Señores Comisión de Regulación de Comunicaciones,

En atención a la publicación del Proyecto de Resolución “Por la cual se modifican las condiciones de remuneración de los servicios móviles definidas en los capítulos II, III, VII y XVI del Título IV de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones”. ”, la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, se permite presentar los siguientes comentarios para su consideración:

Comentario General

Las propuestas contenidas en el Proyecto de Resolución buscan corregir ineficiencias y contribuir a la competencia en el mercado de mensajería y servicios mayoristas. No obstante, su propuesta sobre una reducción en la tarifa de remuneración de los SMS A2P y de los cargos asociados a datos, sin la incorporación de contrapesos antifraude obligatorios, expone de manera significativa al sistema financiero y al ecosistema digital a picos de smishing, abuso del One Time Password (OTP), call pumping y la automatización maliciosa.

Aunque la intención regulatoria suele orientarse a fomentar la competencia, la evidencia muestra que tarifas excesivamente bajas reducen la barrera de entrada para los ciberdelincuentes, facilitando el envío masivo de mensajes fraudulentos. Cuando las tarifas de terminación de SMS caen de manera abrupta, el costo marginal del envío se vuelve prácticamente insignificante. En estos escenarios, la rentabilidad de una campaña de smishing depende exclusivamente de la tasa de conversión: si el envío es casi gratuito, incluso tasas de éxito extremadamente bajas (por ejemplo, del 0,01 %) resultan económicamente atractivas para el atacante.

Esta relación no es meramente teórica. La última intervención tarifaria relevante se dio con la Resolución 7007 de 2022, que redujo la tarifa de terminación de SMS en aproximadamente un 73 %. De acuerdo con datos de la propia Comisión de Regulación de Comunicaciones, el efecto inmediato fue un incremento sostenido en las denuncias por fraude digital y suplantación de identidad, con una tasa anual cercana al 11 %, superando las 75.000 denuncias ante la Superintendencia de Industria y Comercio en el último periodo reportado (2024–2025). Este comportamiento resulta consistente con el hecho de que la mayoría de los delitos informáticos utilizan el SMS como canal inicial o de apoyo para su ejecución.

Adicionalmente, una caída tan agresiva de los cargos de acceso incrementa el riesgo de que el país se vea inundado de “tráfico gris”, proveniente de integradores y agregadores con bajos estándares de verificación de identidad (KYC/KYB), lo que dificulta la trazabilidad del origen del mensaje y la atribución de responsabilidades ante incidentes de fraude.

Vale la pena señalar que Colombia es uno de los pocos países de la región que mantiene una intervención regulatoria directa y particularmente agresiva sobre las tarifas de acceso para SMS A2P. En contraste, mercados como Brasil, Argentina y Chile operan bajo esquemas de libre competencia o acuerdos privados entre operadores para el tráfico de contenidos, donde los precios suelen ser más altos y permiten internalizar los costos asociados a ciberseguridad, monitoreo y control del fraude. En este contexto, Colombia se ubica entre los países con las tarifas más bajas de América Latina, sin que ello se haya traducido en una reducción proporcional del fraude.

El sector financiero resulta especialmente afectado por este entorno. Los Indicadores de Seguridad de la Información y Ciberseguridad de la Superintendencia Financiera de Colombia evidencian que durante 2024 se registraron cerca de 36.000 millones de ataques cibernéticos, lo que representa un incremento del 29 % frente a 2023. Adicionalmente, la CRC ha identificado que el 49,5 % de las quejas recibidas por la DIJÍN corresponden a hurtos por medios informáticos, siendo el SMS el principal vector para el robo de credenciales bancarias.

El fraude digital en Colombia se concentra principalmente en esquemas basados en SMS, los cuales representan cerca del 70 % de las reclamaciones por fraude en canales digitales. Como respuesta, el sector bancario ha debido fortalecer de manera significativa sus capacidades de prevención y control, destinando en 2024 una inversión aproximada de $1,07 billones en ciberseguridad, lo que equivale a un incremento del 97 % frente a 2023, con el fin de mitigar riesgos, proteger las operaciones digitales y preservar la confianza de los usuarios.

Bajo estas premisas, una reducción agresiva de los cargos de acceso, como la proyectada por la CRC, genera un incentivo económico para la proliferación del tráfico gris y del fraude cibernético, trasladando costos significativos al sector financiero. Este escenario no solo obliga a las entidades bancarias a reasumir costos incrementales de mitigación y control, sino que también presiona la capacidad operativa de los entes de control y judicialización, como la Fiscalía y la DIJÍN, al enfrentar un aumento exponencial de la carga procesal, lo que dificulta la persecución efectiva de los delitos informáticos y debilita la respuesta institucional frente al fraude digital.

En este sentido, las recomendaciones que se formulan a continuación no buscan frenar las eficiencias derivadas del ajuste tarifario, sino blindar el ecosistema mediante exigencias mínimas de seguridad de red, trazabilidad, KYC/KYB y métricas objetivas de fraude.

Comentarios específicos:

El artículo 3 del proyecto propone actualizar el valor de la remuneración aplicable a la terminación de mensajes de texto (SMS) en redes móviles, disminuyendo el cargo por terminación de $1,00 a $0,03 pesos por SMS. Esta reducción en el costo de la remuneración de los SMS y de los servicios mayoristas de datos abarata significativamente el tráfico A2P (Application-to-Person) y la capacidad de envío, lo que, si bien puede generar eficiencias, también introduce nuevos incentivos y amplía las superficies de ataque.

En particular, el menor costo marginal del SMS puede propiciar un aumento significativo del volumen de tráfico malicioso, como campañas de smishing, fraude asociado al OTP y distribución de malware mediante enlaces. Asimismo, en escenarios asociados a esquemas de interconexión y señalización (SKA), podrían abrirse ventanas para prácticas como call pumping (inflado artificial de llamadas) y bypass, con impactos directos sobre los procesos de autenticación, las notificaciones transaccionales y los costos operativos del sector financiero. A ello se suma el riesgo de una expansión acelerada de campañas masivas de smishing con dominios look-alike, facilitadas por el bajísimo costo unitario del envío de SMS.

Por otra parte, esta disposición podría incentivar un aumento de ataques de ingeniería social orientados a la obtención de OTP y a la sincronización de ataques. La disponibilidad de

capacidad garantizada por TPS permitiría a organizaciones criminales coordinar ráfagas de tráfico para inducir a los usuarios a revelar credenciales, reduciendo de manera significativa la “ventana de explotación” y aumentando la efectividad del fraude.

Adicionalmente, podrían presentarse mecanismos de elusión de filtros mediante el uso de “servicios adicionales” o acuerdos con tratamiento diferencial de tráfico, generando posibles grietas para evadir firewalls de SMS o listas anti-spam, especialmente si no se establecen obligaciones claras de filtrado y control a nivel de red.

De igual forma, la disponibilidad de datos móviles a bajo costo en determinadas zonas incrementa el riesgo de despliegue de SIM farms y dispositivos IoT utilizados para consumo masivo de datos con fines de tunneling (phishing kits, servidores de comando y control), carding en comercio electrónico y operación de bots automatizados.

Si bien el proyecto prohíbe la degradación del servicio por fuera del esquema negociado, desde una perspectiva de seguridad las entidades financieras se podrían ver obligadas a implementar medidas adicionales de rate limiting y bloqueo de tráfico. En este contexto, se recomienda incorporar una excepción expresa por motivos de ciberseguridad y prevención del fraude, que habilite la aplicación de controles técnicos proporcionales, acompañados de obligaciones de registro, trazabilidad y auditoría.

En virtud de lo anterior, se considera pertinente que las disposiciones de la CRC incluyan medidas específicas de control sobre el tráfico de SMS, orientadas a mitigar los riesgos identificados. En particular, se recomienda establecer la obligación para los PRSTM de implementar firewalls de SMS con capacidades de filtrado de contenido, incluida la detección de URLs fraudulentas, validación del origen del mensaje, mecanismos anti-spoofing del Sender ID, listas dinámicas de bloqueo y esquemas de rate limiting. Estas herramientas permitirían gestionar de forma preventiva el tráfico malicioso sin afectar injustificadamente la calidad del servicio.

Asimismo, se sugiere implementar la realización de auditorías semestrales reportadas a la CRC y a la SIC, en las que se verifique la correcta implementación y operación de dichos firewalls. En este marco, los PRSTM deberían estar facultados para reducir o suspender temporalmente el TPS ante indicios objetivos de abuso, phishing o distribución de malware, sin que estas acciones se consideren una degradación injustificada del servicio.

Así mismo, se recomienda incorporar obligaciones de transparencia en el tráfico A2P, mediante el uso de cabeceras o etiquetas de trazabilidad de origen que permitan identificar de manera clara la ruta del mensaje y el agregador involucrado. Finalmente, se sugiere establecer criterios de “TPS prudente”, de forma que, cuando la relación entre mensajes entregados y rechazados, o los reportes de phishing, superen umbrales previamente definidos, el PRSTM pueda ajustar el TPS del PCA o del integrador técnico en tiempo real, como medida preventiva de ciberseguridad y antifraude.