Colombia Fintech

Bogotá D.C., 23 de junio de 2026

Señores

Comisión de Regulación de Comunicaciones (CRC)
Ciudad

Asunto: Comentarios de Colombia Fintech 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".

Respetado equipo de la Comisión de Comunicaciones de la Comisión de Regulación de Comunicaciones (CRC),

Por medio de la presente comunicación, la Asociación Colombiana de Empresas de Tecnología e Innovación Financiera (en adelante, "**Colombia Fintech**" o la "**Asociación**") presenta a la Comisión de Comunicaciones de la Comisión de Regulación de Comunicaciones (en adelante, la "**Comisión**" y la "**CRC**") sus comentarios frente 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 (en adelante, el "**Proyecto de Resolución**").

Comentario general

Colombia Fintech valora el esfuerzo técnico de la CRC en la estructuración de un proyecto regulatorio de esta complejidad y reconoce que la mitigación del fraude cibernético en los servicios de voz y mensajería constituye un objetivo de la mayor relevancia para la protección de los usuarios y para la confianza en el ecosistema digital. La Asociación comparte el propósito del Proyecto de Resolución y respalda la adopción de medidas técnicas que eleven los estándares de seguridad en la cadena de valor de la mensajería y de las llamadas de voz.

Sin perjuicio de lo anterior, y con el ánimo constructivo que caracteriza la participación de Colombia Fintech en los procesos de consulta pública, la Asociación considera que algunas de las medidas propuestas pueden precisarse para que cumplan eficazmente su finalidad sin generar cargas desproporcionadas, vacíos operativos o efectos no deseados sobre la continuidad de servicios críticos del sector financiero. En particular, los comentarios que se desarrollan a continuación se concentran en cuatro ejes: (i) la robustez técnica y la continuidad operativa del esquema de validación centralizada; (ii) la gobernanza, supervisión y financiación del validador centralizado; (iii) la proporcionalidad de los plazos, reportes y cargas de cumplimiento, especialmente

frente a entidades vigiladas por la Superintendencia Financiera de Colombia (en adelante, SFC) y (iv) la claridad en la clasificación de las modalidades de contenido y su articulación con el régimen de protección de datos y con el Registro de Números Excluidos (RNE).

Comentarios específicos

1. Sistemas de monitoreo de tráfico P2P (Art. 2.1.10.7.2.1.1.)

El artículo 2.1.10.7.2.1.1. establece que los PRST deberán implementar sistemas de monitoreo y control del tráfico P2P, y acreditar ante la CRC que dichos sistemas tienen capacidad de detectar, como mínimo, seis patrones de tráfico atípico: volumen inusual de mensajes salientes, alta dispersión de destinatarios, homogeneidad del contenido, periodicidad mecánica, ausencia de tráfico entrante correlacionado y concentración geográfica o de red.

Si bien la Asociación celebra la incorporación de esta obligación, considera que la norma puede precisarse en dos aspectos relevantes:

1. Ausencia de requisito de evaluación en tiempo real: El artículo no exige que la detección de los patrones descritos opere en tiempo real, sino que parece admitir sistemas de análisis retrospectivo o por lotes (batch). Esto es problemático, dado que el fraude en SMS P2P generalmente se ejecuta en ventanas de tiempo muy cortas (minutos u horas), lo que hace que la detección tardía sea ineficaz. Se sugiere que la CRC precise que los sistemas de monitoreo de tráfico P2P deben operar bajo una arquitectura de procesamiento en tiempo real (real-time o near-real-time), con latencias máximas de detección que la misma CRC podría parametrizar en el marco del CTLFSM. Un estándar razonable de la industria es una latencia de detección inferior a cinco (5) minutos desde el inicio del patrón atípico.
2. Ausencia de requisitos mínimos sobre la arquitectura tecnológica: El artículo deja a libre elección del PRST «las herramientas técnicas, los algoritmos y las metodologías de análisis». Si bien esto respeta el principio de neutralidad tecnológica, introduce el riesgo de que los PRST implementen soluciones insuficientes que cumplan formalmente con la norma sin alcanzar sus objetivos de fondo. Se propone que la CRC, en el marco del CTLFSM, establezca un conjunto mínimo de capacidades funcionales que cualquier solución de monitoreo deba acreditar, independientemente de la tecnología específica escogida. Entre estas capacidades mínimas se sugiere incluir: (i) análisis de series de tiempo con ventanas deslizantes de corto plazo; (ii) detección de

anomalías basada en líneas de base dinámicas (no solo umbrales fijos); (iii) capacidad de correlación multivariada entre los seis patrones listados; y (iv) generación automática de alertas con asignación de niveles de severidad.

2. Monitoreo de tráfico de voz (Art. 2.1.10.7.2.2.2.)

El artículo 2.1.10.7.2.2.2. exige que los PRST implementen sistemas de monitoreo en tiempo real del tráfico de voz con capacidad de detectar cuatro tipos de patrones (volumen inusual, robocall, correlación con listas de numeración fraudulenta y enmascaramiento de numeración). Sin embargo, no establece ningún parámetro de calidad mínima del sistema de monitoreo, ni exige que este sea distinto o independiente del sistema de monitoreo P2P. Se sugiere que la CRC precise que:

1. El sistema de monitoreo de voz y el de P2P deben poder intercambiar señales de alerta, dado que los fraudes modernos son frecuentemente multicanal (combinan SMS y voz en una misma campaña fraudulenta). La correlación cruzada entre eventos detectados en ambos canales es una capacidad crítica para la identificación de campañas de fraude sofisticadas.
2. El sistema de monitoreo de voz debe tener capacidad de actualización dinámica de los patrones de detección, de modo que pueda incorporar nuevas firmas de fraude identificadas a través del CTLFSM sin necesidad de reemplazar la solución tecnológica completa. Esto favorece la adopción de soluciones SaaS de prevención de fraude, que por su naturaleza de actualización continua son más eficientes que las soluciones on-premise con ciclos de actualización largos.

3. Criterios de detección de robocall y su efecto sobre la gestión legítima de cobranza (Arts. 2.1.10.7.2.2. y 2.1.10.7.2.2.2.2.4.)

Los criterios técnicos de detección de patrones de robocall (duración promedio de llamada (ACD) baja y patrones de llamadas cortas y secuenciales) son inherentes a operaciones legítimas de cobranza asistida por agentes virtuales (AI) y a campañas de gestión de cartera vencida de entidades financieras. Las llamadas a deudores en mora tienen ACD estructuralmente más bajo (el cliente cuelga, no contesta o la conversación es breve) y se realizan en secuencias. El numeral 2.1.10.7.2.2.2.2.4 establece adicionalmente que el etiquetado se mantiene activo durante el procedimiento de revisión, lo que impide reversar el daño operativo aun cuando la solicitud sea procedente. El efecto neto es que llamadas legítimas de entidades financieras quedan marcadas como sospechosas en el dispositivo del receptor, deteriorando la tasa de contacto y el cumplimiento del deber de gestión de cobro.

Para este punto, se solicita respetuosamente a la CRC modificar el artículo 2.1.10.7.2.2 para excluir explícitamente del criterio de patrón sospechoso las llamadas originadas desde numeración inscrita en el portal del artículo 6.14.3.1 (sector financiero), o subsidiariamente, que el parágrafo del numeral 2.1.10.7.2.2.2.2.4 se modifique para suspender el etiquetado durante la tramitación de la revisión cuando el solicitante sea una entidad vigilada por la SFC y acredite la legitimidad del uso.

4. Validador centralizado: verificación en tiempo real, continuidad operativa y capacidad mínima (Arts. 6.13.1.5.10., 6.13.2.1.2., 6.13.2.2. y 6.13.4.7.)

El artículo 6.13.4.7.1. establece que los PRST deben integrar sus plataformas de mensajería (SMSC) con el sistema del validador centralizado a través de APIs, para consultar en tiempo real la validez del código corto A2P, el SENDER ID y la plantilla de contenido antes del enrutamiento de cada mensaje. Esta es una de las disposiciones más avanzadas técnicamente del proyecto y, por su carácter de punto único de paso de todo el tráfico A2P nacional, consideramos que merece un desarrollo mayor en materia de robustez, continuidad y capacidad.

A continuación, listamos una serie de puntos relevantes a considerar en este sentido:

1. Comportamiento ante falla o latencia del validador. La norma no establece qué debe hacer el sistema del PRST cuando la consulta al validador falle o tarde más allá del umbral de latencia. Se sugiere que el artículo 6.13.2.2 (Plan de Contingencia del Validador) sea complementado con la obligación de que los PRST cuenten con cachés locales de validación de corto plazo (por ejemplo, con una ventana de validez no superior a 60 minutos), de modo que ante una falla del validador centralizado no se detenga por completo el tráfico A2P legítimo. Estos cachés deben poder ser invalidados de manera remota e inmediata por instrucción del Administrador de Recursos de Identificación cuando se detecte un incidente de fraude activo.
2. Carácter obligatorio de la etiqueta “sin verificar” en contingencia. El artículo 6.13.4.7.2 permite a los PRST marcar mensajes como “sin verificar” en lugar de bloquearlos, pero lo hace como una facultad discrecional y no como una garantía regulatoria. Dado que el bloqueo total afectaría comunicaciones críticas, incluyendo OTP y alertas de seguridad, se solicita que la CRC establezca de manera obligatoria, y no facultativa, el uso de la etiqueta “sin verificar” durante las contingencias del validador, y que defina con precisión el alcance de las listas de emergencia del artículo 6.13.2.2 para las entidades del sector financiero, así como las condiciones en que dicho plan se activa.

3. Señales de riesgo dinámicas. Se propone que la CRC exija que el sistema de consulta en tiempo real del validador sea capaz de incorporar señales de riesgo dinámicas (por ejemplo, basadas en el comportamiento reciente del SENDER ID o en alertas del CTLFSM), y no solo verificar el estado binario «asignado/no asignado» de los recursos. Esto convierte al validador centralizado en un verdadero sistema de inteligencia de fraude en tiempo real, y no solo en un directorio de asignaciones.
4. Capacidad mínima garantizada. El artículo 6.13.2.1.2 define tiempos de respuesta máximos (200/500 ms) y un informe semestral de capacidad, pero no establece un throughput mínimo garantizado en peticiones concurrentes por segundo. Para entidades financieras que operan ráfagas transaccionales (autenticación en checkout, campañas de cobranza, eventos comerciales), el dimensionamiento contra el promedio histórico puede ser insuficiente, y una saturación del validador implicaría que todo el ecosistema A2P nacional pierda capacidad simultáneamente, sin alternativa de fallback inmediata.

En atención a lo anterior, se solicita respetuosamente que la CRC incluya en el artículo 6.13.2.1.2 un throughput mínimo garantizado expresado en peticiones concurrentes por segundo, y que los pliegos del proceso de selección del validador incluyan ese parámetro como criterio técnico mandatorio. Se sugiere un mínimo del orden de mil (1.000) req/s con escalamiento automático ante picos del orden de cinco (5) veces el promedio.

5. Carril prioritario de aprobación para mensajes de autenticación y seguridad (Arts. 6.13.2.1.2., 6.13.4.3.1. y 6.12.1.3.1.)

El artículo 6.13.2.1.2 fija tiempos de respuesta del sistema del validador de 200 ms en promedio. Sin embargo, el artículo 6.13.4.3.1 establece hasta 48 horas para aprobar una plantilla nueva. Ninguna disposición garantiza que los mensajes de autenticación y seguridad (OTP, alertas de inicio de sesión) lleguen en la ventana de segundos que su naturaleza exige. Un OTP con 30 segundos de retraso es inútil para el usuario y compromete la seguridad de las operaciones que pretende proteger.

Se solicita respetuosamente que la CRC establezca un carril prioritario de aprobación de plantillas para la modalidad de autenticación y seguridad (art. 6.12.1.3.1), con un SLA máximo de cuatro (4) horas, y que los PRST estén obligados a priorizar el enrutamiento de los mensajes de esa categoría.

6. Procedimiento de revisión frente al rechazo de plantillas por el validador (Arts. 6.13.4.3.1. y 6.13.1.6.5.)

El artículo 6.13.4.3.1 establece que el validador puede rechazar una plantilla mediante comunicación motivada, pero la norma no contempla ningún procedimiento formal de revisión o segunda instancia para el asignatario que considere injustificado ese rechazo. El artículo 6.13.1.6.5 prohíbe los rechazos injustificados, pero no define consecuencias ni quién los determina. Para una entidad financiera, el rechazo de una plantilla de OTP equivale a una interrupción del servicio.

Se solicita respetuosamente que la CRC establezca un procedimiento expedito de revisión de rechazos ante el Administrador de Recursos de Identificación, con un plazo máximo de resolución de veinticuatro (24) horas para las plantillas de autenticación y seguridad.

7. Diferenciación de plazos para modificaciones de plantillas (Art. 6.13.4.3.2.)

El plazo de hasta 48 horas para procesar modificaciones de plantillas ya aprobadas no distingue entre cambios sustantivos (nueva modalidad, nuevas URLs, cambios de modalidad) y cambios menores (ajustes de copy, longitud del texto, reformulaciones que conservan la modalidad y el tipo de variables). Para productos de mensajería operados por entidades financieras, los ajustes menores son continuos (optimización por métricas de conversión, ajustes de tono, pruebas A/B). El plazo único bloquea el ciclo de mejora del producto sin justificación regulatoria proporcional al riesgo.

Se solicita respetuosamente que la CRC introduzca en el artículo 6.13.4.3.2 una distinción entre modificaciones sustantivas (que mantienen el plazo de 48 horas) y modificaciones menores (entendidas como cambios al texto que preservan la modalidad, las URLs y los campos variables aprobados), con un plazo máximo de 24 horas. Alternativamente, que el validador esté facultado para aprobar tácitamente las modificaciones menores no rechazadas dentro de las primeras 12 horas.

8. Estandarización técnica de campos variables en las plantillas (Art. 6.13.4.2.4.)

El artículo reconoce la existencia de campos variables en las plantillas y exige declarar el tipo de información insertable, pero no establece una sintaxis estándar de marcado (placeholders), ni una tipología cerrada de tipos de variable (numérico, alfanumérico, monetario, fecha, identificador), ni define si los placeholders deben publicarse como especificación técnica del validador antes de su entrada en operación. La ausencia de esa estandarización genera ambigüedad operativa en la integración con proveedores internacionales de mensajería y obstaculiza la migración desde sistemas que ya operan con sintaxis propias.

Se solicita respetuosamente que la CRC adicione al artículo 6.13.4.2.4 un parágrafo que establezca que el validador publicará, con al menos noventa (90) días de antelación a su entrada en operación, una especificación técnica que defina: (i) la sintaxis estándar de placeholders de campos variables (por ejemplo, notación con dobles llaves {{variable}}); (ii) una tipología cerrada y reconocida de tipos de variable que no requiera aprobación caso a caso de cada valor concreto; y (iii) las reglas de validación del contenido insertable.

9. Selección, supervisión independiente y régimen tarifario del validador centralizado (Arts. 6.13.1.2., 6.13.1.3., 6.13.1.4. y 18.)

La Asociación observa que el diseño de gobernanza del validador centralizado podría fortalecerse en tres frentes que están estrechamente vinculados:

1. Experiencia acreditada en detección de fraude. Los requisitos del artículo 6.13.1.3. no incluyen explícitamente la exigencia de que el candidato cuente con experiencia acreditada en la operación de sistemas de detección de fraude en tiempo real en ecosistemas de mensajería A2P. Se sugiere incorporar este criterio de manera expresa, dado que la función del validador no se agota en la verificación documental sino que es central para la prevención del fraude.
2. Independencia y supervisión. El artículo 18.1 asigna la selección del validador centralizado a los PRSTM (los mismos operadores que compiten con algunos de los agentes que el validador deberá certificar). Aunque el artículo 6.13.1.3.4 prohíbe los vínculos accionarios del validador con los agentes que registra, la norma no define un mecanismo independiente de auditoría permanente sobre su actuación ni un procedimiento de quejas con efectos vinculantes. Se solicita que la CRC defina un esquema de supervisión independiente sobre el validador centralizado, con auditorías periódicas obligatorias y un canal formal de quejas ante el Administrador de Recursos de Identificación.
3. Régimen tarifario. El artículo 6.13.1.2 establece que los costos del validador los pagan los asignatarios de código corto A2P bajo el principio de orientación a costos más utilidad razonable. Sin embargo, la norma no fija un tope tarifario ni un mecanismo de revisión periódica, y esos costos se trasladarán a los asignatarios de SENDER ID (entre ellos, las entidades financieras), sin que exista regulación que los limite. Se solicita respetuosamente que la CRC establezca un mecanismo formal de regulación tarifaria sobre el validador centralizado, con revisión periódica y publicación de la metodología de cálculo de costos antes de que entre en vigencia el nuevo régimen.

10. Régimen sancionatorio y responsabilidad del validador centralizado (Arts. 6.13.1.4., 6.13.1.6. y 6.13.5.1.12.)

El artículo 6.13.1.4 establece causales de revisión anticipada de la selección del validador y el artículo 6.13.1.6 define sus prohibiciones. Sin embargo, las consecuencias por incumplimiento se limitan a reportes al Administrador de Recursos de Identificación, pues no existe un régimen de sanciones económicas directas ni un mecanismo de indemnización para los asignatarios afectados por el mal funcionamiento del validador.

Se solicita respetuosamente que la CRC establezca un régimen sancionatorio explícito, proporcional y de aplicación directa para los incumplimientos del validador centralizado, incluyendo la obligación de indemnizar a los asignatarios afectados por interrupciones imputables a su negligencia.

11. Continuidad operativa de la mensajería crítica del sector financiero durante la transición (Arts. 19. y 20., literal a)

El artículo 20 establece que las medidas de voz y P2P entran en vigor con la publicación en el Diario Oficial, mientras el ecosistema A2P queda condicionado a la Fase II. El numeral 19.1.4.3 dispone que los códigos cortos no consolidados al vencimiento de la transición pasarán a estado “no implementado” e iniciarán proceso de recuperación, sin contemplar excepciones para entidades financieras con comunicaciones críticas activas. La interrupción de OTP, alertas de seguridad y notificaciones transaccionales tendría un impacto directo sobre la seguridad de las operaciones de los usuarios.

Se solicita respetuosamente que la CRC incorpore una cláusula explícita de continuidad operativa que garantice la prestación ininterrumpida del servicio de mensajería crítica del sector financiero durante todo el período de transición, con prórroga automática para las entidades que acrediten procesos de migración en curso.

12. Sobre el cronograma de implementación (Arts. 2.1.10.7.2.1.5., 2.1.10.7.2.2.4. y 19., numerales 19.1.1. a 19.1.4.)

Los artículos 2.1.10.7.2.1.5 y 2.1.10.7.2.2.4 fijan tres (3) meses para implementar los sistemas de monitoreo P2P y de voz respectivamente, y el artículo 19 establece seis (6) meses de transición para el ecosistema A2P. Estos plazos son difícilmente compatibles con la realidad técnica de la implementación. De hecho, el propio documento soporte de la CRC reconoce que los SMSC actuales no cuentan con APIs para la integración con sistemas externos y que los cambios en esas plataformas se gestionan con SLA de hasta tres (3) días hábiles.

Se solicita respetuosamente que la CRC replantee el cronograma, contemplando un mínimo de seis (6) meses para las medidas de voz y P2P, y de doce (12) meses para el ecosistema A2P completo, considerando la carga tecnológica real de la implementación.

13. Informes de acreditación, reportes periódicos y cadena de responsabilidad (Arts. 2.1.10.7.2.1.5. y 6.14.1.5.)

El artículo 2.1.10.7.2.1.5. exige que los PRST acrediten la puesta en operación de sus sistemas de monitoreo mediante un informe técnico, y que seis meses después presenten un segundo informe con estadísticas de funcionamiento. Se sugiere que la CRC complemente este mecanismo de acreditación con la exigencia de un reporte trimestral, considerando que la dinámica del fraude exige un monitoreo continuo de la efectividad de los sistemas implementados. El reporte debería incluir indicadores de desempeño mínimos, tales como: tasa de detección (verdaderos positivos sobre el total de patrones fraudulentos identificados), tasa de falsos positivos, tiempo promedio de detección y tiempo de respuesta entre la detección y la acción correctiva.

De otra parte, la obligación de reportar trimestralmente a la CRC el cumplimiento de los programas de formación del artículo 6.14.1.5 está dirigida a los asignatarios de recursos de identificación y a los PRST. No queda claro si aplica directamente a las entidades financieras que usan mensajería A2P sin ser asignatarias directas, o si esa responsabilidad recae en el integrador tecnológico o en el asignatario del código corto.

Se solicita respetuosamente que la CRC: (i) incorpore la exigencia de un reporte periódico de desempeño con los indicadores mínimos señalados y (ii) precise la cadena de responsabilidad en materia de formación y reporte cuando la entidad financiera opera como asignataria de SENDER ID pero no de código corto A2P, definiendo si la obligación de reporte trimestral aplica directamente a estas entidades o se delega en el asignatario del código corto.

14. Claridad en la clasificación de las modalidades de contenido (Arts. 6.12.1.3., 6.13.4.2.3. y 6.4.2.1.8.)

La distinción entre mensajes transaccionales e informativos (art. 6.12.1.3.2) y mensajes comerciales (art. 6.12.1.3.3) no es clara en el contexto del crédito de consumo. Mensajes como «tiene cupo disponible», avisos de activación de producto o comunicaciones sobre beneficios del contrato vigente pueden interpretarse en cualquiera de las dos categorías, con consecuencias radicalmente distintas en términos del consentimiento requerido y del cumplimiento del RNE. La categorización de los mensajes (autenticación, transaccional, comercial y regulatorio) define reglas

estrictas de consentimiento (opt-in y opt-out) y limita estructuralmente la forma en que pueden administrarse y enviarse los mensajes de la categoría comercial. Un ejemplo recurrente es el mensaje “Tu pago fue exitoso. Aprovecha 20% en tu próxima compra”.

Se solicita respetuosamente que la CRC publique una guía interpretativa con ejemplos concretos del sector financiero para cada categoría del artículo 6.12.1.3, antes de que el validador comience a aprobar plantillas, de modo que pueda trazarse con claridad la línea entre un mensaje transaccional y uno comercial.

15. Tratamiento de los mensajes con contenido híbrido (Art. 6.12.1.3.2.)

El artículo define cuatro modalidades discretas (autenticación, transaccional, comercial, regulatorio) con regímenes de consentimiento distintos. En la operación real, un porcentaje significativo de los mensajes A2P de servicios financieros combina elementos de más de una modalidad: por ejemplo, un recordatorio de pago de cuota (transaccional) que incluye una invitación a refinanciar o adelantar saldo (comercial), o una confirmación de transacción (transaccional) que incluye una mención de un programa de beneficios (comercial). El Parágrafo del artículo prevé que un mismo SENDER ID pueda cursar plantillas de modalidades distintas, pero no aborda el caso de mensajes individuales con contenido híbrido. La ambigüedad obliga a fragmentar comunicaciones legítimas (degradando la experiencia del usuario) o a clasificar conservadoramente como comercial todo lo que tenga algún componente promocional (cerrando flujos transaccionales necesarios por falta de opt-in formal).

Se solicita respetuosamente que la CRC adicione al artículo 6.12.1.3 lineamientos para la clasificación de mensajes híbridos, estableciendo que la modalidad aplicable corresponde a la del componente principal del mensaje, entendido como aquel que motiva primariamente su envío y ocupa la porción mayoritaria del contenido, que el validador centralizado publique criterios objetivos para esta determinación, y que el asignatario del SENDER ID justifique la clasificación al momento de someter la plantilla a aprobación.

16. Validación previa de la modalidad comercial y aprobación por silencio (Art. 6.13.3.1.2. y régimen de plantillas)

La obligación de que todo mensaje SMS A2P deba pasar por un validador centralizado y corresponder a una plantilla preaprobada antes de que el operador autorice su entrega al usuario final genera un cuello de botella para la inmediatez de las campañas de marketing, promociones limitadas u ofertas relámpago, que por su naturaleza dependen de ventanas de oportunidad muy cortas.

Se solicita respetuosamente a la CRC que: (i) evalúe excluir la categoría «Comercial/Marketing» de la validación previa; (ii) en caso de mantenerse la validación previa, garantice que las plantillas comerciales permitan un porcentaje amplio de texto variable, del orden del 70%; y (iii) establezca que, si el sistema del validador falla, se congestiona o no entrega respuesta dentro del plazo definido (por ejemplo, quince (15) minutos), el mensaje se entienda aprobado de manera automática.

17. Articulación del RNE con la gestión de cobranza sobre obligaciones vigentes (Art. 2.1.18.1.)

El artículo amplía el alcance del RNE pero no excluye expresamente las comunicaciones de cobranza sobre obligaciones en mora, lo que genera ambigüedad sobre si un deudor inscrito en el RNE puede bloquear el contacto de gestión de cartera de su acreedor.

Se solicita respetuosamente que la CRC aclare expresamente que la gestión de cobro sobre una obligación crediticia vigente no está sujeta a las restricciones del RNE, con independencia de la inscripción del deudor en dicho registro, en articulación con lo ya establecido en la Ley 2300 de 2023 para las entidades vigiladas por la SFC.

18. Naturaleza de las comunicaciones de gestión de cartera vencida (Art. 6.12.1.3.2.)

La norma no precisa si las comunicaciones de negociación de acuerdos de pago, reestructuraciones y propuestas de descuento por pronto pago quedan comprendidas como contenido transaccional o pueden ser reclasificadas como contenido comercial. Esta distinción es crítica: si se clasifican como comercial, las entidades estarían obligadas a contar con una autorización previa y expresa del cliente para enviar ese tipo de mensajes, lo que haría inviable la gestión de cobranza sobre obligaciones que ya existen y son parte de una relación contractual vigente. La clasificación actual como contenido transaccional ya impone, además, restricciones prácticas sobre el lenguaje y el tono de los mensajes de cobranza.

Se solicita respetuosamente a la CRC incluir una precisión explícita en el artículo 6.12.1.3.2 que reconozca que la totalidad del ciclo de gestión de cartera vencida, incluyendo las comunicaciones de negociación de acuerdos sobre obligaciones vigentes, constituye contenido transaccional. La clasificación de plantillas como transaccionales bajo estándares internacionales de los proveedores tecnológicos (por ejemplo, Twilio) respalda técnicamente esta solicitud.

19. Inscripción pública de SENDER ID y numeración: riesgo de suplantación y contactabilidad (Arts. 6.14.2.2., 6.14.3.1. y 2.1.10.7.2.2.2.1.)

El artículo 6.14.2.2 obliga a inscribir públicamente los SENDER ID del sector financiero en un portal de la CRC, y el artículo 6.14.3.1 hace lo propio con la numeración E.164 de voz. Si bien la finalidad de proteger al consumidor permitiéndole verificar la legitimidad del remitente es valiosa, la publicación abierta de todos los identificadores legítimos puede convertirse en un insumo para ataques de suplantación más sofisticados en canales no regulados (WhatsApp, correo o llamadas desde numeración internacional), al proporcionar a actores maliciosos un catálogo consolidado y oficial de los identificadores que deben falsificar. El efecto neto sobre el fraude depende de la capacidad técnica del operador para validar el SENDER ID a la entrega, capacidad que no está garantizada en el régimen actual.

Adicionalmente, en el ámbito de la gestión de cobranza, la inscripción pública de la numeración combinada con el mecanismo de etiquetado expone la operación a un deterioro progresivo de la contactabilidad: una vez que los números inscritos son de consulta pública, los clientes en mora pueden identificarlos y bloquearlos de manera sistemática, sin que la norma prevea un mecanismo para detectar oportunamente ese bloqueo masivo, rotar numeración o habilitar líneas alternativas dentro de un marco regulatorio claro.

Se solicita respetuosamente que la CRC (i) modifique el artículo 6.14.2.2 para que la inscripción de SENDER ID y códigos cortos del sector financiero se realice en un registro de acceso por consulta puntual y autenticada, de modo que el ciudadano verifique caso a caso si un identificador específico corresponde a una entidad legítima— en lugar de un catálogo público navegable, o subsidiariamente condicione la apertura del catálogo a que el ecosistema técnico implemente validación efectiva del SENDER ID a la entrega; y (ii) en el marco de la inscripción de numeración corporativa, establezca un mecanismo de monitoreo de bloqueo masivo, un procedimiento expedito de rotación o sustitución de numeración que no implique reiniciar el proceso de inscripción, y criterios objetivos que distingan el bloqueo legítimo individual del bloqueo sistemático inducido.

20. Régimen simplificado de KYC para entidades vigiladas por la SFC (Arts. 6.13.3.1. y 19., numeral 19.1.2.5.)

El artículo 6.13.3.1 establece un proceso de KYC que replica controles que la SFC ya exige y supervisa sobre las entidades vigiladas: verificación de la existencia jurídica, identificación del beneficiario final, evaluación del perfil de riesgo, entre otros. Para las entidades sometidas a inspección permanente y a obligaciones de SARLAFT, este proceso genera una carga administrativa redundante. El numeral 19.1.2.5 reconoce la situación al dar prioridad a las entidades vigiladas por la SFC, pero no simplifica el KYC.

Se solicita respetuosamente que la CRC establezca un régimen simplificado de KYC para las entidades vigiladas por la SFC, reconociendo la supervisión existente como equivalente y evitando la duplicación de cargas administrativas.

21. Estándar de identificación del beneficiario final (Arts. 6.13.3.1.2. y 6.4.2.1.8.)

El artículo 6.13.3.1.2 exige identificar al beneficiario final mediante el formato que disponga el validador centralizado, y el artículo 6.4.2.1.8 exige una declaración similar suscrita por el representante legal y el revisor fiscal. Para los grupos empresariales con estructuras accionarias internacionales, frecuentes en el sector fintech, esta identificación puede ser técnicamente compleja, y la norma no aclara si acepta las declaraciones ya presentadas ante la UIAF en el marco de SARLAFT.

Se solicita respetuosamente que la CRC aclare el estándar de identificación del beneficiario final aplicable y reconozca expresamente las declaraciones ya presentadas ante la UIAF como suficientes para efectos de este régimen.

22. Asignación de SENDER ID para grupos económicos y flujos previos a la decisión (Art. 6.12.2.)

El Parágrafo 2 establece que la CRC asignará un único SENDER ID por NIT, sin posibilidad de asignación compartida entre personas jurídicas relacionadas. En estructuras de financiamiento donde un mismo flujo de producto al usuario es operado por más de una entidad jurídica del mismo grupo económico (por ejemplo, una compañía de financiamiento vigilada por la SFC y una entidad comercial relacionada), los mensajes de autenticación y verificación se envían al usuario antes de que se determine cuál entidad jurídica otorgará efectivamente el servicio o crédito. Bajo la regla actual no existe un SENDER ID válido para esa etapa del flujo, dado que la atribución a un NIT específico ocurre solo después de la decisión de otorgamiento.

Se solicita respetuosamente que la CRC adicione un parágrafo al artículo 6.12.2 que admita, para grupos económicos debidamente acreditados ante el validador centralizado, la asignación de un SENDER ID compartido vinculado a una marca comercial común y respaldado por los NIT de las entidades del grupo, sujeto al cumplimiento del proceso de KYC por parte de cada entidad participante; o, alternativamente, que se reconozca la figura de “SENDER ID de flujo previo a decisión”, asignable a la entidad operadora del onboarding del grupo.

23. Posición regulatoria de los proveedores internacionales de comunicaciones en la nube (Arts. 6.4.2.1. y 6.12.2.1.)

La resolución no contempla la figura de los proveedores internacionales de comunicaciones en la nube que no tienen la calidad de PRST ni de integrador tecnológico inscritos en Colombia, lo que genera un vacío sobre cómo deben articularse con el nuevo régimen y dónde recae la responsabilidad regulatoria.

Se solicita respetuosamente a la CRC emitir lineamientos específicos sobre la posición regulatoria de los proveedores internacionales de comunicaciones en la nube: si pueden asumir el rol de integrador tecnológico bajo el régimen colombiano, si deben integrarse con el validador centralizado, o si la responsabilidad regulatoria recae íntegramente en la entidad local asignataria del SENDER ID.

24. Articulación de las campañas pedagógicas con los lineamientos de la SFC (Art. 6.14.1.3.)

La obligación de publicar cuatro campañas anuales en redes sociales con el hashtag oficial de la CRC puede entrar en tensión con los lineamientos de comunicación digital que impone la SFC a las entidades vigiladas, generando un conflicto normativo para las compañías de financiamiento.

Se solicita respetuosamente a la CRC aclarar cómo se articula esta obligación con las restricciones de comunicación en redes sociales impuestas por la SFC a sus entidades vigiladas, y si existe la posibilidad de un cumplimiento conjunto, delegado al asignatario del código corto, o mediante un mecanismo alternativo para las entidades del sector financiero.

25. Mecanismos de retroalimentación en las obligaciones de educación y prevención (Capítulo 14, Título VI)

El Capítulo 14 establece obligaciones pedagógicas y de prevención de fraude para los PRST, los asignatarios de código corto A2P y los integradores tecnológicos. Sin embargo, las campañas pedagógicas descritas en el artículo 6.14.1.3. son genéricas y no contemplan mecanismos de retroalimentación basados en datos de fraude real.

Se solicita respetuosamente que la CRC establezca una obligación complementaria: que los PRST y los asignatarios de código corto A2P incorporen en sus sistemas de atención al usuario un mecanismo estandarizado de reporte de fraude por parte de los propios usuarios (por ejemplo, una opción de «reportar mensaje fraudulento» accesible directamente desde el SMS recibido o a través de un canal USSD), cuyos datos alimenten el CTLFSM como insumo de inteligencia de fraude. Esta medida mejora la detección y reduce la dependencia exclusiva de los sistemas automatizados de los PRST.

Colombia Fintech agradece a la CRC la apertura institucional para recibir estos comentarios y reitera su disposición para participar en los espacios técnicos, mesas de trabajo y ejercicios de retroalimentación que la Comisión estime pertinentes, con el fin de contribuir a la construcción de alternativas regulatorias que fortalezcan la prevención del fraude sin afectar la prestación de servicios esenciales para los usuarios.

Cordialmente,

Gabriel Santos García
Presidente Ejecutivo
Colombia Fintech