Señores Comisión de Regulación de Comunicaciones,

En atención a la segunda publicación para comentarios del Documento de formulación del problema relacionado con la *"Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles"* a continuación, la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, y sus Entidades Agremiadas responden a la consulta y realizan algunos comentarios al documento.

COMENTARIOS GENERALES:

En primer lugar, se reconoce y valora la iniciativa de la Comisión de Regulación de Comunicaciones ("CRC") orientada a fortalecer el marco regulatorio para mitigar el fraude cibernético a través de servicios móviles, en particular en los servicios tradicionales de voz y mensajería SMS. Se resalta igualmente el esfuerzo por promover la participación y gestión entre los diferentes actores involucrados, quienes han manifestado su disposición para aportar soluciones efectivas en este ámbito.

Desde la perspectiva del sistema financiero, estos canales continúan siendo vectores críticos de inicio del fraude, especialmente en esquemas de suplantación de entidades financieras, ingeniería social, apropiación de credenciales y activación de fraudes posteriores en canales digitales y de pagos.

El problema identificado en el documento

En esta segunda versión se precisa que a partir de la primera publicación se identificaron las principales causas y consecuencias que permiten delimitar la existencia del problema central, que se basa en la *"ausencia de herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto"*.

Sobre este aspecto, se sugiere tener en cuenta que el problema central no radica exclusivamente en la ausencia normativa, también se ha evidenciado que las herramientas regulatorias actualmente disponibles para prevenir el contacto fraudulento no son efectivas, lo cual justifica plenamente la gestión que se está realizando de revisión y fortalecimiento del marco regulatorio vigente.

Rol habilitador de los servicios móviles y enfoque diferenciado

Resulta acertado que el documento reconozca que, si bien el fraude no siempre se materializa directamente a través de los servicios móviles, estos operan como un canal habilitador inicial de fraudes financieros de alto impacto, lo que los posiciona como un punto estratégico para la intervención preventiva. La segmentación de las alternativas regulatorias aplicables a los servicios de voz y SMS es coherente con las tipologías reales de fraude que afectan al sector financiero —como el smishing, vishing, spoofing y la manipulación del identificador de llamadas (CLI)— y facilita el diseño de controles focalizados y proporcionales. Asimismo, se destaca el avance hacia un enfoque que reconoce la necesidad de distribuir responsabilidades entre los distintos actores del ecosistema (proveedores de redes y servicios de telecomunicaciones, proveedores de contenidos y

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

aplicaciones, integradores y carriers internacionales), mitigando la concentración de cargas regulatorias y promoviendo un esquema de corresponsabilidad equilibrado.

Sender ID, protección de marcas y riesgo sistémico de suplantación

Se identifica una oportunidad para que el esquema de *Sender ID* se consolide como un habilitador efectivo de la confianza digital y como una herramienta de mitigación del riesgo sistémico asociado al fraude. Para ello, resulta indispensable que el uso de nombres o marcas vinculadas a entidades vigiladas esté respaldado por mecanismos robustos de validación, que prevengan la utilización indebida de denominaciones reconocidas por parte de terceros no autorizados. Un esquema que se limite a la mera visualización del nombre del remitente, sin controles efectivos sobre su legitimidad, podría generar una falsa percepción de seguridad en los usuarios y, en consecuencia, incrementar la efectividad de esquemas de fraude de alcance masivo. La asignación de códigos alfanuméricos debería otorgarse exclusivamente a comercios y entidades reales, evitando su uso por empresas fachada o estructuras creadas con fines fraudulentos, lo cual fortalecería la trazabilidad de la cadena de valor y maximizaría el impacto preventivo de la medida.

En este sentido, resulta relevante que el enfoque propuesto avance en la protección de las marcas financieras y reconozca que la suplantación no constituye un riesgo que deba ser gestionado de manera aislada por cada entidad, sino un riesgo de carácter sistémico propio del ecosistema de mensajería, que requiere mecanismos coordinados y homogéneos. El modelo propuesto abre espacio para la adopción de bloqueos preventivos de campañas fraudulentas, con un impacto directo en la reducción del fraude, la protección de los usuarios y la estabilidad del ecosistema digital. No obstante, se estima necesario que este esquema evolucione más allá de validaciones puntuales a cargo de determinados actores, en la medida que los controles fragmentados han demostrado ser insuficientes frente a amenazas de naturaleza sistémica. En consecuencia, se resalta la importancia de avanzar hacia criterios uniformes, esquemas centralizados y reglas claras de gestión que permitan mitigar de manera estructural el uso indebido de marcas bancarias y reducir los impactos reputacionales, operativos y de confianza a nivel sectorial.

Adicionalmente, se identifica una oportunidad estratégica para que las soluciones que desarrolle la CRC se diseñen bajo un enfoque interoperable y orientado a la integración tecnológica, de forma que la información generada no solo sea utilizada para controles propios de la mensajería, sino que pueda ser aprovechada de manera preventiva por las entidades financieras en sus procesos de gestión del fraude, monitoreo y toma de decisiones, fortaleciendo una respuesta anticipada, coordinada y basada en riesgos frente al fenómeno.

Consecuencias disuasivas, evaluación por impacto y articulación intersectorial

Se sugiere tener en cuenta que las exigencias normativas deben propender por una articulación efectiva de los actores del ecosistema y avanzar de manera complementaria en distintos frentes. En particular, se resalta la necesidad de incorporar consecuencias claras, progresivas y automáticas frente a la reincidencia en la facilitación del fraude, especialmente en relación con el uso indebido de códigos cortos, identificadores alfanuméricos y numeración nacional e internacional, en la medida en que la ausencia de medidas suficientemente disuasivas genera un alto retorno económico del fraude y traslada

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

los riesgos y pérdidas al consumidor financiero y a las entidades vigiladas. Asimismo, resulta fundamental que las medidas regulatorias se evalúen en función de su impacto real en la reducción del fraude financiero, y no únicamente con base en la implementación formal de controles técnicos.

En este contexto, se recomienda que, dentro de los actores clave involucrados en el diseño, implementación y seguimiento de las alternativas regulatorias, se incluya de manera expresa a la Superintendencia Financiera de Colombia, dada su competencia en materia de supervisión prudencial, protección al consumidor financiero y gestión de riesgos operativos y tecnológicos. De igual forma, se resalta la importancia de establecer mecanismos de seguimiento continuo que permitan evaluar la efectividad de las medidas adoptadas, evitando cargas excesivas, duplicidad de controles o impactos no deseados sobre la operación de las entidades financieras.

Coordinación sectorial y cobertura de modalidades de alto impacto

La mitigación efectiva del fraude exige una articulación estructural y operativa entre el sector de telecomunicaciones y el sector financiero, particularmente en aspectos como el intercambio oportuno de señales de fraude, campañas activas, el uso controlado de capacidades propias de las redes móviles para robustecer procesos de autenticación financiera, la coordinación con autoridades de supervisión y judicialización, y la definición de protocolos de actuación ante eventos de suplantación.

En este contexto, es necesario que el marco regulatorio contemple de manera expresa modalidades de alto impacto financiero, tales como la prevención del SIM Swapping, el reconocimiento del uso creciente de inteligencia artificial generativa para la suplantación de voz y mensajes, y el rol de los servicios móviles como factor de autenticación en múltiples servicios financieros, en la medida en que estas modalidades representan riesgos sistémicos que trascienden el simple contacto fraudulento y requieren una respuesta regulatoria integral y coordinada.

Se reconoce que el documento objeto de análisis recoge preocupaciones legítimas del sector financiero y propone herramientas que, de ser adecuadamente implementadas, pueden contribuir a la protección del consumidor y a la estabilidad del sistema financiero. No obstante, se recomienda realizar un seguimiento continuo a los avances de estas alternativas, con el fin de asegurar que su implementación permite a las entidades financieras mantener la continuidad y eficiencia de sus servicios, evitando cargas excesivas, duplicidad de controles o riesgos de interrupción en canales críticos, como los asociados a la autenticación de transacciones y la notificación al cliente.

Por su parte, entre los principales retos se identifica la necesidad de calibrar adecuadamente los sistemas de etiquetado y alerta, de manera que se minimicen los falsos positivos que puedan afectar la experiencia del usuario y la confianza en los canales de las entidades financieras. En este punto, resulta relevante otorgar claridad normativa respecto de que la obligación asociada a la implementación, operación y ajuste de dichos sistemas recae en los operadores de servicios móviles.

Así mismo, es necesario que la regulación contemple mecanismos expeditos de reclasificación, revisión y apelación frente a eventuales bloqueos o marcaciones erróneas

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

de comunicaciones legítimas, así como una delimitación clara de responsabilidades entre los distintos actores de la cadena de valor. En este sentido, se estima pertinente que se definan criterios claros y homogéneos para el etiquetado de las comunicaciones, tales como las categorías de “No verificada” o “Probable fraude”, asegurando que se minimicen los falsos positivos, que las alertas sean comprensibles para el usuario final y que los criterios de clasificación se encuentren homologados para todos los sectores impactados.

En general, se resalta la importancia de que la regulación promueva de manera expresa la colaboración entre entidades financieras, operadores de telecomunicaciones y autoridades, con el fin de facilitar el intercambio de información sobre patrones de fraude, rutas sospechosas y mejores prácticas de prevención, que permitan anticipar de forma coordinada la aparición de nuevas modalidades de fraude. Finalmente, se recomienda que, previo a la implementación masiva de nuevas medidas, se promueva la realización de pruebas piloto que permitan ajustar parámetros técnicos y evaluar su impacto en la experiencia del usuario y en la mitigación del fraude.

En atención a lo expuesto en la presente comunicación, y considerando la importancia de esta iniciativa, recomendamos la definición de un cronograma que contemple la realización de mesas técnicas con la participación de todos los actores relevantes, con el propósito de abordar y profundizar en cada uno de los aspectos planteados.

COMENTARIOS PARTICULARES A LAS ALTERNATIVAS:

Alternativas regulatorias para mitigar el fraude mediante mensajes cortos de texto (SMS)

En términos generales, se valoran las medidas propuestas en la medida en que abordan de forma integral distintos controles orientados a la mitigación del fraude en el ecosistema de mensajería SMS. En particular, se reconoce la alternativa asociada a la identificación del remitente a nivel de cada marca, siempre que su implementación se realice de forma individualizada por marca; de lo contrario, podría generar confusión entre los usuarios y aumentar la exposición al fraude por ingeniería social. Por su parte, las alternativas basadas exclusivamente en la diferenciación de mensajes promocionales no se consideran suficientemente eficaces, pues es precisamente en este tipo de tráfico en donde se concentra una proporción significativa del fraude por smishing.

Por su parte, se estima necesario que las alternativas regulatorias incorporen de manera expresa la obligación de implementar controles técnicos preventivos a nivel del canal SMS. En este sentido, resulta pertinente exigir la autenticación del origen de los mensajes mediante mecanismos criptográficos o protocolos seguros, el filtrado y monitoreo activo del tráfico para identificar patrones anómalos como picos de envío, ráfagas de mensajes o rutas internacionales no verificadas, así como la implementación de firewalls de señalización y el endurecimiento de protocolos para prevenir la explotación de vulnerabilidades como el SS7 Hacking. Estas medidas deberían complementarse con el bloqueo dinámico de comunicaciones clasificadas como no verificadas o de probable fraude, acompañado de procesos de revisión, trazabilidad y gestión de excepciones.

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

Frente a las alternativas que contemplan monitoreo por parte de los agregadores, resulta necesario definir de manera clara los procesos de conocimiento del cliente (KYC, por sus siglas en inglés) aplicables para mitigar riesgos de suplantación y uso de estructuras fraudulentas, así como establecer reglas y penalizaciones en caso de participación en el envío de SMS fraudulentos. Adicionalmente, se considera pertinente promover mecanismos de intercambio oportuno de información entre los actores afectados, que permitan la actualización continua de las reglas de monitoreo. En este mismo sentido, también resulta necesario definir niveles de servicio exigibles a los agregadores en materia

de alertas de fraude y los tiempos de reacción esperados para el bloqueo o etiquetado de SMS fraudulentos.

Finalmente, se resalta la necesidad de proteger comunicaciones sensibles mediante listas blancas de dominios de pago, deeplinks firmados, el uso exclusivo de mensajería in-app para operaciones críticas y la migración progresiva hacia soluciones que permitan el cifrado de extremo a extremo del contenido, con el fin de evitar la interceptación del mensaje en claro y proteger la confidencialidad de la información. Todas estas medidas deberían ser obligatorias, auditables y estar acompañadas de métricas de efectividad y niveles de servicio regulatorios que garanticen la resiliencia del canal SMS frente a ataques y fraudes, así como complementarse con la obligatoriedad para los operadores de implementar esquemas de monitoreo del tráfico P2P y mecanismos de reacción frente a los alertamientos generados.

Alternativas regulatorias para mitigar el fraude mediante servicios tradicionales de voz*[1]

Respecto a los servicios tradicionales de voz, se identifica un riesgo estructural asociado a la suplantación, el enmascaramiento de numeración y el uso de inteligencia artificial generativa para la clonación o imitación de voz. En este contexto, es necesario que las alternativas regulatorias incluyan mecanismos técnicos obligatorios de autenticación del origen de las llamadas, orientados a reducir la efectividad del fraude telefónico, tales como la implementación de protocolos como STIR/SHAKEN, complementados con Rich Call Data, así como la creación de un registro nacional de numeración autorizada para llamadas asociadas a servicios financieros.

No obstante, se advierte que los controles centrados exclusivamente en la autenticación del originador pueden resultar insuficientes, en la medida en que el fraude por vishing puede ser ejecutado por usuarios legítimos con intenciones fraudulentas. En este sentido, se considera necesario complementar dichos mecanismos con capacidades de validación y análisis del tráfico de voz que permitan identificar patrones anómalos, tales como tasas inusuales de establecimiento de llamadas, tráfico proveniente de rutas internacionales no verificadas o comportamientos recurrentes asociados a campañas de fraude. Estas capacidades deberían articularse con herramientas basadas en inteligencia artificial que faciliten la detección temprana de señales de fraude y fortalezcan la capacidad de reacción de operadores y autoridades competentes.

*Con servicios tradicionales de voz se hace referencia únicamente a llamadas telefónicas. Esto, con ocasión a que este concepto podría incluir otros servicios como la mensajería de voz.

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

De igual forma, se resalta la importancia de fortalecer la resiliencia frente a ataques asociados a la explotación de protocolos de señalización, mediante la implementación de firewalls especializados para SS7/SIGTRAN, reglas de filtrado, rate limiting, validación de Global Title, auditorías periódicas y pruebas de penetración sobre interconexiones internacionales, con el fin de mitigar riesgos sistémicos asociados al fraude por voz.

La adopción conjunta de estos controles técnicos con acciones orientadas a la educación del usuario puede contribuir a una mayor comprensión y efectividad de los cambios regulatorios propuestos.

Alternativas regulatorias enfocadas en la educación de la ciudadanía

La educación ciudadana se reconoce como uno de los ejes fundamentales para reducir la vulnerabilidad del usuario frente a las distintas tipologías de fraude. En este sentido, se considera necesario fortalecer campañas conjuntas entre la CRC y el sector financiero orientadas a la prevención del fraude por ingeniería social, integradas en aplicaciones bancarias, SMS y otros canales digitales, con mensajes claros y consistentes que refuercen la creación y gestión de contraseñas seguras, la identificación de intentos de suplantación y el uso responsable de llamadas, enlaces y solicitudes de información.

Estas iniciativas educativas deben concebirse como un complemento directo de los controles técnicos y de monitoreo previstos para los servicios de SMS y voz, de manera que refuercen su efectividad y contribuyan a una reducción integral del riesgo de fraude. Asimismo, se destaca la necesidad de implementar acciones de educación masiva y sostenida, incluyendo medios tradicionales como televisión y radio, así como medios digitales, desarrolladas de manera coordinada, intersectorial y continua, conforme a los lineamientos regulatorios.

Alternativas regulatorias asociadas al régimen de administración de los recursos de identificación

El documento pone de manifiesto la necesidad de fortalecer la gestión de los recursos de identificación, la trazabilidad de los eventos de fraude y los mecanismos de reporte oportuno. En este marco, se considera pertinente promover la integración del sector financiero con los sistemas administrados por la CRC para el reporte de campañas fraudulentas, numeración sospechosa y otros eventos relevantes, bajo esquemas interoperables y estandarizados. Asimismo, resulta necesario avanzar hacia mecanismos de bloqueo preventivo e inmediato de los recursos reportados por fraude, con criterios homogéneos, trazabilidad adecuada y procedimientos de revisión claramente definidos.

Desde una perspectiva general, el régimen propuesto resulta adecuado, destacándose la conveniencia de incorporar penalizaciones claras frente al uso indebido y la reincidencia en la utilización de recursos de identificación. Adicionalmente, se resalta la necesidad de implementar controles específicos frente a modalidades como el SIM swapping, mediante verificaciones reforzadas en los procesos de cambio de SIM, el uso de autenticación multifactor, biometría o estándares como FIDO2, así como la generación de alertas preventivas al usuario y la aplicación de bloqueos temporales de originación A2P hasta la

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

culminación de las validaciones correspondientes, dada la relevancia de la red móvil como factor crítico de autenticación para múltiples servicios financieros.

Finalmente, se identifica una oportunidad estratégica para que las soluciones que desarrolle la Comisión se diseñen bajo un enfoque interoperable y API-ready, de forma que la información generada pueda ser consumida de manera preventiva por las entidades en sus procesos de gestión de fraude, monitoreo y toma de decisiones. En este mismo sentido, se sugiere evaluar la incorporación de una alternativa adicional consistente en la exigencia de procesos de KYC por parte de los operadores móviles para la verificación de la identidad de los usuarios que soliciten la reexpedición de SIMs o adquisición de nuevas líneas, medida que ha sido adoptada en otros países y que podría contribuir de manera significativa a la prevención del fraude desde el origen del servicio.

REPUESTAS AL FORMULARIO:

1. **Considerando que la atención coordinada del fraude mediante una estrategia nacional es una necesidad urgente para el país y los usuarios, y que este proyecto regulatorio será un paso de varios en la lucha contra un fenómeno tan dinámico, ¿qué tiempos de implementación estima necesarios para cada una de las medidas propuestas, teniendo en cuenta los desarrollos y capacidades actuales de los PRST y agregadores? ¿Qué retos técnicos, operativos o regulatorios podrían influir en esos plazos? ¿Qué esquemas de transición o fases intermedias propondría para garantizar una metodología ágil con victorias tempranas que permita atender oportunamente la creciente oleada de comunicaciones fraudulentas en el país?**

   El proyecto regulatorio tendrá un impacto relevante en el fortalecimiento de la seguridad de las comunicaciones en el país, lo que se traducirá en un incremento de la confianza de los usuarios para adquirir productos y servicios, así como para realizar y gestionar sus operaciones financieras de manera segura. En este marco, se considera pertinente que los controles previstos se implementen de forma gradual a lo largo de 2026, priorizando en una primera fase aquellos mecanismos que generen beneficios inmediatos para los usuarios y permitan obtener resultados tempranos y medibles en la prevención y mitigación del fraude, sin afectar la continuidad ni la eficiencia de los servicios.

2. **¿Qué ventajas, desventajas, retos y oportunidades identifica en la implementación por parte de la CRC de mecanismos de evaluación periódica de las medidas adoptadas para mitigar el fraude mediante servicios móviles tradicionales de voz y SMS? ¿Qué criterios, metodologías o frecuencias de evaluación considera más adecuados para asegurar la efectividad y actualización continua de estas medidas?**

   Para una implementación exitosa, resulta fundamental contar con un esquema de seguimiento y evaluación continua que permita medir tanto la adopción de las medidas como su efectividad en la mitigación del fraude. Este seguimiento podría realizarse mediante espacios periódicos de revisión —por ejemplo, de carácter trimestral— con la participación de los principales actores del ecosistema (PRST, agregadores, entidades

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

financieras y comercios), en los que se presenten los controles implementados y los resultados observados.

La evaluación periódica facilita ajustes regulatorios oportunos, fortalece la corresponsabilidad entre los actores y mejora la transparencia y confianza del ecosistema.

En cuanto a las oportunidades, este enfoque permite identificar tempranamente nuevas tipologías de fraude, promover el intercambio de información y priorizar la adopción de medidas más efectivas. Respecto a los criterios y metodologías, se recomienda utilizar indicadores claros y comparables, como la evolución de eventos fraudulentos, tiempos de detección y respuesta, y niveles de adopción de los controles.

3. **¿Cuáles considera que son los principales aciertos y limitaciones de las alternativas propuestas para mitigar el contacto fraudulento a través de servicios tradicionales de voz y mensajes de texto? ¿Qué elementos adicionales o diferentes propondría para mejorar la eficacia de estas medidas?**

   El principal acierto de las alternativas propuestas radica en que, consideradas de manera conjunta, permiten una mitigación integral del fraude que actualmente se genera a través de estos medios. No obstante, de manera complementaria a los controles propuestos, se considera necesario: (i) establecer mecanismos colaborativos que permitan alimentar y fortalecer los controles de monitoreo; (ii) definir niveles de servicio (SLA) para aquellas alternativas que impliquen monitoreo, bloqueo y generación de alertas; (iii) establecer procesos de KYC y validación de identidad por parte de los operadores para todos los adquirentes de líneas telefónicas, medida que ha mostrado resultados positivos en otros países, como Alemania; (iv) abordar de manera específica la problemática asociada a la reexpedición de tarjetas SIM; y (v) reforzar las medidas orientadas a la mitigación del phishing.

4. **¿Qué métricas, indicadores o criterios considera que deberían establecerse en la industria para evaluar de manera efectiva la reducción del fraude y el impacto de las alternativas regulatorias propuestas en este documento? ¿Qué variables cuantitativas o cualitativas serían más útiles para medir la evolución del fraude, la protección al usuario y la eficacia de las medidas implementadas, y cómo podrían ser recolectadas y/o reportadas de forma coordinada entre los diferentes actores del sector?**

   Un criterio relevante para evaluar el impacto de las medidas en la mitigación del fraude es el volumen de contactos y reportes recibidos por las entidades financieras y las entidades gubernamentales asociados a eventos de smishing y vishing. La evolución de este indicador permitiría identificar patrones, evaluar la efectividad de las alternativas regulatorias implementadas y medir su impacto en la protección al usuario.

   De manera complementaria, resulta pertinente contar con un compendio consolidado de las casuísticas más recurrentes, que permita analizar los principales patrones y modalidades de fraude reportados. Esta información serviría como insumo para la retroalimentación y ajuste continuo de los controles existentes, así como para la adopción o priorización de nuevas medidas, y podría ser recolectada y compartida de forma coordinada entre los distintos actores del sector, bajo criterios comunes de reporte y estandarización de la información.

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

5. **Frente a las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS) ¿Qué retos y beneficios identifica en la implementación de un proceso obligatorio de conocimiento del cliente (KYC) para agregadores de SMS? ¿Qué criterios mínimos considera indispensables para que este proceso sea efectivo y no excluyente?**

   La implementación de un proceso obligatorio KYC para los agregadores de SMS presenta beneficios relevantes en la mitigación del fraude, al constituirse como el primer control para prevenir la dispersión de mensajes fraudulentos. Este mecanismo fortalece la trazabilidad y reduce el riesgo de suplantación o uso indebido del canal SMS.

   No obstante, el principal reto consiste en definir un nivel de KYC suficientemente robusto para identificar empresas legítimas y verificar la coherencia entre su actividad comercial y el contenido de los mensajes enviados, sin generar barreras de entrada ni afectar la competencia. Para su efectividad, resulta indispensable establecer criterios mínimos claros y proporcionales, así como implementar procesos periódicos de actualización del KYC que permitan un seguimiento continuo al uso adecuado del canal.

6. **Teniendo en cuenta que los agregadores pueden actuar tanto en acuerdos directos como en esquemas en cadena para tráfico internacional, ¿qué diferencias, riesgos u oportunidades identifica entre estos dos tipos de tráfico?**

   Se considera necesario establecer controles generales que sean aplicables tanto al tráfico nacional como al internacional, con el fin de garantizar un nivel mínimo homogéneo de protección frente al fraude. Sin embargo, dadas las particularidades del tráfico internacional, especialmente cuando se estructura a través de esquemas en cadena, resulta pertinente que ciertos controles sean más estrictos en estos casos.

   En particular, el tráfico internacional presenta riesgos asociados a una mayor exposición al fraude, limitaciones en la trazabilidad del origen real del mensaje, menores niveles de KYC sobre los actores involucrados en la cadena, y restricciones prácticas para la aplicación de medidas correctivas o sancionatorias una vez ocurrido un evento fraudulento. Estas condiciones reducen la capacidad de reacción efectiva del ecosistema y elevan el impacto potencial sobre los usuarios finales.

   No obstante, la diferenciación regulatoria también representa una oportunidad para fortalecer los esquemas de control, priorizando exigencias adicionales para el tráfico internacional, tales como mayores estándares de identificación del origen, monitoreo reforzado y mecanismos preventivos más robustos. Este enfoque permitiría mitigar los riesgos asociados sin afectar de manera innecesaria el tráfico legítimo, promoviendo un uso más seguro y confiable de los servicios móviles.

7. **¿Considera pertinente la implementación de un proceso centralizado o distribuido para la validación de agregadores, marcas y campañas antes de cursar tráfico A2P?**

   Ambas alternativas, un proceso centralizado o uno distribuido, pueden contribuir a la mitigación del fraude en el tráfico A2P, en la medida en que fortalecen los mecanismos de validación previa de agregadores, marcas y campañas antes de cursar el tráfico. No obstante, con base en las referencias internacionales analizadas en el documento, así

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

como en consideraciones asociadas a la trazabilidad, la estandarización de criterios y la clara asignación de responsabilidades, se considera más conveniente optar por un proceso centralizado.

Un esquema centralizado permitiría aplicar criterios homogéneos de validación, reducir asimetrías entre actores, facilitar la supervisión regulatoria y mejorar la trazabilidad del origen del tráfico y de las campañas autorizadas. Adicionalmente, este enfoque favorece una identificación más clara de responsabilidades frente a eventuales incidentes de fraude, así como una respuesta más ágil y coordinada ante comportamientos irregulares.

8. **¿Cuáles serían los principales desafíos para un sistema centralizado de validación de remitentes y campañas?**

   El principal desafío de un sistema centralizado de validación de remitentes y campañas consiste en diseñar un proceso de inscripción y validación que articule de forma coherente la verificación de agregadores, remitentes y campañas, garantizando la legitimidad y consistencia del objetivo de los mensajes. Adicionalmente, el sistema debe equilibrar la robustez de los controles con la eficiencia operativa y la diversidad de modelos del ecosistema. Para fortalecer la transparencia y la corresponsabilidad, resulta pertinente compartir de manera periódica resultados agregados del proceso con los principales actores, como insumo para la mejora continua de los controles.

9. **¿Qué ventajas y desafíos identifica en un modelo distribuido basado en DLT?**

   Los principales retos se concentran en los aspectos técnicos y de gobernanza, particularmente en la delimitación de responsabilidades frente a eventos de fraude. Adicionalmente, resulta necesario garantizar una adecuada experiencia de usuario, mediante la detección y bloqueo efectivo de SMS fraudulentos, manteniendo bajos niveles de falsos positivos.

10. **¿Qué requerimientos funcionales debería tener una solución para validar la autenticidad de las URL contenidas en SMS?**

    Una solución para validar la autenticidad de las URL contenidas en SMS debería integrar mecanismos de evaluación conjunta del contenido del mensaje, la URL incluida y el nivel de riesgo asociado, considerando variables técnicas como el dominio u host, la reputación de la URL y la validez de los certificados SSL. Esto permitiría detectar oportunamente enlaces maliciosos y mitigar la distribución de phishing, reduciendo la exposición de los usuarios a fraudes.

11. **¿Qué impactos prevé en la obligación de bloquear o marcar mensajes sin identificadores validados?**

    La obligación de bloquear o marcar mensajes sin identificadores validados puede tener un impacto en la mitigación del fraude, al limitar la suplantación de identidad. Para evitar afectaciones al tráfico legítimo, resulta necesario establecer un proceso de transición gradual y un mecanismo de registro sencillo y estandarizado de los mensajes, que permita a los actores adaptarse sin afectar la entrega de comunicaciones legítimas.

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

12. **¿Qué ventajas y riesgos identifica en la clasificación obligatoria de mensajes por tipo de contenido?**

    Las principales ventajas se relacionan con el uso adecuado del consentimiento del usuario y la priorización de mensajes críticos, como alertas de seguridad, OTP o notificaciones financieras. El principal riesgo radica en garantizar una correcta categorización que evite que mensajes fraudulentos sean clasificados como prioritarios.

13. **¿Qué capacidades mínimas debería tener el sistema de monitoreo de tráfico por parte de los agregadores?**

    El sistema de monitoreo de tráfico de los agregadores debe contar con un motor de evaluación de riesgo en tiempo real, detección de patrones anómalos, reglas de control parametrizables y análisis de URLs. Adicionalmente, debe incorporar mecanismos de retroalimentación continúa basados en reportes de fraude, asegurar la trazabilidad de las acciones ejecutadas y generar reportes estandarizados que faciliten la supervisión y la mejora continua.

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

14. **¿Qué beneficios y limitaciones identifica en la asignación de identificadores exclusivos por marca?**

    Los beneficios dependen de la veracidad de la marca asociada a cada identificador, dado el riesgo de suplantación. En términos de trazabilidad, los beneficios serían mayores en la medida en que existan acciones efectivas frente a los agregadores y las marcas involucradas.

15. **¿Qué efectividad tendría la obligatoriedad de usar Sender ID únicos?**

    La obligatoriedad de usar Sender ID únicos puede contribuir a reducir la suplantación y fortalecer la confianza en el canal SMS, siempre que se implemente de forma articulada con los demás controles propuestos. De manera aislada, su efectividad sería limitada, por lo que resulta más adecuada como parte de un enfoque integral de mitigación del fraude.

16. **¿Considera pertinente limitar el uso de Sender ID a mensajes transaccionales?**

    Se considera pertinente que el uso de Sender ID aplique a todas las categorías de mensajes SMS y no solo a los transaccionales, dado que los mayores niveles de fraude se concentran actualmente en mensajes comerciales o publicitarios. Limitarlo únicamente a mensajes transaccionales podría generar brechas que faciliten prácticas fraudulentas, mientras que su aplicación transversal fortalecería la identificación del remitente, la trazabilidad y la protección del usuario.

17. **¿Qué criterios considera relevantes para definir patrones atípicos en el tráfico SMS P2P?**

    Para identificar patrones atípicos en el tráfico SMS P2P, son relevantes variables como la velocidad y frecuencia de envío, el volumen y número de destinatarios, la presencia y características de URLs, la repetición de contenidos, la antigüedad de la línea o código originador y el nivel de confianza del originador. La evaluación conjunta de estos criterios permite detectar usos indebidos del canal sin generar impactos significativos sobre los usuarios legítimos.

18. **¿Qué ventajas y desventajas identifica en la imposición de límites máximos de SMS P2P?**

    La principal ventaja es garantizar el uso legítimo del canal y mitigar el fraude. Los umbrales específicos podrían definirse por los PRST, considerando los usos habituales del servicio.

19. **¿Qué mecanismos de colaboración considera necesarios para una detección y judicialización más efectiva del fraude?**

    Para una detección y judicialización más efectiva del fraude, se requieren mecanismos de colaboración intersectorial que articulen a agregadores, operadores, entidades financieras y conglomerados comerciales. Estos esquemas deben operar bajo una gobernanza clara, liderada por la autoridad regulatoria nacional, que facilite el intercambio de información, la identificación de patrones y la coordinación con las autoridades competentes para la investigación y sanción de las conductas fraudulentas.

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

20. **Frente a las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz ¿Qué diferencias, riesgos y oportunidades observa entre tráfico nacional e internacional?**

    El tráfico internacional presenta mayores riesgos debido a limitaciones en la trazabilidad y en la efectividad de las medidas correctivas. En este contexto, se considera necesario establecer controles diferenciados, con reglas más estrictas para el tráfico internacional, sin perjuicio de aplicar de manera integral las temáticas propuestas para mitigar el fraude en llamadas nacionales.

21. **¿Qué mecanismos tiene actualmente implementados su organización para mitigar el spoofing?**

    Actualmente se desarrollan campañas de comunicación orientadas a la mitigación del fraude en este canal.

22. **¿Qué efectos prevé en la prohibición de llamadas internacionales con CLI nacional?**

    Entre los efectos positivos se destacan la mitigación del fraude, una mayor trazabilidad y el fortalecimiento de la confianza de los usuarios. Para la gestión de excepciones, podrían contemplarse listas específicas con procesos de KYC que eviten afectar servicios legítimos.

23. **¿Qué retos identifica en esquemas de etiquetado obligatorio en llamadas internacionales?**

    El principal reto consiste en diferenciar adecuadamente entre líneas que deban ser etiquetadas como “No verificadas” o “Probable fraude”, así como en lograr una adopción efectiva del esquema y que la etiqueta proporcione información útil al usuario.

24. **¿Qué oportunidades y retos identifica en la adopción de STIR/SHAKEN?**

    La adopción de STIR/SHAKEN ofrece una oportunidad para fortalecer la autenticación del origen de las llamadas y reducir la suplantación asociada al spoofing, aumentando la confianza en el servicio de voz. No obstante, el principal reto es asegurar su efectividad en la detección del fraude, la correcta categorización de las llamadas y una experiencia de usuario adecuada, evitando falsos positivos. Por ello, se considera necesario complementar estos protocolos con mecanismos adicionales como sistemas de filtrado y listas Do Not Originate (DNO, por sus siglas en inglés) para lograr una mitigación integral del fraude.

25. **¿Qué parámetros deberían estandarizarse para el monitoreo del tráfico de voz?**

    Se requiere el uso de tecnologías que evalúen el riesgo de cada llamada considerandos variables como originador, receptor, recurrencia, velocidad y duración, ajustando continuamente los parámetros para reducir falsos positivos.

26. **¿Qué actores deberían participar en una plataforma nacional de alertas?**

    Una plataforma nacional de alertas debería involucrar a entes gubernamentales, PRST, entidades financieras y grandes conglomerados comerciales, bajo un esquema de gobernanza claro. Esta articulación permitiría compartir alertas oportunas, identificar

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com

patrones de fraude y fortalecer la respuesta coordinada del ecosistema frente a incidentes de fraude.

27. ¿Qué ventajas y desafíos observa en rangos exclusivos de numeración comercial?

La efectividad de la medida es limitada si se implementa de manera aislada, pero podría aportar ventajas si se articula con las demás temáticas del proyecto.

28. ¿Qué impactos tendría el etiquetado obligatorio de llamadas comerciales manteniendo la numeración actual?

Podría mantenerse una alta exposición al fraude por vishing, además de generar un impacto operativo significativo.

El etiquetado obligatorio de llamadas comerciales manteniendo la numeración actual podría tener impactos limitados en la mitigación del fraude, en particular frente a esquemas de vishing, dado que los actores maliciosos continuarían aprovechando la suplantación de numeración para engañar a los usuarios. En este escenario, la exposición al fraude podría mantenerse, al no resolverse de manera estructural los problemas de autenticación y trazabilidad del origen de las llamadas.

Adicionalmente, esta medida podría generar un impacto operativo significativo para los actores del ecosistema, asociado a la adaptación de sistemas, procesos de marcación y gestión de excepciones, sin que ello se traduzca necesariamente en una reducción proporcional del riesgo de fraude. En este sentido, el etiquetado de llamadas resulta más efectivo cuando se articula con otros controles, como mecanismos de validación del origen, autenticación de llamadas y filtrado del tráfico, en línea con el enfoque integral propuesto en el documento.

29. ¿Qué beneficios y riesgos identifica en la creación de listas DNO?

Se considera necesario contar con un control transversal de las listas DNO entre los distintos PRST, garantizando bloqueos oportunos y coordinados. El principal desafío radica en asegurar su aplicación efectiva y uniforme en todos los PRST.

Carrera 9 No. 74-08 piso 9 Edificio Profinanzas
Bogotá D.C. Colombia
Tel: 60 1 3266600
www.asobancaria.com