TECHNOVATION

Consultoría fintech especializada en crédito digital Latinoamérica

INFORME EJECUTIVO PÚBLICO

Ley 2573 y crédito digital: cuando el cliente dice “yo no fui”

Principales aprendizajes del webinar sobre suplantación, evidencia digital, trazabilidad, riesgo y respuesta operativa en procesos de originación de crédito.

EVENTO	FECHA	DURACIÓN	FORMATO
Webinar Ley 2573 Crédito Digital	24 de junio de 2026	58 minutos	Executive roundtable

Resumen ejecutivo

El webinar abordó una pregunta crítica para originadores de crédito digital y entidades que gestionan validación de identidad, reporte a centrales de riesgo o procesos de cobranza: **¿puede la organización reconstruir y defender técnicamente una originación cuando un cliente alega suplantación?**

> **La tesis central fue clara: tener controles no es lo mismo que poder probarlos.**

La Ley 2573 fue el punto de partida, pero la conversación se concentró en la capacidad operativa de demostrar diligencia, coordinar áreas internas, conservar evidencia útil y gestionar adecuadamente los eventos de posible fraude o suplantación. El foco no fue generar alarma, sino entregar una lectura práctica para que las entidades revisen su operación, sus proveedores, sus datos y sus procedimientos.

Panel y perspectivas

Juan Pablo Londoño

CEO de Technovation · Moderador

Condujo la discusión desde la operación real de crédito digital: identidad, trazabilidad, evidencia y capacidad de defensa de la originación.

Pedro Novoa

MS Legal · Habeas data e impacto en crédito

Aterrizó las implicaciones prácticas de la ley, la carga probatoria, la suspensión de cobros/reportes y los errores frecuentes en validación de identidad.

Juan Pablo López

Ex Director de Investigaciones SIC

Aportó la mirada investigativa: la autoridad no solo evalúa contratos, sino diligencia, gobierno, repetición de patrones, evidencia y respuesta de la organización.

Óscar Gutiérrez

Ciencia de datos y riesgo de crédito

Conectó suplantación, riesgo operativo, modelos, pérdida esperada, gobierno de datos y trazabilidad como soporte técnico de la defensa.

El problema operativo: la evidencia fragmentada

En una originación digital, el proceso suele verse lineal. Sin embargo, cada etapa puede depender de sistemas, proveedores y responsables distintos. Esa fragmentación es el principal reto cuando se debe reconstruir la historia completa del crédito.

Cliente → **Selfie** → **OCR** → **OTP** → **Scoring** → **Firma** → **Desembolso** → **Cobranza**

La pregunta no es solo si se hicieron validaciones. La pregunta crítica es si la entidad puede demostrar, de forma completa, ordenada y entendible, qué ocurrió en cada paso.

Identidad **Trazabilidad** **Respuesta operativa** **Gobierno de datos** **Evidencia exportable**

Aprendizajes principales

1

La carga práctica de la prueba se desplaza hacia la entidad

Ante una alegación de suplantación, la entidad debe estar preparada para demostrar que actuó con diligencia y que aplicó controles razonables de validación, prevención y respuesta.

2

El contrato ya no es suficiente como única defensa

La discusión no se agota en mostrar términos y condiciones, firma electrónica o aceptación. La pregunta es qué hizo la organización para evitar que el contrato naciera de una suplantación.

3

La repetición de reclamaciones puede revelar fallas estructurales

Un caso aislado puede ser fraude; múltiples casos con el mismo patrón pueden evidenciar problemas de canal, proveedor, gobierno, control o modelo operativo.

4

Contratar proveedores no traslada la responsabilidad

El uso de biometría, validación documental, OTP, firma o scoring con terceros no elimina la obligación de diseñar, supervisar y mejorar el sistema de originación y respuesta.

5

El cumplimiento documental debe convertirse en cumplimiento operativo

Políticas, manuales y contratos son necesarios, pero no sustituyen la evidencia real de cómo funcionó el procedimiento en un caso concreto.

6

La suplantación también es un evento de riesgo operativo

No debería tratarse como mora ordinaria. Debe evaluarse por frecuencia, impacto, pérdida operativa, reputación, legalidad, reportes y capacidad de prevención.

7

Los datos son una herramienta de reconstrucción y defensa

Device data, logs, hashes, proveedores, timestamps, decisiones, autorizaciones y secuencia de eventos permiten reconstruir técnicamente el proceso y detectar vulnerabilidades.

8

La respuesta interna debe ser coordinada

Inconsistencias entre servicio al cliente, operaciones, tecnología, legal, cobranza y riesgo pueden ser interpretadas como ausencia de gobierno del proceso.

Qué deberían revisar las entidades esta semana

1. Gobierno de identidad y datos

- Política de tratamiento de datos y autorizaciones actualizadas.
- Responsables claros por validación, conservación y respuesta.
- Auditoría de proveedores que intervienen en la originación.

2. Trazabilidad de originación

- Línea de tiempo reconstruible por operación.
- Logs, timestamps y evidencias exportables.
- Capacidad de asociar cada evidencia a una solicitud específica.

3. Protocolo de reclamaciones

- Ruta para recibir, clasificar, suspender y escalar casos.
- Criterios para suspender cobros y reportes cuando corresponda.
- Plantillas de respuesta coherentes entre áreas.

4. Riesgo y analítica

- Variables de alerta temprana asociadas a fraude o suplantación.
- Separación entre mora, fraude externo y fraude oportunista.
- Retroalimentación a modelos, reglas y matrices de riesgo operativo.

Preguntas críticas para equipos directivos

- ¿Podemos reconstruir una originación completa en menos de 48 horas?
- ¿Sabemos dónde está cada evidencia y quién la custodia?
- ¿La evidencia es exportable, entendible y útil para responder a una autoridad o al cliente?
- ¿Nuestros proveedores entregan trazabilidad suficiente o solo resultados finales?
- ¿Cobranza, riesgo, servicio, legal y tecnología responden con la misma narrativa?
- ¿Estamos tratando posibles suplantaciones como simple mora?

Recomendaciones ejecutivas

Centralizar evidencia

Construir un expediente digital por operación que permita consultar, exportar y explicar la secuencia completa.

Diseñar protocolo

Documentar tiempos, responsables, suspensión de cobro/reporte, escalamiento y respuesta ante denuncias o alegaciones.

Auditar proveedores

Verificar qué evidencia genera cada proveedor, cuánto tiempo la conserva y cómo se accede a ella.

Unificar narrativa

Alinear áreas para que la respuesta no cambie entre servicio, legal, tecnología, riesgo y cobranza.

Medir riesgo operativo

Clasificar suplantación como evento de riesgo operativo, con frecuencia, impacto y controles preventivos.

Usar datos

Aprovechar datos transaccionales, device intelligence, patrones y trazabilidad para prevenir, detectar y defender.

Conclusión

El principal aprendizaje del espacio es que la Ley 2573 acelera una conversación que el mercado ya debía tener: la madurez de una operación de crédito no se mide solo por aprobar y desembolsar rápido, sino por su capacidad de demostrar que lo hizo correctamente.

Si este informe deja más preguntas que respuestas, cumple su objetivo.

La intención es que cada entidad revise su operación, identifique brechas y fortalezca su capacidad de defensa frente a escenarios de suplantación.