SoFi Tech Solutions

Combatir el fuego con fuego: cómo detener el fraude de identidad y de primera mano, las estafas románticas, el fraude a personas mayores y mucho más.

El manual de servicios financieros, tecnología financiera y fraude de marca para detener las redes criminales digitales

Esta es la realidad a la que se enfrentan hoy en día todas las organizaciones de servicios financieros, fintech y marcas: los estafadores están lanzando ataques impulsados por la inteligencia artificial a un ritmo más rápido del que la mayoría de los sistemas pueden adaptarse.

Mientras las organizaciones debaten los plazos de implementación, los delincuentes ya están utilizando la inteligencia artificial y el aprendizaje automático para eludir los sistemas tradicionales de detección de fraudes en tiempo real. Hoy en día, para prevenir el fraude de forma eficaz, las organizaciones deben igualar la sofisticación tecnológica de los delincuentes.

En pocas palabras, hay que combatir el fuego con fuego.

Según el estudio Javelin 2025 Identity Fraud Study, los costos del fraude de identidad aumentaron considerablemente en 2024, con pérdidas totales en Estados Unidos que ascendieron a algo más de 27 000 millones de dólares, lo que supone un impresionante aumento del 19 % con respecto a los 22 800 millones de dólares de 2023.

Lo que hace que este aumento sea especialmente alarmante es su amplitud: todos los tipos de fraude registrados por Javelin aumentaron en pérdidas. La apropiación de cuentas (ATO), una de las favoritas de los estafadores, registró el mayor aumento, pasando de 12,700 millones de dólares en 2023 a casi 16,000 millones en 2024.

En México y América Latina la historia no es muy diferente, pues de acuerdo con cifras de distintas organizaciones como la CONDUSEF, solo en México el fraude por suplantación de identidad registró un crecimiento explosivo del 84% durante 2024. Las pérdidas económicas en el país por fraudes bancarios alcanzaron cerca de los 14,500 millones de pesos, consolidando al fraude como el delito con mayor incidencia a nivel nacional, según el reporte de la ENVIPE 2025 del INEGI.

A nivel regional, la Federación Latinoamericana de Bancos (FELABAN) estima que el cibercrimen drena anualmente cerca de 90,000 millones de dólares de la economía de LATAM.

Los estafadores se mueven más rápido y a mayor escala, burlando las antiguas defensas y dejando a muchas organizaciones luchando por mantener el ritmo.

Esta guía está dirigida a instituciones financieras, empresas de tecnología financiera y marcas que estén dispuestas a mejorar su estrategia contra el fraude, transformando la gestión del fraude de una postura defensiva a un enfoque proactivo y centrado en el cliente que impulse la estabilidad, la seguridad y el crecimiento a largo plazo.

Se prevé que las pérdidas por fraude en los pagos en línea superen los 362 000 millones de dólares en los próximos cinco años, y cada vez es más difícil y costoso combatir el fraude que provoca esas pérdidas.

Ponga a su equipo a la ofensiva: La escalada de la guerra contra el fraude financiero

Una mitigación eficaz del fraude es más que una simple prevención de pérdidas: es la base de la confianza de los clientes y del crecimiento a largo plazo. El éxito requiere una combinación personalizada y basada en datos de tecnología, análisis y experiencia.

Cada ataque sofisticado y cada nueva técnica de estafa ponen de relieve la naturaleza implacable de este desafío, en el que los delincuentes aprovechan la inteligencia artificial y el aprendizaje automático, al tiempo que explotan las vulnerabilidades más rápido de lo que muchas organizaciones pueden responder.

El aumento de los fraudes por apropiación de cuentas es indicativo de un problema sistémico mucho mayor. Los delincuentes se dirigen a una amplia variedad de cuentas, incluidas cuentas corrientes y de crédito, correo electrónico, carteras digitales, teléfonos móviles y redes sociales.

Las normas de autenticación laxas, como la autenticación multifactorial opcional o las políticas de contraseñas permisivas, han impulsado el auge de los fraudes por apropiación de cuentas.

Los ciberdelincuentes no solo logran evadir la detección por parte de los consumidores cuando cometen un gran número de apropiaciones no autorizadas de cuentas financieras y no financieras, sino también por parte de los propietarios de esas cuentas.

Este entorno exige que los bancos y las cooperativas de crédito, las empresas de tecnología financiera y las marcas replanteen fundamentalmente su enfoque de la prevención del fraude. Nunca ha habido tanto en juego, y el costo de la inacción sigue aumentando con cada trimestre que pasa.

CAPÍTULO 1

¿Por qué la IA es esencial para sus estrategias de lucha contra el fraude?

Hoy en día, el fraude requiere más que un enfoque único para todos; es esencial contar con defensas adaptables y en capas. La era de los sistemas estáticos basados en reglas ha pasado, sustituida por soluciones dinámicas e inteligentes que evolucionan junto con las amenazas emergentes.

Manténgase a la vanguardia implementando la inteligencia artificial y el aprendizaje automático para identificar nuevos patrones de fraude, como la creación de identidades sintéticas, los esquemas de abuso de personas mayores, la manipulación de fraudes de primera mano y las estafas en constante evolución que los sistemas tradicionales no detectan. También es fundamental proteger la experiencia del cliente minimizando los falsos positivos, de modo que los clientes legítimos disfruten de un registro y unas transacciones rápidas y seguras. La detección de fraudes basada en la inteligencia artificial es esencial para lograr este equilibrio.

La investigación de Javelin muestra que los consumidores que tienen conocimientos prácticos sobre inteligencia artificial apoyan más que sus instituciones financieras utilicen la IA para proteger sus cuentas e identidades.

Aunque poco menos de la mitad (47 %) de los consumidores se sienten en general bien informados sobre la IA y su funcionamiento, el 81 % de ellos se sienten muy cómodos con que sus instituciones financieras utilicen la IA para la seguridad de sus cuentas y la protección contra el fraude.

Esta aceptación por parte de los consumidores es fundamental, ya que los bancos están empezando a incorporar más IA en sus estrategias de mitigación del fraude y en sus prácticas de verificación y autenticación de identidad. Las instituciones financieras se encuentran entre las entidades que más confianza inspiran a los consumidores, y parte de la construcción y el mantenimiento de esa confianza consiste en garantizar que los consumidores comprendan lo que su proveedor financiero está haciendo para protegerlos.

Las estrategias contra el fraude basadas en IA pueden lograr:

- Identificación en tiempo real de fraudes con identificaciones falsas, abusos a personas mayores y estafas en constante evolución.
- Una experiencia del cliente fluida con un mínimo de falsos positivos.
- Supervisión equilibrada en tiempo real y posterior a la transacción.
- Análisis en tiempo real de millones de patrones de gasto y comportamientos de transacción únicos.

CAPÍTULO 2

Siete preguntas que debe hacer al elegir un proveedor de gestión de fraudes

Un socio sólido en materia de fraude debe ser capaz de ayudarle a combatirlo con la misma tecnología y herramientas que utilizan los estafadores. Esto significa implementar los últimos avances en inteligencia artificial y aprendizaje automático para reducir el riesgo, las pérdidas y los gastos operativos, al tiempo que se protege a los clientes. Para mejorar sus resultados en materia de fraude, necesita un socio con una amplia experiencia que equilibre una sólida protección contra el fraude con una experiencia del cliente fluida, lo que favorece la confianza, el cumplimiento normativo y la eficiencia operativa a gran escala.

Detección mediante AI / Machine Learning

Pregunte a los proveedores: "Muéstrame cómo se adapta tu sistema cuando los estafadores cambian de táctica. ¿Puedes demostrar que aprendes de los nuevos patrones de fraude en tiempo real?". Su socio debe basarse en modelos avanzados de IA que aprenden continuamente de millones de patrones de gasto únicos, lo que permite una rápida adaptación a los nuevos esquemas de fraude a medida que surgen.

Controles personalizables

Pregunte a los proveedores: "Explíqueme cómo personalizaría las políticas de fraude para nuestro modelo de negocio específico y nuestra tolerancia al riesgo. ¿Qué limitaciones existen?". Cada organización se enfrenta a perfiles de riesgo y requisitos operativos únicos. El socio adecuado proporciona una gestión de políticas flexible que se adapta a sus necesidades específicas en lugar de obligarle a ajustarse a marcos predeterminados.

Cobertura integral

Pregunte a los proveedores: "Muéstrame tu flujo de trabajo completo de gestión del fraude, desde la supervisión de las transacciones hasta la resolución de disputas. ¿Cómo garantizas el cumplimiento normativo en cada etapa?". Sus servicios de operaciones contra el fraude deben incluir todo, desde la supervisión de las transacciones hasta el seguimiento de las disputas, garantizando una cobertura completa en todo el ciclo de vida de la gestión del fraude.

Resultados transparentes

Pregunte a los proveedores: "¿Pueden mostrarme exactamente cómo toma decisiones su sistema en materia de fraude? ¿Qué métricas específicas proporcionarán para medir el retorno de la inversión y el rendimiento?". Evite las soluciones de caja negra. Las organizaciones necesitan comprender cómo se toman las decisiones y medir el impacto de sus inversiones en prevención del fraude. Exija análisis e informes detallados que permitan una optimización continua.

Rigor normativo

Pregunte a los proveedores: "¿Cómo se mantienen al día con los requisitos de KYC, AML, OFAC, GDPR, PCI y Nacha? ¿Pueden mostrarme su proceso de actualización de cumplimiento?". El cumplimiento no es estático, requiere una atención y adaptación continuas a medida que evolucionan los requisitos.

Gestión proactiva de riesgos

Pregunte: "Más allá de detectar el fraude, ¿cómo nos ayudan a identificar las amenazas emergentes y a optimizar nuestra estrategia contra el fraude? ¿Pueden compartir ejemplos de recomendaciones estratégicas que hayan hecho a clientes similares?". Espere un análisis de datos personalizado y recomendaciones estratégicas basadas en las tendencias del sector y en su perfil de riesgo específico.

Escalabilidad y API

Pregunte: "¿Con qué rapidez se puede integrar su solución en nuestros sistemas existentes? ¿Pueden demostrar capacidades de toma de decisiones en tiempo real y mostrarme su documentación sobre API?". Asegúrese de que pueden integrar la toma de decisiones directamente en sus sistemas existentes para obtener protección instantánea y paneles de control automatizados.

Señales de alerta a tener en cuenta al evaluar a los socios contra el fraude:

- Gestión de políticas inflexible que limita la personalización
- Falta de métricas de rendimiento concretas o falta de voluntad para compartir resultados
- Análisis opacos («caja negra») sin criterios de decisión claros que complican su pista de auditoría
- Falta de detección o toma de decisiones en tiempo real

CAPÍTULO 3

Cómo desarrollar una estrategia moderna de prevención del fraude

Las estrategias eficaces contra el fraude unen a las personas, la coordinación de datos y la automatización en todos los puntos de transacción. La gestión moderna del fraude exige un enfoque holístico que conecte a la perfección la tecnología, el análisis y la experiencia humana para crear una protección integral, que incluye:

Supervisión en tiempo real

Evalúe al instante las transacciones (crédito, débito, ACH, BNPL y nuevas vías de pago) con una puntuación de riesgo dinámica impulsada por IA que aplica sofisticados modelos de riesgo para adaptarse a los patrones emergentes.

Gestión automatizada de disputas

Los flujos de trabajo optimizados resuelven las disputas rápidamente y sacan a la luz patrones de fraude más profundos que, de otro modo, podrían pasar desapercibidos. Busque soluciones que gestionen todo el ciclo de vida de las disputas, agregando inteligencia que se adapte a las tendencias de fraude.

Análisis de consorcios y redes

La amplia inteligencia del sector y la información de toda la red permiten la detección temprana de fraudes de identidad sintética, campañas de phishing, estafas románticas, estafas a personas mayores dirigidas a clientes vulnerables y amenazas emergentes. Este enfoque de inteligencia compartida permite a las organizaciones beneficiarse del aprendizaje colectivo sobre nuevos patrones de fraude.

Revisiones de riesgo continuas dirigidas por expertos

Los controles adaptativos se actualizan periódicamente para hacer frente a las nuevas amenazas y los cambios en materia de cumplimiento normativo. Los sistemas deben basarse en las últimas tendencias del sector y en los conocimientos analíticos para adoptar un enfoque integral.

Atención al cliente

Dote a los usuarios de herramientas y recursos para reconocer, denunciar y prevenir el fraude. La educación y la participación convierten a los clientes en socios en la prevención del fraude, lo que a menudo permite detectar actividades sospechosas antes de que se produzcan pérdidas.

Integración perfecta de API

Las API avanzadas incorporan la toma de decisiones directamente en los sistemas para ofrecer protección instantánea y paneles de control automatizados y prácticos. Esta integración garantiza que la inteligencia sobre el fraude llegue a todos los sistemas relevantes en tiempo real.

Aumento de los riesgos de fraude: A quiénes afecta y cómo adelantarse

Las empresas de tecnología financiera no pueden permitirse ignorar estas tendencias de fraude: a medida que aumentan las estafas y las apropiaciones de cuentas mediante inteligencia artificial, cada cliente afectado representa una pérdida de ingresos, multas reglamentarias y daños a la marca que tardan años en repararse en el mercado actual de servicios financieros, impulsado por la confianza.

CATEGORÍAS DE RIESGO CLAVE A SEGUIR:

Fraude de identidad

Cómo funciona:
Los estafadores combinan datos robados y sintéticos (por ejemplo, números de seguro social) para abrir nuevas cuentas, crear historiales «limpios» u obtener acceso no autorizado.

A quiénes afecta:
Niños, inmigrantes, consumidores con historial crediticio limitado, cualquier persona cuyos datos se vean expuestos en violaciones de seguridad.

Cómo detener el fraude:
- Verificación de identidad mediante IA en el momento del registro
- Comprobaciones de velocidad entre instituciones
- Datos compartidos del consorcio contra el fraude
- Puntuación de riesgo continua

Apropiación de cuentas

Cómo funciona:
Utilizando credenciales robadas o obtenidas mediante phishing, los estafadores obtienen el control de cuentas bancarias, de correo electrónico o redes sociales legítimas de los clientes para robar fondos o cambiar información personal.

Quiénes se ven afectados:
Todos los grupos demográficos, con un mayor riesgo para los usuarios móviles/digitales y aquellos con una autenticación débil.

Cómo detener el fraude:
- Biometría conductual y huellas digitales de dispositivos
- Autenticación multifactorial sólida y en tiempo real
- Verificaciones de velocidad de inicio de sesión y desafíos escalonados

Ataques de phishing y suplantación de identidad

Cómo funciona: Los delincuentes envían correos electrónicos, mensajes de texto o llamadas falsas haciéndose pasar por marcas de confianza (bancos, agencias, soporte técnico) y presionan a sus víctimas para que hagan clic en enlaces, introduzcan datos confidenciales o transfieran fondos con urgencia.

A quiénes afecta: Adultos mayores, nuevos inmigrantes, personas con menos conocimientos tecnológicos y cualquier consumidor activo en el ámbito digital.

Cómo detener el fraude:

- Identificadores de llamadas/bloqueadores de llamadas spam basados en inteligencia artificial.
- Alertas de pago/fraude en tiempo real.
- Educación y capacitación proactiva de los clientes.
- Scripts de fraude en el canal y advertencias de estafa.

Zelle, Venmo y otras estafas de pago P2P

Cómo funciona: Los estafadores solicitan dinero a través de aplicaciones de pago entre particulares (P2P) (Zelle, Venmo o Cash App), a menudo alegando una emergencia, haciéndose pasar por representantes bancarios o tecnológicos, o fingiendo una transacción.

A quién afecta: Consumidores con cuenta bancaria, especialmente trabajadores temporales, adultos jóvenes y usuarios de plataformas de pago P2P.

Cómo detener el fraude:

- Puntuación y limitación del riesgo de las transacciones P2P
- ¿Está seguro? Alertas basadas en el contexto
- Listas negras de números y bloqueos de transacciones basados en escenarios

Estafas de inversión (criptomonedas)

Cómo funciona: A las víctimas se les prometen altos rendimientos de falsas plataformas de intercambio de criptomonedas, esquemas Ponzi o estafas para hacerse rico rápidamente, que a menudo se difunden a través de ingeniería social o plataformas de negociación falsas.

A quiénes afecta: Jóvenes adultos, inversionistas y cualquier persona que busque inversiones alternativas o nuevas tecnologías

Cómo detener el fraude:

- Monitoreo de carteras y etiquetado de salidas
- Análisis de patrones de transacciones
- Alertas de fraude superpuestas para transferencias de criptomonedas
- Educación al cliente y herramientas de identificación de estafas

Fraude propio: disputas y tergiversación

Cómo funciona: Los clientes realizan reclamaciones falsas o hacen un uso indebido de los procesos de disputa (por ejemplo, alegando que una transacción legítima es fraudulenta), exagerando las pérdidas y haciendo un uso indebido de las devoluciones.

A quién afecta: A todos los segmentos de clientes; se observa un aumento frecuente en situaciones de dificultades financieras o de creciente presión económica.

Cómo detener el fraude:

- Análisis del comportamiento y de las transacciones
- Reconocimiento de patrones de disputas mediante IA
- Educación sobre reclamaciones falsas
- Umbrales adaptativos en las revisiones de disputas

Estafas románticas y a personas mayores dirigidas a clientes vulnerables.

Cómo funciona: Los estafadores se ganan la confianza durante semanas o meses (a menudo a través de plataformas de citas o redes sociales) y luego se aprovechan de la vulnerabilidad emocional de las víctimas para obtener fondos o credenciales.

A quién afecta: Solteros (especialmente mujeres mayores), personas mayores, usuarios emocionalmente vulnerables, aislados o sin experiencia digital.

Cómo detener el fraude:

- Supervisión mediante IA/ML de los patrones de transferencia/comunicación
- Alertas para categorías de pago recurrentes y de riesgo
- Alfabetización digital y educación sobre estafas
- Comparación de patrones adaptativa para estafas a largo plazo

Compromiso del correo electrónico empresarial (BEC)

Cómo funciona:
Los estafadores comprometen o suplantan correos electrónicos de empresas o proveedores, solicitando cambios urgentes en transferencias bancarias o ACH a cuentas fraudulentas, además de utilizar técnicas de ingeniería social y spear phishing.

A quiénes afecta:
Pequeñas empresas, equipos financieros de empresas, cualquier persona autorizada para realizar pagos.

Cómo detener el fraude:
- Verificación del nombre del beneficiario
- Devolución de llamadas obligatoria/verificación en dos pasos para cambios en transferencias bancarias o ACH
- Supervisión de cuentas y comportamientos
- Análisis de pagos salientes

Skimming y shimming

Cómo funciona:
Se instalan dispositivos de forma encubierta en cajeros automáticos, surtidores de gasolina o puntos de venta para capturar los datos de las tarjetas desde la banda magnética o el chip. Los datos se clonan y se venden o se explotan directamente.

A quiénes afecta:
A los usuarios de tarjetas de débito y crédito en cajeros automáticos, puntos de venta o terminales desatendidos (por ejemplo, lugares muy transitados).

Cómo detener el fraude:
- Pagos sin contacto y tokenizados
- Alertas de transacciones en tiempo real por uso sospechoso
- Desactivación de tarjetas utilizadas en terminales comprometidas conocidas

Estafas de reembolso/pago en exceso

Cómo funciona:
El estafador envía «demasiado» dinero (normalmente a través de una cuenta pirateada) y solicita que se le reembolse el exceso, dejando a la víctima responsable del pago original si se revierte.

A quiénes afecta:
Propietarios de pequeñas empresas, vendedores en línea (por ejemplo, mercados, Etsy, trabajadores temporales).

Cómo detener el fraude:
- Retener durante más tiempo los fondos procedentes de fuentes marcadas
- Detección automatizada de anomalías y comprobaciones con IA
- Advertencias claras a los clientes contra reembolsos/pagos en exceso desconocidos

Estafas emergentes que aprovechan las nuevas tecnologías

Cómo funciona:
Los delincuentes utilizan nuevas herramientas digitales, voz/vídeo de IA (deepfakes), estafas con códigos QR o suplantación de identidad a través de canales emergentes.

A quiénes afecta:
Los primeros usuarios, los usuarios de tecnología financiera, cualquier persona expuesta a nuevas aplicaciones de pago o canales de comunicación desconocidos.

Cómo detener el fraude:
- Detección adaptativa de fraudes y simulación de escenarios.
- Actualizaciones continuas de las reglas de IA/ML.
- Alertas tempranas a nivel de red/consorcio.
- Formación en tiempo real para el personal y los clientes.

CAPÍTULO 4

¿Cómo pueden los líderes de servicios financieros mejorar sus programas contra el fraude?

Los bancos y las empresas de tecnología financiera que se enfrentan a carteras fragmentadas de proveedores de soluciones contra el fraude están impulsando la consolidación para reducir la complejidad y eliminar costosos solapamientos. Un programa integral contra el fraude requiere un enfoque sistemático que aborde simultáneamente las personas, los procesos y la tecnología. Los líderes de los servicios financieros deben comenzar con estos siete pasos:

Evalúe su riesgo

Analice las tendencias históricas de fraude y las vulnerabilidades específicas de su organización y su base de clientes. Comprender dónde entra el fraude en su ecosistema y cómo evoluciona con el tiempo proporciona la base para realizar mejoras estratégicas. Esta evaluación se vuelve aún más crítica dada la tendencia al alza constante de los ataques de fraude en todos los tipos.

Defina sus métricas

Establezca indicadores clave de rendimiento (KPI) para la relación entre el fraude y las ventas, los costos de las disputas, los falsos positivos y las medidas de la experiencia del cliente. Unas métricas claras permiten evaluar objetivamente la eficacia del programa y orientar las decisiones de asignación de recursos. Contar con capacidades de medición precisas es esencial para demostrar el retorno de la inversión.

Audite los recursos

Probablemente ya cuente con varios socios para la lucha contra el fraude, pero ¿hay solapamientos o lagunas? Trace un mapa de las capacidades, las áreas de cobertura y los costos de los proveedores para identificar redundancias y puntos ciegos. Esto revelará oportunidades de consolidación que reducen la complejidad y mantienen una protección integral.

Controles por capas

Utilice la supervisión en tiempo real, el análisis posterior a la transacción, los paneles de control automatizados y la inteligencia de incorporación. La supervisión durante la autorización, junto con un análisis más amplio, permite un reconocimiento integral de patrones en todas las etapas de la transacción.

Elija socios flexibles

Priorice la transparencia y la reducción comprobada del fraude por encima de marcos rígidos o sistemas opacos. Los socios deben demostrar resultados medibles y proporcionar una visibilidad clara de sus procesos de toma de decisiones. Dada la rápida evolución del panorama de amenazas, la flexibilidad y la adaptabilidad son fundamentales.

Supervise y adáptese

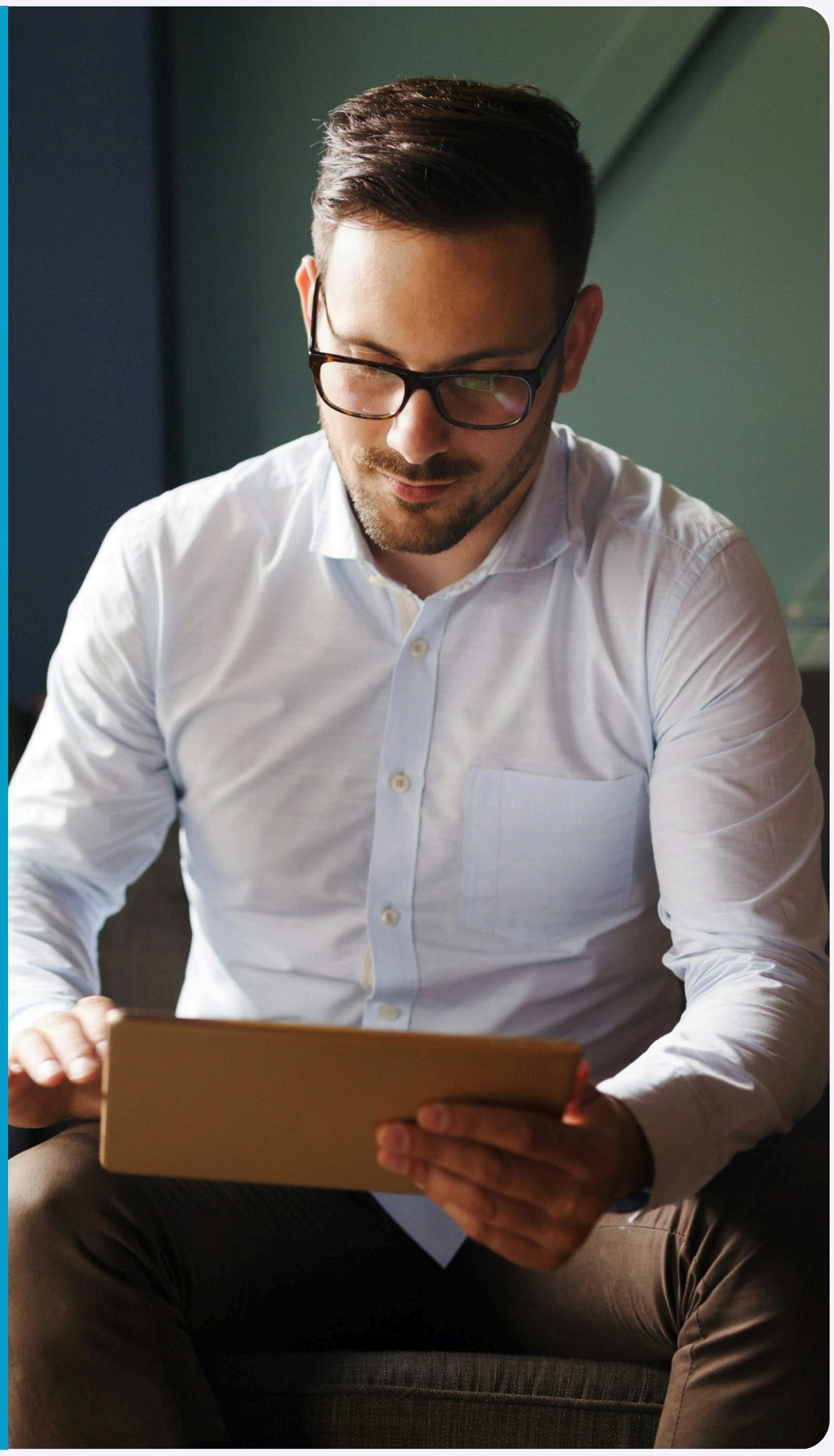
Revise periódicamente el rendimiento y efectúe los ajustes necesarios. Las tácticas de fraude evolucionan constantemente, lo que requiere una evolución correspondiente en las estrategias defensivas. La contratación continua de servicios contra el fraude garantiza una adaptación constante a las nuevas amenazas.

Eduque

Proporcione alertas, recursos de prevención y mecanismos de notificación claros para los clientes. Una base de clientes informada amplía significativamente sus capacidades de detección de fraudes. Esta educación cobra especial importancia a medida que aumenta la adopción de la inteligencia artificial y los consumidores necesitan comprender cómo les protege su institución financiera.

Checklist de optimización para responsables de programas antifraude:

- Análisis histórico de riesgos y evaluación de vulnerabilidades
- Indicadores clave de rendimiento claros para índices de fraude, costos de disputas y experiencia del cliente
- Auditoría tecnológica que compare las capacidades internas con las ofertas de los socios
- Controles por capas en tiempo real y posteriores a la transacción
- Supervisión continua, adaptación y educación del cliente.



Resultados reales con SoFi Tech Solutions

Las organizaciones que utilizan la plataforma de riesgo de pagos (PRP) y los servicios de operaciones contra el fraude de SoFi Tech Solutions han logrado mejoras significativas y cuantificables en la eficacia de su gestión del fraude.

Caso práctico 1

Una empresa fintech B2C que implementó los controles PRP en tiempo real de SoFi Tech Solutions experimentó una reducción del 35 % en las transacciones fraudulentas, al tiempo que mantuvo una experiencia de cliente fluida. La combinación de la puntuación dinámica del fraude y los controles personalizables eliminó los falsos positivos que antes frustraban a los clientes legítimos.

Caso práctico 2

Una plataforma bancaria digital para pymes aprovechó el panel de control de riesgos y el análisis integral de fraudes de SoFi Tech Solutions para optimizar sus políticas contra el fraude. Gracias a las consultas periódicas con el equipo de operaciones contra el fraude de SoFi Tech Solutions y al acceso al Risk Data Mart, lograron una mejora del 15 % en la precisión de la detección de fraudes, al tiempo que redujeron los falsos positivos. La información sobre el rendimiento permitió perfeccionar las políticas basadas en datos, lo que mejoró tanto la seguridad como la experiencia del cliente.

Caso práctico 3

Los clientes que utilizan la puntuación de riesgo de transacciones de SoFi Tech Solutions (Gscore), una puntuación de riesgo basada en el aprendizaje automático que evalúa el riesgo de las transacciones con tarjeta en tiempo real, obtuvieron un ahorro medio del 18 % en disputas por fraude y un ahorro del 11 % en gastos operativos. Además, observaron una mejora adicional del volumen de transacciones de 24 puntos básicos (pb), lo que mejoró los pb de intercambio de ingresos en promedio.

Caso práctico 4

Un servicio bancario en línea líder implementó el panel de control de riesgos PRP y los servicios de consultoría de SoFi Tech Solutions para perfeccionar continuamente su estrategia contra el fraude. Las revisiones periódicas del rendimiento y el acceso a análisis de tendencias agregados les permitieron adelantarse a los patrones de fraude emergentes, lo que se tradujo en una mayor eficacia de las políticas y una mayor confianza de los clientes gracias a la prevención proactiva del fraude.

Estos resultados demuestran que una gestión eficaz del fraude no consiste solo en prevenir pérdidas, sino en permitir el crecimiento del negocio mediante una mayor confianza de los clientes y una mayor eficiencia operativa.

La plataforma de riesgo de pagos SoFi Tech Solutions:Un enfoque integral

Nada daña más rápidamente las relaciones con los clientes que bloquear transacciones legítimas o crear fricciones innecesarias en momentos críticos. Ahí es donde la plataforma de riesgo de pagos SoFi Tech Solutions, una plataforma de detección de fraudes y gestión de riesgos basada en inteligencia artificial, proporciona información sobre riesgos en tiempo real que distingue entre amenazas reales y el comportamiento normal de los clientes, garantizando la seguridad sin comprometer la experiencia del usuario.

Los usuarios pueden lograr la mejor respuesta para cada cliente mediante controles en tiempo real (supervisión de autorizaciones) con revisiones exhaustivas posteriores a las transacciones y supervisión en todos los canales. Este enfoque dual detecta las amenazas en múltiples etapas, lo que evita pérdidas durante la propia transacción y permite aprender de los patrones que surgen con el tiempo. El motor de verificación instantánea SoFi Tech Solutions (GIVE) mejora esta capacidad al proporcionar una verificación inmediata de la identidad o de las cuentas bancarias externas para confirmar su existencia, estado y señales de riesgo asociadas en momentos críticos.

Los programas contra el fraude más eficaces reconocen que la automatización requiere algo más que ajustar las reglas existentes; también se integra con las operaciones comerciales. Las organizaciones que utilizan SoFi Tech Solutions Fraud Operations se benefician de un asesoramiento continuo sobre riesgos que adapta su estrategia a medida que surgen las amenazas y evolucionan las necesidades empresariales. En la primera mitad de 2025, el equipo de Operaciones contra el Fraude de SoFi Tech Solutions ahorró a los clientes más de 1,2 millones de dólares en las áreas de identidad, primera parte, ACH, abuso de disputas y fraude a personas mayores.

ESTRATEGIAS ADAPTABLES QUE AYUDAN A LAS ORGANIZACIONES A MOVERSE MÁS RÁPIDO Y PROTEGER LA EXPERIENCIA DEL CLIENTE

Los programas dinámicos contra el fraude, respaldados por análisis, tecnología adaptable y asesoramiento de expertos, pueden transformar la prevención del fraude en un activo empresarial. Para las instituciones financieras, las fintech y las marcas, un enfoque proactivo reduce el riesgo y los costos, al tiempo que fomenta la confianza de los clientes, la eficiencia y el crecimiento.

La gestión proactiva del fraude ofrece:

- Reducción del riesgo y los costos operativos
- Mayor confianza y satisfacción de los clientes
- Ventaja competitiva gracias a una seguridad superior
- Base para un crecimiento empresarial sostenible

¿Por qué los clientes eligen SoFi Tech Solutions para los servicios de fraude?

SoFi Tech Solutions ofrece operaciones escalables y eficientes que se ajustan a las normas reglamentarias y a las tendencias cambiantes en materia de fraude. Nuestra amplia experiencia en la detección de fraudes y la gestión de riesgos permite a los clientes centrarse en el crecimiento de su negocio principal, al tiempo que protegen a sus clientes.

Cobertura integral contra el fraude

Desde la detección en tiempo real hasta la investigación y resolución de casos, SoFi Tech Solutions ofrece servicios integrales contra el fraude adaptados a las necesidades específicas de cada programa.

Soluciones personalizables

Diseñamos controles contra el fraude que se adaptan a perfiles de riesgo específicos, objetivos de programas y expectativas de experiencia del cliente.

Excelencia operativa

Nuestros equipos dedicados a la lucha contra el fraude siguen protocolos de investigación detallados, análisis de las causas fundamentales y prácticas de documentación claras, lo que garantiza una gestión de casos de calidad y el cumplimiento de los acuerdos de nivel de servicio.

Cumplimiento normativo

Nuestro equipo permite el cumplimiento de las directrices KYC, AML, OFAC y Nacha, minimizando el riesgo de incumplimiento.

Tecnología avanzada

Aprovechando las herramientas líderes del sector, el análisis de datos y el aprendizaje automático, nos mantenemos a la vanguardia de las tendencias en materia de fraude, al tiempo que minimizamos los falsos positivos y las fricciones operativas.

Gestión proactiva de riesgos

Más allá de la detección y la gestión del fraude, identificamos las amenazas emergentes, recomendamos ajustes en las normas y compartimos información para mejorar la postura general de los clientes frente al fraude.

La evolución de una gestión reactiva del fraude a una estrategia proactiva y centrada en el cliente representa algo más que una simple mejora operativa. Genera una ventaja competitiva. Las organizaciones que adoptan esta transformación se posicionan no solo para sobrevivir al panorama actual de amenazas, sino para prosperar a pesar de los retos que plantea.

La clave está en comprender que la gestión moderna del fraude se basa fundamentalmente en el equilibrio entre:

- La seguridad y la experiencia del cliente
- La protección en tiempo real y el análisis posterior a la transacción
- La inteligencia automatizada y la experiencia humana.

Al integrar múltiples herramientas de prevención del fraude, incluidas plataformas de riesgo, sistemas de verificación y consultoría operativa, las organizaciones pueden pasar de una gestión del fraude puramente defensiva a un valor empresarial estratégico.

SoFi Tech Solutions

¿Está listo para mejorar la detección de fraudes en los pagos y proteger la experiencia de sus clientes?

SoFi Tech Solutions ofrece un enfoque integral para la detección de fraudes, al tiempo que reduce el riesgo y mejora el retorno de la inversión.

Prevención de fraudes que se adapta a sus necesidades

Ya sea que esté reduciendo activamente el fraude en tarjetas de crédito, ACH, BNPL o pagos instantáneos, SoFi Tech Solutions le proporciona las herramientas que necesita para detectar, prevenir y mitigar los delitos financieros antes de que afecten a sus resultados.

Analistas de fraude experimentados a su lado

A lo largo de la colaboración de los servicios de fraude de SoFi Tech Solutions con nuestros clientes, ofrecemos asesoramiento continuo sobre riesgos, utilizando las últimas tendencias clave del sector, los datos de nuestro consorcio y conocimientos analíticos para ofrecer un enfoque integral de lucha contra el fraude.

¿Está listo para ponerse en contacto con un especialista en fraude?
Póngase en contacto con nosotros hoy mismo para realizar una evaluación de su programa de fraude.

tech.sofi.com Contáctanos