el 24 de junio de 2020, intentó sin éxito efectuar una operación mediante el aplicativo del Banco, por lo que, de manera inmediata, efectuó el cambio de su usuario y de su clave, advirtiendo, posteriormente a tal suceso, que se había realizada la siguiente operación no reconocida:

Tarjetas de Débito N° 5118-****-****-2432			
HORA	FECHA	CONCEPTO	IMPORTE
12:35	25/05/2020	Débito compras	S/ 3 196,30

(ix) ante ello, se apersonó a una de las agencias del Banco y mediante la Banca Telefónica efectuó el bloqueo de su tarjeta de débito y cuenta de ahorros asociada, registrándose tal hecho mediante el Código 383817. Además, interpuso el Reclamo 2020084006; y,

(x) de las denuncias policiales que efectuó, se desprendía que cuestionaba el registro de tres operaciones inusuales las cuales desconocía, tomando conocimiento de las mismas al momento de verificar sus movimientos a través de su aplicativo de banca móvil.

2. Asimismo, el señor [redacted] solicitó como medida correctiva, que el Banco cumpla con devolver el importe total de S/ 18 693,30, correspondiente a las operaciones no reconocidas. Adicionalmente, requirió condenar al denunciado al pago de las costas y costos del procedimiento.

3. Mediante Resolución 1 del 29 de marzo de 2021, la Secretaría Técnica de la Comisión de Protección al Consumidor – Sede Lima Sur N° 1 (en adelante, la Secretaría Técnica) emitió, entre otras cosas, el siguiente pronunciamiento:

> *"**PRIMERO:** admitir a trámite la denuncia del 22 de febrero de 2021 presentada por el señor J[redacted] contra S[redacted]A por presunta infracción a los artículos 18° y 19° de la Ley N° 29571, Código de Protección y Defensa del Consumidor, en tanto la entidad bancaria no habría adoptado las medidas de seguridad pertinentes al permitir que se efectuaran tres (3) operaciones no reconocidas con cargo a la Cuenta de Ahorro N° 679-****500 de titularidad del denunciante. Dichas operaciones se detallan a continuación:*

Tarjetas de Débito N° 6118-****-****-2432			
HORA	**FECHA**	**CONCEPTO**	**IMPORTE**
12:35	25/05/2020	Débito compras	S/ 3 196,30
12:41	25/05/2020	Pago efectivo-bi	S/ 5 900,00
Tarjetas de Débito N° 4285-**-****-4582**			
01:43	24/06/2020	Pago efectivo-bi	S/ 9 597,00
TOTAL		**S/ 18 693,30**	

[Sic]

4. El 29 de abril de 2021, el Banco presentó sus descargos respecto de las conductas imputadas en su contra, con arreglo a las siguientes consideraciones:

(i) Las operaciones cuyo concepto era "*pago efectivo-bi*", fueron realizadas desde el aplicativo móvil de su entidad, con el ingreso de la contraseña alfanumérica del cliente y su clave digital, tal y como se acreditaba con las impresiones de pantalla de su sistema. Tales reportes evidenciaban que se realizó el envío y validación correcta del OTP para las referidas transacciones (*Selsigning*) realizadas el 24 de mayo y 24 de junio de 2020, lo que acreditaba que la clave digital había sido enviada al número de teléfono del cliente;

(ii) la operación de consumo por el importe de S/ 3 196,30 fue válidamente autorizada, tal y como se verificaba de las impresiones de pantallas de su sistema;

(iii) las claves dinámicas fueron enviadas al cliente mediante el canal predeterminado por este, siendo que en el año 2019 dicho consumidor afilió su número telefónico y correo electrónico, en una agencia bancaria a través de biométrico. Posteriormente, el 9 de abril de 2020 desafilió ambos medios de comunicación para que luego el 27 de mayo de 2020 vuelva afiliarlos;

(iv) era imposible para su representada determinar si había sido el señor Yataco u otra persona quien realizó las operaciones controvertidas, puesto que sus sistemas, únicamente, validaban que las claves

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

ingresadas sean las correctas, siendo que, en cualquier caso, el denunciante sería el responsable al tener conocimiento exclusivo de la información pertinente, debiendo bloquear el aplicativo inmediatamente, ya sea por extravío o robo del móvil; y,

(v) alertó al denunciante sobre el bloqueo de su tarjeta de débito, informando que se comunique inmediatamente con su representada, conforme se apreciaba en los mensajes que fueron adjuntados por el propio consumidor en su escrito de denuncia.

5. Mediante Resolución 4 del 6 de setiembre de 2021, la Secretaría Técnica de la Comisión corrió traslado a las partes del procedimiento del Informe Final de Instrucción 0624-2021/CC1-ST de la misma fecha (en adelante, IFI), otorgándoles un plazo de cinco (5) días hábiles para que formulen sus descargos.

6. El 14 de setiembre de 2021, el Banco presentó sus observaciones al IFI, bajo las siguientes consideraciones:

(i) Las operaciones de transferencia materia de cuestionamiento fueron válidamente autorizadas desde el aplicativo móvil de su representada, con el ingreso de la contraseña alfanumérica del cliente y su clave digital, conforme se detallaba en las impresiones de pantalla de su sistema; y,

(ii) la operación de consumo materia de cuestionamiento fue válidamente realizada a través del ingreso de datos como el número de la tarjeta, el nombre del tarjetahabiente, la fecha de vencimiento y el código CVV2 (que se encontraba al reverso de la tarjeta).

7. Mediante Resolución 2545-2021/CC1 del 22 de setiembre de 2021, la Comisión de Protección al Consumidor – Sede Lima Sur N°1 (en adelante, la Comisión) arribó a la siguiente decisión:

(i) Declaró fundada la denuncia interpuesta por el señor Yataco contra el Banco, por infracción de los artículos 18° y 19° del Código, al considerar que no había quedado acreditado que la entidad bancaria haya adoptado las medidas de seguridad pertinentes, al permitir que se efectuaran tres (3) operaciones no reconocidas con cargo a la Cuenta de Ahorros 679-****500 de titularidad del denunciante por el importe total de S/ 18 693,30, sancionándolo con una multa de 4,25 UIT;

(ii) ordenó al Banco, como medida correctiva reparadora, que, en un plazo no mayor de quince (15) días hábiles, contado a partir del día siguiente de la notificación de la citada resolución, cumpla con devolver el importe de S/ 18 693,30, correspondiente a las tres (3) operaciones no reconocidas, en la Cuenta de Ahorros 679-****500 de titularidad del denunciante, más los intereses legales correspondientes hasta la fecha de cumplimiento del mandato;

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

(iii) condenó al denunciado al pago de las costas y costos del procedimiento; y,
(iv) dispuso la inscripción del Banco en el Registro de Infracciones y Sanciones del Indecopi (en adelante, RIS).

8. El 21 de octubre de 2021, el Banco apeló la Resolución 2545-2021/CC1, reiterando los argumentos invocados en sus descargos y agregando adicionalmente lo siguiente:

(i) Respecto de las operaciones efectuadas por los importes de S/ 5 900,00 y S/ 9 597,00, vía aplicativo del Banco, su representada aportó las capturas de sus sistemas internos, encontrándose entre ellas el documento denominado "Pantallas *Splunk*", a fin de acreditar el acceso a la banca móvil –mediante el ingreso de la clave secreta alfanumérica y la clave digital respectiva, debidamente remitida al cliente vía SMS o correo electrónico afiliado-, así como la autenticación de las operaciones en mención, las mismas que se efectuaron válidamente, ello mediante el ingreso exitoso de la clave digital para autorizar dichas transacciones;
(ii) de los *prints* de pantalla de su sistema *Splunk* se desprendía la consignación de la glosa "*Succesful*" la misma que se generaba una vez efectuado el correcto registro y validación de claves en el sistema, quedando así acreditada la validez de las transacciones efectuadas en los meses de mayo y junio de 2020 por los importes de S/ 5 900,00 y S/ 9 597,00, respectivamente;
(iii) hasta el 27 de mayo de 2020, el denunciante tenía afiliada a su cuenta corriente el servicio de banca móvil bajo el ID fd3fd052-e9c0-4s86-8977-6a490dfcaee8, luego fue modificado por el ID ff4bfcb2-d07b-4ca4-a45f-91a8de2038c1 hasta el 8 de julio de 2020, códigos que coincidían con aquellos que se encontraban consignados en las Pantallas *Splunk* de las operaciones en cuestión;
(iv) en la resolución recurrida la Comisión mencionó que de los medios probatorios aportados por el Banco, se apreciaba que la operación realizada el 25 de mayo de 2020, por el importe de S/ 5 900,00, se encontraba registrada en una fecha que no coincidía con aquella señalada en los estados de cuenta, por lo que a consideración de dicho órgano resolutivo ello implicaba que no quedara acreditada la validez de tal operación; sin embrago, cabía precisar que ello se debía al desfase en cuanto al registro de la operación en el sistema, lo cual nada tenía que ver con su realización y/o validez;
(v) en aplicación del principio de Presunción de Veracidad, su representada solicitaba que la autoridad de consumo considerara y valorara sus argumentos respecto de la operación de S/ 5 900,00, efectuada el 25 de mayo de 2020;
(vi) respecto de la operación efectuada por el importe de S/ 3 196,00, la misma que obedecía a un consumo en establecimiento comercial

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

realizado vía internet, su entidad alegó que la misma era realizada mediante el ingreso del número de la tarjeta, el nombre del tarjetahabiente, la fecha de vencimiento, el código CVV2 (siendo este último aquel que se encontraba al reverso de la tarjeta);

(vii) contrariamente a lo indicado por la Comisión, el *print* de pantalla del registro del consumo en cuestión, sí daba cuenta del código de autorización generado a través del código denominado "Trace", el mismo que podía ser generado una vez que se ingresara el Código CVV de manera válida;

(viii) de manera posterior a la realización del primer consumo, su entidad procedió con alertar al cliente, informándole a través de un mensaje de texto sobre la compra realizada en el establecimiento comercial de Saga Falabella, mensaje que fue recibido en el celular registrado por el cliente; y,

(ix) la graduación de la multa impuesta vulneraba el Principio de Razonabilidad en tanto no se encontraba debidamente motivada, por cuanto estaba respaldada por hechos subjetivos.

9. El 5 de abril de 2022, el Banco presentó un escrito mediante el cual reiteró los mismos argumentos invocados a lo largo del procedimiento y adjuntando *prints* de sus sistemas adicionales para la acreditación de la validez de las operaciones controvertidas en el procedimiento.

10. Mediante los Requerimientos 107 y 108 del 8 de junio de 2022, emitidos por la Secretaría Técnica de la Sala, se solicitó al denunciante y al Banco que, en un plazo no mayor de dos (2) días hábiles de notificados tales documentos, presenten los estados de movimientos de la Cuenta de Ahorros 679-*****500, correspondientes al periodo comprendido entre noviembre de 2019 a abril de 2020.

11. El 14 de junio de 2022, el señor Yataco y el Banco presentaron escritos mediante los cuales absolvieron los requerimientos efectuados por la Secretaría Técnica de la Sala.

ANÁLISIS

Sobre la presunta infracción del deber de idoneidad

12. El artículo 18° del Código[1] define la idoneidad de los productos y servicios como la correspondencia entre lo que un consumidor espera y lo que

[1] **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. Artículo 18°.- Idoneidad.**
Se entiende por idoneidad la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, en función a lo que se le hubiera ofrecido, la publicidad e información transmitida, las condiciones y circunstancias de la transacción, las características y naturaleza del producto o servicio, el precio, entre otros factores, atendiendo a las circunstancias del caso. La idoneidad es evaluada en función a la propia naturaleza del producto o servicio y a su aptitud para satisfacer la finalidad para la cual ha sido puesto en el mercado.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

efectivamente recibe, en función a la naturaleza de los mismos, las condiciones acordadas, la publicidad e información transmitida, entre otros factores, atendiendo a las circunstancias del caso.

13. Asimismo, el artículo 19° de la normativa referida establece que los proveedores son responsables por la calidad e idoneidad de los productos y servicios que ofrecen en el mercado[2]. En aplicación de esta norma, los proveedores tienen el deber de entregar los productos y prestar los servicios al consumidor en las condiciones ofertadas o previsibles, atendiendo a la naturaleza de los mismos, la regulación que sobre el particular se haya establecido y, en general, a la información brindada por el proveedor o puesta a disposición.

14. El supuesto de responsabilidad administrativa en la actuación del proveedor impone a este la carga de sustentar y acreditar que no es responsable por la falta de idoneidad del producto colocado en el mercado, sea porque actuó cumpliendo con las normas debidas o porque pudo acreditar la existencia de hechos ajenos que lo eximen de responsabilidad. Así, una vez acreditado el defecto por el consumidor, corresponde al proveedor acreditar que este no le es imputable, conforme a lo establecido en el artículo 104° del Código[3].

15. Por otro lado, es pertinente indicar que el artículo 173° del TUO de la LPAG señala que la carga de la prueba recae sobre los administrados[4], lo cual guarda relación con lo establecido por el artículo 196° del Código Procesal Civil,

---

Las autorizaciones por parte de los organismos del Estado para la fabricación de un producto o la prestación de un servicio, en los casos que sea necesario, no eximen de responsabilidad al proveedor frente al consumidor.

[2] **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. Artículo 19°.- Obligación de los proveedores.**
El proveedor responde por la idoneidad y calidad de los productos y servicios ofrecidos; por la autenticidad de las marcas y leyendas que exhiben sus productos o del signo que respalda al prestador del servicio, por la falta de conformidad entre la publicidad comercial de los productos y servicios y éstos, así como por el contenido y la vida útil del producto indicado en el envase, en lo que corresponda.

[3] **LEY 29571. CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR. Artículo 104°.- Responsabilidad administrativa del proveedor.**
El proveedor es administrativamente responsable por la falta de idoneidad o calidad, el riesgo injustificado o la omisión o defecto de información, o cualquier otra infracción a la establecido en el presente Código y demás normas complementarias de protección al consumidor, sobre un producto o servicio determinado.

El proveedor es exonerado de responsabilidad administrativa si logra acreditar la existencia de una causa objetiva, justificada y no previsible que configure ruptura del nexo causal por caso fortuito o fuerza mayor, de hecho determinante de un tercero o de la imprudencia del propio consumidor afectado.

En la prestación de servicios, la autoridad administrativa considera, para analizar la idoneidad del servicio, si la prestación asumida por el proveedor es de medios o de resultado, conforme al artículo 18.

[4] **TEXTO ÚNICO ORDENADO DE LA LEY 27444, LEY DEL PROCEDIMIENTO ADMINISTRATIVO GENERAL. Artículo 173°.- Carga de la prueba.**

(...)
173.2 Corresponde a los administrados aportar pruebas mediante la presentación de documentos e informes, proponer pericias, testimonios, inspecciones y demás diligencias permitidas, o actuar alegaciones.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prensa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

aplicado de manera supletoria al presente procedimiento[5], y según el cual quien alega un hecho asume la carga de probarlo[6].

16. En el presente caso, el señor Yataco denunció que la entidad bancaria no habría adoptado las medidas de seguridad pertinentes al permitir que se efectuaran tres (3) operaciones no reconocidas con cargo a la Cuenta de Ahorros 679-*****500 de su titularidad. Dichas operaciones se detallan a continuación:

Tarjetas de Débito N° 5118-****-****-2432			
HORA	FECHA	CONCEPTO	IMPORTE
12:35	25/05/2020	Débito compras	S/ 3 196,30
12:41	25/05/2020	Pago efectivo-bi	S/ 5 900,00
Tarjetas de Débito N° 4285-****-****-4502			
01:43	24/06/2020	Pago efectivo-bi	S/ 9 597,00
TOTAL		S/ 18 693,30	

17. En sus descargos, el Banco alegó que las operaciones cuyo concepto era "*pago efectivo-bi*", fueron realizadas desde el aplicativo móvil de su entidad, con el ingreso de la contraseña alfanumérica del cliente y su clave digital, tal y como se acreditaba con las impresiones de pantalla de su sistema. Tales reportes evidenciaban que se realizó el envío y validación correcta del OTP[7] (clave dinámica) para las referidas transacciones (*Selsigning*) registradas el 25 de mayo[8] y 24 de junio de 2020, lo que acreditaba que la clave digital había sido enviada al número de teléfono del cliente.

18. De otro lado, el Banco alegó que la operación de consumo por el importe de S/ 3 196,30 fue válidamente autorizada, tal y como se verificaba de las impresiones de pantalla de sus sistemas.

19. La Comisión declaró fundada la denuncia interpuesta por el señor Yataco contra el Banco, por infracción de los artículos 18° y 19° del Código, al considerar que no había quedado acreditado que la entidad bancaria haya adoptado las medidas de seguridad pertinentes al permitir que se efectuaran tres (3) operaciones no reconocidas con cargo a la Cuenta de Ahorros 679-*****500 de titularidad del denunciante por el importe total de S/ 18 693,30.

20. En vía de apelación, el Banco alegó los siguientes argumentos:

---

5 **CÓDIGO PROCESAL CIVIL. Disposiciones Complementarias. Disposiciones Finales. Primera.** Las disposiciones de este Código se aplican supletoriamente a los demás ordenamientos procesales, siempre que sean compatibles con su naturaleza.

6 **CÓDIGO PROCESAL CIVIL. Artículo 196°.- Carga de la prueba.** Salvo disposición legal diferente, la carga de probar corresponde a quien afirma hechos que configuran su pretensión, o a quien los contradice alegando nuevos hechos.

7 OTP: One Time Password – clave dinámica.

8 Entiéndase que en este punto que se hace referencia a las operaciones realizadas el 24 de mayo de 2020 (fecha real).

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

(i) Los medios probatorios aportados (consistentes en reportes de sus sistemas) corroboraban que el denunciante ingresó a su plataforma de banca móvil mediante el ingreso de la clave secreta alfanumérica y la clave digital respectiva, y que seguidamente, autorizó las transferencias a través de claves digitales remitidas a su número telefónico

(ii) respecto de la operación efectuada por el importe de S/ 3 196,00, la misma que obedecía a un consumo de establecimiento comercial realizado vía internet, su entidad alegó que la misma era realizada mediante el ingreso del número de la tarjeta, el nombre del tarjetahabiente, la fecha de vencimiento, el código CVV (siendo este último aquel que se encontraba al reverso de la tarjeta);

(iii) contrariamente a lo indicado por la Comisión, el *print* de pantalla del registro del consumo en cuestión, sí daba cuenta del código de autorización generado a través del código denominado "Trace", el mismo que podía ser generado una vez que se ingresara el Código CVV de manera válida; y,

(iv) de manera posterior a la realización del primer consumo, su entidad procedió con alertar al cliente, informándole a través de un mensaje de texto sobre la compra realizada en el establecimiento comercial de Saga Falabella, mensaje que fue recibido en el celular registrado por el cliente.

21. Atendiendo a los hechos denunciados por el consumidor y los argumentos opuestos por el Banco en su recurso de apelación, este Colegiado en mayoría procederá a dilucidar si la entidad financiera adoptó las medidas de seguridad pertinentes, a fin de corroborar si las operaciones materia de denuncia fueron procesadas de manera válida.

22. Teniendo en cuenta ello, este Colegiado en mayoría efectuará, en primer lugar, un análisis sobre las medidas de seguridad referidas al deber de monitoreo y detección de operaciones inusuales efectuadas con cargo a la Cuenta de Ahorros 679-****500 del denunciante, a efectos de determinar si correspondía generar una alerta de consumo inusual o sospechoso; y, una vez superada dicha evaluación, se procederá a analizar si se realizó un cargo justificado de las mismas, cumpliendo con los requisitos de validez pertinentes.

I. <u>Sobre el comportamiento habitual de consumo del cliente</u>

23. Ahora bien, el numeral 5 del artículo 2° de la Resolución SBS N° 6523-2013, Reglamento de Tarjetas de Crédito y Débito, modificado de manera posterior por Resolución SBS 5570-2019 (en adelante, el Reglamento), define que el comportamiento habitual de consumo del usuario se refiere al tipo de operaciones que usualmente realiza cada uno con sus tarjetas, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales pueden ser determinados a partir de la información histórica de las operaciones de cada usuario que registra la empresa.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prensa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

24. Por su parte, el artículo 17° del mismo Reglamento establece lo siguiente:

> "***Artículo 17°. - Medidas de seguridad respecto al monitoreo y realización de las operaciones***
> *Las empresas deben adoptar como mínimo las siguientes medidas de seguridad con respecto a las operaciones con tarjetas que realizan los usuarios:*
> *1. Contar con sistemas de monitoreo de operaciones, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual de consumo del usuario.*
> *2. Implementar procedimientos complementarios para gestionar las alertas generadas por el sistema de monitoreo de operaciones.*
> *3. Identificar patrones de fraude, mediante el análisis sistemático de la información histórica de las operaciones, los que deberán incorporarse al sistema de monitoreo de operaciones.*
> *(...)"*

25. Esta Sala considera que la finalidad del artículo 17° del Reglamento descansa en la protección de los usuarios frente al cargo de transacciones fraudulentas en las cuentas de sus tarjetas de crédito o débito, a partir de, entre otros aspectos, la revisión del movimiento histórico de transacciones en las respectivas cuentas, lo cual evidentemente involucra el análisis de operaciones que permitan a la empresa supervisada generar razonablemente un historial de consumo respecto al uso de dicho producto por parte de su cliente.

26. Como se aprecia, la normativa sectorial exige que el historial de consumo que las entidades del sistema financiero construyan respecto a cada uno de sus clientes, e integrarlo a su sistema de monitoreo, debe responder a una serie de factores que la entidad bancaria o financiera determine a partir del análisis sistemático de la información histórica del usuario.

27. Cabe mencionar que, el artículo 2° numeral 5 del citado Reglamento, define que el comportamiento habitual de consumo del usuario se refiere al tipo de operaciones que usualmente realiza cada uno con sus tarjetas, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales pueden ser determinados a partir de la información histórica de las operaciones de cada usuario que registra la empresa.

28. Ahora bien, de lo señalado por las partes a lo largo del procedimiento y de la revisión de los medios probatorios obrantes en el expediente, se tiene que las tres (3) operaciones cuestionadas fueron cargadas a la Cuenta de Ahorros 193- 879-****500 de titularidad del denunciante los días 24 de mayo y 25 de junio.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prensa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

29. Ahora bien, en este punto, corresponde determinar si las operaciones cuestionadas coincidían con el patrón de consumo del cliente. Para ello, dichas transacciones deben ser evaluadas de acuerdo con el comportamiento habitual del denunciante respecto de otras operaciones realizadas con cargo a la Cuenta de Ahorros 193- 679-****500.

30. Así, de la revisión de los estados de movimientos de la Cuenta de Ahorros 193- 679-****500 de titularidad del señor Yataco[9], se verificó lo siguiente:

    (i) En el estado de movimientos, correspondiente al mes de noviembre de 2019, se registró un cargo total por la suma de S/ 340,00;
    (ii) en el estado de movimientos, correspondiente al mes de enero de 2020, se registró un cargo total por la suma de S/ 1 048,00;
    (iii) en el estado de movimientos, correspondiente al mes de febrero de 2020, se registró un cargo total por la suma de S/ 23 590,00;
    (iv) en el estado de movimientos, correspondiente al mes de marzo de 2020, se registró un consumo total por la suma de **S/ 25 725,00**; y,
    (v) en el estado de movimientos, correspondiente al mes de abril 2020, se registró un consumo total por la suma de S/1 387,36.

31. De lo antes mencionado, se puede verificar que en el estado de movimientos donde se registró el reporte total más elevado de consumos y/u operaciones fue en el del periodo correspondiente al mes de marzo 2020, apreciándose que la totalidad de operaciones en dicho periodo ascendió a **S/ 25 725,00.**

32. En tal sentido, corresponde evaluar si el Banco se encontraba obligado a levantar una alerta por uso irregular o sospechoso de la tarjeta de débito asociada a la cuenta de ahorros del señor Yataco que implique el bloqueo preventivo de la misma por las operaciones no reconocidas, en atención a la comparación de estas con el comportamiento de consumo previo registrado por la titular del referido producto financiero.

33. Así, se tiene que las dos (2) primeras transacciones discutidas, registradas el 25 de mayo de 2020[10], sumaban un total de S/ 9 098,30 -bajo las glosas de "Débito compras" y "Pago efectivo-bi"-, siendo que añadiendo a dicho importe el total de operaciones realizadas hasta antes del 25 de mayo de 2020 en dicho mes, se obtiene como monto resultante el importe de S/ 9 991,61, el mismo que no superaba el **máximo total registrado** por el señor Yataco en el mes de marzo de 2020, por la suma ascendente a **S/ 25 725,00.**

---

9 En fojas 224 a 237 del expediente administrativo.

10 Fecha consignada en el estado de movimientos del denunciante, debiéndose entender que tales operaciones fueron realizadas el 24 de mayo de 2020 como fecha real.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prensa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

34. De la misma forma, se tiene que de la suma comprendida por el importe correspondiente a la operación objetada del 24 de junio de 2020, ascendente a S/ 9 597,00 -bajo la glosa de "Pago efectivo-bi"-, y el total de operaciones realizadas hasta antes del 24 de junio de 2020 en dicho mes, se obtiene como monto resultante el importe de S/ 10 842,00, el mismo que no superaba el **máximo total registrado** por el señor Yataco en el mes de marzo de 2020, por la suma ascendente a **S/ 25 725,00**, por lo que este Colegiado en mayoría concluye que la transacción referida, también materia de denuncia, se encontraba dentro del patrón de consumo del consumidor (según su historial de operaciones).

35. En ese sentido, esta Sala en mayoría advierte que ante la realización de las tres (3) operaciones objetadas el Banco no se encontraba obligado a generar alerta alguna por operación inusual o fraudulenta, en tanto tales transacciones se encontraban dentro del patrón de consumo evidenciado en el histórico de operaciones del señor Yataco.

II. Sobre la validez de las operaciones cuestionadas por la denunciante

36. Ahora bien, es relevante destacar que no resulta ser un hecho controvertido que la Tarjeta de Débito 5118-****-****-2432 se encontraba afiliada a la Cuenta de Ahorros 679-****500 y que la misma se hallaba activa en la oportunidad en que se efectuaron las operaciones controvertidas comprendidas por aquellas ascendentes a S/ 3 196,30 y S/ 5 900,00, efectuadas el 25 de mayo de 2020, así como el hecho de que, posteriormente, ante el bloqueo de la referida tarjeta[11], la cuenta haya sido afiliada a la Tarjeta de Débito 4285-****-****-4502, la misma que se encontraba activa al momento de la realización de la operación de S/ 9 597,00 del 24 de junio de 2020.

37. Sobre el particular, cabe precisar que en los casos de operaciones con tarjeta de débito o crédito no se desconoce la posibilidad que las mismas puedan ser objeto de usos fraudulentos; sin embargo, este uso se vería limitado en tanto no se tuviera acceso a la clave secreta, **cuyo resguardo es responsabilidad exclusiva del tarjetahabiente**. Por ello, de acreditarse que la operación se realizó con el uso conjunto de estos dos elementos, la transacción debe reputarse como válidamente realizada.

38. Adicionalmente, cabe agregar que la comprobación de un hecho negativo -como la no realización de una operación con la tarjeta de débito o crédito otorgada a un cliente- no es factible para un consumidor. Por el contrario, en su condición de proveedor del servicio financiero, es la empresa del sistema financiero quien debe probar que tal transacción se realizó utilizando las

[11] Efectuado el 24 de mayo de 2020 a las 10:30:59 horas, conforme lo acreditó el Banco mediante su *print* de pantalla denominado Consulta de Tarjetas – Bloqueo de Tarjeta obrante en la foja 68 (reverso) del expediente.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 – Perú Telf. 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

medidas de seguridad puestas a disposición de cada cliente por el propio proveedor. Lo anterior, en atención a la ventaja que posee la entidad bancaria en cuanto al manejo de información y de medios disponibles para probar que la operación cuestionada sí se efectuó.

- Sobre las operaciones "Pago Efectivo – bi", por los importes de S/ 5 900.00 y S/ 9 597.00

39. Ahora bien, cabe precisar que el proveedor señaló que las operaciones fueron efectuadas a través de su plataforma de banca móvil, siendo que esta afirmación no ha sido refutada por su contraparte, a lo que adicionó que el consumidor requería ingresar al canal virtual mediante el ingreso de contraseña alfanumérica y clave digital.

40. Así pues, previamente a analizar si las transacciones cuestionadas fueron, o no, autorizadas de acuerdo con las medidas de seguridad contempladas por el proveedor, es menester verificar si el señor Yataco accedió a la banca móvil del denunciado para efectos de realizar las operaciones registradas el 25 de mayo[11] y 24 de junio de 2020).

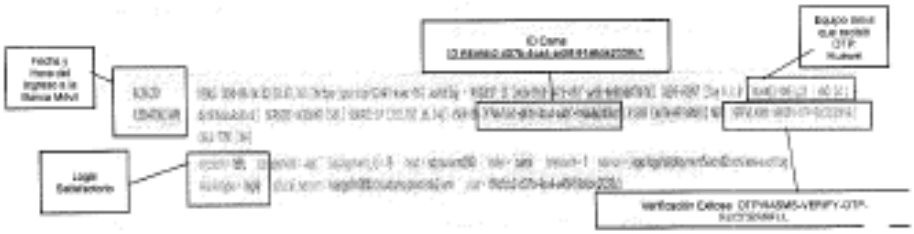
41. Para tal fin, aportó el reporte de su sistema denominando "Pantallas *Splunk*" el mismo que daba cuenta del ingreso a la banca móvil para cada una de las operaciones analizadas en este punto, conforme se aprecia a continuación:

Ingreso a Banca Móvil para realización de operación S/ 5 900.00 del 25 de mayo de 2020

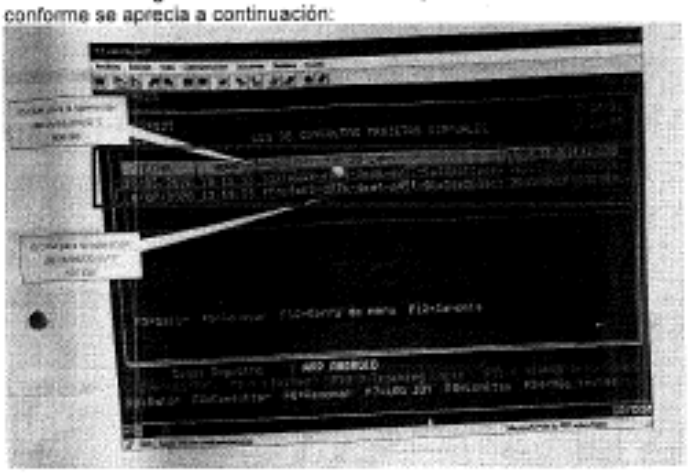
[11] Fecha consignada en el estado de movimientos del denunciante, debiéndose entender que tales operaciones fueron realizadas el 24 de mayo de 2020 como fecha real.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 – Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

Ingreso a Banca Móvil para realización de operación S/ 9 597,00 del 24 de junio de 2020



42. Aunado a lo anterior, cabe traer a colación el reporte del Banco denominado "Log de Consultas Tarjetas Virtuales"[11], del cual se desprenden los códigos de identificación "ID Cams" asignados al denunciante, y que son consignados al momento del registro de cada una de las operaciones materia de análisis, conforme se aprecia a continuación:



43. Del medio probatorio observado, se desprende que este guarda concordancia con el argumento del Banco, referente al hecho de que hasta el 27 de mayo de 2020, el denunciante tenía afiliada a su cuenta el servicio de banca móvil bajo el código de identificación ID fd3fd052-e9c0-4a96-8977-6a490dfcaee8 y

11 En la foja 65 (anverso) del expediente.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

que, posteriormente, fue modificado por el código de identificación ID ff4bfcb2-d07b-4ca4-a45f-91a6de2038c1 hasta el 8 de julio de 2020, siendo estos códigos los mismos que coincidían con aquellos que se encontraban consignados en las Pantallas *Splunk* que acreditaban el ingreso a la banca móvil para la realización de las operaciones en cuestión, visualizadas en el punto 41 de la presente resolución, acreditando así el correcto acceso del denunciante a dicho aplicativo para la realización de ambas transacciones.

44. En esa línea, se tiene que de la revisión de tales medios probatorios se aprecian los siguientes datos: (i) fecha y hora: 24 de mayo de 2020 a las 12:30:10 horas (en referencia a la operación registrada el 25 de mayo de 2020), y 24 de junio de 2020, a las 01:38:47 horas); (ii) código de identificación del denunciante (ID fd3fd052-e9c0-4s86-8977-6a490dfcaee6 y ff4bfcb2-d07b-4ca4-a45f-91a6de2038c1, respectivamente para cada operación); (iii) nota "OTPVIASMS-VERIFY-OTP-SUCCESSFUL" -glosa que significaba el correcto registro y validación de las claves en el sistema, conforme lo explicado por el Banco en su apelación-, (iv) glosas: account=SEL sourcetype=log4 (que significaban *login* satisfactorio) los cuales son conducentes a acreditar el correcto acceso del denunciante a la banca móvil del Banco.

45. Habiéndose determinado ello, corresponde dilucidar si, ante dicho ingreso, se efectuaron las operaciones cuestionadas por el interesado, de acuerdo con los mecanismos de seguridad necesarios para tal fin.

46. Al respecto, cobra relevancia señalar que, con arreglo a los argumentos del proveedor, ambas operaciones habían sido autorizadas, mediante el ingreso de su clave secreta y la clave digital correspondiente.

47. Atendiendo a tal afirmación, se denota que las dos (2) operaciones materia de análisis fueron efectuadas mediante dos (2) mecanismos de autenticación distintos (una clave secreta y una clave digital); en el mismo orden de ideas, el denunciado refirió que la clave digital respectiva a cada operación había sido remitida al teléfono celular y correo electrónicos afiliados por el denunciante (lo cual evidencia que este mecanismo constituía una clave dinámica).

48. Bajo tales premisas, cabe verificar si las transacciones ascendentes a S/ 5 900,00 y S/ 9 597,00 (con cargo a la Cuenta de Ahorros 679-*****500) fueron efectuadas de acuerdo con los requisitos de validez invocados por el propio denunciado.

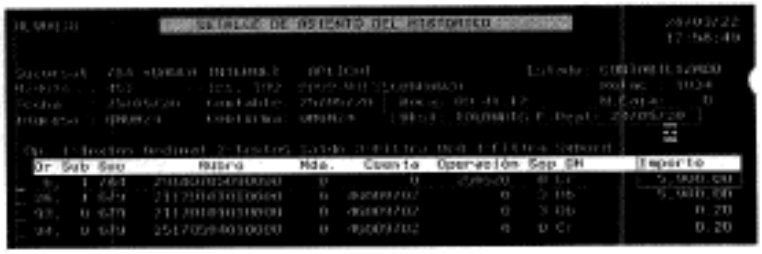
49. Al respecto, el Banco refirió que los reportes del medio probatorio "Pantallas *Splunk*"[14] demostraban la veracidad de sus afirmaciones sobre el particular.

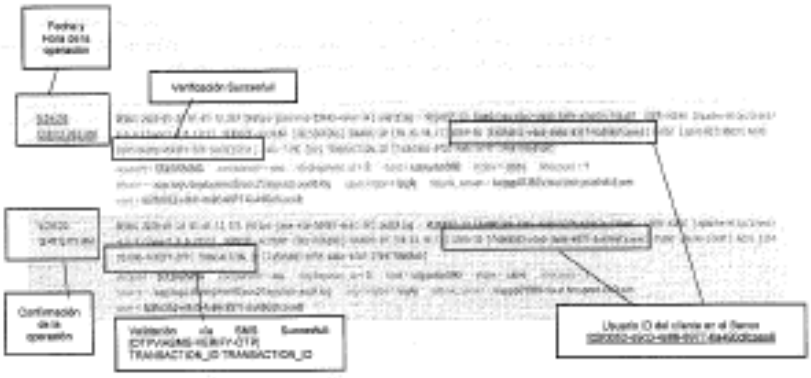
[14] En la foja 84 (reverso) del expediente.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prensa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

50. En efecto, conforme es posible cotejar de las imágenes expuestas a continuación, los instrumentos aportados por el denunciado permiten a este Colegiado identificar el registro y aprobación de las claves secretas empleadas para brindar la aquiescencia a las operaciones y las claves digitales empleadas con tal fin, conforme se visualiza a continuación:

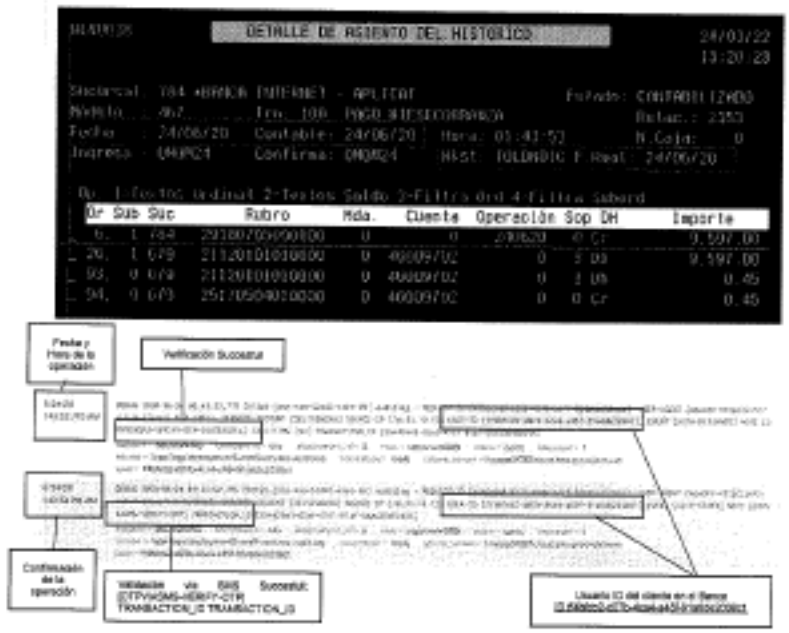
Operación de S/ 5 900,00





[Ver imagen en la siguiente página]

Operación de S/ 9 597,00



51. En principio, este Colegiado advierte, de la revisión de las imágenes citadas previamente, que los sistemas del Banco registran dos (2) fechas para hacer referencia a cada una de las operaciones discutidas, siendo estas las siguientes: "fecha contable" y "fecha real". Así, se desprende lo siguiente:

    (i) La operación que en el estado de movimientos figura registrada el día 25 de mayo de 2020 (fecha contable), ha sido realizada el día 24 de mayo del mismo año, identificando tal fecha como "real".
    (ii) La operación que en el estado de movimientos figura registrada el día 24 de junio de 2020 (fecha contable), ha sido realizada el mismo día -esto es, el 24 de junio del mismo año-, identificando tal fecha como "real".

52. Del resumen citado previamente, se concluye que no existe una contradicción entre las fechas consignadas en los estados de movimientos de la cuenta del denunciante y los medios probatorios aportados por la entidad financiera, sino

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prensa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

que esta diferencia encuentra su sustento en el detalle presentado previamente.

53. En ese sentido, si bien la Comisión consideró en la resolución recurrida que la operación ascendente a S/ 5 900,00, registrada en el estado de movimientos de la cuenta de ahorros del denunciante en fecha 25 de mayo de 2020, no había quedado debidamente acreditada como válida por cuanto que, de los medios probatorios aportados por el Banco se desprendían reportes que diferían en cuanto a la fecha de su registro, lo cierto es que, ello obedecía a un desfase en el registro de la operación en el sistema del proveedor, lo cual era independiente y no tenía incidencia en su realización y validez (efectuada en fecha real el 24 de mayo de 2020).

54. Lo anterior guarda concordancia con lo alegado por el propio denunciante mediante su escrito de denuncia, en tanto que dicho consumidor precisó textualmente que el domingo 24 de mayo de 2020 se había percatado sobre la realización de dos (2) operaciones con cargo a su cuenta de ahorros, las mismas que no reconocía, afirmación que respaldaba el hecho de que la operación registrada en el estado de movimientos de la cuenta de ahorros del señor Yataco, con fecha 25 de mayo de 2020, haya sido realmente efectuada un día antes, esto es, el 24 de mayo de 2020.

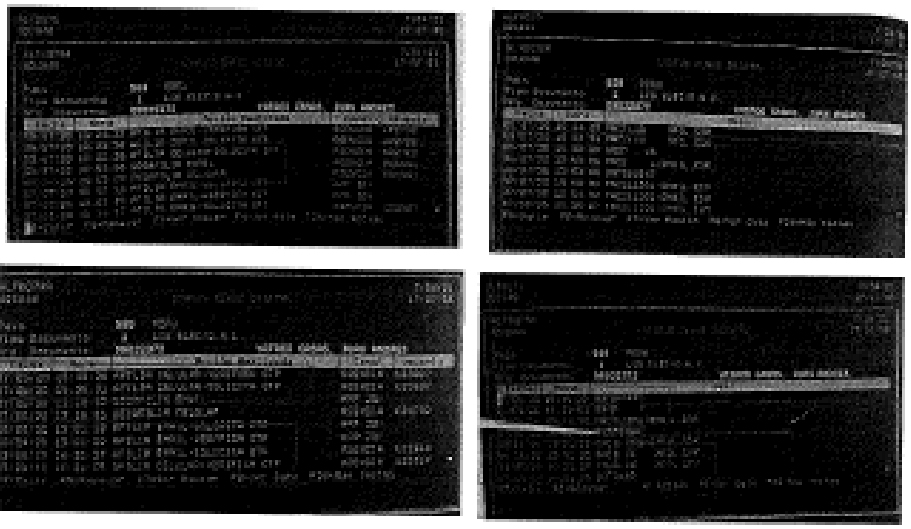
55. Ahora bien, habiendo quedado acreditado que las fechas consignadas en tales reportes no denotan el cargo de operaciones ejecutadas indebidamente, es pertinente continuar con el análisis de los medios probatorios presentados y acotar que los mismos recogen la siguiente información: (i) fecha y hora de las operaciones (24 de mayo de 2020, a las 12:41:12 horas -fecha real- y 24 de junio de 2020, a las 01:47:52 horas); (ii) fecha contable de la operación; (iii) código de identificación del denunciante (ID fd3fd052-e9c0-4e86-6977-6a490dfcaee8 y ff4bfcb2-d07b-4ca4-a45f-91a6de2038c1, respectivamente para cada operación); (iv) nota "OTPVIASMS-VERIFY-OTP-SUCCESSFUL" -glosa que significaba el correcto registro y validación de las claves en el sistema, conforme lo explicado por el Banco en su apelación-.

56. A ello se aúna que el proveedor sustentó que el envío de las claves digitales empleadas para autorizar las transacciones controvertidas al teléfono celular del denunciante, vía SMS, se acreditaba bajo la consignación de la nota [OTPVIASMS-VERIFY-OTP] TRANSACTION_ID en sus sistemas, código que se encuentra registrado en los medios probatorios citados previamente, tal como ha sido corroborado por esta Sala en la presente resolución.

57. En este punto, cabe agregar que, conforme los *prints* de pantalla del sistema del Banco denominado "Status Clave Digital" que se visualizan a continuación, se encontraba acreditado que el denunciante mantuvo afiliados al servicio de banca móvil, su correo electrónico -facil1**1@gmail.com- y número de celular -997**3847- al momento en que se llevaron a cabo las operaciones

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

cuestionadas y analizadas en este punto, siendo tales datos los mismos que el señor Yataco consignó en su escrito de denuncia, evidenciándose de esa forma que las claves que autorizaron las operaciones controvertidas fueron remitidas al denunciante, sin que este haya presentado documento alguno que desvirtúe tal afirmación:



58. En suma, este Colegiado en mayoría es de la opinión que, de la valoración conjunta de los medios probatorios ofrecidos por la entidad financiera y de la explicación brindada por el proveedor denunciado respecto del significado de cada uno de los términos contenidos en tales documentos, es posible colegir que las transacciones analizadas fueron procesadas en cumplimiento de los requisitos de validez exigidos para su ejecución, no existiendo en el procedimiento indicio alguno que controvierta la veracidad de los mismos.

59. En ese sentido, dado que quedó acreditado que las dos (2) transacciones cuestionadas por el señor Yataco fueron aprobadas atendiendo a los requisitos de validez contemplados para ello, es preciso exonerar de responsabilidad administrativa al proveedor, por la comisión de la conducta infractora atribuida en su contra.

- Sobre el consumo por el importe de S/ 3 198.30

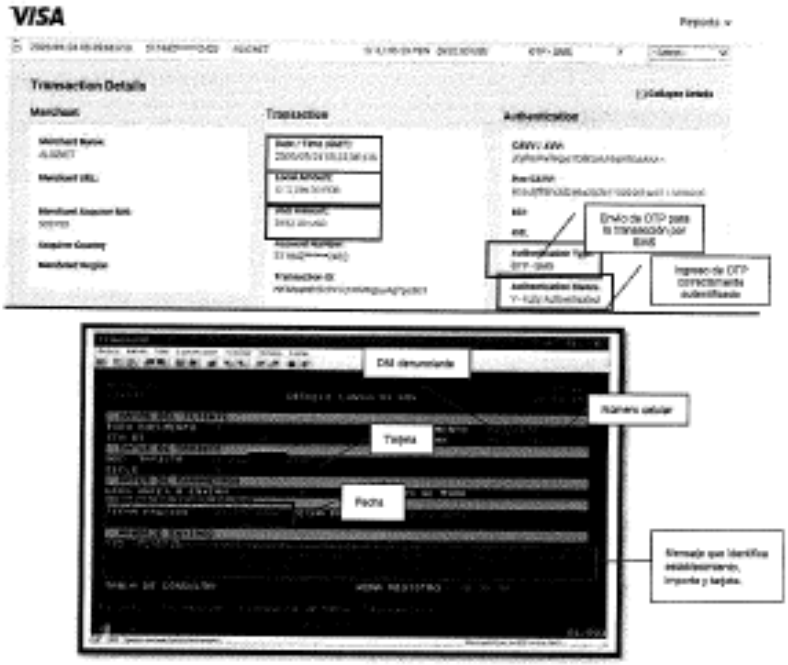
60. Al respecto, como se señaló previamente, en los casos de operaciones con tarjeta de débito no se desconoce la posibilidad de que las mismas puedan ser

objeto de usos fraudulentos; sin embargo, este uso se vería limitado en tanto no se tuviera acceso a la clave secreta, cuyo resguardo es responsabilidad exclusiva del tarjetahabiente; por ello, de acreditarse que la operación se realizó con el uso conjunto de estos dos elementos, la transacción debe reputarse como válidamente realizada. Con relación a las operaciones "con tarjeta no presente", no se requiere la presencia de la tarjeta física, solicitándose que la autorización se realice a través de medios electrónicos, como por ejemplo vía internet en el que se requiere el ingreso de datos impresos en el medio de pago, tales como fecha de vencimiento y el código CVV2 o clave dinámica, con lo que se verifica la autorización del cliente.

61. En esa línea, cabe mencionar que, respecto de la operación en cuestión en este punto, el Banco señaló que el referido consumo había sido realizado siguiendo el circuito operativo normal previsto para este tipo de operaciones, de acuerdo a la siguiente imagen:

62. Sobre el particular el Banco presentó tres (3) *prints* de pantalla de sus sistemas para acreditar la validez de la operación cuestionada, tal y como se observa a continuación:

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe



63. Ahora bien, de acuerdo con lo informado por el Banco, la primera imagen daba cuenta del registro de la operación cuestionada, en el que se detallan elementos como el número de operación (001000), número de tarjeta (5118-****-****-2432), código de autorización (200), monto de la operación (S/ 3 196,30), establecimiento comercial (Saga Falabella) y el canal donde se realizó la operación (por internet en tanto se consignó la glosa *"on line"*).

64. Asimismo, de la revisión de la segunda imagen correspondiente a Visa, se observa la glosa "Authentication Type: OTP-SMS que deja constancia del envío de la clave SMS, así como su correcta autentificación bajo la glosa: Authentication Status: Y-Fully Authenticated, ello, conforme fue explicado por el Banco en su escrito de apelación.

65. Adicionalmente, la tercera imagen da cuenta de la comunicación del Banco (vía mensaje de texto al celular del denunciante), posterior a la realización del

consumo objetado, mediante la cual se procedió a alertar al cliente sobre la compra realizada en el establecimiento de Saga Falabella.

66. Ahora bien, cabe precisar que, si bien la Comisión concluyó en el análisis de su pronunciamiento en que no se había acreditado el ingreso del código CVV respecto de la operación en cuestión, lo cierto es que, ante esta instancia el Banco brindó una explicación sobre tal ingreso, al alegar que tal punto se encontraba acreditado bajo el código denominado "Trace" (constituyendo este el código de autorización), el mismo que era generado, únicamente, al ingresar el código CVV en forma válida.

67. Aunado a lo dicho anteriormente, debe precisarse que la parte denunciante no ha presentado ningún argumento o medio de prueba que cuestione lo dicho (argumentos) o aportado (medios probatorios) por el Banco, a fin de controvertir la veracidad de los mismos; por lo que, en aplicación del principio de presunción de veracidad[15] que rige el procedimiento administrativo, debe considerarse la validez de los medios probatorios aportados por el Banco, los mismos que fueron debidamente puestos a conocimiento del denunciante.

68. En consecuencia, dado que quedó acreditado que la operación analizada en este punto fue válidamente autorizada, mediante el debido cumplimiento de los requisitos de validez contemplados para tal fin, es preciso exonerar de responsabilidad administrativa al proveedor, por la comisión de la conducta infractora atribuida en su contra.

69. Por las consideraciones expuestas, corresponde revocar la resolución recurrida, en el extremo que declaró fundada la denuncia interpuesta por el señor Yataco contra el Banco, y, en consecuencia declarar infundada la misma por presunta infracción de los artículos 18° y 19° del Código, al haber quedado acreditado que la entidad bancaria adoptó las medidas de seguridad respectivas, a fin de procesar tres (3) operaciones ascendentes a S/ 3 196,30, S/ 5 900,00 y S/ 9 597,00, con cargo a la Cuenta de Ahorros 679-*****500 del denunciante, en tanto se verificó que fueron válidamente autorizadas.

70. Finalmente, en tanto la presente denuncia ha resultado infundada, corresponde dejar sin efecto la medida correctiva ordenada, la sanción impuesta, la condena al pago de costas y costos del procedimiento, así como

---

[15] **TEXTO ÚNICO ORDENADO DE LA LEY DEL PROCEDIMIENTO ADMINISTRATIVO GENERAL, aprobado por DECRETO SUPREMO N° 004-2019-JUS.**
Artículo IV. Principios del procedimiento administrativo.
1. El procedimiento administrativo se sustenta fundamentalmente en los siguientes principios, sin perjuicio de la vigencia de otros principios generales del Derecho Administrativo:
(...)
1.7. **Principio de presunción de veracidad.**- En la tramitación del procedimiento administrativo, se presume que los documentos y declaraciones formulados por los administrados en la forma prescrita por esta Ley, responden a la verdad de los hechos que ellos afirman. Esta presunción admite prueba en contrario.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf. 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

la inscripción del proveedor en el RIS; por lo que carece de objeto emitir un pronunciamiento sobre los alegatos destinados a cuestionar los referidos puntos.

RESUELVE:

PRIMERO: Revocar la Resolución 2545-2021/CC1 del 22 de setiembre de 2021, que declaró fundada la denuncia interpuesta por el señor [redacted] Casas contra [redacted]., y en consecuencia, se declara infundada la misma, por presunta infracción de los artículos 18° y 19° de la Ley N° 29571, Código de Protección y Defensa del Consumidor, al haber quedado acreditado que la entidad bancaria adoptó las medidas de seguridad respectivas, a fin de procesar tres (3) operaciones ascendentes a S/ 3 196,30, S/ 5 900,00 y S/ 9 597,00, con cargo a la Cuenta de Ahorros 679-****500 del denunciante, en tanto se verificó que fueron válidamente autorizadas.

SEGUNDO: Dejar sin efecto la Resolución 2545-2021/CC1, en los extremos que ordenó a [redacted] el cumplimiento de una medida correctiva, le impuso una sanción de 4,25 UIT, lo condenó al pago de costas y costos del procedimiento, y dispuso su inscripción en el Registro de Infracciones y Sanciones del Indecopi.

Con la intervención de los señores vocales Javier Eduardo Raymundo Villa García Vargas, Juan Alejandro Espinoza Espinoza, Julio Baltazar Durand Carrión y Oswaldo Del Carmen Hundskopf Exebio.

JAVIER EDUARDO RAYMUNDO VILLA GARCÍA VARGAS
Presidente

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

El voto en singular de la señora Vocal Roxana María Irma Barrantes Cáceres, respecto de la conducta infractora correspondiente a la falta de adopción de medidas de seguridad por parte de Scotiabank Perú S.A.A. por la ejecución de tres (3) operaciones realizadas con cargo a la cuenta de ahorros de titularidad de la denunciante, es el siguiente:

La Vocal que suscribe el presente voto considera, respecto a la denuncia presentada por el señor [redacted] (en adelante, el señor Yataco) contra [redacted] n adelante, el Banco) por el procesamiento de tres (3) operaciones realizadas con cargo a su cuenta de ahorros, lo siguiente:

1. El artículo 18° de la Ley 29571, Código de Protección y Defensa del Consumidor (en adelante, el Código) define la idoneidad de los productos y servicios como la correspondencia entre lo que un consumidor espera y lo que efectivamente recibe, en función de lo que se le hubiera ofrecido, la publicidad e información transmitidas, entre otros factores, atendiendo a las circunstancias del caso. La idoneidad es evaluada en función de la propia naturaleza del producto o servicio y de su aptitud para satisfacer la finalidad para la cual ha sido puesto en el mercado. A su vez, el artículo 19° del Código indica que el proveedor responde por la idoneidad y calidad de los productos y servicios ofrecidos.

2. De conformidad con lo dicho, los proveedores tienen el deber de brindar los productos y servicios ofrecidos en las condiciones acordadas o en las que resulten previsibles, atendiendo a la naturaleza y circunstancias que rodean la adquisición del producto o la prestación del servicio, así como de la normatividad que rige su prestación.

3. El supuesto de responsabilidad administrativa en la actuación del proveedor impone a este la carga procesal de sustentar y acreditar que no es responsable por la falta de idoneidad del bien colocado en el mercado o del servicio prestado, sea porque actuó cumpliendo con las normas debidas o porque pudo acreditar la existencia de hechos ajenos que lo eximen de responsabilidad. Así, una vez acreditado el defecto por el consumidor o la autoridad administrativa, corresponde al proveedor acreditar que aquel no le es imputable.

4. Con relación a las medidas de seguridad a las que se encuentran legalmente obligadas las entidades financieras durante la prestación de sus servicios, tenemos que la Resolución SBS 6523-2013, que aprobó el Reglamento de Tarjetas de Crédito y Débito (en adelante, el Reglamento), en su artículo 17° prescribe lo siguiente:

> ***"Artículo 17.- Medidas de seguridad respecto al monitoreo y realización de las operaciones***

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 – Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

Las empresas deben adoptar como mínimo las siguientes medidas de seguridad con respecto a las operaciones con tarjetas que realizan los usuarios:
1. Contar con sistemas de monitoreo de operaciones, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual de consumo del usuario.
2. Implementar procedimientos complementarios para gestionar las alertas generadas por el sistema de monitoreo de operaciones.
3. Identificar patrones de fraude, mediante el análisis sistemático de la información histórica de las operaciones, los que deberán incorporarse al sistema de monitoreo de operaciones.
4. Establecer límites y controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude.
[...]".

5. De la lectura del citado artículo advertimos que las entidades financieras que colocan en el mercado productos financieros se encuentran obligadas, como mínimo, a implementar sistemas de monitoreo que les permitan detectar oportuna y eficientemente la realización de operaciones que no respondan a la conducta habitual de consumo de sus clientes.

6. Así, se debe tener en consideración que, respecto de las operaciones que se efectúen con las tarjetas de débito o crédito[8] de sus clientes, configura su responsabilidad y una condición legal mínima en los servicios financieros que ofrecen en el mercado, integrada a la expectativa (idoneidad) del cliente, la garantía que deben otorgar los proveedores en la adopción de medidas de seguridad necesarias para asegurar que el patrimonio de los consumidores, cuya administración se encuentra a su cargo, se encuentre debidamente resguardado de terceros malintencionados.

7. De este modo, al constituir las operaciones fraudulentas un riesgo típico derivado del desarrollo de actividades en el uso de las tarjetas de débito y crédito, los bancos deben adoptar medidas de seguridad suficientes e idóneas para reducir la posibilidad de su realización.

8. Sobre ello, la Vocal que suscribe el presente voto considera que el artículo 17° del Reglamento citado previamente, alude mínimamente a la obligación de toda entidad financiera de conocer el comportamiento habitual de consumo de sus clientes, en virtud a la recopilación de información que tiene a su disposición, producto del registro y seguimiento efectuado a todos los movimientos ocurridos durante las relaciones de consumo que han entablado con los clientes, en apoyo de las tecnologías de la información implementadas

[8] Resolución 2354-2015/PSC-INDECOPI del 23 de julio de 2015.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

en su entidad y de las que puede obtener el perfil de consumo que cada usuario practica en uso de sus productos financieros.

9. Ahora bien, a efectos de determinar ello, es pertinente traer a colación el numeral 5 del artículo 2° del Reglamento el cual señala que se deberá entender como comportamiento habitual del cliente financiero *"al tipo de operaciones que usualmente realiza cada usuario con sus tarjetas, considerando diversos factores, como por ejemplo el país de consumo, tipos de comercio, frecuencia, canal utilizado, entre otros, los cuales pueden ser determinados a partir de la información histórica de las operaciones de cada usuario que registra la empresa"*.

10. Precisamente, de conformidad con la definición de la Real Academia Española, lo *"habitual"* evoca aquello *"que se hace, padece o posee con continuación o por hábito"*.

11. Fijado el parámetro de análisis anteriormente detallado, la Vocal que suscribe el presente voto considera que, a efectos de determinar el comportamiento habitual de un cliente, las entidades financieras deberán observar la combinación, esto es, el conjunto de diversos factores, tales como: monto, frecuencia, canal, entre otros, cuyo contraste a las características propias de cada cliente, según su histórico de consumos en cada producto evaluado, usualmente reflejado en los estados de cuenta y/o consulta de saldos y movimientos correspondientes, permitirá detectar operaciones sospechosas de fraude, con la finalidad de advertir al cliente sobre su realización, preservando su patrimonio.

12. De hecho, este seguimiento cercano al comportamiento habitual de consumo es parte del conocimiento que una entidad financiera debe poseer respecto de sus clientes en el marco de las reglas prudenciales que rigen el sistema financiero y las más recientes reglas sobre "conoce a tu cliente" recomendadas en el marco de la lucha contra el lavado de activos.

13. Si bien acorde a anteriores votos suscritos por la presente Vocal, con relación al factor referido al monto, se ha enfatizado que su medición no se encuentra delimitada al consumo total mensual generado por cada cliente en los meses anteriores a la operación controvertida, motivo por el cual discrepo del voto en mayoría; sino que debe responder a verificar si acaso el importe objeto de las transacciones cuestionadas atendía a lo usual o cotidiano dispuesto por el consumidor en operaciones anteriores e individualizadas; estimo que a dicho indicador deberá sumarse, el cotejo de la frecuencia y el canal en que se produjo dicha operación y, a partir de ello, determinar si era habitual, o, en su defecto, ameritaba que la entidad lo advirtiera al titular.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prensa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

14. Entonces, en virtud de los fundamentos vertidos previamente, la Vocal que suscribe el presente voto considera pertinente ampliar los alcances de dicho criterio aplicable a los casos vinculados a denuncias por falta de medidas de seguridad en la realización de operaciones no reconocidas por los usuarios de servicios financieros, a fin de revestir de un contenido más completo al análisis de comportamiento habitual del cliente, estableciéndose la obligación de la entidad financiera de evaluar el conjunto de factores que constituye el comportamiento habitual de cada consumidor; ello de conformidad con lo dispuesto en numeral 1 del artículo 17° del Reglamento.

15. En el presente caso, el señor Yataco denunció al Banco, toda vez que la entidad bancaria no adoptó las medidas de seguridad necesarias, al haber permitido que se procesaran tres (3) transacciones no reconocidas por su parte, con cargo a la Cuenta de Ahorros 679-*****500 de su titularidad, las mismas que se detallan a continuación:

Tarjetas de Débito N° 5118-****-****-3432			
HORA	FECHA	CONCEPTO	IMPORTE
12:35	25/05/2020	Débito compras	S/ 3 196,30
12:41	25/05/2020	Pago efectivo-bi	S/ 5 900,00
Tarjetas de Débito N° 4355-****-****-4582			
01:43	24/05/2020	Pago efectivo-bi	S/ 9 597,00
TOTAL		S/ 18 693,30	

16. La Comisión declaró fundada la denuncia interpuesta por el señor Yataco, por infracción de los artículos 18º y 19º del Código, al considerar que no había quedado acreditado que la entidad bancaria haya adoptado las medidas de seguridad pertinentes, al permitir que se efectuaran tres (3) operaciones no reconocidas con cargo a la Cuenta de Ahorros 679-*****500 de titularidad del denunciante por el importe total de S/ 18 693,30.

17. Ahora bien, el Colegiado en mayoría, al momento de emitir un pronunciamiento sobre el punto objeto de controversia, analizó si las transacciones discutidas se ejecutaron en el marco del comportamiento habitual de consumo del cliente y en cumplimiento de los requisitos de validez exigidos para su ejecución, ello por cuanto consideró que tales factores fueron cuestionados en el marco del procedimiento.

18. En este punto, la Vocal que suscribe el presente voto estima relevante puntualizar que, incluso si el consumidor no hubiera manifestado su disconformidad con la conducta de su contraparte, en lo concerniente al deber de monitoreo de operaciones contemplado en el artículo 17° del Reglamento, correspondía a la autoridad administrativa evaluar el cumplimiento de dicha garantía legal, al constituir parte del cumplimiento del deber de idoneidad en virtud de las medidas de seguridad adoptadas por el proveedor frente a las transacciones cuestionadas.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú| Telf. 224 7800 | Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe | Web: www.indecopi.gob.pe

19. En ese sentido, más allá del formato de redacción que un consumidor pueda utilizar en su denuncia o el tenor de la misma, se entiende que cuando este cuestiona ante la Administración el cargo de un consumo no reconocido, lo hace con el fin de que se verifique que la entidad financiera adoptó todas las medidas de seguridad a las que se encontraba obligada, motivo por el cual es necesario realizar un análisis conjunto de tales medidas de seguridad.

20. Considerando ello y en atención al marco normativo antes desarrollado, la Vocal que suscribe el presente voto considera que corresponde verificar si el señor Yataco -con anterioridad a las operaciones cuestionadas- había realizado transacciones que, de forma individual, superaban el monto de las operaciones no reconocidas, así como si anteriormente había efectuado operaciones con la misma frecuencia y a través del mismo canal que aquellas controvertidas.

21. De la revisión de los estados de movimientos de la Cuenta de Ahorros 679-****500 de titularidad del denunciante, emitidos con anterioridad a la fecha en que se realizaron las operaciones materia de controversia, correspondientes a los meses de noviembre de 2019, enero, febrero, marzo y abril de 2020, se advierte lo siguiente:

Periodo	Cantidad de consumos total por mes	Consumo mayor en el periodo	Monto total de consumos en el mes	Cantidad de consumos máxima por día	¿Operaciones por Banca Móvil y/o por internet?
Noviembre 2019	2	S/ 240,00	S/ 340,00	1	SI
Enero 2020	5	S/ 500,00	S/ 1 048,00	2	SI
Febrero 2020	20	S/ 7 000,00	S/ 23 590,00	4	SI
Marzo 2020	11	**S/ 18 000,00**	S/ 25 725,00	2	SI
Abril 2020	11	S/ 500,00	S/1 387,36	2	SI

22. A partir de la información extraída de dichos documentos, se puede arribar a las siguientes conclusiones:

Sobre el canal para operaciones:

(i) El cliente registró consumos mediante Banca Móvil y/o Banca por internet durante todos los periodos de facturación analizados.

Sobre la frecuencia de operaciones:

(ii) Se verifica que el interesado realizó hasta cuatro (4) operaciones por día, lo cual ocurrió el 13 de febrero de 2020, y efectuó hasta veinte (20) transacciones mensuales en el periodo de febrero de 2020.

Sobre la máxima operación individual

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf. 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

(ii) La operación máxima individual registrada por el tarjetahabiente se realizó el 13 de marzo de 2020, por la suma de S/ 18 000,00, consistente en una transferencia vía internet.

Sobre el máximo total registrado

(iv) El monto total máximo consumido mensualmente ascendía a S/ 25 725,00.

23. El Colegiado, en mayoría, concluyó que ninguna de las operaciones discutidas excedía el importe máximo total mensual registrado previamente en los estados de movimientos de la cliente.

24. No obstante, de acuerdo con la posición adoptada por la Vocal que suscribe el presente voto, dicho análisis resulta incompleto, al omitir considerar las características de cada operación individualizada que el titular de la cuenta de ahorros -a la que se cargaron las operaciones discutidas en el presente caso- realizó previamente a la ocurrencia de las transacciones materia de análisis.

25. Atendiendo a ello, de un contraste individual entre cada operación materia de denuncia y las transacciones efectuadas previamente con cargo a la cuenta de ahorros del consumidor, la suscrita advierte que ninguna de las operaciones cuestionadas (por sí sola) superaba el monto **individual** máximo registrado por el señor Yataco, ascendente a S/ 18 000,00.

26. En efecto, las tres (3) transacciones discutidas ascendían, cada una, a importes ascendentes a: S/ 3 196,30; S/ 5 900,00 y S/ 9 597,00, siendo que ninguno de los valores detallados previamente superó el monto **individual** máximo registrado por el señor Yataco, ascendente a S/ 18 000,00.

27. Asimismo, cabe adicionar que el interesado efectuaba hasta cuatro (4) operaciones por día, con cargo a su cuenta de ahorros, de modo que la prosecución de hasta dos (2) transacciones en un mismo día -conforme se dio en el presente caso respecto de las operaciones del 25 de mayo de 2020- no resultaba inusual al empleo histórico de su producto financiero. De igual modo, cabe agregar que las dos (2) transacciones del 25 de mayo de 2020 y la operación del 24 de junio de 2020, cuestionadas en el presente caso, se encontraban dentro de la cantidad total máxima de operaciones por mes, conforme lo registrado en el histórico de consumo del denunciante, esto es, por debajo de las veinte (20) operaciones al mes.

28. Aunado a ello, se tiene que las dos (2) primeras transacciones discutidas, realizadas el 25 de mayo de 2020[17], sumaban un total de S/ 9 096,30 -bajo las

[17] Fecha en que se registraron las dos (2) primeras operaciones discutidas por el denunciante, en el estado de cuenta correspondiente a mayo de 2020, teniendo en cuenta que su realización se dio el 24 de mayo de 2020 como fecha real.

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 – Perú| Telf. 224 7800 | Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe | Web: www.indecopi.gob.pe

glosas de "Débito compras" y "Pago efectivo-bf"-, siendo que añadiendo a dicho importe el total de operaciones realizadas hasta antes del 25 de mayo de 2020, se obtiene como monto resultante el importe de S/ 9 991,81, el mismo que no superaba el **máximo total registrado** por el señor Yataco en el mes de marzo de 2020, por la suma ascendente a **S/ 25 725,00.**

29. De la misma forma, se tiene que de la suma comprendida por el importe correspondiente a la operación objetada del 24 de junio de 2020, ascendente a S/ 9 597,00 -bajo la glosa de "Pago efectivo-bf"-, y el total de operaciones realizadas hasta antes del 24 de junio de 2020, se obtiene como monto resultante el importe de S/ 10 842,00, el mismo que no superaba el **máximo total registrado** por el señor [redacted] el mes de marzo de 2020, por la suma ascendente a **S/ 25 725,00.**

30. Asimismo, de la revisión del registro histórico de consumos del titular de la cuenta de ahorros en cuestión, se desprende que el denunciante había efectuado diversas operaciones vía Banca Móvil, motivo por el cual dicho canal, que además coincidía con el que fue empleado para la ejecución de las operaciones controvertidas, tampoco resultaba ajeno al comportamiento habitual de consumo de la cliente.

31. Por consiguiente, la Vocal que suscribe el presente Voto considera que las operaciones controvertidas **no** se encontraban fuera del comportamiento habitual de consumo de la cliente, por cuanto resultaban concordes al registro histórico del canal, frecuencia y cuantía de consumos individuales exhibido por el denunciante.

32. Habiéndose determinado ello, la suscrita manifiesta su conformidad con el análisis desarrollado por el Colegiado en mayoría, respecto del procesamiento válido de las operaciones cuestionadas, efectuadas: (i) vía banca móvil (ascendentes a S/ 3 196,30 y S/ 5 900,00), en la medida que se verificó que estas fueron válidamente autorizadas a través del empleo del correcto ingreso de la clave secreta y la clave digital para el acceso al aplicativo del Banco y la consecuente autenticación de cada operación a través del envío vía SMS y el correcto ingreso de la clave dinámica; y, (ii) vía página web (establecimiento comercial), mediante la consignación de los datos impresos de la tarjeta de débito de titularidad del denunciante en la página web del establecimiento comercial respectivo, para luego proceder con la validación de la operación en cuestión (ascendentes a S/ 9 597,00) a través del envío vía SMS y el correcto ingreso de la clave dinámica.

33. Por consiguiente, la vocal que suscribe el presente voto estima pertinente revocar, por fundamentos distintos al Colegiado en mayoría, la resolución recurrida, en el extremo que declaró fundada la denuncia interpuesta contra el Banco, y en consecuencia, declarar infundada la misma, por presunta

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

infracción de los artículos 18° y 19° del Código, al haber quedado acreditado que dicho proveedor adoptó las medidas de seguridad requeridas para el procesamiento de tres (3) operaciones efectuadas con cargo a la Cuenta de Ahorros 679-*****500 de titularidad del denunciante, el 25 de mayo de 2020 (ascendentes a S/ 3 196,30 y S/ 5 900,00) y 24 de junio de 2020 (ascendente a S/ 9 597,00)

ROXANA MARÍA IRMA BARRANTES CÁCERES

INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

RESOLUCIÓN QUE DECLARA AGOTADA LA VÍA ADMINISTRATIVA

Indecopi

TRIBUNAL DE DEFENSA DE LA COMPETENCIA
Y DE LA PROPIEDAD INTELECTUAL
Sala Especializada en Protección al Consumidor

CÉDULA DE NOTIFICACIÓN

Lima, 27 de junio de 2022

Expediente en comisión 0409-2021/CC1

Señor (es)
JUAN ANDRES YATACO CASAS
CORREO-E [redacted]
LIMA, LIMA, LIMA CERCADO.-

De mi consideración:

Adjunto a la presente, copia de la Resolución N° 1267-2022/SPC-INDECOPI, emitida por la Sala Especializada en Protección al Consumidor del Tribunal de Defensa de la Competencia y de la Propiedad Intelectual del INDECOPI, en su sesión de fecha 21 de junio de 2022.

Atentamente,

Firmado digitalmente por SANCHEZ FONSECA Cecilia Violeta FAU 20133840328 hard
Motivo: Soy el autor del documento
Fecha: 28.06.2022 16:00:00 -05:00

CECILIA VIOLETA SÁNCHEZ FONSECA
Ejecutivo 1 – Coordinadora Legal

Adj.: Copia de la Resolución N° 1267-2022/SPC –INDECOPI

- La resolución adjunta agota la vía administrativa, de conformidad con lo dispuesto en el literal e) del artículo 228° del Decreto Supremo 004-2019-JUS, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General.
- La resolución adjunta puede ser impugnada ante el Poder Judicial a través del proceso contencioso administrativo dentro del plazo de 3 meses posteriores a la notificación de la misma, de conformidad con lo dispuesto en el artículo 18.1 del Decreto Supremo 011-2019-JUS, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley 27584, Ley que Regula el Proceso Contencioso Administrativo.
- Se informa a los administrados que, conforme a la Sexta Disposición Complementaria Final del Decreto Legislativo N° 1511, durante los Estados de Emergencia Sanitaria y Emergencia Nacional establecidos por el Gobierno Nacional, las notificaciones de los actos administrativos y demás actuaciones emitidas por el INDECOPI en el marco de los procedimientos administrativos que se inicien y los que se encuentran en curso, se realizan vía correo electrónico u otro medio digital.
- Cabe señalar que la citada norma establece que la notificación dirigida a la dirección de correo electrónico señalada por el administrado se entiende válidamente efectuada cuando el INDECOPI remita la comunicación, surtiendo efectos al día siguiente de la remisión del correo electrónico.
- Para información sobre el procedimiento, usted podrá visitar nuestro Sistema de Seguimiento de Expedientes en la siguiente dirección electrónica: http://servicio.indecopi.gob.pe/portalSAE/.
- La cita para lectura de expedientes queda suspendida temporalmente.

Ingreso en sala N° 2606-2021/SPC-APELACION