



Bogotá D. C., 23 de junio de 2026

Señores

COMISIÓN DE REGULACIÓN DE COMUNICACIONES - CRC

medidasantifraude@crcom.gov.co

Asunto: Comentarios al proyecto de resolución “*Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones*”.

Referencia: Proyecto regulatorio CRC 2000-41-7-1.

Experian Colombia S.A. en su calidad de operador de información se permite presentar los comentarios al proyecto de Resolución identificado en la referencia. En particular, consideramos que las medidas propuestas sobre Sender ID, código corto A2P, validación centralizada, monitoreo, listas DNO, etiquetado de llamadas y comités técnicos constituyen una base regulatoria relevante para reducir riesgos de smishing, vishing, spoofing, ingeniería social y otras modalidades de suplantación.

Estimamos necesario complementar el proyecto con la posibilidad de tener acceso restringido, seguro y estandarizado de alertas técnicas no personales sobre recursos de identificación asociados a incidentes de uso potencialmente engañoso o presuntamente fraudulento, incluyendo, cuando corresponda, códigos cortos A2P, Sender ID, numeración llamante o CLI, URLs, dominios y plantillas.

I. Fundamento legal de la solicitud

La Ley Estatutaria 2573 de 2026 tiene por objeto proteger a las personas suplantadas frente a reportes negativos ante operadores de información y frente al cobro de obligaciones derivadas de suplantación de identidad ante operadores de telecomunicaciones, entidades financieras-crediticias y demás establecimientos comerciales con competencia en la materia.

Esta ley reconoce expresamente la suplantación de identidad digital, que puede materializarse mediante programas informáticos, páginas electrónicas, correos electrónicos, ingeniería social y mensajes de texto. Por tanto, existe una relación directa entre los vectores de fraude que aborda el proyecto de la CRC y las obligaciones de prevención, validación, atención y reporte establecidas por la Ley 2573 las cuales son aplicables también a los operadores de telecomunicaciones.

Particularmente, el artículo 5 de la Ley 2573 impone a los operadores de telecomunicaciones, entidades financieras-crediticias y demás establecimientos competentes, entre otros deberes, adoptar medidas de seguridad digital suficientes y razonables para establecer la veracidad de la identidad de las personas y los documentos presentados; adoptar mecanismos de validación de información; atender oportunamente solicitudes y quejas de personas suplantadas; y adelantar investigaciones internas para determinar el origen del fraude.

Adicionalmente, el numeral 2 del artículo 5 dispone que, cuando exista denuncia de falsedad personal o delitos conexos, debe realizarse el reporte correspondiente a los operadores de



información, marcándolo como “víctima de falsedad personal”, sin que ello impacte la puntuación de la presunta víctima.

Así mismo, el artículo 7 de la misma ley modificó el régimen de habeas data financiero para que, en casos de suplantación, la fuente solicite la modificación del dato negativo, récord, score o cualquier dato que refleje el comportamiento del titular, incorporando la leyenda “Víctima de Falsedad Personal”.

Por ello, la información técnica sobre recursos de identificación asociados a incidentes de fraude es instrumental para que los operadores de información puedan complementar las finalidades de prevención, corrección, marcación, protección del titular y verificación intensificada previstas en la Ley 2573.

II. Comentarios al Proyecto de Resolución

1. Articulación con operadores de información regulados bajo la ley 1266 de 2008

Todos los actores que participan en el ecosistema de telecomunicaciones, financiero, comercial y tecnológico comparten el deber de prevenir que los servicios legítimos sean utilizados como instrumentos de engaño, suplantación o afectación patrimonial. En esa medida, combatir el fraude implica reconocer que detrás de cada mensaje, llamada o interacción digital puede existir una persona cuya identidad, buen nombre, tranquilidad y proyecto de vida merecen ser protegidos. Por ello, las medidas orientadas a mitigar estas conductas deben concebirse como una responsabilidad común, basada en la cooperación, la corresponsabilidad y la preservación de la confianza pública en el ecosistema digital.

Por esta razón, las alertas técnicas, patrones de riesgo, indicadores de fraude o señales tempranas detectadas en el sector de telecomunicaciones no deberían permanecer aisladas, sino que, bajo parámetros estrictos de seguridad, finalidad, necesidad, proporcionalidad, circulación restringida y trazabilidad, deberían poder alimentar los mecanismos de prevención, detección, atención y mitigación ya existentes en el ecosistema de información crediticia, financiera y de servicios.

Los operadores de información regulados por la Ley 1266 de 2008 cumplen un rol relevante en la prevención y gestión de riesgos asociados a la suplantación de identidad, la falsedad personal y la generación de obligaciones no consentidas. En ese sentido, su participación controlada dentro del esquema de acceso a la información previsto por el proyecto de resolución permitiría que la finalidad protectora de la Ley 2573 se materialice de forma más efectiva, especialmente cuando las señales provenientes del sector de telecomunicaciones puedan anticipar o advertir riesgos que, de no ser gestionados oportunamente, terminen impactando el historial crediticio de los usuarios.

Esta articulación permitiría, entre otros objetivos, identificar patrones de riesgo asociados a modalidades recurrentes de fraude; activar verificaciones intensificadas antes de la apertura de productos o servicios; facilitar la gestión de reclamaciones por suplantación; prevenir reportes negativos derivados de obligaciones presuntamente fraudulentas; evitar afectaciones indebidas al score o perfil crediticio del titular; y soportar de manera más eficiente la correcta marcación de la condición de “Víctima de Falsedad Personal”, cuando ello resulte procedente.

En consecuencia, sugerimos respetuosamente a la CRC que contemple expresamente la posibilidad de que determinada información técnica, operativa o agregada derivada de eventos de fraude pueda ser compartida, bajo condiciones restringidas y seguras, con los operadores de información regulados por la Ley 1266 de 2008.



De esta manera, la regulación no solo fortalecería la capacidad de reacción del sector de telecomunicaciones, sino que permitiría una respuesta intersectorial más efectiva frente a fenómenos de fraude que, por su naturaleza, trascienden la prestación del servicio de comunicaciones y afectan directamente la identidad, el patrimonio, el historial crediticio y los derechos de los usuarios.

Agradecemos a la CRC la apertura de este espacio de participación y quedamos atentos a ampliar técnicamente la propuesta, participar en mesas de trabajo o aportar insumos adicionales que permitan robustecer las medidas contra el fraude.

Cordial Saludo,

Experian Colombia S.A.