PONTIFICIA UNIVERSIDAD
CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

Informe Jurídico de Resolución N°1267-2022/SPC-INDECOPI Patrón de consumo habitual ¿INDECOPI realiza una correcta evaluación sobre el concepto?

Trabajo de Suficiencia Profesional para optar el Título de Abogada que presenta:

Nicole Adriana Gamarra Aliaga

ASESOR:

Carlos Jesús Zúñiga Melgarejo

Lima, 2025

Informe de Similitud

Yo, ZUÑIGA MELGAREJO, CARLOS JESUS, docente de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, asesor(a) del Trabajo de Suficiencia Profesional titulado “Informe Jurídico de Resolución N°1267-2022/SPC-INDECOPI – Patrón de Consumo ¿En verdad protege al consumidor?”, del autor(a) GAMARRA ALIAGA, NICOLE ADRIANA, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 29%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 27/02/2025.

- He revisado con detalle dicho reporte y el Trabajo de Suficiencia Profesional, y no se advierten indicios de plagio.

- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lima, 27 de febrero del 2025

ZUÑIGA MELGAREJO, CARLOS JESUS	
DNI: 70818401	Firma: 
ORCID: https://orcid.org/0009-0002-9463-2895	

AGRADECIMIENTOS

En primer lugar, agradezco a mis padres Héctor y Gloria, por brindarme el apoyo incondicional en este largo camino profesional que me ha llevado a este punto de mi carrera, por todo el esfuerzo que hicieron hasta el día de hoy para que yo pueda cumplir mis objetivos personales y académicos. El cariño de ellos fue lo que me impulsaba cada día para poder perseguir mis sueños y metas a pesar de las difíciles circunstancias que se han suscitado en los últimos años. A Nicolás, mi hermano que siempre me brinda una motivación extra cada que nos vemos, con su energía y entusiasmo me ayuda a mantenerme enfocada en mis metas.

Agradecer a mis docentes por haber compartido y transmitido sus conocimientos necesarios para poder redactar el presente informe. Por su apoyo en cada consulta y cuestionamiento que han sido absueltos por el amor a la carrera.

Por último, agradecer a Indira y Greyci, quienes han sido parte importante en este largo camino profesional, por el apoyo mutuo en todos estos años frente a las circunstancias que atravesábamos juntas. Agradezco de tener unas grandes profesionales como amigas que me brindó la Universidad.

DEDICATORIA:

A mis padres, por su apoyo incondicional.

A mi hermano Nicolás, por impulsarme a seguir adelante.

A mis mejores amigas, quienes siempre estuvieron para mí.

A Lukita, por ser mi fiel compañerito en tiempo de estudio.

Nicole.

RESUMEN

El presente informe se enfoca en la interpretación y análisis de la Sala Especializada de Protección al Consumidor del INDECOPI, acerca de un caso controversial de operaciones no reconocidas y las medidas de seguridad que brindó la empresa financiero, analizando tipo de evaluación que la Sala realiza para poder identificar si las operaciones correspondían efectivamente a operaciones usuales por parte del usuario, o en realidad eran tomadas como inusuales, por lo que el banco debió haber bloqueado inmediatamente la tarjeta del consumidor. En ese sentido, se realizará un análisis de las operaciones efectuadas, si estas han sido efectuadas por el uso de las tarjetas o han sido materializadas por otras vías alternas que brindan las empresas financieras, sean los aplicativos móviles o banca por internet. Asimismo, un análisis de que normativa aplicable debería de ser evaluada y desarrollada dentro del caso. Por último, se abordará la evaluación del concepto de patrón de consumo habitual dentro de los hechos ocasionados y en la casuística diaria frente a este tipo de operaciones y similares.

Palabras clave

Operaciones no reconocidas, patrón de consumo habitual, medidas de seguridad, fraude electrónico, deber de idoneidad.

ABSTRACT

This report focuses on the interpretation and analysis of the Specialized Consumer Protection Chamber of INDECOPI, regarding a controversial case of unrecognized operations and the security measures provided by the financial company, analyzing the type of evaluation that the Chamber carries out to to be able to identify whether the operations actually corresponded to usual operations by the user, or were actually considered unusual, so the bank should have immediately blocked the consumer's card. In this sense, an analysis of the operations carried out will be carried out, whether they have been carried out through the use of cards or have been carried out through other alternative means provided by financial companies, whether mobile applications or internet banking. Likewise, an analysis of what applicable regulations should be evaluated and developed within the case. Finally, the evaluation of the concept of habitual consumption pattern within the events caused and in the daily caseload regarding this type of operations and similar ones will be addressed.

Keywords

Unrecognized operations, habitual consumption pattern, security measures, electronic fraud, duty of suitability.

ÍNDICE

PRINCIPALES DATOS DEL CASO

No. Exp. / No. Resolución o sentencia / nombre del caso	Exp. N° 0409-2021/CC1 / RESOLUCIÓN 1267-2022/SPC-INDECOPI / YATACO VS SCOTIABANK
Área(s) del derecho sobre las cuales versa el contenido del presente caso	Deber de idoneidad, Servicios Financieros, Derecho Administrativo – Protección al Consumidor Sector Bancario
Identificación de las resoluciones y sentencias más importantes	• Informe Final de Instrucción 0624-2021/CC1-ST • Resolución 2545-2021/CC1 • Resolución 1267-2022/SPC-INDECOPI
Demandante / Denunciante	Juan Andrés Yataco Casas
Demandado / Denunciado	Scotiabank Perú S.A.A.
Instancia administrativa o jurisdiccional	Tribunal de Defensa de la Competencia y de la Propiedad Intelectual Sala Especializada en Protección al Consumidor - INDECOPI
Terceros	-
Otros	-

I. INTRODUCCIÓN

1.1 Justificación de la elección de la resolución

Dentro del caso a desarrollar, podemos encontrar la discusión del concepto de "comportamiento habitual de consumo del usuario". El término en mención, se encuentra dentro del artículo 17 del Reglamento de Tarjetas de Crédito y Débito (en adelante, el Reglamento), el cual establece las Medidas de seguridad respecto al monitoreo y realización de las operaciones. Para ello, encontramos que hay dos posiciones que se contraponen, siendo la primera, la de la mayoría de los Vocales; los cuales concluyeron que para determinar el "comportamiento habitual de consumo del usuario" toda vez que evalúan, únicamente, el consumo total efectuado por el usuario en el mes. No obstante, encontramos la otra posición de la vocal Roxana María Irma Barrantes Cáceres, cuya postura se fundamenta en que este concepto debería ser evaluado mediante un análisis individual de las operaciones realizadas por los usuarios, es decir, para que se cumpla el deber de idoneidad de las entidades financieras en este caso, debería de examinar más minuciosamente distintos factores como el monto, frecuencia, canal, que establezca las características propias de cada cliente. Por tanto, siguiendo esta idea, lo que se quiere lograr con esta forma de analizar el consumo habitual del cliente, es que tengamos un patrón de los consumos habituales efectuados por los usuarios. En ese sentido, teniendo en cuenta ambas posturas nos enfrentamos con una situación particular, que son los consumos extraordinarios que realizarían los usuarios de vez en cuando, siendo operaciones que no son usuales por su misma naturaleza, siendo sus propios consumos, mas no producto de un fraude electrónico. Entonces, cabe la pregunta si el banco se encuentra en la obligación de cumplir con lo que establece el numeral 2 del artículo 22 del Reglamento, el cual establece las acciones de bloquear la tarjeta del usuario, al haber sido consumos realizados por el mismo usuario; sin embargo, no es una operación habitual de este.

En segundo lugar, encontramos otro tema controversial dentro de la Resolución, el cual es que se está teniendo en cuenta al Reglamento para evaluar operaciones realizadas por el aplicativo móvil de la entidad financiera. Es necesario tener en cuenta que el Reglamento promueve "el reforzamiento de

medidas de seguridad empleadas por las empresas del sistema financiero que emitan tarjetas de crédito para efectos de verificar la identidad del titular o usuario de la tarjeta y limitar el uso fraudulento de dichos medios de pago"[1]. Ello refiere que el Reglamento y sus disposiciones solo refieren a las operaciones que se han efectuado mediante tarjeta de crédito. No obstante, en el presente caso nos encontramos ante operaciones ligadas a una tarjeta de débito y la cuenta de ahorros ligada a esta. Entonces, teniendo ello en cuenta, encontramos otra interrogante sobre la consecuencia en los casos que se realizaron operaciones sin el uso de la tarjeta de crédito/debito del usuario, solo se efectuaron las operaciones por su cuenta de ahorros u otro producto que no sea la tarjeta de la entidad financiera. Esta pregunta es necesaria para el desarrollo del caso, toda vez que dos de las operaciones no reconocidas han sido efectuadas por el aplicativo móvil de la entidad financiera, mas no de la misma tarjeta del usuario.

En conclusión, encontramos que la presente Resolución tiene distintas interrogantes cuya evaluación es necesaria para poder mitigar las vulneraciones que reciben los usuarios de las entidades financieras.

1.2 Presentación del caso

La Resolución trae a colación el problema entre el señor Juan Andrés Yataco Casas (en adelante, Sr. Yataco) y la entidad financiera Scotiabank Perú S.A.A. (en adelante, el Banco), teniendo como el principal problema sobre tres operaciones no reconocidas por parte del Sr. Yataco que dos de ellas habrían sido efectuadas por el aplicativo móvil del Banco y una de ellas por el uso de la tarjeta.

Teniendo esta breve introducción del caso, podemos observar que existen problemas que destacan, una de ellas es la identificación de consumos habituales del usuario para poder identificar que las operaciones efectuadas han constituido operaciones inusuales. En este caso, la entidad financiera debió haber advertido por las medidas de seguridad respecto al monitoreo y realización

[1] Resolución S.B.S. N º264-2008 / Reglamento de Tarjetas de Crédito

de las operaciones que se encuentra obligado a realizar por lo establecido en el artículo 17 del Reglamento.

En adición a ello, encontramos un problema adicional accesorio que es la evaluación de la aplicación del Reglamento en el presente caso, toda vez que esta norma solamente aplicaría a las operaciones que han sido efectuadas por tarjetas de débito o crédito. Como bien se ha mencionado en el primer párrafo de este punto, se han efectuado dos operaciones mediante el aplicativo móvil del Banco, sin haber hecho uso de la tarjeta del usuario, si bien ambos son productos que otorga la entidad financiera, debemos de tener en consideración que ambos son productos distintos, que tienen una operación similar pero no igual. Por tanto, la pregunta recae en que norma es la idónea y precisa para poder analizar el caso de las operaciones realizadas por aplicativo móvil. Adicional a ello, se debe evaluar la diligencia del usuario, en este caso del Sr. Yataco, al haber bloqueado sus tarjetas inmediatamente y haber interpuesto denuncia policial una vez efectuados estas operaciones no reconocidas.

Al tener información sobre los acontecimientos de los hechos y las posibles interrogantes que se crean a partir de estos, encontramos dos posturas, la de la mayoría de los Vocales, el cual consiste en la evaluación de consumo habitual sobre la totalidad del monto consumido por mes, siendo que el consumo habitual de una persona no debería de exceder este monto total; por otra parte, encontramos el voto en discordia de la Vocal Roxana Barrantes, la cual menciona que la evaluación sobre el consumo habitual debería de ser sobre un análisis individual de cada consumo que ha ido realizando el usuario a lo largo del tiempo desde que obtuvo el producto del banco, y poder entender cuáles eran sus consumos habituales, teniendo en cuenta diferentes factores como el lugar de consumo, los tipos de comercio que se dirige, frecuencia, canales donde se realizaron las operaciones, los montos realizados, entre otros, de manera que puedan ser evaluadas individualmente y no se realice una comparación de los montos consumidos mensualmente.

Para apoyar mi posición sobre el presente caso y su posible solución a las problemáticas derivadas de este, considero que los principales instrumentos normativos serán los siguientes:

- Resolución S.B.S. N° 6523-2013 / Reglamento de Tarjetas de Débito y Crédito
- Ley 29571 / Código de Protección y Defensa del Consumidor
- Ley N° 29985 / Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.
- Resolución S.B.S. N° 504-2021 / Reglamento para la Seguridad de la Información y la Ciberseguridad (Aprobada en fecha 19 de Febrero de 2021, y vigencia a partir de Julio del 2021)

II. IDENTIFICACIÓN DE LOS HECHOS RELEVANTES

2.1. Antecedentes

- En fecha 24 de Mayo de 2020, el Sr. Yataco advirtió que se efectuaron dos operaciones no reconocidas dentro de la cuenta de ahorros que tenía con el Banco, siendo una operación realizada con su tarjeta de débito con el concepto “debito compras” por el monto S/.3,196.30 soles y otra por una operación con el aplicativo móvil con el concepto “pago efectivo-bi” por el monto S/. 5,900.00 soles. El Sr. Yataco procede a bloquear la tarjeta vinculada a esa cuenta de ahorros inmediatamente.
- El 24 de Junio del mismo año intentó efectuar una operación sin resultado efectivo; sin embargo, se había realizado otra operación no reconocida con el mismo concepto de “pago efectivo-bi” por el monto de S/. 9,597.00 soles por el aplicativo móvil. De la misma manera que en las anteriores operaciones, el Sr. Yataco procede a bloquear el producto financiero.
- Con fecha 22 de Febrero de 2021, el Sr. Yataco procede a denunciar al Banco por presunta infracción de deber de idoneidad ante el Órgano Resolutivo de Procedimientos Sumarísimos de Protección al Consumidor N°2.

2.2 Hechos relevantes del caso

a. Defensa del Banco Scotiabank

Con fecha 29 de Abril de 2021, el Banco presentó sus descargos, de acuerdo con el siguiente detalle:

- Las operaciones que tenían el concepto de **"pago efectivo-bi"** han sido efectuadas desde el aplicativo móvil, y estas han sido acreditas con el uso de su contraseña y clave digital, siendo esta última enviada al número del cliente.
- La operación de consumo con el concepto de "debito compras" ha sido válidamente autorizada.
- Era imposible determinar si ha sido o no el Sr. Yataco quien efectuó las operaciones suscitadas, ya que el sistema de la entidad financiera validó las claves ingresadas, siendo estas las correctas.

b. Informe Final de Instrucción

Con fecha 06 de Setiembre de 2021, la Secretaría Técnica de Comisión de Protección al Consumidor N°1 emite el Informe Final de Instrucción N° 0624-2021/ST-CC1 (en adelante, el IFI) llegó a las conclusiones que el Banco habría vulnerado los artículos 18 y 19 del Código de Protección y Defensa del Consumidor (en adelante, el Código de Consumo), toda vez que no ha quedado acreditado que el Banco adoptó medidas de seguridad pertinentes ante estas tres operaciones no reconocidas.

Asimismo, recomienda sancionar a el Banco con una multa de 4.25 UIT por la infracción 18 y 19 del Código de Consumo.

c. Observaciones del Banco ante el Informe Final de Instrucción

El 14 de Setiembre del mismo año, el Banco presenta sus observaciones ante el IFI, recalcando que las operaciones en cuestión fueron autorizadas válidamente desde el aplicativo móvil de la representada. Asimismo, la operación realizada con la tarjeta de débito fue efectuada con los datos de la tarjeta que solo tendría y debería tener acceso el Sr. Yataco.

d. Resolución de Primera Instancia

Con fecha 22 de Setiembre de 2021, la Comisión de Protección al Consumidor – Sede Lima Sur N° 1, mediante Resolución 2545-2021/CC1, emite su decisión conforme a los siguientes puntos:

- Declaró fundada la denuncia interpuesta por el Sr. Yataco por infracción de los artículos 18 y 19 del Código de Consumo, toda vez que no ha quedado acreditado que el Banco haya adoptado medidas de seguridad pertinentes.
- Sancionó al Banco con una multa de 4.25 UIT por las infracciones mencionadas en el punto anterior.
- Ordena que cumple con pagar el importe de S/. 18,693.30 soles, el ascendente total de las operaciones no reconocidas

e. Apelación del denunciado

El 21 de Octubre del mismo año, el Banco apeló la Resolución de primera instancia en base a los siguientes argumentos:

- Con respecto a las operaciones de concepto “pago efectivo-bi”, el Banco presentó capturas de sus sistemas internos con la finalidad de demostrar que los ingresos al aplicativo móvil y la autenticación de las operaciones efectuadas han sido realizados válidamente, debido a que se envió un por vía SMS y correo electrónico el acceso a su banca móvil.
- Dentro de las capturas de pantallas brindadas, se encuentra la consignación de “Successfull” que acredita que el registro y validación de claves han sido efectuadas debidamente.
- Solicita la aplicación de Presunción de Veracidad para considerar las capturas de pantallas se considerarán presentes para la evaluación.
- Con respecto a la operación de “debito compras”, insistió que se realizó la compra con los datos correctos de la tarjeta y datos del tarjetahabiente.

f. Resolución de Segunda Instancia

Con fecha 20 de Junio de 2022, la Sala Especializada en Protección al Consumidor emite Resolución N°1267-2022/SPC, en la cual considera los siguientes argumentos con respecto a las operaciones no reconocidas:

- Para el análisis de medidas de seguridad tenían que evaluar sobre el comportamiento habitual de consumo del usuario y para ello efectúan una revisión de los estados de movimientos de la Cuenta de Ahorros del usuario. No obstante, este análisis realiza la comparación del monto totalmente consumido mensualmente frente a los demás meses.
- La Sala se percata que el mes que tuvo el consumo más alto fue el de marzo de 2020, siendo este el monto de S/.25,725.00. Monto que superaba el monto total de las operaciones no reconocidas. Por tanto, el Banco no se encontraba en la obligación de generar alguna alerta por operación inusual o fraudulenta.
- Con respecto a la validez de las operaciones cuestionadas, la Sala considera que las operaciones realizadas han sido validadas satisfactoriamente por el usuario, toda vez que las capturas de pantallas brindadas por el banco demuestran que el Banco cumplió con verificar que el ingreso al aplicativo móvil se haya validado correctamente. Recalcó que, en caso de las operaciones con tarjeta de crédito y débito no se puede verificar que hayan sido de uso fraudulento y que el resguardo de los datos de esta es responsabilidad exclusiva del tarjetahabiente.

De acuerdo con los puntos anteriormente mencionados, la Sala resuelve lo siguiente:

- Revoca la Resolución de Primera Instancia, declarando infundada la denuncia interpuesta por el Sr. Yataco, ya que queda acreditado que el Banco sí habría adoptado medidas seguridad respectivas.
- Deja sin efecto el extremo de la sanción de 4.25 UIT.

No obstante, es pertinente mencionar que una de las vocales de la Sala emite un voto singular con respecto a la evaluación acerca del concepto del “consumo habitual”.

g. Voto singular en discordia de la Vocal Roxana María Irma Barrantes Cáceres

La Vocal Barrantes, emite un voto singular en la misma Resolución de Segunda Instancia, dentro del cual, emite su propia evaluación referente al concepto de "consumo habitual" conforme al siguiente detalle:

- Con respecto al artículo 17 del Reglamento, es obligación de toda entidad financiera de conocer el comportamiento habitual de consumo de sus clientes, por la recopilación de información y seguimiento de sus movimientos.
- Enfatiza que la medición de este consumo habitual no debe estar delimitada al consumo total mensual generado por cada cliente, sino debe verificarse si el importe de estas operaciones atendía a los consumos usuales o cotidiano dispuesto por el consumidor en operaciones anteriores individualizadas.
- Para la evaluación de identificar si las operaciones realmente fueron inusuales, se realiza una comparación de la cantidad de consumos en los cuatro primeros meses de ese año, el consumo mayor en el periodo, el monto total de consumos en el mes y la cantidad consumos máximo por día.
- Llega a la conclusión que los montos de las operaciones no reconocidas no podrían haber sido reportados como operaciones inusuales, toda vez que la operación máxima individual que había realizado el usuario había sido por la suma de S/.18,000.00 soles en el mes de Marzo.

III. IDENTIFICACIÓN DE LOS PRINCIPALES PROBLEMAS JURÍDICOS

Podemos observar que la presente Resolución contiene ciertos problemas jurídicos que son de análisis relevante para el desarrollo del caso.

3.1 Problema principal

La cuestión fundamental que aborda toda la resolución es la interpretación del concepto de "consumo habitual" del usuario lo que traería como

consecuencia la identificación de operaciones inusuales. En ese contexto, la pregunta principal que viene a colación es:

- ***¿El Banco Scotiabank aplicó medidas de seguridad en las operaciones no reconocidas que advirtió el Sr. Yataco? ¿Va acorde a los fallos que INDECOPI venía resolviendo?***

3.2 Problemas secundarios

Para poder tener una respuesta clara sobre ello, también considero que debería evaluarse las siguientes preguntas:

- ***¿Cabe aplicar el Reglamento de Tarjetas de Crédito y Débito a pesar de que dos de las operaciones hayan sido realizadas por aplicativo móvil sin haber realizado uso de la Tarjeta del usuario?***
- ***¿Qué medidas preventivas debe tomar las entidades financieras para evitar operaciones presuntamente fraudulentas?***
- ***¿Cuáles son las características que las entidades financieras deberían de tomar en cuenta y generar un "patrón de consumo habitual" de sus usuarios?***

3.3 Problema complementario

Por último, cabe ahondar en la falta de valoración de pruebas que INDECOPI debió haber realizado en el presente caso con respecto a las medidas de seguridad que debió implementar frente a las operaciones no reconocidas:

- ***¿INDECOPI realizó una valoración de pruebas adecuada acerca de la evaluación de "patrón de consumo habitual" y acerca de las medidas de seguridad que el Banco debió aplicar en las operaciones que no se encontraban procesadas al momento del bloqueo de su tarjeta?***

IV. POSICIÓN DEL CANDIDATO/A

4.1 Respuestas preliminares a los problemas principal y secundarios

¿El Banco Scotiabank aplicó medidas de seguridad en las operaciones no reconocidas que advirtió el Sr. Yataco? ¿Va acorde a los fallos que INDECOPI venía resolviendo?

Conforme al principio de Pro Consumidor, y el deber de Idoneidad de las empresas, junto con la aplicación de las normas pertinentes, la idea es buscar una solución que mejore la identificación de consumos no habituales. Para ello deberíamos de tener en cuenta las Resoluciones que, tanto de la Comisión como de la Sala venían evaluando, así como las características que debía tener las operaciones no reconocidas para que las entidades financieras alerten sobre una presunta operación fraudulenta. Asimismo, se deberá tener en cuenta las obligaciones que tienen las entidades financieras frente a sus usuarios de acuerdo con la normativa vigente que se viene evaluando ante este tipo de casos. Es pertinente mencionar, que en el presente caso, las medidas de seguridad adoptadas por el banco deben guardar relación con la modalidad en que estas se efectuaron junto con los factores de autenticación que establece la normativa emitida por la SBS para la protección de las operaciones efectuadas por los usuarios dentro del sistema financiero. En ese sentido, se tendrá que evaluar si el banco cumplió con todo lo establecido en la norma y teniendo en cuenta la evaluación que se ha venido realizando por INDECOPI.

¿Cabe aplicar el Reglamento de Tarjetas de Crédito y Débito a pesar de que dos de las operaciones hayan sido realizadas por aplicativo móvil sin haber realizado uso de la Tarjeta del usuario?

Al referirnos a productos que ofrecen las entidades bancarias que se encuentran vinculadas a las Tarjetas de Débito y Crédito, se debería aplicar el Reglamento mencionado. De acuerdo con el deber de idoneidad que los proveedores se encuentran obligados a brindar a los usuarios, estos deben de tomar en consideración la normativa emitida por la SBS enfocadas a una garantía legal que brinda el proveedor a los usuarios respecto a los productos y/o servicios. Asimismo, de acuerdo con las nuevas modalidades de transferencia de dinero,

se debe tener en cuenta la normativa que regula las mismas y analizar si son pertinentes dentro del caso, toda vez que van de la mano con las operaciones que realizan los usuarios en el día a día. Por ello, considero relevante analizar la Ley N° 29985, Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.

Por tanto, considero que sí se debería de aplicar el Reglamento, pero no solo limitarnos a lo que se establece en dicho cuerpo legal, sino también, trayendo a colación diferentes normativas que refuerce las medidas de seguridad que las entidades financieras se encuentran obligadas a brindar a los usuarios.

¿Qué medidas preventivas debe tomar las entidades financieras para evitar operaciones presuntamente fraudulentas?

Si bien las medidas de seguridad se encuentran establecidas dentro del Subcapítulo I del Reglamento, debemos considerar que los proveedores deberían atender ciertos parámetros que van de la mano con el concepto de patrón de consumo habitual para identificar que tipo de operaciones se encuentran asociadas a las transacciones que efectúan los usuarios de los productos financieros. Asimismo, tener en cuenta que estas medidas de seguridad no deberían de limitarse a operaciones que se efectúen con el producto específicamente de las tarjetas de crédito o débito; sino que también se debe considerar los productos que ofrece el banco porque se está viendo involucrado el deber de idoneidad que debe ofrecer las entidades financieras. En ese sentido, las operaciones que realicen los usuarios serán determinados no solamente por el tipo de producto, sino también el historial de operaciones que cada producto financiero se encuentra realizando desde que el usuario adquirió el mismo. De esta manera, se podrá precisar de manera específica el patrón de consumo de cada producto que posee el usuario.

¿Cuáles son las características que las entidades financieras deberían de tomar en cuenta y generar un "patrón de consumo habitual" de sus usuarios?

Si bien esta pregunta ya se encuentra dentro de la definición del numeral 5 del artículo 2 del Reglamento, es necesario mencionar que INDECOPI ha venido evaluando este concepto basándose únicamente en los montos de las operaciones no reconocidas que los usuarios han advertido. Si bien es cierto que el monto de las operaciones es un punto muy importante a tener en cuenta dentro del análisis del concepto de "patrón de consumo" debemos analizar los demás factores como lo es el tipo de comercio, canal por el que se ejecutó las operaciones, lugar de consumo, frecuencia del mismo, entre otras características que van en conjunto con el histórico de movimientos de los usuarios. En ese sentido, la Sala también debería de realizar este análisis con respecto a estos factores, sin limitarse únicamente a los montos controvertidos de la operación.

¿INDECOPI realizó una valoración de pruebas adecuada acerca de la evaluación de "patrón de consumo habitual" y acerca de las medidas de seguridad que el Banco debió aplicar en las operaciones que no se encontraban procesadas al momento del bloqueo de su tarjeta?

De acuerdo a este punto, nos enfocaremos principalmente en la omisión por parte de INDECOPI en no tomar en cuenta los medios probatorios que ha remitido tanto el denunciante como el Banco Scotiabank. Para ello, analizaremos si la Resolución Final recabó la suficiente información para poder emitir un fallo acorde al Principio de Verdad Material, la cual se encuentra establecida dentro de la Ley de Procedimiento Administrativo General. Al no tener en cuenta este principio, la Resolución no se encuentra motivada debidamente, puesto que no recurrió a la obtención de toda información pertinente y suficiente para concluir si el Banco empleó o no las medidas de seguridad correspondientes. Es fundamental tener en cuenta que el patrón de consumo habitual no solo se enfoca en los montos que se ha venido realizando por los seis últimos meses, sino que también los demás factores que alega el Reglamento como el tipo de comercio, frecuencia y canal en las que se realizan los movimientos. No

obstante, este tipo de evaluación no se encuentra realizado en ninguna de las instancias de INDECOPI, siendo que la Sala se pronuncia únicamente si los montos de las operaciones no reconocidas se encontraban dentro de su patrón de consumo habitual, dejando de lado los demás factores. Ante este pronunciamiento, es claro que, tanto la Comisión como la Sala no emitió resolución alguna que requiera información tanto para el Banco como para el denunciante. Recordemos que ante las relaciones de consumo nos encontramos en una asimetría informativa, siendo el Banco en mejor posición de acreditar los hechos del presente caso, ya sea por el sistema que tiene implementado como la información sobre el flujo de procesamiento de operaciones.

4.2 Posición individual sobre el fallo de la resolución

La Resolución emitida por la Sala no tuvo suficiente motivación que fundamentara si las medidas de seguridad adoptada por el Banco fueron idóneas respecto a lo que establece la norma, toda vez que no se aprecia una evaluación sobre las características del consumo habitual del denunciante. Como se puede apreciar en la resolución solo se toma en cuenta el monto total consumido por mes del usuario; es decir, no se toma en consideración las demás características que se detalla en la norma como el tipo de comercio, la frecuencia, canal utilizado, entre otros factores o características que son fundamentales para poder tener una mayor precisión sobre el patrón de consumo habitual del Sr. Yataco y del producto financiero que se ven involucrados en el caso, el cual vendría ser la tarjeta de débito y su cuenta de ahorro, toda vez que son operaciones efectuadas con los datos de la tarjeta y mediante el aplicativo móvil.

Asimismo, considero que desde la Primera Instancia hubo una mala imputación de cargos, toda vez que no se ha tenido en consideración los medios probatorios brindados por el sr. Yataco, puesto que solo se ha imputado una presunta infracción al Banco, el cual versa sobre las tres operaciones no reconocidas, mas no toma en consideración los bloqueos de sus tarjetas que ha efectuado el denunciado cuando advirtió estas operaciones no reconocidas, siendo estas procesadas al siguiente día de haberlas bloqueado.

En esa línea de ideas, debemos de tener en cuenta que al ser un procedimiento sancionador únicamente se inicia de oficio ya que es la Secretaría Técnica que es encargada de imputar los cargos por presuntas infracciones, al igual que la emisión de las resoluciones de admisión de la denuncia, señalando los hechos y las presuntas infracciones derivados de estos.

Entonces, en mi posición, considero que, independientemente de la evaluación que realizan los vocales de la Sala, se debe tomar en consideración otros factores en relación a las medidas de seguridad que empleó el Banco y no solo enfocarse en los montos transferidos en dichas operaciones no reconocidas, hecho que no se encuentra desarrollado dentro de la Resolución.

V. ANÁLISIS DE LOS PROBLEMAS JURÍDICOS

Para poder analizar las múltiples preguntas que derivan de la Resolución, debemos responder primero las preguntas secundarias que nos guiarán con la respuesta de la pregunta principal.

5.1. ¿Cabe aplicar el Reglamento de Tarjetas de Crédito y Débito a pesar de que dos de las operaciones hayan sido realizadas por aplicativo móvil sin haber realizado uso de la Tarjeta del usuario?

Conforme a lo señalado anteriormente, encontramos que dos de las tres operaciones no reconocidas, no han sido efectuadas por el uso de tarjeta del usuario; sino que han sido realizadas por el uso del aplicativo móvil. En ese sentido, el objetivo del Reglamento es claro, dentro de su artículo 1, menciona que es aplicable a todas las empresas de operaciones múltiples autorizadas a expedir y administrar tarjetas de crédito y débito[2]. De la lectura de dicho artículo, entendemos que el Reglamento se enfocaría en las tarjetas que emite el banco, mas no en los aplicativos móviles donde se efectúan distintos tipos de operaciones; no obstante, debemos de tener en cuenta que se aplica a las empresas, mas no limita los productos que estas pueden ofrecer, lo que da

[2] Resolución S.B.S. N º6523-2013 / Reglamento de Tarjetas de Crédito y Débito.

cabida a que no se restringe únicamente a los productos de tarjetas de crédito y débito.

Dicho ello, considero pertinente señalar que, tanto en el artículo 7 y 13 del mismo cuerpo legal, se detallan los servicios adicionales asociados a las tarjetas de crédito y débito, respectivamente, estableciendo que "las operaciones realizadas a través de internet, desde páginas web y/o aplicaciones de dispositivos móviles, entre otros, distintos a los provistos por la empresa"[3]. Dicho ello, podemos advertir que los otros productos ofrecidos por las entidades financieras (cuentas de ahorro, cuentas de depósito a plazo fijo, cuenta sueldo, entre otros) y estén vinculadas a las tarjetas que contrata el usuario, será aplicable la norma en mención.

No obstante, cabe preguntarnos si solo basta la regulación de tarjetas de crédito y débito para el correcto funcionamiento de transacciones efectuadas mediante aplicativos móviles de las entidades financieras. Para ello, es importante precisar que este tipo de operaciones también tienen su propia regulación, para entrar más a detalle sobre este tema es fundamental traer a colación la Ley N°29985, Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera (en adelante, Ley de Dinero Electrónico), la que tiene por objeto, contemplada dentro de su artículo 1, la regulación de emisión de dinero electrónico, determinar las empresas autorizadas a emitirlo y establecer el marco regulatorio de estas empresas[4]. Asimismo, en su numeral dos, dispone que esta emisión comprende las operaciones de emisión del dinero electrónico, reconvención a efectivo, transferencias, pagos y cualquier movimiento u operación relacionada con el valor monetario del que disponga el titular[5].

De acuerdo con lo establecido líneas previas, es claro que esta ley regula las operaciones que se efectúan mediante los aplicativos móviles de las empresas financieras. No obstante, podemos ver un término novedoso, el cual es el de

[3] Ídem
[4] Ley N°29985, Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.
[5] Ídem

dinero electrónico, dentro del artículo 2 del cuerpo legal mencionado, lo definen como un valor monetario representado por un crédito exigible a su emisor[6], este tiene 5 características, las cuales son: i) almacenada en soporte electrónico; ii) aceptado como medio de pago por entidades o personas distintas al emisor, tiene efecto cancelatorio; iii) emitido por un valor igual a los fondos recibidos; iv) convertible en dinero en efectivo; v) no constituye depósito y no genera intereses[7]. Teniendo en cuenta la definición y característica del dinero electrónico que nos menciona la ley, debemos analizar el funcionamiento de este dentro del mercado; para ello, Rodriguez menciona que "el funcionamiento del dinero se inicia cuando el cliente (nacional o residente extranjero" se acerca a un agente (canal no bancario) y efectúa la conversión de dinero en dinero electrónico (dinero virtual) por el mismo valor entregado para su almacenamiento en un soporte electrónico"[8]. De acuerdo con lo mencionado, podemos apreciar que es un mecanismo que día a día podemos ver aplicado dentro del mercado. El uso de aplicativos móviles para realizar transferencias, pagos, recibir depósitos; el uso de las billeteras electrónicas para realizar consumos en diferentes establecimientos, son ejemplos de la dinámica que tiene el uso del dinero electrónico dentro de nuestra cotidianeidad.

De acuerdo con la definición y funcionamiento del dinero electrónico, nos sirve como una norma que complementa al Reglamento. En ese sentido, el artículo 17 del mismo establece las medidas de seguridad respecto al monitoreo y realización de las operaciones, las mismas que abarcan transacciones vía internet, páginas web y aplicaciones de dispositivos móviles (las cuales podrían ser los mismos aplicativos móviles de las entidades financieras). Además, debemos considerar que dentro del artículo 6 numeral 3 de la Ley de Dinero electrónico menciona lo siguiente:

> *"6.3* ***Contratos.*** *La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones establece las modalidades de contratación*

[6] Ídem
[7] Ídem
[8] Rodriguez, V. (2014) Dinero electrónico en Perú ¿Por qué es importante en la inclusión financiera? Quipukamayoc, Vol. 22 N°41, pp. 186.

aplicables al dinero electrónico, las que pueden ser escritas, electrónicas u otras, de acuerdo a la naturaleza de los productos, sus características y las circunstancias en que estos se ofrecen, ***en concordancia con lo dispuesto en la Ley 29571,*** *Código de Protección y Defensa del Consumidor;* ***la Ley 28587****, Ley Complementaria a la Ley de Protección al Consumidor en Materia de Servicios Financieros, y las* ***normas reglamentarias emitidas para garantizar su cumplimiento.****"*[9] (Subrayado mío)

Este detalla que la ley de dinero electrónico deberá de aplicarse en armonía con lo que establece el Código de Consumo y a la Ley de Protección al Consumidor. Por tanto, encontramos que los reglamentos también son aplicables dentro del uso del dinero electrónico.

La importancia de mencionar las normas de líneas precedentes tiene como fin la interpretación sistemática de la normativa involucrada en temas de protección al consumidor financiero. Ello, por el hecho que estas leyes son aplicables para las entidades financieras que emiten el dinero electrónico, y son las mismas que expiden y administran las tarjetas de crédito y débito, que resultan ser las mismas entidades financieras que son supervisadas por la SBS. De tal manera se estaría aplicando el Principio de Protección Mínima, establecida en el numeral 6 del mismo artículo, el cual establece que "el Código contiene las normas de mínima protección a los consumidores y no impide que las normas sectoriales puedan dispensar un nivel de protección mayor"[10].

En definitiva, si bien el Reglamento contemplan el uso de aplicativos móviles y operaciones vía internet, también debemos tener presente que dentro de nuestra legislación existe la Ley de Dinero Electrónico que es una norma complementaria aplicable en los casos que lo ameriten. En conclusión, sí es pertinente la aplicación del Reglamento en el presente caso y en la evaluación sobre las medidas de seguridad que brinda las entidades financieras hacia los usuarios que tienen productos con los mismos, sin limitarse únicamente al contrato de tarjetas de crédito o débito.

[9] Ley N°30096 / Ley de Delitos Informáticos
[10] Ley N°29571, Código de Protección y Defensa del Consumidor.

5.2. ¿Qué medidas preventivas debe tomar las entidades financieras para evitar operaciones presuntamente fraudulentas?

Para poder responder está pregunta, debemos recordar que dentro del subcapítulo I del capítulo IV del Reglamento establece las medidas de seguridad que deberían de ser aplicables a las tarjetas de crédito y débito; sin embargo, nos enfocaremos en los artículos 16 y 17. El artículo 16 se enfoca principalmente en las medidas de seguridad que deben adoptar frente al uso de los usuarios, es decir, la garantía legal que tienen las entidades financieras frente al usuario con respecto al producto que estos brindan al público en general. Considero importante enfatizar el numeral 7 del artículo en mención el cual establece que "el proceso de autenticación del usuario debe realizarse según lo establecido en el artículo 19 del Reglamento de Ciberseguridad, mediante factores categorizados en dicho reglamento; asimismo, señala que los proveedores deben seguir las recomendaciones técnicas de los estándares EMV emitidos por EMVCo dependiendo el tipo de operación que se ejecute"[11]. Es claro que los factores de autenticación serán distintas en cada caso, por lo que la norma establece los siguientes parámetros para cada operación:

> "7.1. Para operaciones con tarjeta presente se requieren dos factores, donde el primero es el chip de la tarjeta o su representación digital. El segundo factor puede ser una clave secreta (PIN) u otro que establezca la Superintendencia.
>
> 7.2. Para operaciones con tarjeta no presente se requieren dos factores, donde el primero son los datos contenidos en la representación física o digital de la tarjeta. El segundo factor puede ser un código de verificación dinámico de la tarjeta u otro factor verificable en línea requerido al usuario en el marco del estándar EMV 3DS (…)."[12]

Como podemos ver, los dos primeros numerales se enfocan en las operaciones que se efectúan con tarjeta presente o con tarjeta no presente. En ambos casos, es necesario que se valide con dos factores, en la operación con tarjeta presente se debe tener en cuenta el chip de la tarjeta (o representación digital) y la clave

[11] Resolución S.B.S. N º6523-2013 / Reglamento de Tarjetas de Crédito y Débito.
[12] Ídem

secreta (PIN) que es de único conocimiento por parte del usuario; en la operación con tarjeta no presente, el caso es distinto, lo que se necesita son los datos contenidos en la tarjeta, ya sea en la representación física o digital de la misma, y un código de verificación dinámico de la tarjeta. La principal entre los dos tipos de operaciones es el uso de PIN, en una es necesaria que se ejecute, en otra prescinden de la misma, pero es necesario los datos de la tarjeta y el código de verificación dinámico (el cual podría ser reemplazado con otro de acuerdo con el marco estándar EMV 3DS).

Ahora bien, dentro del caso, para la operación "débito compras" debe tenerse en cuenta estas medidas de seguridad que el proveedor debió ejecutar ante esta operación.

Cabe recalcar que el artículo no solo se enfoca en solo esos dos tipos de operaciones, sino también hace mención a otras operaciones como se muestra a continuación:

> "7.3. Para operaciones con billeteras móviles de terceros basadas en tokenización de tarjetas, la afiliación de la tarjeta para el uso de este servicio conforme al numeral 7.2 y las operaciones subsiguientes que se realicen deben ser autenticadas mediante la tokenización de la tarjeta y un segundo factor de distinta naturaleza.
>
> (…)
>
> 7.5 Para operaciones en que no se valide el segundo factor por limitaciones fuera de su control, la empresa debe establecer reglas de aceptación o rechazo, en función al nivel de riesgo de fraude, según el sistema de monitoreo de transacciones descrito en el artículo 17° del presente reglamento. Dichas limitaciones pueden estar asociadas al terminal de atención, las prácticas del comercio o la tecnología utilizada por el usuario"[13]

En estos supuestos, encontramos un tipo más de operación, la cual se enfoca en las operaciones por billeteras móviles de terceros que tienen como base a las tarjetas, y detalla el proceso de la afiliación con la tarjeta de los usuarios y las

[13] Ídem

siguientes operaciones que el usuario puede realizar con estas billeteras digitales. Por otro lado, en el inciso 5 detalla la consecuencia en caso el segundo factor no se encuentre validado, el cual sería que la entidad financiera tiene el deber de establecer reglas de aceptación o rechazo de acuerdo con el nivel de posible riesgo a fraude conforme muestra el sistema de monitoreo de transacciones del producto.

En aras de un mejor entendimiento al caso, considero pertinente desarrollar el término de billeteras digitales y el funcionamiento de la misma. La billetera digital es definida como "una aplicación móvil instalada en un celular que utiliza un proceso de enmascaramiento (…) para facilitar las transferencias entre usuarios de dicha billetera, que pueden ser clientes de la empresa del sistema financiero que la emitió o clientes de diferentes empresas"[14]. Como podemos ver esta billetera móvil tiene como objetivo facilitar las operaciones que usualmente los usuarios realizaban de manera presencial a un mecanismo digital por el aplicativo que desarrolló la entidad financiera. Debemos tener presente que el contexto de la expansión del uso de este tipo de aplicativos se desarrolla en el 2020, debido a las restricciones que estableció el Estado de Emergencia. Teniendo dicho contexto, el gobierno define a estas como "un aplicativo móvil que se descarga en tu celular para realizar operaciones financieras, sin contacto con dinero en efectivo, optimizando tu tiempo y, además, reduciendo la posibilidad de contagio de la COVID-19, pues puedes realizar tus operaciones sin salir de casa"[15]. Por tanto, podemos encontrar que ambas definiciones coinciden que se trata de un aplicativo móvil para realizar diferente tipo de operaciones por el mismo aplicativo que se encuentra en el celular del usuario.

De acuerdo con lo detallado en líneas precedentes, podemos encontrar que en este artículo se añade otra norma a tomar en cuenta, el cual es el Reglamento de Ciberseguridad dentro de la cual se establece los factores de autenticación

[14] Vega, M & Vasquez, J (2022) El Banco Central de Reserva del Perú y el desarrollo del Sistema de Pagos en el Perú.
https://www.bcrp.gob.pe/docs/Publicaciones/Revista-Moneda/moneda-189/moneda-189-03.pdf
[15] Presidencia de consejos de Ministros (S/F) Conocer más sobre las billeteras digitales disponibles en el Perú.
https://www.gob.pe/14930-conocer-mas-sobre-las-billeteras-digitales-disponibles-en-el-peru

para la ejecución de transacciones por parte de los usuarios que se detallará más adelante. No obstante, considero pertinente resaltar que este numeral fue añadido en el artículo 16 mediante Resolución SBS N°02286-2024, por lo que en fecha que ocurrió las operaciones no reconocidas, aún no se encontraba vigente esta normativa.

Ahora bien, debemos analizar el artículo 17 del Reglamento el cual se centra en el monitoreo y realización de las operaciones, conforme se establece a continuación:

> **"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 correspondan al comportamiento habitual de consumo del usuario.**
> 2. Implementar procedimientos complementarios para **gestionar 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."[16] (Subrayado mío)

Encontramos que se introduce el nuevo concepto de "comportamiento habitual de consumo del usuario", el cual se verá desarrollado gracias al sistema de monitoreo que deberán implementar las entidades financieras, de manera que pueda identificar patrones de fraude acorde al análisis sistemático de las operaciones que ha venido efectuando el usuario desde la obtención del producto.

De acuerdo con los artículos mencionados anteriormente, encontramos que la norma es clara con las medidas de seguridad que debería de adoptar las

[16] Resolución S.B.S. N º6523-2013 / Reglamento de Tarjetas de Crédito y Débito.

entidades financieras, las cuales abarca los factores de autenticación de transacciones efectuados tanto con las tarjetas físicas, no físicas y billeteras digitales; así como también se centra al sistema que debe implementar para detectar posibles operaciones que no corresponden al consumo habitual del usuario. En ese sentido, debemos recordar el deber de idoneidad que tienen las entidades financieras establecida en el artículo 18 del Código de Consumo, el cual dispone lo siguiente:

> "**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.
>
> (…)"[17] (Subrayado mío)

Asimismo, dentro del artículo 19 del mismo cuerpo legal, encontramos las obligaciones de los proveedores, que establece lo siguiente:

> "**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."[18] (subrayado mío)

[17] Ley N°29571, Código de Protección y Defensa del Consumidor.
[18] Ídem

De acuerdo con lo contemplado dentro del Código de Consumo, encontramos que el deber de idoneidad debe de brindar toda entidad que brinda un servicio o producto dentro del mercado. Asimismo, esta obligación de cada proveedor de brindar un servicio idóneo "como parte de la expectativa de los consumidores, genera que estos esperen de sus bancos la implementación de una serie de medidas en atención a la realidad comercial y el riesgo que involucran los sistemas financieros"[19].

Es claro que el deber de idoneidad abarca una amplia aplicación dentro de los servicios ofrecidos por parte de las entidades financieras; sin embargo, en esta ocasión nos centraremos solamente ante el funcionamiento idónea sobre las medidas de seguridad que estas se encuentran obligadas a prestar. Para ello, de acuerdo con la Resolución N°0124-2024/INDECOPI-CHT, dentro del punto 18, establece lo siguiente:

> "La Sala estima relevante puntualizar que, de acuerdo con la garantía legal contemplada en el Reglamento (…) **el parámetro de idoneidad en la prestación de servicios y productos financieros en el marco de la afectación de las cuentas o líneas de crédito de los consumidores,** se encuentra comprendido -de forma unívoca- por las medidas de seguridad atribuidas a las entidades financieras por la normativa sectorial, encontrándose entre ellas, **ineludiblemente, el deber de monitoreo y detección de consumos inusuales o sospechosos.**"[20] (subrayado mío).

Entonces, el deber de idoneidad tiene una interpretación que abarca no solamente a la prestación de servicio como crédito y ahorros, sino también al resguardo de las operaciones que se hacen de estos productos o servicios. Es así, que es pertinente la mención del artículo 20[21] del Código de Consumo, donde detalla las garantías que el proveedor brinda y está obligado, siendo legales, explícitas e implícitas. Para poder identificar qué tipo de garantía sería la adopción de medidas de seguridad implementadas por las entidades

[19] LEX. (2021, 29 de Noviembre) ¿Las medidas de seguridad forman parte del deber de idoneidad en la prestación de servicios financieros?. Pasión por el Derecho. https://lpderecho.pe/medidas-seguridad-deber-idoneidad-prestacion-servicios-financieros/

[20] Resolución N°0124-2024/CPC-INDECOPI

[21] Ley N°29571, Código de Protección y Defensa del Consumidor.

financieras frente a las operaciones no reconocidas, deberíamos de explicar cada una de ellas, de acuerdo a lo que menciona la norma son:

> "a. Una garantía es legal cuando por mandato de la ley o de las regulaciones vigentes no se permite la comercialización de un producto o la prestación de un servicio sin cumplir con la referida garantía. (…)
>
> b. Una garantía es explícita cuando se deriva de los términos y condiciones expresamente ofrecidos por el proveedor al consumidor en el contrato, (…)
>
> c. Una garantía es implícita cuando, (…) se entiende que el producto o servicio cumplen con los fines y usos previsibles para los que han sido adquiridos por el consumidor considerando, entre otros aspectos, los usos y costumbres del mercado"[22].

Como podemos apreciar de lo citado en líneas precedentes, el artículo 17 se detalla la implementación de los procesos de autenticación, los cuales deberá de efectuar las entidades financieras con el fin de proteger a sus usuarios frente a vulnerabilidades que se puedan presentar[23]. En ese sentido, la norma es clara al establecer dentro de su artículo 19 del Reglamento de Ciberseguridad, que, para las operaciones efectuadas por canal digital, se requiere una autenticación reforzada, requiriendo las siguientes condiciones:

> "a) Utilizar una combinación de factores de autenticación, según el literal j) del artículo 2 del presente Reglamento que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro.
>
> b) Generar un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez.
>
> c) Cuando la operación sea exitosa, notificar los datos de la operación al usuario."[24]

Por tanto, vemos que sí hay un reglamento que obliga a las entidades del Estado que implementen estas medidas dentro de su autenticación de operaciones, el cual es el Reglamento de Ciberseguridad, siendo este artículo ser leído

[22] Ídem
[23] Resolución S.B.S. N° 504-2021 / Reglamento para la Seguridad de la Información y la Ciberseguridad
[24] Ídem

conjuntamente con el artículo 17 del Reglamento de Tarjetas de Crédito y Débito que dispone las medidas de seguridad respecto al monitoreo y realización de las operaciones. Teniendo ello en cuenta, la garantía que impone el Reglamento es la de medidas de seguridad y el sistema de monitoreo de operaciones que se encuentran obligados a implementar.

En conclusión, las entidades financieras tienen que cumplir con las medidas de seguridad que establece el Reglamento, las cuales son el uso de factores de autenticación leído conjuntamente con lo que establece el Reglamento de Ciberseguridad; además del monitoreo de operaciones que deben implementar para determinar qué tipo de transacciones calzan como fraudulentas de acuerdo con el comportamiento habitual de consumo del usuario. En ese sentido, las entidades financieras se encuentran obligadas a implementar medidas de seguridad para que las operaciones realizadas por su tarjeta (o productos que se encuentren vinculadas a estas) sean efectuadas con factores de autenticación y generar alertas a los usuarios en caso se detecten transacciones fraudulentas.

5.3. ¿Cuáles son las características que las entidades financieras deberían de tomar en cuenta y generar un "patrón de consumo habitual" de sus usuarios?

En este capítulo nos centraremos en el concepto de "patrón de consumo habitual" o también conocido como el "comportamiento habitual de consumo" del usuario. Dentro del punto anterior, ya encontramos que hay un deber de resguardar por parte de las entidades financieras hacia sus propios usuarios, teniendo un monitoreo y realización de operaciones para identificar posibles transacciones fraudulentes. Cabe mencionar que la SBS se pronuncia al respecto del concepto de patrón de consumo, el cual establece que "se refiere 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 se determinados a partir de la información histórica de las operaciones de cada

usuario que registra la empresa"[25]. De lo anteriormente mencionado, está claro que la SBS tiene como definición que para una correcta evaluación de consumo habitual se debe de tener en cuenta distintos factores como los ya señalados.

Asimismo, dentro de la jurisprudencia emitida por el INDECOPI, encontramos que se ha señalado distintos análisis sobre el concepto, entre estos, encontramos a la Resolución 2041-2021/SPC-INDECOPI, la misma que señala lo siguiente:

> "la normativa sectorial exige que el patrón 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.**"[26]

La Sala advierte lo que indica la normativa acerca del análisis del patrón de consumo, el cual debería de ser analizado con una serie de factores sistemáticamente con la información histórica que recaba sobre el usuario. Este análisis se desarrolla de manera más amplia en el siguiente considerando el cual se detalla a continuación:

> "la información histórica a la que hace referencia la norma **no se encuentra limitada únicamente al patrón de consumo de la denunciante,** obtenido de la revisión del movimiento histórico de transacciones de cada tarjetahabiente en particular, sino que también puede deducirse de las **características de cada operación en particular y de cómo estas singularidades, en atención a la información que maneja la entidad financiera sobre otras operaciones y proveedores,** puede identificar una operación como sospechosa de fraude, debiendo analizarse en tales casos el establecimiento en el cual se efectúa la compra, la frecuencia y continuidad con la que se realiza la transacción, el importe consumido, entre otros."[27] (Subrayado mío)

De acuerdo con el fallo de la Sala, determina que la información histórica debe tomar en cuenta las características de las operaciones que realiza el usuario,

[25] Resolución S.B.S. N° 6523-2013 / Reglamento de Tarjetas de Crédito y Débito
[26] Resolución N°2041-2021/SPC-INDECOPI
[27] Ídem

teniendo en cuenta el establecimiento de la compra, continuidad, frecuencia, entre otras particularidades de las operaciones, lo cual va acorde con lo establecido por la SBS. Sin embargo, encontramos en otros pronunciamientos de la Sala que toma en consideración el mismo análisis con respecto al comportamiento habitual de consumo del usuario, de acuerdo con el pronunciamiento de la Resolución N°0027-2022/SPC-INDECOPI, el cual advierte lo siguiente:

> "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] (Subrayado mío)

Conforme a las consideraciones de la Sala señalada en líneas precedentes, se puede observar que hay un criterio adoptado en distintos casos correspondiente a operaciones no reconocidas, la cual trae a colación las características que debe tener el patrón de consumo habitual del usuario, toda vez que a partir de ella la entidad financiera pueda adoptar medidas de seguridad para prevenir operaciones fraudulentas. En esa línea de ideas, la Resolución N°0206-2023 /SPC-INDECOPI se pronuncia sobre las acciones inmediatas que debería ejecutar la entidad financiera ante la alerta de un posible movimiento fraudulento, el cual señala lo siguiente:

> "las medidas de seguridad a las que se encuentran sujetas la entidad financiera implican el monitoreo de las operaciones del cliente, a efectos de que -ante la ejecución de una operación- la entidad financiera pueda identificar la ocurrencia de una acción inusual y/o posiblemente fraudulenta y, así, **desplegar acciones inmediatas con el fin de mitigar las consecuencias negativas derivadas de dicha acción**."[29]

[28] Resolución N°0027-2022/SPC-INDECOPI
[29] Resolución N°206-2023/SPC-INDECOPI

De acuerdo con lo señalado por la Sala, la entidad financiera debe desplegar "acciones inmediatas" para poder mitigar las consecuencias negativas que provengan de la operación no reconocida, dichas acciones se refieren al bloqueo preventivo en cuanto se advierte que la transacción, conforme se explica en la Resolución N°1292-2020/SPC-INDECOPI, el cual establece lo siguiente:

> "el sistema de monitoreo del Banco tiene por objeto detectar operaciones inusuales o fraudulentas y, ante ello, adoptar **mecanismos idóneos (comunicación con cliente, bloqueo, otros) que eviten el cargo de futuras operaciones en desmedro del patrimonio del cliente**; sin embargo, dicho sistema no es uno de naturaleza predictiva, por lo que **no puede evitar el procesamiento de la operación que genera la alerta respectiva.**"[30] (Subrayado mío)

De acuerdo a lo señalado por la Sala en el año 2020, queda claro que las acciones inmediatas a efectuar serán luego de la primera operación que genere esta alarma, es decir, la primera operación de los movimientos que resulten presuntamente fraudulentos será procesada siempre y cuando cumpla con la validez respectiva, a partir de la segunda operación de las operaciones no reconocidas es cuando la entidad financiera debe ejecutar las acciones inmediatas para cesar estos movimientos fraudulentos, toda vez que la Sala considera que el sistema no es de naturaleza predictiva.

Ahora bien, considero pertinente mencionar que la Sala se pronunció sobre el concepto de "patrón de consumo habitual" en Resolución N°0088-2020/SPC-INDECOPI, estableciendo lo siguiente:

> "la norma **no se encuentra limitada únicamente al patrón de consumo del denunciante, obtenido de la revisión del movimiento histórico de transacciones de cada tarjetahabiente en particular**, sino que también puede deducirse de las características de cada operación en particular y de cómo estas singularidades, en atención a la **información que maneja la entidad financiera sobre otras operaciones y proveedores,** puede identificar una operación como sospechosa de fraude, debiendo analizarse en tales casos el **establecimiento**

[30] Resolución N°1292-2020/SPC-INDECOPI

> **en el cual se efectúa la compra, la frecuencia y continuidad con la que se realiza la transacción, el importe consumido,** entre otros."[31]

La Sala señala que no se pueden guiar únicamente el movimiento histórico de las transacciones efectuadas por el usuario, sino también los otros factores que se analiza como lo es el establecimiento, frecuencia, continuidad. Mencionado ello, la Sala, en este caso, se inclina por analizar los otros factores del patrón de consumo habitual, sin la necesidad de enfocarse únicamente en los montos de las operaciones.

Por otro lado, en el año 2024, dentro de la Resolución N°2293-2024/SPC-INDECOPI, la Sala manifiesta un cambio de criterio con respecto a las Resoluciones que anteriormente ha ido emitiendo, lo cual radica en lo que se muestra a continuación:

> "La Sala realiza un cambio de criterio, considerando que las entidades financieras deben contar con **mecanismos tecnológicos para garantizar que todas las operaciones que vayan a ser cargadas a los productos financieros** de sus clientes se hayan realizado de forma correcta, es decir que se encuentren dentro de su comportamiento habitual de consumo y que hayan sido autorizadas con los requisitos de validez necesarios para cada tipo de operación."[32] (subrayado mío)

Siguiendo con el siguiente considerando que se detalla a continuación:

> "en aquellos casos donde la **operación que debió generar la alerta respectiva no corresponda al comportamiento habitual de consumo del cliente**, no será necesario verificar si, en la realización de dicha operación, concurrieron los requisitos de validez necesarios para su autorización, pues con lo primero **bastará para tener por acreditada la responsabilidad administrativa de la entidad financiera por el cargo indebido de esta operación y las posteriores**."[33] (Subrayado mío)

[31] Resolución N°0088-2020/SPC-INDECOPI
[32] Resolución N°2293-2024/SPC-INDECOPI
[33] Ídem

Conforme se muestra en la Resolución citada, la Sala ha cambiado de criterio con respecto a la primera operación en cuanto a los posibles movimientos fraudulentos. La Sala, actualmente considera que la primera operación debe de ser considerada en la alerta al usuario, y por consecuencia bloquear dicha operación en cuanto se ejecuta y este no coincida con el patrón de consumo del usuario. Sin embargo, es preciso mencionar que la base de este argumento se encuentra en los mecanismos tecnológicos que están en la obligación de tener las entidades financieras.

De acuerdo con la revisión de las Resoluciones mencionadas, podemos concluir que la Sala se enfoca únicamente en el patrón de consumo habitual, independientemente de si estas operaciones no reconocidas han sido válidamente realizadas, es decir, si estas operaciones han sido ejecutadas con los factores de autenticación mencionadas en el capítulo anterior. Este análisis de patrón de consumo habitual tiene como base poder orientar a la implementación del sistema de monitoreo de operaciones de las entidades financieras, con el fin de que estas cumplan con su deber de idoneidad.

Entonces, como hemos podido advertir de los pronunciamientos de la Sala, está claro que las entidades financieras deben tomar en consideración no solo el monto involucrado en las operaciones no reconocidas, sino también distintos factores como el establecimiento donde se ha efectuado el movimiento, canal utilizado, frecuencia de uso del producto financiero, entre otros criterios que la entidad financiera debe considerar para abarcar un mayor grado de seguridad a los usuarios de las entidades financieras. Entonces, es claro que la Sala ha venido evaluando una serie de características que las entidades financieras deben de contemplar para poder encaminar a su sistema de monitoreo y personalizar el patrón de consumo habitual de acuerdo con la información histórica del usuario.

Advirtiendo ello, considero que lo anterior mencionado va de la mano con la información personal que tiene del usuario, es decir, el rango de edad del usuario, la profesión que informó el usuario, lugar de residencia, entre otras características. De esta manera se puede tener una mayor precisión de las

transacciones que usualmente efectúa el usuario, debido a las mismas cualidades que corresponden al usuario.

En virtud de las conclusiones mencionadas, estas serán punto de partida para desarrollar la pregunta principal con respecto al caso en concreto.

5.4. ¿INDECOPI realizó una valoración de pruebas adecuada acerca de la evaluación de "patrón de consumo habitual" y acerca de las medidas de seguridad que el Banco debió aplicar en las operaciones que no se encontraban procesadas al momento del bloqueo de su tarjeta?

Estas preguntas complementarias tienen como objetivo analizar si la Sala realizó una correcta valoración de pruebas en base a lo que había adjuntado el denunciante y sobre las pruebas que podría haber presentado el Banco por la asimetría de la información en esta relación de consumo entre la entidad financiera y el denunciante. Para ello, debemos tener presente los principios de verdad material que INDECOPI debió considerar al emitir el fallo en el presente caso. El principio de verdad material se encuentra establecido en el artículo IV del Título preliminar, numeral 1.11, el cual dispone lo siguiente:

> **"1.11. Principio de verdad material.-** En el procedimiento, la autoridad administrativa competente **deberá verificar plenamente los hechos que sirven de motivo a sus decisiones,** para lo cual deberá **adoptar todas las medidas probatorias necesarias autorizadas por la ley, aun cuando no hayan sido propuestas por los administrados** o hayan acordado eximirse de ellas. (…)"[34]

Conforme a este punto, la ley es clara al mencionar que la autoridad administrativa tiene la obligación de verificar los hechos para que emita un fallo debidamente motivado; adoptando medidas probatorias autorizadas por ley, incluso si estas no han sido propuestas por el administrado. En ese sentido, INDECOPI tiene la facultad de requerir información al proveedor para tener mayor alcance de los hechos, de manera que emite una resolución debidamente motivada. Asimismo, debemos recordar que INDECOPI se pronunció sobre esta

[34] Ley N°27444 Ley del Procedimiento Administrativo General.

asimetría informativa entre el proveedor y consumidor, mencionando que “de las dos partes es el proveedor el que se encuentran en mejor posición para poder determinar que la falla no puede serle atribuida. Ello porque el control y manejo que tiene sobre el proceso productivo y/o el de comercialización y su propia experiencia de mercado le permiten, en el común de los casos, ser quien puede determinar a menor costo la idoneidad del producto”[35]. Es claro que INDECOPI tiene conocimiento que los proveedores tienen mayor capacidad de demostrar los hechos del caso con pruebas suficientes porque tienen mayor acceso a las mismas. En ese sentido, de acuerdo con Guzmán Napuri, “la verdad material implica que, en el momento de la correspondiente toma de decisiones, la Administración debe remitirse a los hechos, independientemente de lo alegado o probado por el particular”[36], lo cual es una de las grandes diferencias frente al proceso civil, en la que el juez solo toma en consideración las pruebas brindadas por las partes al proceso[37].

Asimismo, el Ministerio de Justicia y Derechos Humanos considera que “la autoridad administrativa se encuentra obligada a verificar la verdad, esto es, a reunir todos los elementos de juicio necesarios para saber que ocurrió en un caso y, de esa manera, tomar todas las medidas que sean necesarias para garantizar los derechos de las personas. Para tal efecto, la autoridad puede utilizar todas sus facultades para producir y requerir las pruebas que considere necesarias”[38]. Es claro que la autoridad administrativa, en este caso la Sala o la Comisión, estaba en la obligación de requerir información al Banco no solo sobre las operaciones no reconocidas, sino también otros medios probatorios que recaen sobre los otros elementos que son importantes evaluar para considerar estas operaciones como fraudulentas o no. Dentro de estas puede ser el requerimiento de flujo de procesamiento de las operaciones para entender el

[35] Rodriguez, G. (2008). ¿Asimetría informativa o desigualdad en el mercado?: apuntes sobre el verdadero rol de la protección al consumidor. *Foro Jurídico*, (08).
[36] Napurí, G. (2009). Los principios generales del derecho administrativo. *Ius et veritas,* (38).
[37] Ídem
[38] Ministerio de Justicia y Derechos Humanos (2016) Guía prática sobre la actividad probatoria en los procedimientos administrativos.

hecho de porque dos de estas operaciones fueron procesadas a pesar de que la tarjeta fue bloqueada horas antes.

En ese sentido, dentro de las Resoluciones emitidas por la Comisión y la Sala no encontramos una actuación probatoria correspondiente en la que se aplique el principio de verdad material, no solo porque no se tuvo en cuenta los Estados de Cuenta del usuario Sr. Yataco, sino que tampoco requirió información al Banco sobre el flujo de procesamiento de sus operaciones, toda vez que dos de las operaciones fueron efectuadas en fecha 24 de Mayo de 2020, fecha en la que la tarjeta fue bloqueada; sin embargo, fueron procesadas al día siguiente. Es claro que INDECOPI debió pronunciarse sobre este hecho en específico, ya que va ligado directamente a las medidas de seguridad que el Banco debe implementar. No obstante, tanto la Comisión como la Sala no han analizados estás dos operaciones en particular, las cuales podrían haberse evitado el procesamiento de las mismas, toda vez que la tarjeta se encontraba bloqueada.

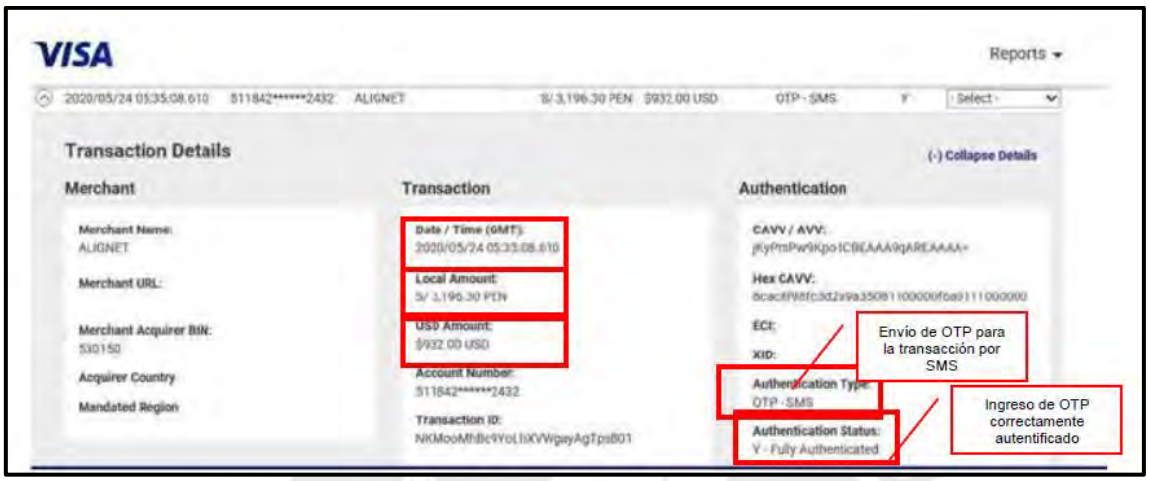
Además de lo anterior señalado, encontramos que la autoridad administrativa no realizó una debida actuación probatoria, en tanto no se tuvo en cuenta los Estados de Cuenta del Sr. Yataco de los últimos 6 meses, analizando los factores de patrón de consumo que se requiere para detectar posibles operaciones fraudulentas. Entre otros medios probatorios que INDECOPI estaba en la capacidad de requerir al Banco, pudo haber sido el detalle del flujo de procesamiento de las operaciones, de manera que se analice si el Banco se encontraba en la posibilidad de no procesar esas operaciones, toda vez que la tarjeta ya se encontraba bloqueada, y de esa manera, emitir el fallo con la motivación adecuada y una correcta actuación probatoria sobre los mismos.

5.5. *¿El Banco Scotiabank aplicó medidas de seguridad en las operaciones no reconocidas que advirtió el Sr. Yataco*? ¿Va acorde a los fallos que INDECOPI venía resolviendo?

Para poder responder estas preguntas, debemos tener presente las fechas y características de las operaciones no reconocidas que está en el caso. Por tanto, es conveniente que se evalué cada operación de manera independiente.

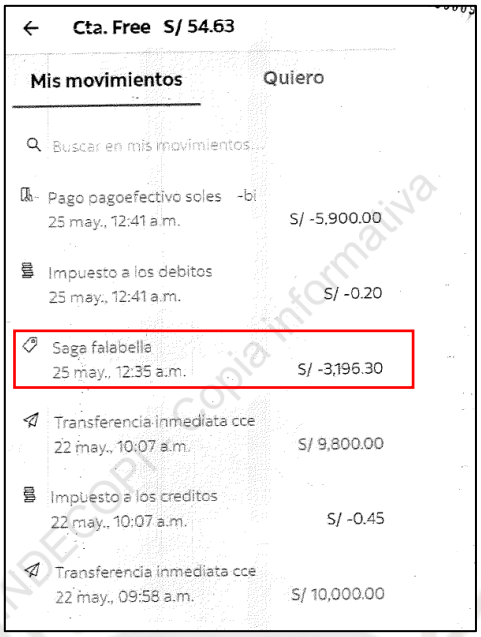
De la operación de fecha 25 de Mayo de 2020 por el monto de S/3,196.30

Con respecto a esta operación, el Banco señaló que ha seguido un circuito operativo, mostrando una captura de pantalla que acredita que se envió una clave SMS al celular del Sr. Yataco y este ingresó dicha clave a la página web de manera correcta; tal como se puede apreciar en la siguiente imagen:



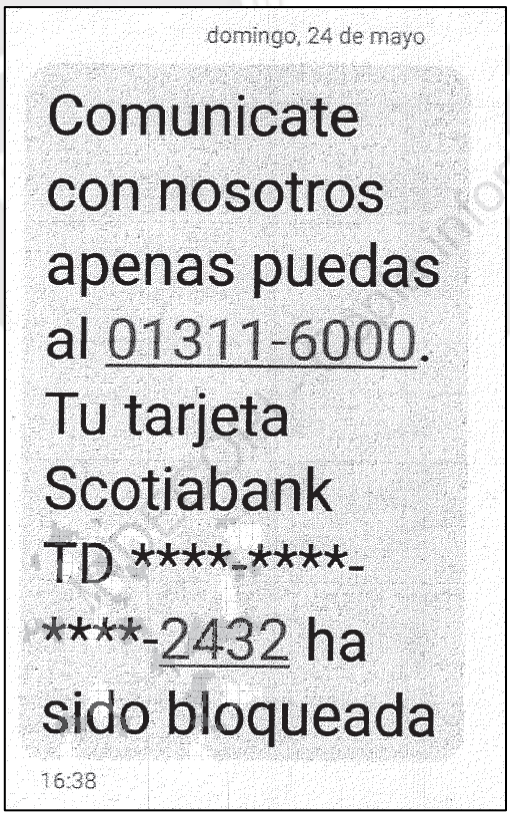
Fuente: Resolución N°1267-2022/SPC-INDECOPI

Como se puede apreciar, la operación se realizó en fecha 24 de Mayo de 2020 a las 05:35, por el monto de S/3,196.30, el cual se le notificó mediante un mensaje SMS al celular que se le encontraba registrado al Sr. Yataco, de manera que confirme dicha operación. Referente a esta operación, es preciso mencionar que hay una diferencia en la fecha que se procesa con la fecha que verdaderamente se ejecutó el movimiento. En ese sentido, la cuestión a analizar es la fecha y hora según la información que muestra el Estado de Cuenta del Sr. Yataco:



Fuente: Expediente N°409-2021/CC1

De acuerdo con los medios probatorios que adjunta el Sr. Yataco, se puede observar que este bloqueó dicha tarjeta el 24 de mayo del 2020, conforme se advierte en la siguiente imagen:

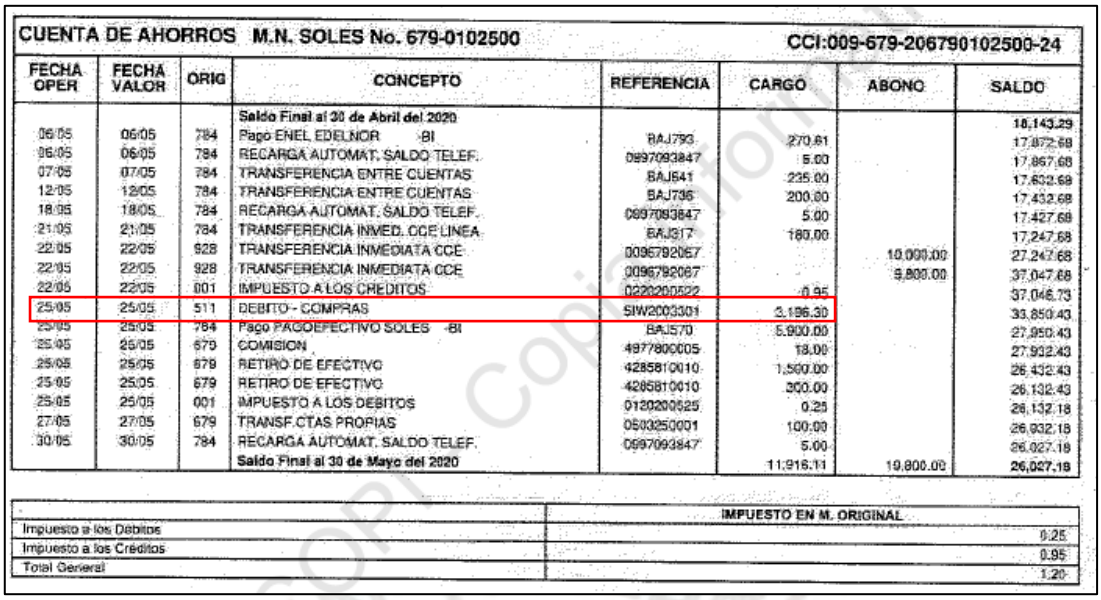


Fuente: Expediente N°409-2021/CC1

En ese sentido, podemos encontrar que el Banco no aportó medios probatorios que acrediten el hecho de que no pudo cancelar esta operación antes de ser procesadas en fecha 25 de Mayo de 2020, por lo que hay cierta probabilidad de que el Banco pudo evitar el procesamiento de las operaciones al momento que se efectuó el bloqueo de la tarjera conforme se muestra el Estado de Cuenta del Sr. Yataco.

Además de esta omisión por parte del Banco, podemos advertir que la Sala no se pronuncia sobre el análisis de estas fechas, siendo que únicamente se enfocan sobre la definición de patrón de consumo habitual del usuario teniendo como referencia únicamente al monto de los movimientos que ha venido efectuando el usuario. Sin embargo, no encontramos que analicen los otros factores como tipo de comercio, frecuencia y canal utilizado.

Como podemos apreciar, la operación en el presente caso corresponde a un movimiento que tiene como concepto “débito - compras” realizada con tarjeta no presente, siendo que no se evalúa la frecuencia que el Sr. Yataco ha realizado compras por esta página web de Saga Falabella, o si el usuario en los últimos meses ha efectuado este tipo de transacciones. Asimismo, de acuerdo a la imagen mostrada a continuación, se puede ver el detalle que, al menos en ese mes, no realizó compras por internet o movimientos que tengan como concepto “débito - compras”:



CUENTA DE AHORROS M.N. SOLES No. 679-0102500 CCI:009-679-206790102500-24

FECHA OPER	FECHA VALOR	ORIG	CONCEPTO	REFERENCIA	CARGO	ABONO	SALDO
			Saldo Final al 30 de Abril del 2020				18,143.29
06/05	06/05	784	Pago ENEL EDELNOR -BI	BAJ793	270.61		17,872.68
06/05	06/05	784	RECARGA AUTOMAT. SALDO TELEF.	0997093847	5.00		17,867.68
07/05	07/05	784	TRANSFERENCIA ENTRE CUENTAS	BAJ641	235.00		17,632.68
12/05	12/05	784	TRANSFERENCIA ENTRE CUENTAS	BAJ736	200.00		17,432.68
18/05	18/05	784	RECARGA AUTOMAT. SALDO TELEF.	0997093847	5.00		17,427.68
21/05	21/05	784	TRANSFERENCIA INMED. CCE LINEA	BAJ317	180.00		17,247.68
22/05	22/05	928	TRANSFERENCIA INMEDIATA CCE	0096792067		10,000.00	27,247.68
22/05	22/05	928	TRANSFERENCIA INMEDIATA CCE	0096792067		9,800.00	37,047.68
22/05	22/05	001	IMPUESTO A LOS CREDITOS	0220200522	0.95		37,046.73
25/05	25/05	511	DEBITO - COMPRAS	SIW2003301	3,196.30		33,850.43
25/05	25/05	784	Pago PAGOEFECTIVO SOLES -BI	BAJ570	5,900.00		27,950.43
25/05	25/05	679	COMISION	4977800005	18.00		27,932.43
25/05	25/05	679	RETIRO DE EFECTIVO	4285810010	1,500.00		26,432.43
25/05	25/05	679	RETIRO DE EFECTIVO	4285810010	300.00		26,132.43
25/05	25/05	001	IMPUESTO A LOS DEBITOS	0120200525	0.25		26,132.18
27/05	27/05	679	TRANSF.CTAS PROPIAS	0503250001	100.00		26,032.18
30/05	30/05	784	RECARGA AUTOMAT. SALDO TELEF.	0997093847	5.00		26,027.18
			Saldo Final al 30 de Mayo del 2020		11,916.11	19,800.00	26,027.18

	IMPUESTO EN M. ORIGINAL
Impuesto a los Debitos	0.25
Impuesto a los Créditos	0.95
Total General	1.20

Fuente: Expediente N°409-2021/CC1

De acuerdo con la imagen mostrada, el cual es un medio probatorio remitido por el denunciante, durante ese mes no se ha efectuado operaciones con la descripción “débito - compras”, hecho que no se pudo advertir por la autoridad administrativa. En ese sentido, referente a esta operación en específica, se debió evaluar si durante los últimos 6 meses hubo operaciones con este concepto; no obstante, durante el procedimiento no encontramos que la autoridad administrativa haya evaluado los demás factores de patrón de consumo habitual referente a esta operación.

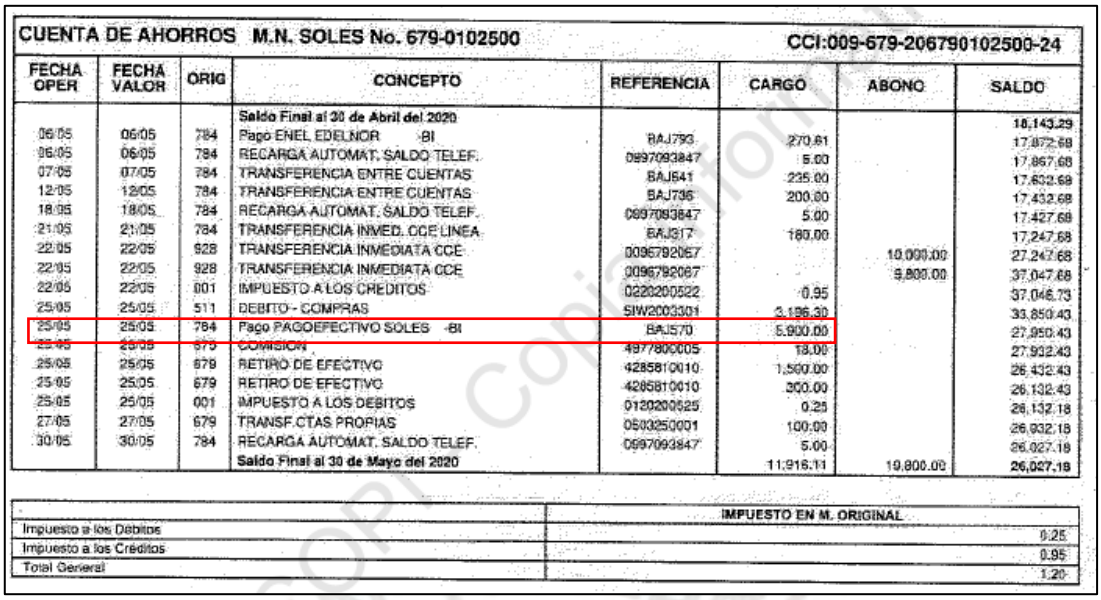
De la operación de fecha 25 de Mayo de 2020 por el monto de S/5,900.00

Siguiendo con el mismo análisis de la operación anterior, procederemos a analizar el circuito que el Banco efectuó respecto a dicha operación, conforme se muestra en la siguiente imagen:

Fuente: Resolución N°1267-2022/SPC-INDECOPI

La captura detalla la fecha y hora del ingreso a la banca móvil, el ingreso satisfactorio, el equipo donde se registró la banca móvil, y la verificación exitosa sobre el OTP enviado al equipo móvil, al igual que en el anterior caso, la verificación es exitosa mediante el envío de un mensaje vía SMS. De acuerdo con la imagen, entendemos que el ingreso a la banca móvil, en la que primero se cerciora que sea en el mismo dispositivo móvil donde se ha vinculado esta desde un principio debe llegar una verificación OTP, además de la clave con la que se ingresa a la misma. Mencionado esto, encontramos que todos los puntos, el Banco acredita que sí se ha logrado un ingreso satisfactorio. No obstante, la imagen acredita que la operación fue realizada el 24 de Mayo de 2020 en horas 12:30 a.m. Sin embargo, conforme se mostró el estado de cuenta de ese mes, esta operación, al igual que la anterior operación, fue procesada al día siguiente; sin tener en cuenta el bloqueo de la tarjeta realizado por el Sr. Yataco en fecha 24 de Mayo de 2020.

Asimismo, si bien es cierto que sí se puede acreditar por el estado de cuenta del usuario que solía realizar movimientos por su aplicativo móvil, debemos analizar el tipo de movimientos que realizaba dentro de la misma, ello, porque dentro del medio probatorio adjuntado por el Sr. Yataco, se detalla que las operaciones que efectuaba eran transferencias y retiros de dinero, mas no este tipo de movimiento llamado “pago efectivo-bi”, conforme se puede observar en el historial de operaciones del mes de Mayo:



CUENTA DE AHORROS M.N. SOLES No. 679-0102500 CCI:009-679-206790102500-24

FECHA OPER	FECHA VALOR	ORIG	CONCEPTO	REFERENCIA	CARGO	ABONO	SALDO
			Saldo Final al 30 de Abril del 2020				18,143.29
06/05	06/05	784	Pago ENEL EDELNOR -BI	BAJ793	270.61		17,872.68
06/05	06/05	784	RECARGA AUTOMAT. SALDO TELEF.	0997093847	5.00		17,867.68
07/05	07/05	784	TRANSFERENCIA ENTRE CUENTAS	BAJ641	235.00		17,632.68
12/05	12/05	784	TRANSFERENCIA ENTRE CUENTAS	BAJ736	200.00		17,432.68
18/05	18/05	784	RECARGA AUTOMAT. SALDO TELEF.	0997093847	5.00		17,427.68
21/05	21/05	784	TRANSFERENCIA INMED. CCE LINEA	BAJ317	180.00		17,247.68
22/05	22/05	928	TRANSFERENCIA INMEDIATA CCE	0096792067		10,000.00	27,247.68
22/05	22/05	928	TRANSFERENCIA INMEDIATA CCE	0096792067		9,800.00	37,047.68
22/05	22/05	001	IMPUESTO A LOS CREDITOS	0220200522	0.95		37,046.73
25/05	25/05	511	DEBITO - COMPRAS	SIW2003301	3,196.30		33,850.43
25/05	25/05	784	Pago PAGOEFECTIVO SOLES -BI	BAJ570	5,900.00		27,950.43
25/05	25/05	679	COMISION	4977800005	18.00		27,932.43
25/05	25/05	679	RETIRO DE EFECTIVO	4285810010	1,500.00		26,432.43
25/05	25/05	679	RETIRO DE EFECTIVO	4285810010	300.00		26,132.43
25/05	25/05	001	IMPUESTO A LOS DEBITOS	0120200525	0.25		26,132.18
27/05	27/05	679	TRANSF.CTAS PROPIAS	0503250001	100.00		26,032.18
30/05	30/05	784	RECARGA AUTOMAT. SALDO TELEF.	0997093847	5.00		26,027.18
			Saldo Final al 30 de Mayo del 2020		11,916.11	19,800.00	26,027.18

	IMPUESTO EN M. ORIGINAL
Impuesto a los Debitos	0.25
Impuesto a los Créditos	0.95
Total General	1.20

Fuente: Expediente N°409-2021/CC1

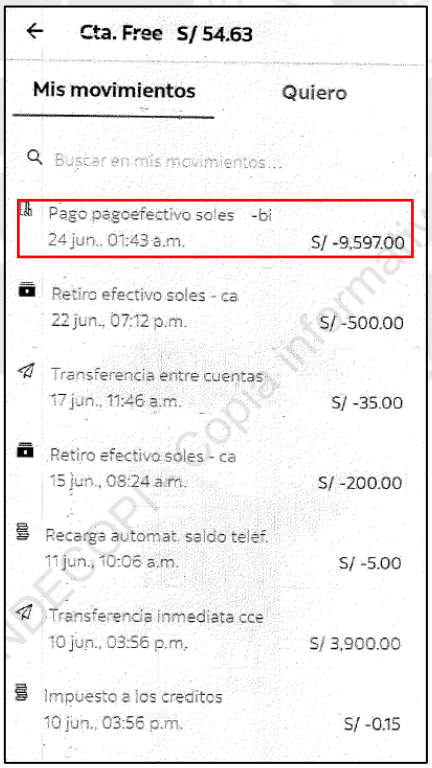
Al igual que en la operación anterior, considero que no se realizó una evaluación correspondiente del concepto de patrón de consumo habitual, toda vez que no se evaluó correctamente la frecuencia de los movimientos que tiene por el concepto de “pago efectivo-bi” durante los seis últimos meses. Además del hecho que esta operación también fue procesada luego de que el Sr. Yataco haya bloqueado su tarjeta.

De la operación de fecha 24 de Junio de 2020 por el monto de S/9,597.00

Esta operación, a diferencia de las otras dos, se efectuó un mes después de las otras dos operaciones cuestionadas, además de que fue realizada con otra tarjeta de débito, siendo el flujo de ejecución conforme se muestra en la siguiente imagen:

Fuente: Resolución N°1267-2022/SPC-INDECOPI

De acuerdo con la imagen, encontramos que todos los pasos previos para ingresar a la banca móvil han sido acreditados correctamente como en la anterior operación de monto S/5,900. Ahora bien, a diferencia de la casuística de las dos operaciones anteriores, esta sí coincide con la fecha en la que se efectuó y con la que se procesó; sin embargo, de acuerdo al pantallazo adjuntado por el Banco, esta se efectuó a las 01:38 a.m., mientras que en el Estado de cuenta del Sr. Yataco señala que se procesó a las 01:43 a.m:



Fuente: Expediente N°409-2021/CC1

Conforme se puede visualizar, es uno del mismo tipo de operación “pago efectivo-bi”, movimiento el cual no se ha evaluado si esta operación correspondía a su comportamiento de consumo habitual del denunciante. Conforme se muestra en el estado de cuenta del usuario del mes de Junio, no hay otra operación con la misma categoría:

CUENTA DE AHORROS M.N. SOLES No. 679-0102500 — **CCI:009-679-206790102500-24**

FECHA OPER	FECHA VALOR	ORIG	CONCEPTO	REFERENCIA	CARGO	ABONO	SALDO
			Saldo Final al 31 de Mayo del 2020				26,027.18
05/06	05/06	784	RECARGA AUTOMAT. SALDO TELEF.	0997093847	5.00		26,022.18
05/06	05/06	679	RETIRO EFECTIVO SOLES - CA	9IÑ0004741	500.00		25,522.18
10/06	10/06	928	TRANSFERENCIA INMEDIATA CCE	0096792067		3,900.00	29,422.18
10/06	10/06	001	IMPUESTO A LOS CREDITOS	0220200610	0.15		29,422.03
11/06	11/06	784	RECARGA AUTOMAT. SALDO TELEF.	0997093847	5.00		29,417.03
15/06	15/06	679	RETIRO EFECTIVO SOLES - CA	9IÑ0004743	200.00		29,217.03
17/06	17/06	784	TRANSFERENCIA ENTRE CUENTAS	BAJ831	35.00		29,182.03
22/06	22/06	679	RETIRO EFECTIVO SOLES - CA	9IÑ0004746	500.00		28,682.03
24/06	24/06	784	Pago PAGOEFECTIVO SOLES BI	BAJ691	9,597.00		19,085.03
24/06	24/06	928	TRANSFERENCIA INMEDIATA CCE	0096792067		120.00	19,205.03
24/06	24/06	679	RETIRO CON HOJA INSTRUCCIONES	0520440001	19,184.00		21.03
24/06	24/06	001	IMPUESTO A LOS DEBITOS	0120200624	1.40		19.63
			Saldo Final al 30 de Junio del 2020		30,027.55	4,020.00	19.63

Fuente: Expediente N°409-2021/CC1

Asimismo, el usuario ya había advertido el mes anterior (Mayo) que esas operaciones no las había reconocido, por tanto, el Banco debió advertir que esas operaciones no correspondían a su patrón de consumo habitual, lo que no sucedió en el presente caso. Tanto en este mes como en el anterior, se puede detectar que el concepto de “pago efectivo-bi” han sido operaciones que no reconoce el usuario y fueron los únicos que han sido considerados fraudulentos por el usuario, se puede concluir que el Banco no detectó como tales, toda vez que el monto no era inusual; sin embargo, sí lo era el concepto.

Del análisis de “patrón de consumo habitual” de INDECOPI

Para analizar el fallo de la Sala con respecto a estas tres operaciones, debemos citar el análisis que brinda la autoridad administrativa referente a los mismos:

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.**

Fuente: Resolución N°1267-2022/SPC-INDECOPI

Podemos observar que la Sala solo se pronuncia sobre los montos de las operaciones no reconocidas frente al historial que tenía el Sr. Yataco. De acuerdo con lo señalado en el capítulo 5.3. respecto a los pronunciamientos de la autoridad administrativa, sobre la evaluación del patrón de consumo del usuario, este ha venido realizando un análisis conforme a las operaciones efectuadas, sobre la alerta que el Banco debió enviar al usuario por los movimientos que el usuario ha ejecutado, siendo que este procesará la primera operación cuando se acredite que ha sido efectuada válidamente. No obstante, en el presente caso, la Sala realizó una evaluación en base al consumo habitual mensual, mas no individualizado, este no estaría siendo suficiente para poder considerar operaciones usuales o inusuales. En el presente caso, podemos advertir que la Sala solo se enfocó en los montos de las operaciones frente a los montos mensuales que el Sr. Yataco habría realizado en los últimos seis meses. Por otro lado, la postura de la vocal Roxana Barrantes, analiza cada consumo individualizado; no obstante, tanto la mayoría de la Sala como la vocal con su voto singular hacen caso omiso a los otros factores que no son evaluados como el tipo de comercio, la frecuencia y el canal. Si bien el monto de las operaciones es un punto muy importante a tener en cuenta, también se debe advertir los otros

factores del patrón de consumo habitual que detalla el Reglamento, evaluación que no es tomado en cuenta por la Sala en la presente Resolución.

Entonces, las medidas de seguridad del Banco, si bien han sido acreditadas en un primer momento conforme se aprecia en los pantallazos que adjunta el Banco como medio probatorio. No obstante, con respecto a la evaluación de patrón de consumo habitual, este concepto específicamente no ha sido valorado ni evaluado en el presente caso, toda vez que han sido movimientos con conceptos inusuales, que el usuario no habría realizado anteriormente.

Asimismo, con respecto a las dos operaciones efectuadas el 24 de Mayo de 2020, advertimos que han sido procesados al día siguiente, haciendo caso omiso al bloqueo de tarjeta del usuario. Lo que trae como consecuencia, a su vez, que al no ser operaciones categorizadas como inusuales por el Banco, se pudo realizar la tercera operación sin advertencia alguna, por el hecho que ya había una operación anteriormente realizada por el mismo concepto “pago efectivo-bi”.

De la normativa vigente a la fecha de los hechos

A lo largo del informe hemos citado normativa que no se encontraba vigente en ese momento; sin embargo, a la fecha de la redacción del presente informe sí se encuentra en vigor. En ese sentido, considero pertinente señalar qué normativa debió aplicarse en el presente caso, teniendo en cuenta la normativa vigente en ese entonces y las que se ha venido señalando en el presente informe.

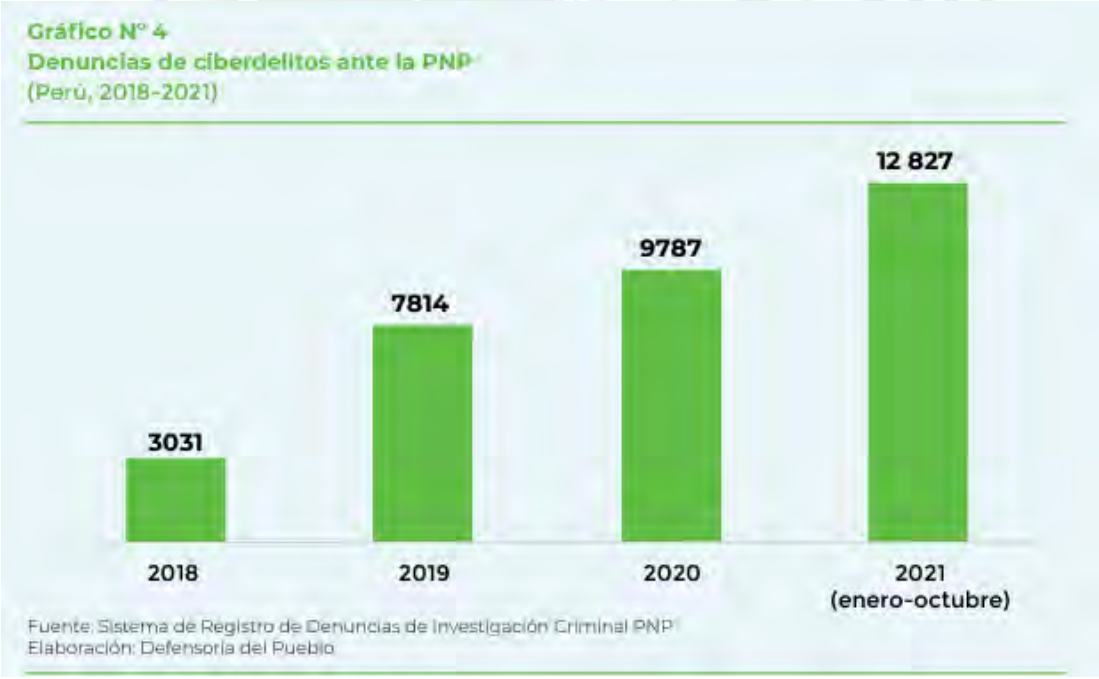
Fecha Julio de 2020

La normativa vigente para esta fecha es el Reglamento de Tarjetas de Crédito y Débito; no obstante, esta no contenía el artículo 16 numeral 7; artículo que sí se analizó en el presente informe. En ese sentido, dicho Reglamento no tenía detallado el proceso de autenticación para realizar las operaciones. Por tanto, las operaciones debieron ser validadas de acuerdo a lo establecido en el Reglamento sin las modificaciones posteriores a Julio 2020. En esa línea de ideas, encontramos que no se tenía en cuenta los tipos de operaciones (con tarjeta presente, no presente y billeteras móviles) detalladas en el artículo 16.7 del mismo cuerpo legal, por lo cual considero pertinente mencionar que las

medidas de seguridad ejecutadas por el Banco para la validación de las operaciones fueron conforme a ley, debido a que la medida de seguridad en ese entonces era la clave dinámica y no había ningún pronunciamiento de la SBS con respecto a este tipo de factor de autenticación. En ese sentido, el envío de clave por mensaje SMS era considerado un factor de autenticación válida para poder realizar operaciones que van asociadas a las tarjetas de los usuarios. En conclusión, de acuerdo con la normativa vigente en el año 2020, las operaciones cuestionadas fueron válidamente correctas y se considera que el mismo usuario efectuó las mismas.

Fecha actual

A lo largo de los últimos años, se puede advertir que las cifras de ciberdelitos han ido en aumento. De acuerdo con el Reporte Defensorial N°001-2023-DP/ADHPD elaborada por Defensoría del Pueblo, señalan que "las denuncias se cuadruplicaron entre los años 2018 y 2021, pasando de 3031 a 12,827"[39], conforme se muestra en el siguiente gráfico:



[39] Defensoría del Pueblo (2016) La Ciberdelincuencia en el Perú: Estrategias y Retos del Estado (Informe Defensorial N° 001-2023-DP/ADHPD)
https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Fuente: Defensoría del Pueblo (2016) La Ciberdelincuencia en el Perú: Estrategias y Retos del Estado (Informe Defensorial N° 001-2023-DP/ADHPD)

De acuerdo con lo ya mencionado en el punto anterior, el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad entró en vigencia luego de los hechos acontecidos; sin embargo, trajo nuevas soluciones para evitar la ciberdelincuencia, los artículos 17 y 19 son los que se encargan de reforzar la seguridad de las operaciones que se efectúan mediante canales digitales, lo que ya queda a discreción de las entidades financieras el uso de estos factores de autenticación de usuarios, los cuales pueden ser de tres categorías "algo que solo el usuario conoce, algo que solo el usuario posee, algo que el usuario es, que incluye las características biométricas"[40]. Son factores que depende de cada entidad financiera puede implementar dentro de sus aplicativos móviles.

Entonces, ello demuestra que el legislador peruano, en este caso la misma SBS se encargó de crear un Reglamento que indique que tipo de factores de autenticación debería de implementar las entidades financieras, y estos no se limitan un carácter único, sino que la entidad financiera implementa de acuerdo a su discrecionalidad y su propio sistema que tenga implementado para sus aplicativos móviles y canales digitales. No obstante, debemos tener en cuenta que la SBS dentro de su boletín informativa, advierte que "la contraseña de un solo uso (OTP), enviada a través de mensaje SMS, no es considerado como un factor de autenticación válido, dado que su transmisión no es segura y expone a los usuarios a incidentes de seguridad de la información"[41]. En ese sentido, teniendo la advertencia de la SBS, INDECOPI debería de considerar este hecho que las claves enviadas por mensaje SMS no deberían de ser considerados como factores de autenticación.

[40] Resolución S.B.S. N° 054-2021 / Reglamento para la Gestión de Seguridad de la Información y la Ciberseguridad

[41] Superintendencia de Banca y Seguros (2022) Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario. https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222/1000

Teniendo en consideración la normativa vigente en el año 2020 y actualmente, considero oportuno realizar una comparación de las normativas aplicables en el presente caso, siendo que en el 2020 había menor regulación que a la fecha actual:

	NORMATIVA VIGENTE AL 2020	**NORMATIVA VIGENTE ACTUALIDAD**
OPERACIONES NO RECONOCIDAS MAYO - JUNIO 2020	Resolución S.B.S. N° 6523-2013 / Reglamento de Tarjetas de Débito y Crédito (sin las modificaciones de las Resoluciones SBS emitidas en 2023 y 2024)	Resolución S.B.S. N° 6523-2013 / Reglamento de Tarjetas de Débito y Crédito
	Ley N° 29985 / Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.	Ley N° 29985 / Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.
	-	Resolución S.B.S. N° 504-2021 / Reglamento para la Seguridad de la Información y la Ciberseguridad

Como se puede observar, la regulación ha venido en aumento con el fin de que resguarden este tipo de operaciones, lo que genera mayor protección a los usuarios, tanto del uso de las tarjetas que tienen en su propiedad, como las billeteras móviles y aplicativos que tienen con las entidades financieras. Por tanto, este incremento de regulación se ve reflejada en los cambios de criterios que ha venido teniendo INDECOPI respecto a este tema de operaciones no reconocidas.

En ese sentido, el Banco aplicó las medidas de seguridad que se encontraba en su alcance y conforme a lo que establecía la ley, toda vez que la validez de las operaciones se encontraba ligadas a la clave enviada por mensaje SMS enviada al usuario, como un factor de autenticación. No obstante, con respecto a la evaluación de concepto de patrón de consumo habitual, el Banco no aplicó las medidas correspondientes frente a las dos primeras operaciones, evitando el procesamiento de esta; así como también no detectó las posibles operaciones

fraudulentas, toda vez que estas tenían como factores inusuales con respecto al canal, frecuencia y tipo de comercio. Debemos tener en cuenta que este tipo de características INDECOPI sí evaluaba dentro de sus resoluciones emitidas, ya que estos factores se encuentran dentro del mismo Reglamento.

VI. CONCLUSIONES Y/O RECOMENDACIONES

El tema de operaciones no reconocidas es un tema muy controversial, debemos tener en cuenta que a la fecha de las operaciones no reconocidas del presente caso, el Reglamento y la normativa que disponía esta materia de ciberseguridad y billeteras digitales, no se encontraba tan regulado como se encuentra hoy en día. Sin embargo, es indispensable que no solo se regule mayor normativa, sino que esta se vea reflejada dentro de los fallos que emite INDECOPI. Si bien son entidades distintas, INDECOPI debe aplicar esta normativa y aplicarlas en los casos en concreto si el caso así lo requiera, para una mayor seguridad jurídica al establecer lineamientos que deben tener las entidades financieras con respecto a la protección del usuario en línea con lo que establece la SBS y lo que considera INDECOPI una posible infracción.

De acuerdo a ello, la mayoría de la Sala realiza una evaluación la totalidad del monto consumido en un periodo mensual para determinar el patrón de consumo del usuario, mientras que la vocal Roxana Barrantes realiza una evaluación más individualizada de la operación no reconocida frente a las demás transacciones que efectuaba el usuario. Sin embargo, ambas posiciones no están tomando en consideración los demás factores que caracteriza al “comportamiento habitual de consumo del usuario”, como el tipo de comercio, la frecuencia y el canal utilizado. De esa manera, la evaluación de INDECOPI debería de ser más detallada sin restringirse solamente en valorar los montos controvertidos, sino también en los demás factores.

Si bien a la actualidad INDECOPI cambio de criterio con respecto a que la primera operación que sea considerado posiblemente fraudulenta se debe tomar acciones inmediatas a la primera detección, mientras que anteriormente se tomaba a partir de la segunda operación realizada en un intervalo de tiempo muy corto entre cada una, demuestra que la Sala de INDECOPI está previniendo a

las entidades financieras que el sistema de monitoreo que estas emplean deberán de tomar en consideración no solamente el monto y el intervalo de tiempo que se realice estas operaciones, sino también los demás factores que se detalla en el reglamento, como el canal, frecuencia y tipo de comercio en la que se efectúe. Pese a que esta Resolución no mencione explícitamente este tipo de análisis frente a las operaciones, se entiende que para un mayor detalle de las operaciones no se deben enfocar únicamente en el monto, sino también los demás factores. Asimismo, INDECOPI señaló dentro de esta Resolución que se hizo este cambio de criterio tiene como base a la obligación y posición que tienen las entidades financieras para poder adoptar mecanismos tecnológicos dentro de su sistema.

Por otro lado, debemos enfocarnos en la omisión que tuvo el Banco sobre el bloqueo de su tarjeta frente a las operaciones que aún no se encontraban procesadas, siendo que el usuario advirtió al Banco que estas operaciones no las había realizado el denunciante. En ese sentido, el Banco estuvo en la posibilidad de cancelar y no procesar dos de esas tres operaciones no reconocidas antes de que se procesen efectivamente; sin embargo, no aplicó medida de seguridad alguna frente a estas dos operaciones. Este hecho INDECOPI no lo analizó en ninguna de las dos instancias, lo que evidencia que no se hizo una actuación de medios probatorios correspondiente, afectando de manera sustancial al principio de verdad material.

En esa misma línea de ideas, dentro de todo el procedimiento del presente caso, podemos advertir que INDECOPI no ha solicitado requerimiento de información al Banco para poder emitir un fallo conforme con los hechos sucedidos, lo que acredita una falta de actuación probatoria nuevamente, toda vez que INDECOPI no recabó toda la información necesaria para poder llegar a una conclusión referente a las operaciones. Es claro que pudo solicitar los Estados de Cuenta de los últimos 6 meses del usuario, al igual que analizar el procesamiento de las dos primeras operaciones efectuadas.

Por último, a lo largo de estos años podemos encontrar un aumento en legislación normativa sobre este tipo de casos correspondientes a operaciones

no reconocidas; junto a ello vienen los cambios de criterios que viene realizando la Sala, lo que podría generar poca seguridad jurídica al estar en constantes cambios y no haya un lineamiento concreto del que se puedan guiar las entidades financieras.

BIBLIOGRAFÍA

- Defensoría del Pueblo (2016) La Ciberdelincuencia en el Perú: Estrategias y Retos del Estado (Informe Defensorial N° 001-2023-DP/ADHPD) https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf
- Ley N°27444 Ley del Procedimiento Administrativo General.
- Ley N°29571, Código de Protección y Defensa del Consumidor.
- Ley N°29985, Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera.
- Ley N° 30096 / Ley de Delitos Informáticos
- LEX. (2021, 29 de Noviembre) ¿Las medidas de seguridad forman parte del deber de idoneidad en la prestación de servicios financieros?. Pasión por el Derecho. https://lpderecho.pe/medidas-seguridad-deber-idoneidad-prestacion-servicios-financieros/
- Ministerio de Justicia y Derechos Humanos (2016) Guía práctica sobre la actividad probatoria en los procedimientos administrativos.
- Napurí, G. (2009). Los principios generales del derecho administrativo. Ius et veritas, (38).
- Presidencia de consejos de Ministros (S/F) Conocer más sobre las billeteras digitales disponibles en el Perú. https://www.gob.pe/14930-conocer-mas-sobre-las-billeteras-digitales-disponibles-en-el-peru
- Resolución N°0027-2022/SPC-INDECOPI
- Resolución N°0088-2020/SPC-INDECOPI

- Resolución N°0124-2024/CPC-INDECOPI
- Resolución N°1292-2020/SPC-INDECOPI
- Resolución N°2041-2021/SPC-INDECOPI
- Resolución N°206-2023/SPC-INDECOPI
- Resolución N°2293-2024/SPC-INDECOPI
- Resolución S.B.S. N º264-2008 / Reglamento de Tarjetas de Crédito
- Resolución S.B.S. N°504-2021 / Reglamento para la Seguridad de la Información y la Ciberseguridad
- Resolución S.B.S. N°6523-2013 / Reglamento de Tarjetas de Crédito y Debito
- Rodriguez, G. (2008). ¿Asimetría informativa o desigualdad en el mercado?: apuntes sobre el verdadero rol de la protección al consumidor. Foro Jurídico, (08).
- Rodriguez, V. (2014) Dinero electrónico en Perú ¿Por qué es importante en la inclusión financiera?. Quipukamayoc, Vol. 22 N°41, pp. 186.
- Superintendencia de Banca y Seguros (2022) Autenticación reforzada: mayor seguridad para operaciones que puedan generar perjuicio al usuario. https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1222/1000
- Vega, M & Vasquez, J (2022) El Banco Central de Reserva del Perú y el desarrollo del Sistema de Pagos en el Perú. https://www.bcrp.gob.pe/docs/Publicaciones/Revista-Moneda/moneda-189/moneda-189-03.pdf

ANEXOS

PROCEDENCIA : COMISIÓN DE PROTECCIÓN AL CONSUMIDOR – SEDE LIMA SUR Nº1
PROCEDIMIENTO : DE PARTE
DENUNCIANTE : JUAN ANDRÉS YATACO CASAS
DENUNCIADO : SCOTIABANK PERÚ S.A.A.
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 Juan Andrés Yataco Casas contra Scotiabank Perú S.A.A.; y, en consecuencia, se declara infundada la misma, por presunta infracción de los artículos 18º y 19º 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 Scotiabank Perú S.A.A. 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.

Lima, 20 de junio de 2022

ANTECEDENTES

1. El 21 de febrero de 2021, el señor Juan Andrés Yataco Casas (en adelante, el señor Yataco) denunció a Scotiabank Perú S.A.A. (en adelante, 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	24/06/2020	Pago efectivo-bi	S/ 9 597,00
TOTAL		**S/ 15 497,00**	

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) 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 pago 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 Yataco 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.

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

3. Mediante Resolución 1 del 29 de marzo de 2021, la Secretaría Técnica de la Comisión de Protección al Consumidor – Sede Lima Sur Nº 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 Juan Andrés Yataco Casas contra Scotiabank Perú S.A. por presunta infracción a los artículos 18° y 19° de la Ley Nº 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 Nº 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 Nº 4285-**-****-4502**			
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 Nº1 (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 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, 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 "*Succesfull*" 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-91a6de2038c1 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 18º.- 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 19º.- 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 lo 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 aducir alegaciones.

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

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 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.

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 Prosa 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- 679-****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 Prosa 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/ 9 096,30 -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 Prosa 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 16:38:58 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.

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.

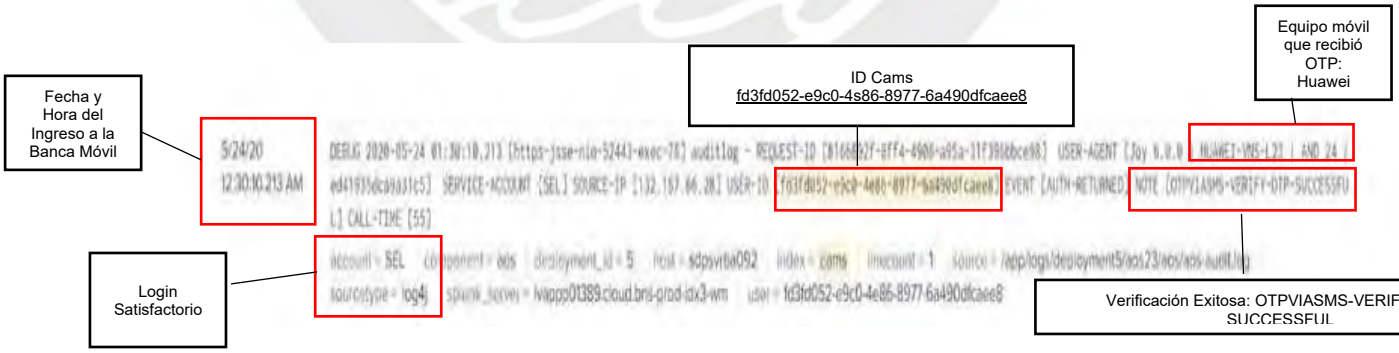
- Sobre las operaciones "Pago Efectivo – bi", por los importes de S/ 5 900,00 y S/ 9 597,00

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[12] 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:

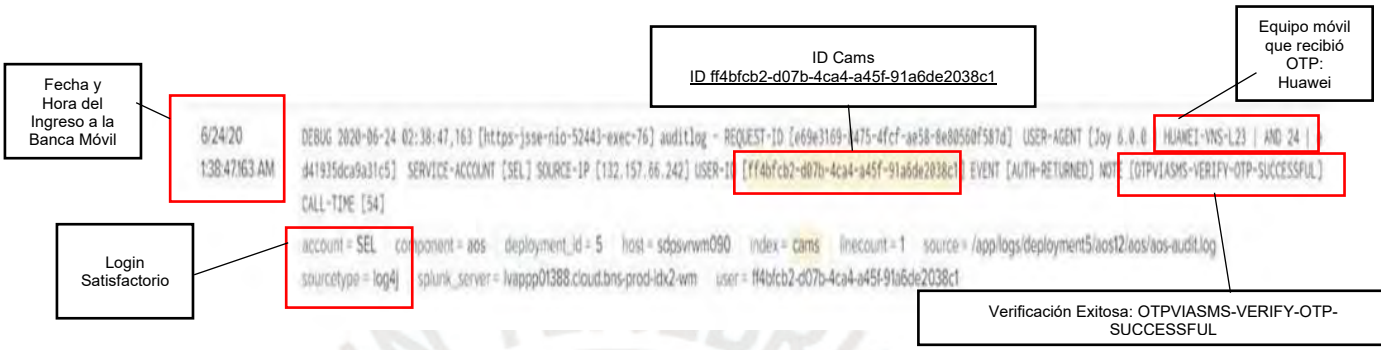
Ingreso a Banca Móvil para realización de operación S/ 5 900,00 del 25 de mayo de 2020



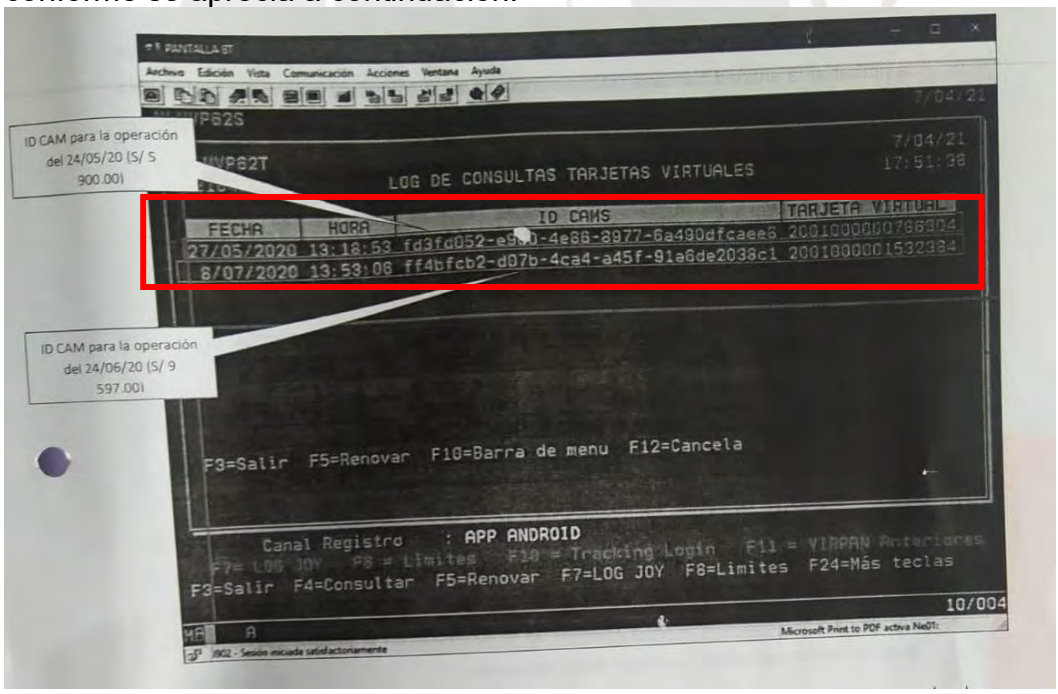
[12] Fecha consignada en el estado de movimientos del denunciante, debiéndose entender que tales operaciones fueron realizadas el 24 de mayo de 2020 como fecha real.

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"[13], 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-e9c0-4s86-8977-6a490dfcaee8 y

[13] En la foja 85 (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-e9c0-4s86-8977-6a490dfcaee8 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.

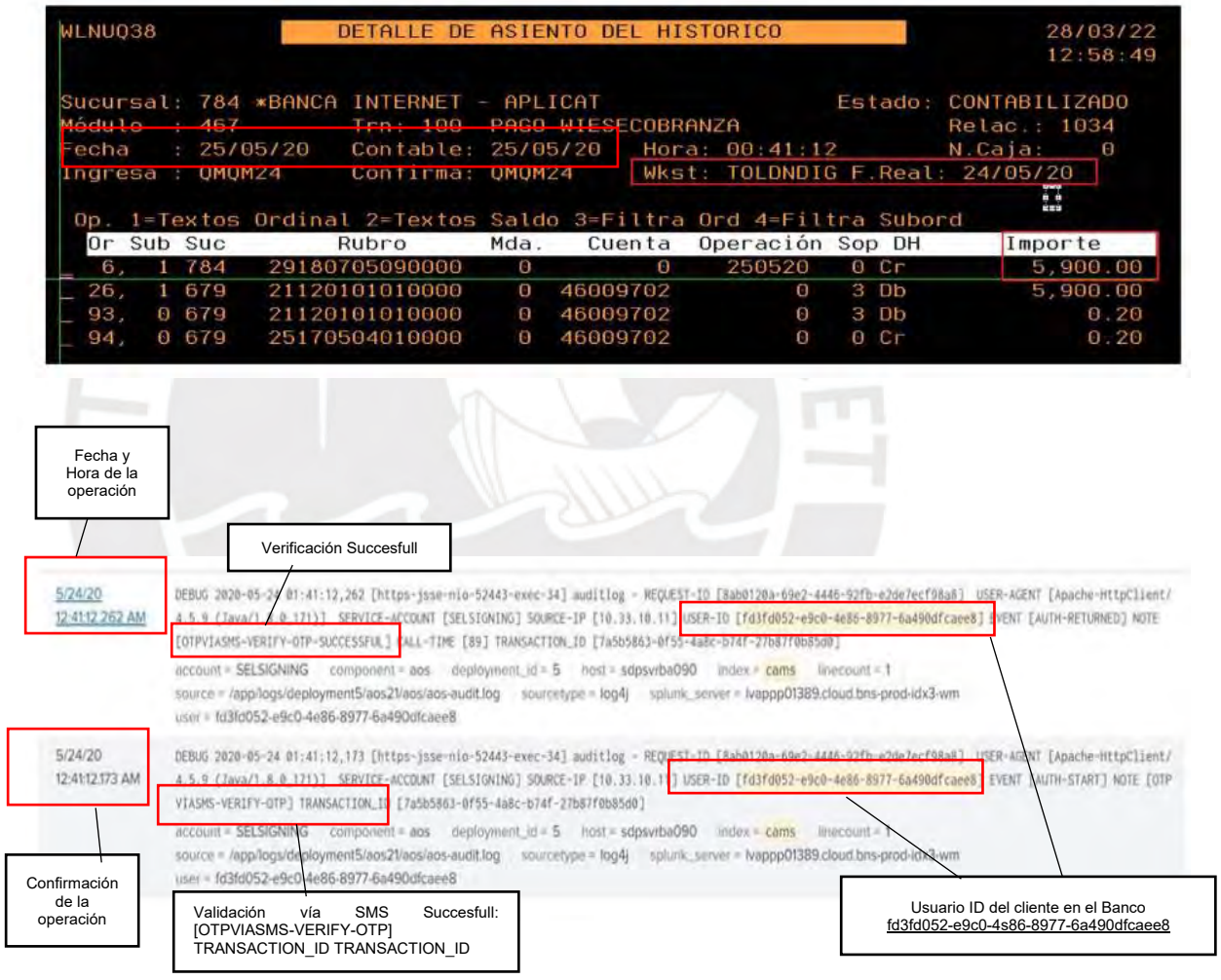
49. Al respecto, el Banco refirió que los reportes del medio probatorio "Pantallas *Splunk*"[14] demostraban la veracidad de sus afirmaciones sobre el particular.

[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 Prosa 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:

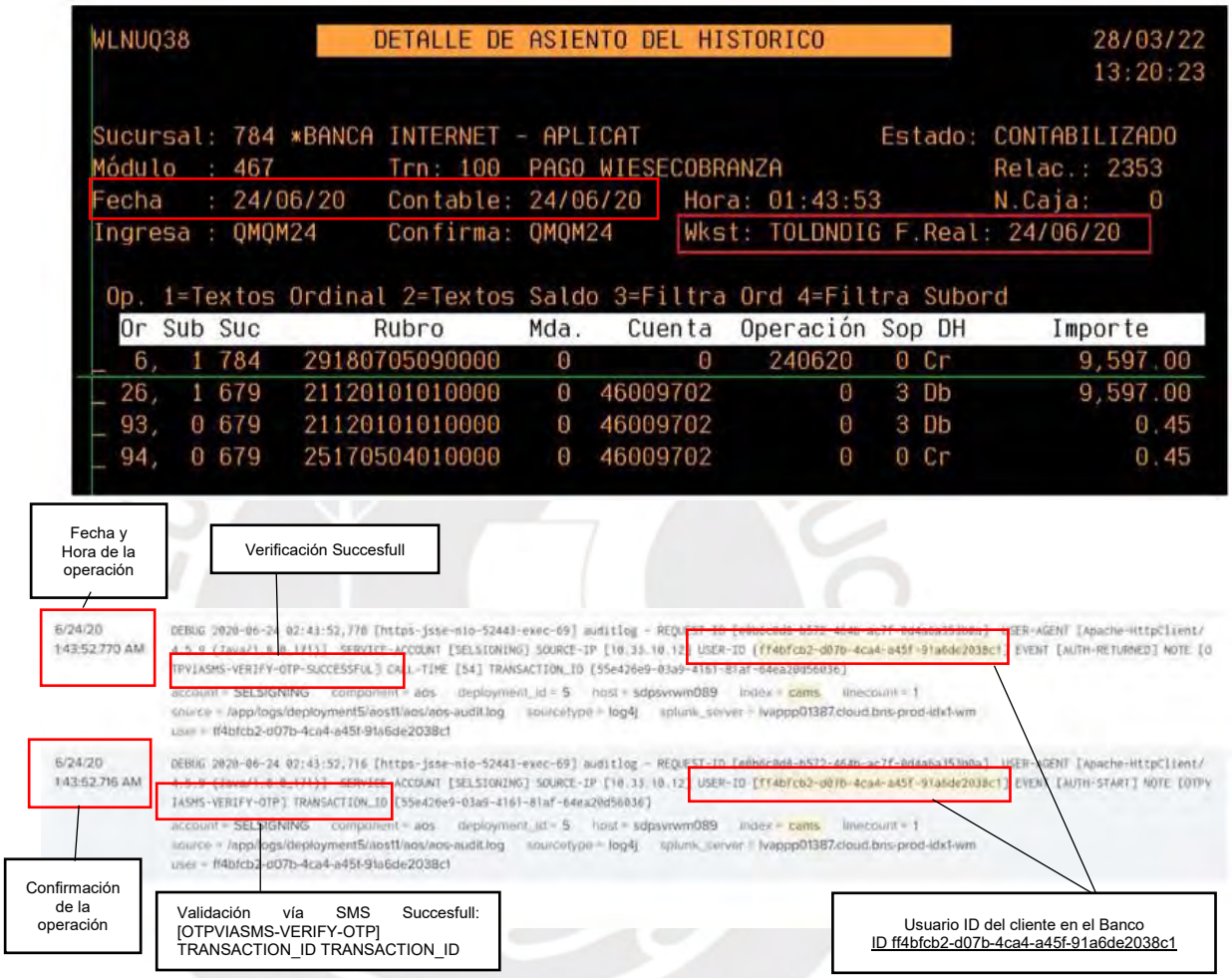
Operación de S/ 5 900,00



[Ver imagen en la siguiente página]

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

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 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 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.

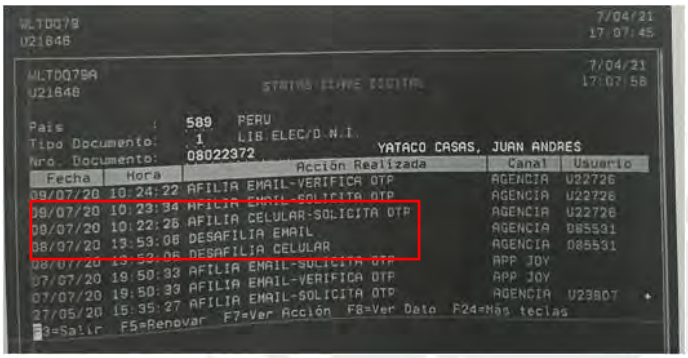
55. Ahora bien, habiendo quedado acreditado que las fechas consignadas en tales reportes no denotan el cargo de operaciones ejecutadas indebidamente, es pertinente continuar con el análisis de los medios probatorios presentados y acotar que los mismos recogen la siguiente información: (i) fecha y hora 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-e9c0-4s86-8977-6a490dfcaee8 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-.

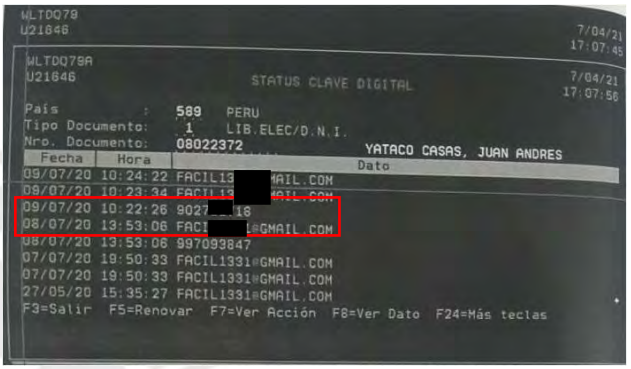
56. A ello se aúna que el proveedor sustento que el envío de las claves digitales empleadas para autorizar las transacciones controvertidas al teléfono celular del denunciante, vía SMS, se acreditaba bajo la consignación de la nota [OTPVIASMS-VERIFY-OTP] TRANSACTION_ID en sus sistemas, código que se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

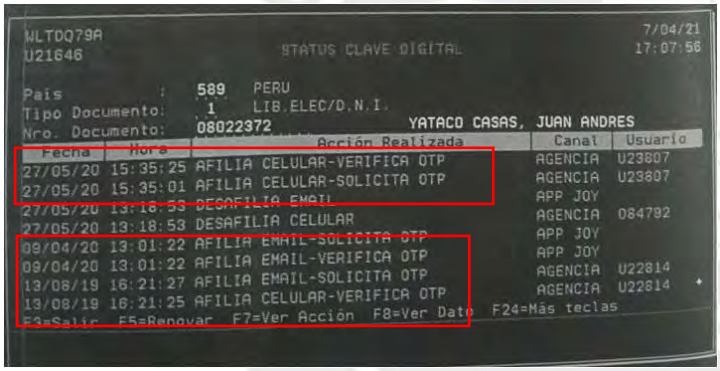
57. En este punto, cabe agregar que, conforme los *prints* de pantalla del sistema del Banco denominado “Status Clave Digital” que se visualizan a continuación, se encontraba acreditado que el denunciante mantuvo afiliados al servicio de banca móvil, su correo electrónico –facil1**1@gmail.com- y número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

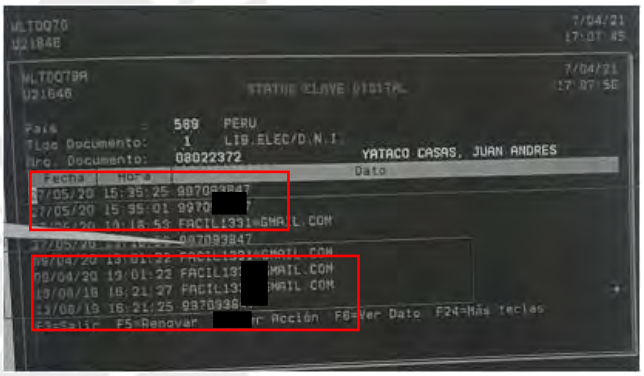
INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

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.

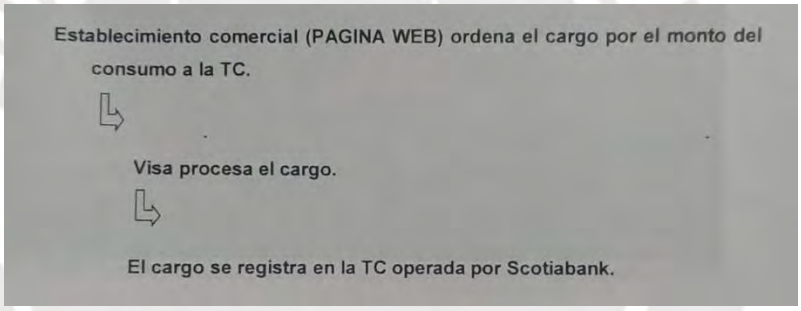
- <u>Sobre el consumo por el importe de S/ 3 196,30</u>

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

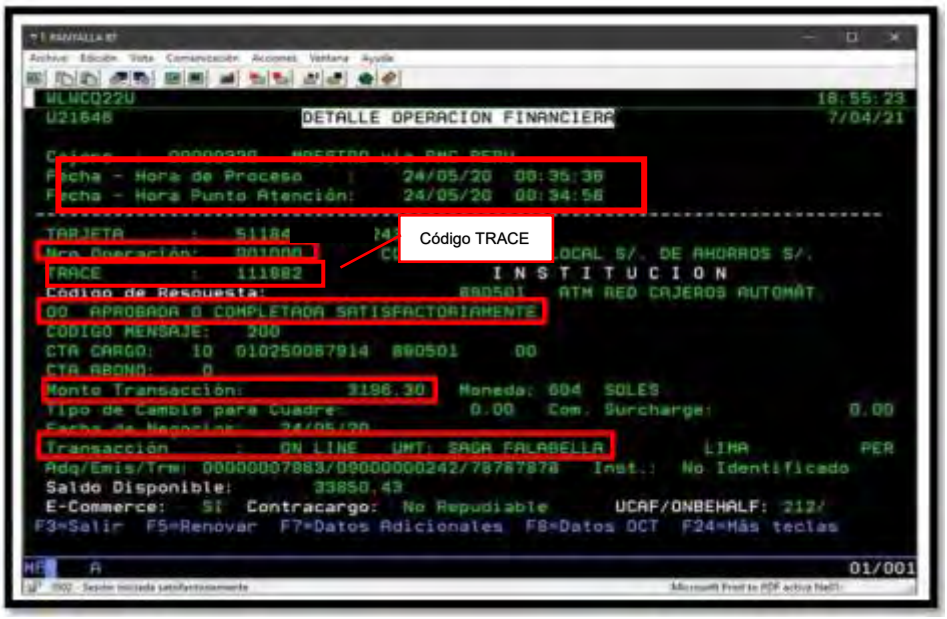
INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
Calle De la Prosa 104, San Borja, Lima 41 - Perú Telf: 224 7800 / Fax: 224 0348
E-mail: postmaster@indecopi.gob.pe / Web: www.indecopi.gob.pe

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.

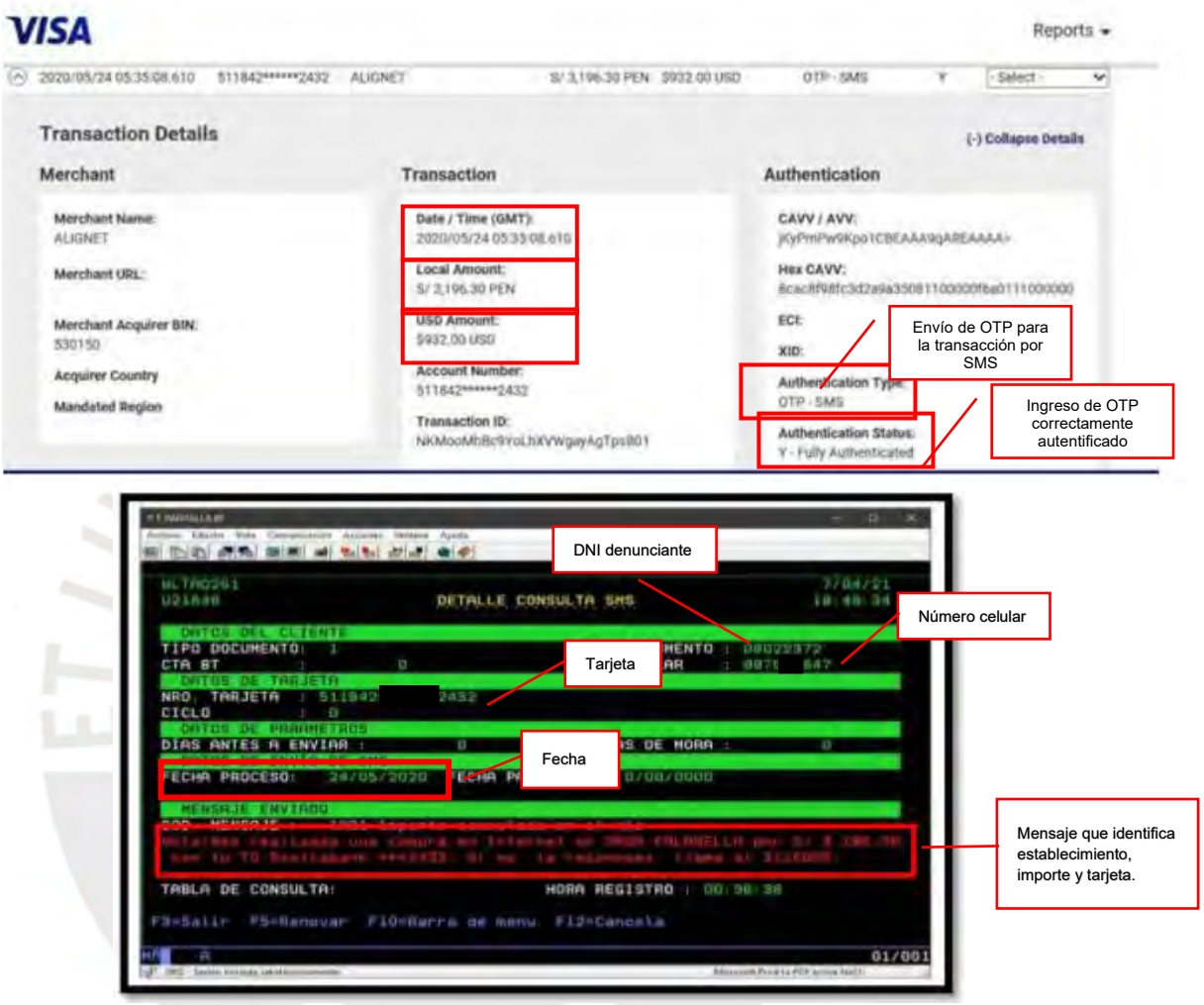
61. En esa línea, cabe mencionar que, respecto de la operación en cuestión en este punto, el Banco señaló que el referido consumo había sido realizado siguiendo el circuito operativo normal previsto para este tipo de operaciones, de acuerdo a la siguiente imagen:



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

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

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 19º 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 Juan Andrés Yataco Casas contra Scotiabank Perú S.A.A.; y en consecuencia, se declara infundada la misma, por presunta infracción de los artículos 18º y 19º 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 Scotiabank Perú S.A.A. 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 Juan Andrés Yataco Casas (en adelante, el señor Yataco) contra Scotiabank Perú S.A.A. (en 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[16] 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

[16] 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 Prosa 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-**-****-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**	

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	Sí
Enero 2020	5	S/ 500,00	S/ 1 048,00	2	Sí
Febrero 2020	20	S/ 7 000,00	S/ 23 590,00	4	Sí
Marzo 2020	11	**S/ 18 000,00**	S/ 25 725,00	2	Sí
Abril 2020	11	S/ 500,00	S/1 387,36	2	Sí

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

(iii) 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-bi”-, 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/ 9 991,61, 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.**

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-bi”-, 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 Yataco en 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 18º 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