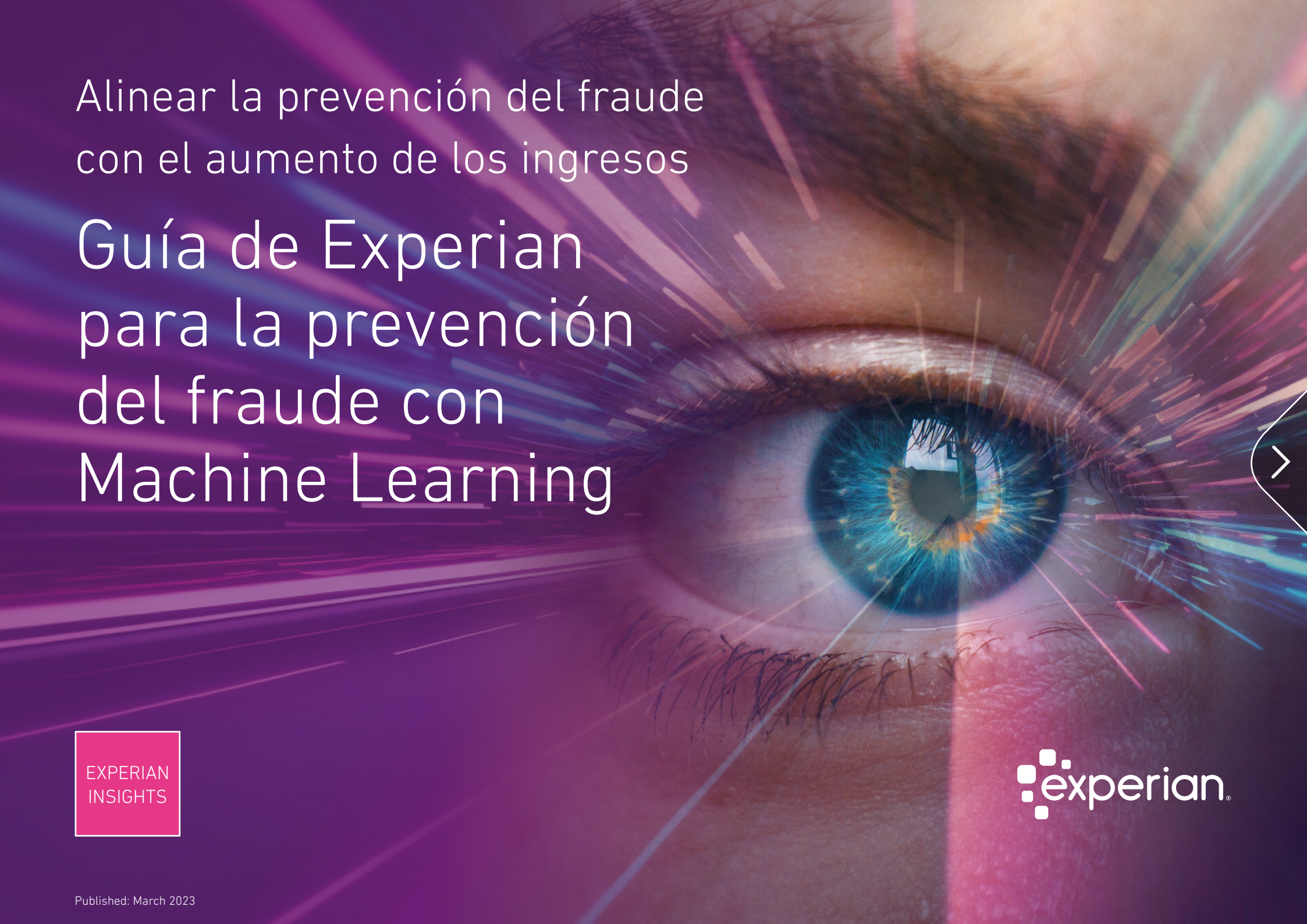
Alinear la prevención del fraude con el aumento de los ingresos

Guía de Experian para la prevención del fraude con Machine Learning



EXPERIAN INSIGHTS

Published: March 2023

Contenidos

El fraude inhibe el crecimiento Y aunque el comercio digital ha florecido gracias a las restricciones relacionadas con la pandemia, también lo han hecho los defraudadores, que aprovechan el aumento de la actividad en línea para aumentar la escala y la variedad de sus ataques. Dado que estos ataques son cada vez más sofisticados, es un reto para las empresas anticiparse a las últimas amenazas. Un estudio reciente de Juniper Research indica un crecimiento del 16% en las pérdidas por fraude en el comercio electrónico, con 41.000 millones de dólares perdidos en todo el mundo en 2022.

En un entorno de fraude en constante evolución, los sistemas de prevención que dependen de un enfoque tradicional basado en reglas tendrán dificultades para adaptarse, ya que las reglas se quedan obsoletas enseguida, lo que provoca el bloqueo de clientes reales e impide que se identifiquen los patrones de fraude más recientes.

¿Cómo pueden las empresas mejorar la prevención del fraude sin afectar a la experiencia del cliente ni a la conversión? ¿Cómo pueden mejorar la precisión de la detección del fraude cuando los ataques son más sofisticados?

La solución más potente para afrontar este reto es la integración del aprendizaje automático, o Machine Learning (ML), en las estrategias contra el fraude. Hay modelos de ML complejos que permiten a las empresas aumentar la detección del fraude al tiempo que identifican con mayor precisión a los clientes auténticos.

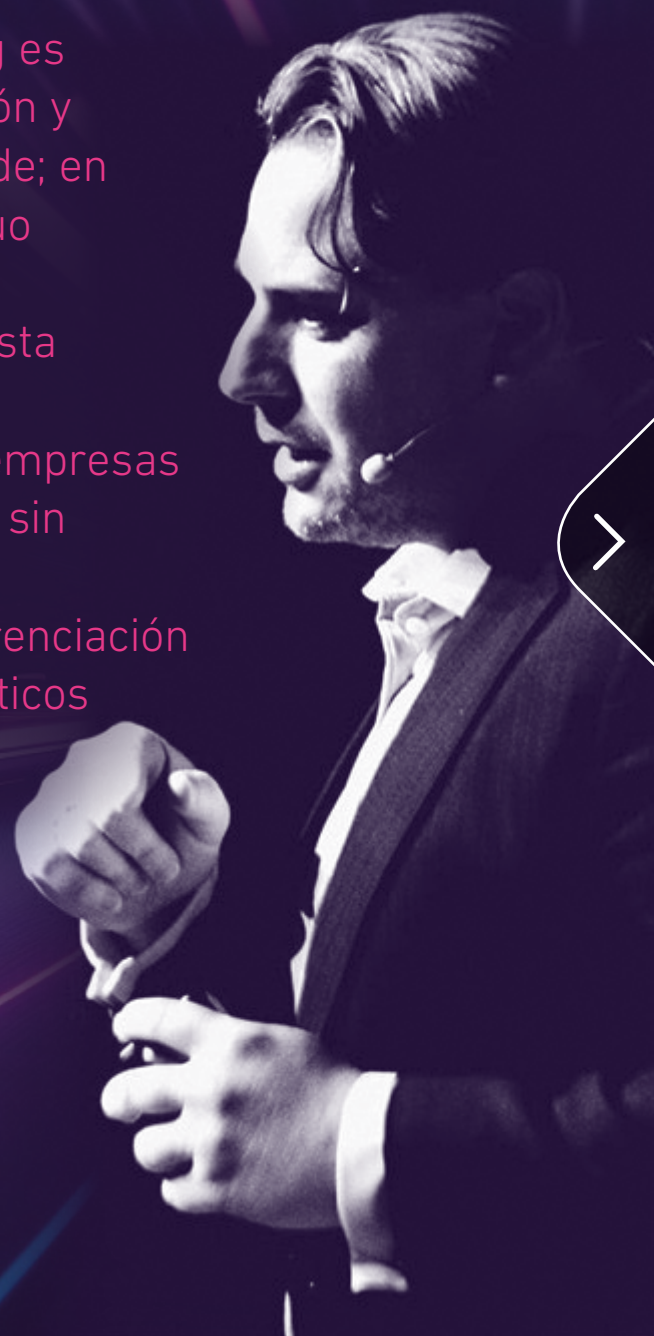
En esta guía, exploramos cómo la Inteligencia Artificial y el Machine Learning se están convirtiendo en atributos esenciales en la batalla contra el fraude. Analizaremos todo el proceso de una forma accesible para ofrecerte una idea clara de cómo esta tecnología puede ayudarte a reducir la tasa de fraude a la vez que aumentas tus ingresos.

Este informe hace referencia a la terminología del fraude y a los tipos de fraude más comunes. Para facilitar la comprensión, hemos elaborado un glosario de terminología de ML y fraude y una explicación de los tipos de fraude más comunes a los que se enfrentan los negocios en línea.

Por favor, ten en cuenta que utilizamos los términos Machine Learning e Inteligencia Artificial con las abreviaturas ML e IA de manera intercambiable en esta guía.

El Machine Learning es lo último en detección y prevención del fraude; en respuesta al continuo aumento de la ciberdelincuencia, esta tecnología puede proporcionar a las empresas niveles de precisión sin precedentes en la identificación y diferenciación entre clientes auténticos y fraudulentos.

Luciano Scalise
MD Decision Analytics, Experian
EMEA & APAC



Hay amenazas sofisticadas que aumentan las pérdidas

En los últimos años, se ha producido un incremento considerable del ciberfraude. El catalizador de este repunte es el acceso aparentemente fácil que tienen los estafadores a la información robada sobre tarjetas de crédito, cuentas bancarias y pagos a través de la red oscura.

En combinación con el gran volumen de información de identidad disponible a través de las brechas de datos, la gravedad de este problema es significativa.

El alcance del problema se agrava por el creciente nivel de organización de las redes de fraude y uso que hacen de la tecnología para crear métodos cada vez más elaborados de llevar a cabo el fraude. Cabe recordar que cada vez que un avance tecnológico se pone a disposición de las organizaciones, también se pone a disposición de los estafadores.

Por lo tanto, es evidente que la prevención del fraude que depende de sistemas basados en reglas codificadas carece con frecuencia de precisión cuando se trata de fraudes sofisticados. Esto significa que los estafadores pasan desapercibidos, mientras que muchos clientes legítimos son rechazados por falsos positivos, lo que supone una pérdida considerable de ingresos potenciales.

> Combatir el fraude es difícil porque los ataques evolucionan constantemente y son cada vez más sofisticados.

El fraude es un problema, pero también lo son los rechazos erróneos

No cabe duda de que el fraude supone un gran coste para las empresas. Sin embargo, es posible que el esfuerzo por evitar las transacciones fraudulentas haya alimentado un problema aún mayor: el rechazo erróneo de clientes legítimos. De hecho, las investigaciones sugieren que el coste de los rechazos erróneos puede ser a menudo mucho mayor que el valor de las pérdidas por fraude. Esto pone de relieve la magnitud del problema: las empresas no solo se enfrentan a las pérdidas provocadas por el aumento del fraude, sino también a una considerable pérdida de ingresos derivada de los falsos positivos de sistemas de prevención del fraude imprecisos.

Uno de los mayores quebraderos de cabeza para los responsables de la toma de decisiones en materia de identidad y fraude es buscar el equilibrio entre la prevención del fraude y la generación de ingresos.

CASI UNA DE CADA 3 EMPRESAS consideran que la incapacidad para alinear las estrategias de prevención del fraude y de incremento de los ingresos es el principal desafío que les impide gestionar con éxito los costes y riesgos del fraude*.

Demasiadas barreras para la prevención del fraude hacen que se rechace erróneamente una gran proporción de clientes buenos, lo que repercute negativamente en los ingresos. Sin embargo, si no se presta suficiente atención a la prevención, las pérdidas por fraude aumentan.

* Base: 587 tomadores de decisiones de EMEA en empresas de Servicios Financieros y Telecomunicaciones
Fuente: Un estudio por encargo realizado por Forrester Consulting en nombre de Experian, agosto de 2022

Expectativas de los clientes con baja fricción frente a mayores amenazas de fraude

Para las empresas de alto crecimiento, una buena conversión es de vital importancia para alcanzar los objetivos de ingresos. La conversión se produce esencialmente cuando un usuario completa la acción deseada en línea, como realizar una compra o rellenar un formulario de solicitud. La prevención del fraude es, por tanto, un delicado equilibrio de la experiencia del cliente (CX), y algunas empresas del sector del comercio electrónico están dispuestas a aceptar tasas de fraude más elevadas para mantener altas las tasas de conversión. Pero, a medida que las tácticas utilizadas por los estafadores se vuelven más sofisticadas, este enfoque debe cambiar; de lo contrario, se perderá una mayor proporción de ingresos a causa del fraude.

La prevención del fraude es la principal prioridad empresarial

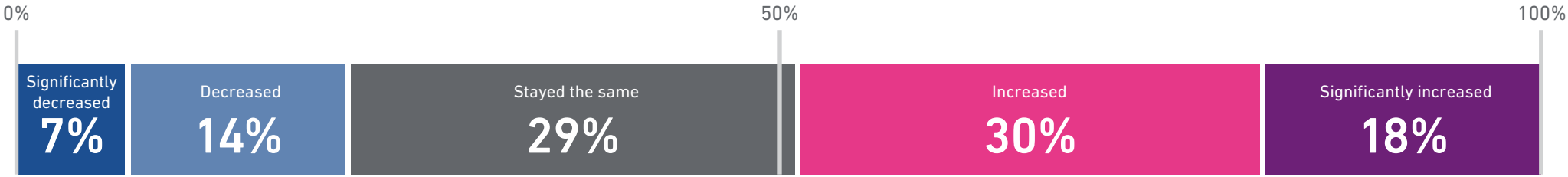
Nuestros estudios indican un cambio reciente en el enfoque de las empresas. En la encuesta a empresas y consumidores Experian EMEA 2022, "invertir para mejorar la protección contra el fraude" era una de las principales prioridades para el 73% de las empresas encuestadas. Convertir la prevención del fraude la prioridad número uno para 2022. El fraude siempre ha sido una prioridad, pero el aumento constante de las pérdidas está impulsando una mayor atención por parte de los altos directivos. Con un aumento interanual de las pérdidas por fraude en el 48% de las empresas, estas reconocen que hay que hacer algo para combatir este problema.

Sabemos lo difícil que es encontrar el equilibrio adecuado entre permitir que los clientes auténticos completen su compra o solicitud y detener a los estafadores.

Para abordar este reto, las empresas están priorizando cada vez más las inversiones en prevención del fraude y ciberseguridad. ¿Pero en qué área es mejor invertir?

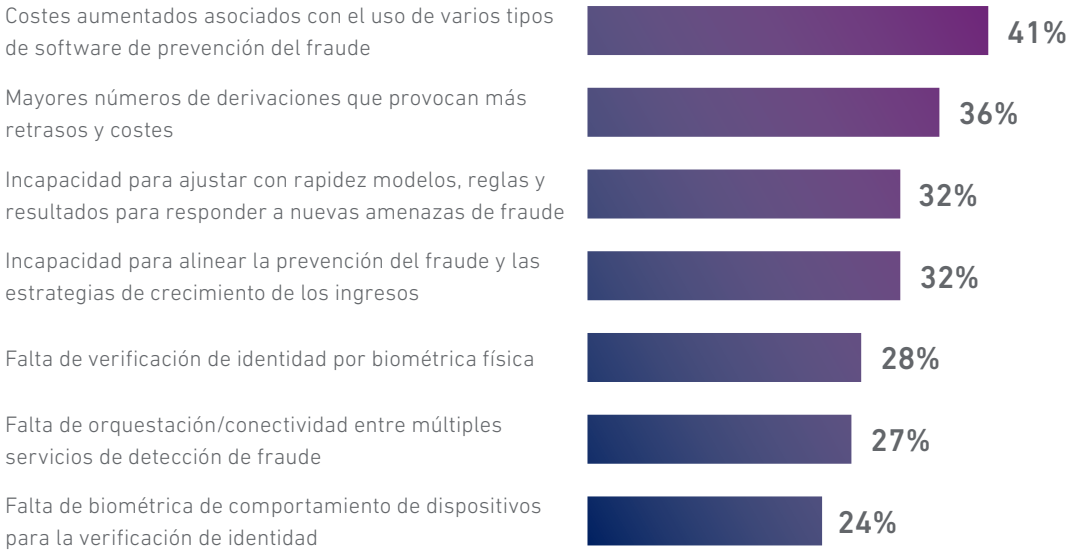
Esto nos lleva de nuevo al análisis avanzado y, en especial, al Machine Learning.

Rendimiento de las pérdidas por fraude en los últimos 12 meses (%)



Base: 587 tomadores de decisiones de EMEA en empresas de Servicios Financieros y Telecomunicaciones
Fuente: Un estudio por encargo realizado por Forrester Consulting en nombre de Experian, agosto de 2022.
Nota: Los porcentajes pueden no igualar el 100% por los redondeos.

Principales desafíos que impiden que las empresas gestionen con éxito los costes y riesgos de fraude aumentado



Base: 587 tomadores de decisiones de EMEA en empresas de Servicios Financieros y Telecomunicaciones
Fuente: Un estudio por encargo realizado por Forrester Consulting en nombre de Experian, agosto de 2022.
Nota: Los porcentajes pueden no igualar el 100% por los redondeos.

Es evidente que a un número cada vez mayor de empresas les resulta difícil responder al creciente riesgo de fraude. Utilizar el sistema de prevención del fraude con ML adecuado puede ayudar a las empresas a enfrentarse a todos estos problemas detectando con precisión a los estafadores, reduciendo las derivaciones y los falsos positivos y proporcionando una plataforma única para gestionar múltiples tipos de software de prevención del fraude. Otra ventaja de este enfoque es que mejora la experiencia del cliente al reducir la fricción que supone una compra o solicitud.

El papel del Machine Learning en la identificación del fraude

La forma más sencilla de entender cómo funcionan los modelos de Machine Learning es pensar en cómo aprendemos los seres humanos. Antes de emprender cualquier tarea, pasamos por un proceso de recopilación de información. Utilizamos esta información y nuestra experiencia para adquirir los conocimientos que necesitamos para completar la tarea. El ML se basa en el mismo principio, en el sentido de que la Inteligencia Artificial aprende de la experiencia para identificar la combinación correcta de características que dan un resultado determinado.

Para identificar a un sospechoso de fraude, los modelos de ML analizan un gran número de transacciones y aprenden qué combinación de características tiene más probabilidades de dar lugar a un fraude.

Cada una de estas características recibe un peso que indica su importancia a la hora de integrar todas estas reglas dinámicas. El sistema se alimenta constantemente de nuevos datos recopilados para garantizar que el modelo de ML pueda adaptarse rápidamente a las nuevas amenazas de fraude.

Machine Learning vs. Sistemas de prevención del fraude basados en reglas

En el pasado, muchas empresas dependían de un sistema basado únicamente en reglas para prevenir el fraude. A medida que las técnicas de fraude se han ido volviendo más sofisticadas, ha quedado patente la inadecuación de este tipo de sistema. Los sistemas basados en reglas se vuelven rápidamente enrevesados y contradictorios, lo que aumenta la tasa de falsos positivos y el número de revisiones manuales.

También están limitados por la comprensión humana, ya que se crean manualmente y pueden pasar por alto correlaciones sutiles en los datos, especialmente en patrones de fraude emergentes.

Otro problema asociado a los sistemas de prevención del fraude basados en reglas se produce durante los momentos de mayor actividad, como el "Black Friday". En momentos como estos, en los que el volumen de transacciones aumenta drásticamente, se da el correspondiente incremento de las revisiones manuales, ya que los umbrales de las reglas se sobrepasan. En consecuencia, las empresas que dependen únicamente de la prevención del fraude basada en reglas necesitan disponer de agentes de fraude adicionales para evitar grandes acumulaciones de casos para revisar. En cambio, la detección de fraude con Machine Learning puede mantener sistemáticamente los mismos niveles altos de precisión sin necesidad de un esfuerzo manual adicional durante los picos de ventas.

Supongamos que un posible cliente solicita una dirección de envío diferente a la de facturación, es algo muy normal.

Sin embargo, en determinadas circunstancias, podría estar relacionado con una actividad sospechosa y, en última instancia, fraudulenta. Puede depender de la geolocalización de esas dos direcciones. El Machine Learning aprenderá esto y marcará las combinaciones de direcciones específicas que hayan mostrado un patrón de fraude, en lugar de una regla más binaria que pueda afectar también a los clientes "buenos". Esta capacidad de comprender los matices de los datos es la clave de la detección del fraude con ML y lo que lo diferencia de otros tipos de tecnología de prevención del fraude, como los conjuntos de reglas permanentes.

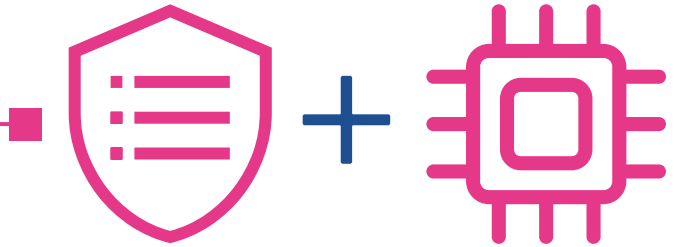
Machine Learning	Basado en reglas
El ML utiliza la IA para identificar patrones y correlaciones sutiles para crear características.	El especialista en fraudes identifica patrones y correlaciones de fraude y, entonces, crea reglas.
Una puntuación de probabilidad de 0 a 100 permite al usuario establecer el apetito de riesgo.	Umbrales y flujos de trabajo más rígidos que carecen de precisión.
Ajuste automático de las características a medida que surgen nuevas técnicas de fraude.	Ajuste manual de las reglas a medida que surgen nuevas técnicas de fraude.
Análisis proactivo y ágil de las tendencias de fraude en tiempo real.	Reglas preprogramadas reactivas que requieren una aportación constante para seguir siendo relevantes.
Escalabilidad y coste: Los algoritmos son más eficaces con grandes conjuntos de datos.	Difíciles de ampliar y más caros de mantener a medida que crece el conjunto de datos.

La solución: combinar reglas y Machine Learning

Aunque el ML ha mejorado enormemente los sistemas de prevención del fraude, sigue habiendo lugar para normas inequívocas. Por ejemplo, habría que impedir de inmediato que los dispositivos incluidos en una lista negra realicen transacciones/solicitudes en una plataforma en línea.

Un enfoque basado en las mejores prácticas implica combinar modelos ML adaptativos con reglas tradicionales, lo que permite a las empresas lograr mayor precisión en las decisiones y flexibilidad para adaptarse a patrones de fraude cambiantes.

Otra técnica de prevención del fraude que puede integrarse en un sistema basado en ML para mejorar la precisión de la detección es la huella digital de dispositivos. Por lo general, se utiliza para identificar a los clientes a través de una serie de puntos de datos del navegador y del dispositivo. Sin embargo, cuando se combina con el ML, esta información puede utilizarse para identificar comportamientos sospechosos mediante la evaluación dinámica de los diferentes atributos del dispositivo.



Un cambio radical en la detección del fraude: el proceso del ML

1

Recoger los datos

Los modelos de ML necesitan un conjunto de datos amplio con transacciones calificadas como fraudulentas y como no fraudulentas para entrenar y probar el modelo.

2

Limpiar los datos

Antes de poder usar los datos, hay que analizarlos con cuidado para eliminar cualquier información incoherente o sesgada.

3

Seleccionar un algoritmo

Hay varios algoritmos diferentes (por ejemplo, árboles de decisión, regresión logística) que pueden usarse para la detección de fraudes, la selección de la combinación adecuada depende de la aplicación.

4

Entrenar el modelo

Esto implica proporcionar datos limpios al algoritmo y ajustar los parámetros del modelo para minimizar la tasa de error.

5

Evaluar el modelo

Una vez entrenado el modelo, hay que evaluar su rendimiento con un conjunto de datos de prueba distinto del conjunto de entrenamiento. Así se obtiene una métrica que permite comparar las predicciones del modelo con resultados conocidos.

6

Ajustar el modelo

Si el modelo no presenta el nivel de precisión adecuado, se ajustan los parámetros y se añaden algoritmos.

7

Implementar el modelo

En esta fase, el modelo ya se puede usar en un entorno real.

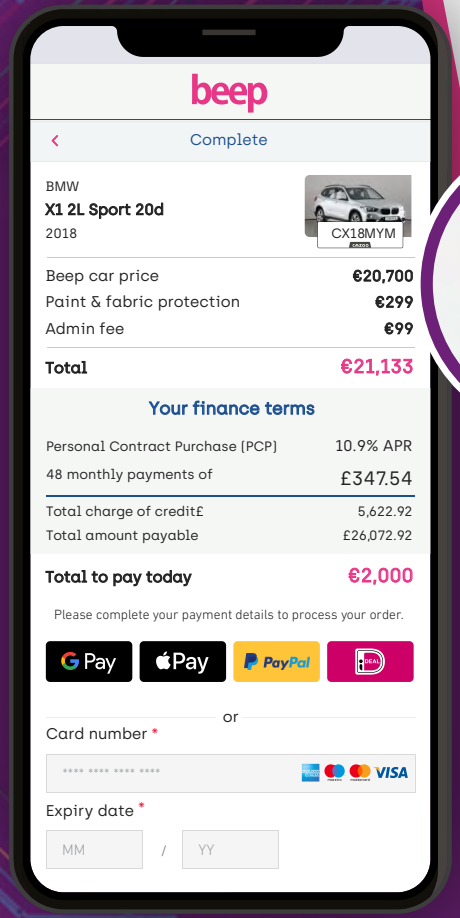
8

Reentrenar el modelo

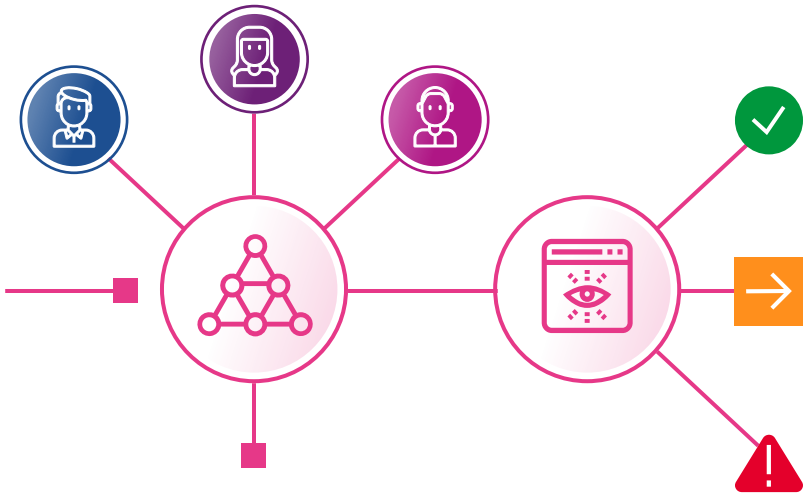
Todas las transacciones que se marquen como fraudulentas o para revisión manual se utilizan para volver a entrenar el modelo constantemente y mejorar su precisión.

Un modelo de ML en el proceso de decisión

El cliente inicia una transacción/aplicación en línea.



El modelo analiza los datos del cliente en una fracción de segundo y los compara con los conjuntos de datos evaluados previamente.



El modelo crea una predicción y hace una recomendación basada en el apetito de riesgo.

Aprobar
Si se acepta la transacción/ aplicación, pasa por la cadena de pago o el proceso de aprobación

Revisar
Los casos de revisión pasan a gestión de casos, donde un agente de fraude los evalúa manualmente

Rechazar
La transacciones/apliaciones consideradas de alto riesgo se rechazan

Ejemplos del tipo de datos usados para entrenar un modelo de ML

- **Casos de fraude confirmados**
  Fraudes reales detectados o rechazados
- **Credit card chargebacks**
  Successful transactions subsequently charged back.
- **Revisiones manuales**
  Decisions made by fraud agents.
- **Datos del dispositivo**
  Dispositivos que han sido marcados como fraudulentos en el pasado

El modelo de ML aprende de cada decisión que se toma y, por tanto, se vuelve más preciso con el tiempo.

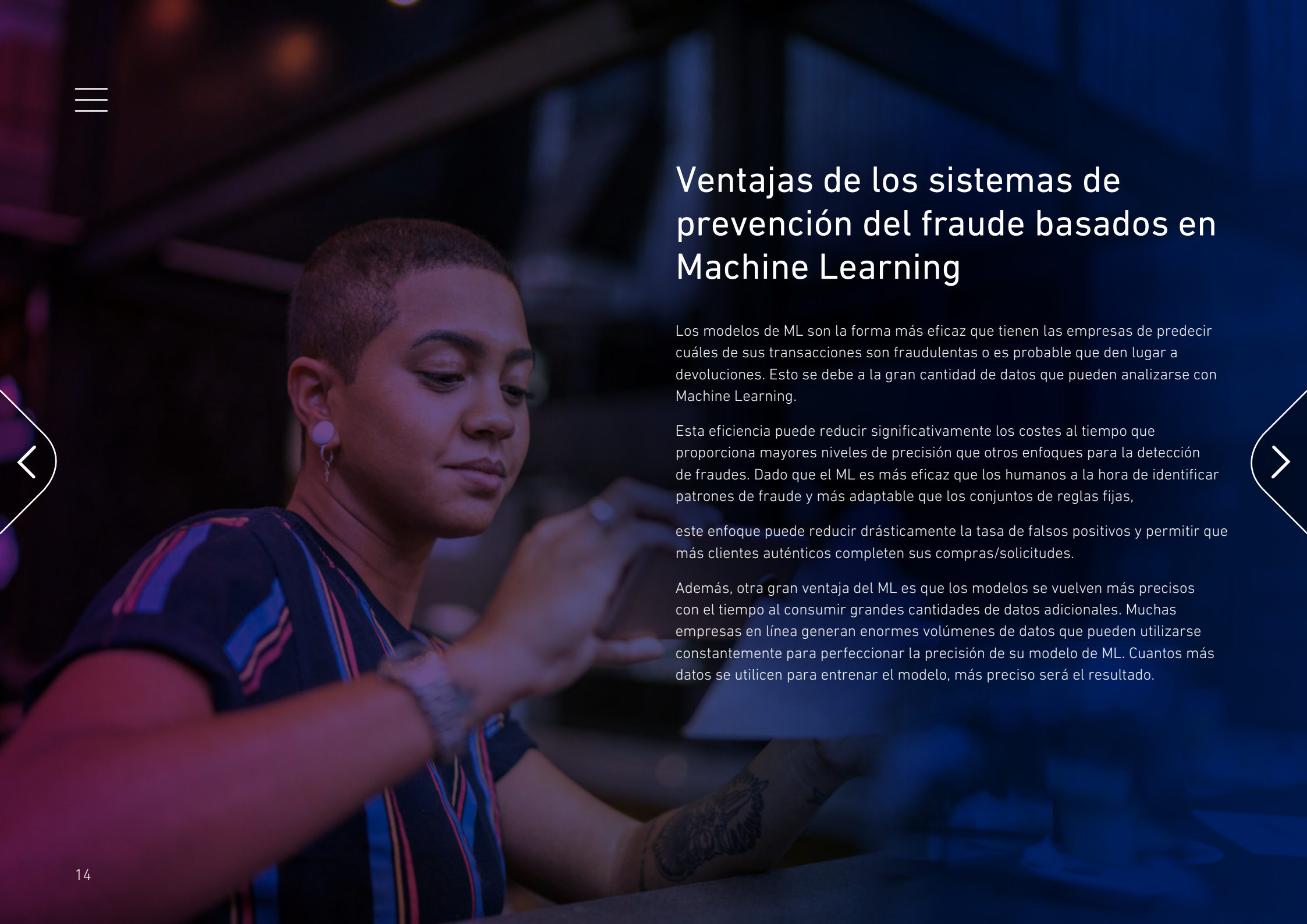
Explicar los resultados del Machine Learning

Es importante que cualquier modelo de ML ofrezca a los usuarios un resumen de las principales características empleadas para tomar cada decisión. Esto permite a las empresas entender las decisiones que toma el modelo y ofrecer una explicación a sus clientes de por qué se ha rechazado una compra o solicitud.

Para cada decisión de rechazo, el modelo de ML proporcionará las características más importantes relacionadas con ese resultado.

Estas características pueden ser cuestiones como una dirección de entrega y facturación diferente o una diferencia en el idioma del navegador y la dirección IP del dispositivo del usuario. Al indicar cada característica que se ha utilizado para tomar una decisión, el modelo de ML es transparente y ninguna decisión queda oculta en una "caja negra".

La propuesta de Ley de Inteligencia Artificial de la UE hará obligatoria la "explicabilidad" de los modelos de ML para los países de la Unión. Sin embargo, es probable que esta normativa se utilice como referencia internacional con una adopción generalizada.



Ventajas de los sistemas de prevención del fraude basados en Machine Learning

Los modelos de ML son la forma más eficaz que tienen las empresas de predecir cuáles de sus transacciones son fraudulentas o es probable que den lugar a devoluciones. Esto se debe a la gran cantidad de datos que pueden analizarse con Machine Learning.

Esta eficiencia puede reducir significativamente los costes al tiempo que proporciona mayores niveles de precisión que otros enfoques para la detección de fraudes. Dado que el ML es más eficaz que los humanos a la hora de identificar patrones de fraude y más adaptable que los conjuntos de reglas fijas,

este enfoque puede reducir drásticamente la tasa de falsos positivos y permitir que más clientes auténticos completen sus compras/solicitudes.

Además, otra gran ventaja del ML es que los modelos se vuelven más precisos con el tiempo al consumir grandes cantidades de datos adicionales. Muchas empresas en línea generan enormes volúmenes de datos que pueden utilizarse constantemente para perfeccionar la precisión de su modelo de ML. Cuantos más datos se utilicen para entrenar el modelo, más preciso será el resultado.

Beneficios de la prevención del fraude con Machine Learning

Más precisión

1 Los algoritmos de ML pueden analizar cantidades enormes de datos para detectar patrones y tendencias que pueden pasar desapercibidos para especialistas en fraude humanos. Esto conduce a un nivel de precisión mayor del que es posible con métodos de identificación de fraude manuales.

Reducción de costes y escalabilidad

2 La escalabilidad se consigue fácilmente con los modelos de ML, ya que el aumento de los datos disponibles solo mejora el modelo. Esto permite a más proveedores de servicio y comerciantes en línea reducir los costes asociados con sus operaciones antifraude.

Modelos en constante evolución

3 Los modelos de ML pueden adaptarse continuamente y mejorar con el tiempo a medida que se identifiquen nuevas técnicas de fraude. Este proceso de retroalimentación constante les permite mantenerse a la vanguardia de los patrones de fraude y responder a las amenazas emergentes en tiempo real.

Menos falsos positivos

4 La precisión de los modelos de ML para el fraude supone que casi todas las transacciones se clasifiquen de manera fiable. La ventaja es que tanto los clientes auténticos como los fraudulentos se identifican automáticamente. A diferencia de lo que ocurre con un conjunto de reglas rígido, los modelos de ML pueden adaptarse a amenazas de fraude cambiantes sin volverse demasiado enrevesados e identificar mal a clientes reales.

Reducción de revisiones manuales

5 Muchos negocios en línea trabajan con cantidades enormes de transacciones a diario y esto suele requerir un gran equipo de especialistas en fraude para revisar transacciones potencialmente fraudulentas, especialmente en épocas con picos de demanda. El coste y el tiempo que conllevan las revisiones manuales implica que el 60% de los comercios online preferirían reducir su dependencia de ellas o eliminarlas por completo.

La mayor precisión de los modelos de ML hace que muchos menos casos requieran revisión manual. Una vez que un especialista en fraude ha evaluado un caso, se añaden los datos al modelo para que en el futuro no haya que revisar transacciones similares. Esto reduce la carga de trabajo del equipo antifraude y les permite dedicar más tiempo a los casos más complejos.

Decisiones más rápidas sin tiempo de inactividad

6 Incluso el mejor especialista en fraudes puede tardar horas en analizar un conjunto de datos complejo y llegar a una conclusión. En cambio, los modelos de ML pueden realizar este análisis en menos de un segundo, ofreciendo mayor nivel de precisión. Los sistemas de ML pueden mantener este nivel de precisión de manera consistente y seguir ofreciendo decisiones exactas sin parar. Esto es especialmente importante en temporadas altas, cuando el volumen de transacciones es más alto de lo habitual.

Decisiones automáticas

7 Utilizando el ML en la prevención del fraude, automatizas una gran proporción de transacciones, lo que supone una toma de decisiones más rápida y una experiencia de cliente mejorada para más clientes. Los sistemas antifraude basados en ML pueden evaluar automáticamente grandes volúmenes de transacciones sin perder el alto nivel de precisión.

Retos para la implementación de prevención del fraude con ML

Como ocurre con cualquier tecnología rompedora, hay una serie de consideraciones clave a la hora de usar el ML para prevenir el fraude. Es fundamental que las empresas sean conscientes de estos problemas potenciales para garantizar que su modelo de ML funcione con precisión, eficacia y dentro de los marcos legales. Hemos identificado los cinco aspectos más importantes que deben tenerse en cuenta al empezar a utilizar un sistema de prevención del fraude con ML.

Cantidad y calidad de los datos

1 La precisión de cualquier modelo de ML depende de los datos empleados para entrenarlo. Las empresas que están en proceso de lanzar su propio modelo de ML antifraude necesitan contar con un volumen suficiente de datos limpios para garantizar que sus algoritmos puedan diferenciar entre transacciones/aplicaciones auténticas y fraudulentas. Sin un suministro de datos adecuado, cualquier modelo de ML será propenso a predicciones imprecisas.

Explicabilidad

2 La propuesta de **Ley de Inteligencia Artificial de la Unión Europea** será la primera normativa que regule el uso de la IA y es probable que se adopte en todo el mundo como referencia para controlar el uso de la IA en todos los aspectos de nuestras vidas. Para cumplir con esta legislación, es esencial que las empresas utilicen modelos de ML totalmente transparentes, que eviten los algoritmos de "caja negra" a la hora de evaluar a los clientes. Las empresas que no la cumplan se enfrentan a posibles acciones judiciales y a cuantiosas multas de hasta 30 millones de euros o el 6% de su facturación anual global.

Evitar sesgos

3 Si el conjunto de datos utilizado para entrenar un modelo de ML incluye algún sesgo, el modelo incorporará ese sesgo a su capacidad de predicción. El resultado puede ser la predicción inexacta de fraudes basada en el sesgo del modelo, como una ubicación geográfica o país específicos. La calidad del conjunto de datos es clave para evitar introducir sesgos potenciales que reduzcan la precisión de un modelo aumentando los falsos positivos.

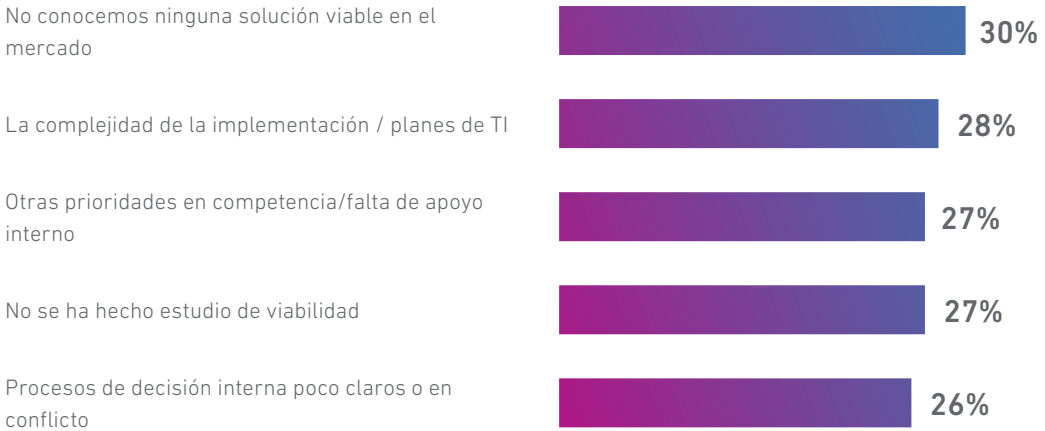
Privacidad

4 Los modelos de ML antifraude pueden implicar el tratamiento de datos sensibles, como transacciones financieras e información personal. Es importante que todas las empresas que pretendan utilizar el ML para la prevención del fraude conozcan la legislación aplicable en materia de privacidad de los datos y se aseguren de que cuentan con las medidas adecuadas para proteger la privacidad de sus clientes potenciales.

Aumento de la complejidad informática

5 **Nuestra investigación** revela que el mayor desafío al que se enfrentan los negocios al adoptar la IA y el ML es el aumento de la complejidad informática necesaria para manejar esta tecnología. Establecer un sistema de ML para la prevención del fraude es una habilidad altamente especializada que queda fuera de las capacidades de muchas empresas en línea. La manera más fácil de superar este desafío es asociarse con expertos con experiencia que entiendan los requisitos operativos y legales que implica el establecimiento de un sistema de prevención del fraude con ML.

Los obstáculos que impiden a las empresas implementar modelos de Machine Learning para prevenir el fraude



Base: 1905 tomadores de decisiones empresariales de veinte países
Fuente: Un estudio por encargo realizado por NorthStar Research Partners en nombre de Experian, junio de 2022

Nuestra investigación sugiere que el mayor obstáculo que impide a las empresas utilizar el ML para la detección del fraude es la falta de conocimiento de soluciones viables. No cabe duda de que a medida que se extienda la amenaza del fraude en línea, aumentará la familiaridad con el ML, ya que las empresas se verán obligadas a explorar alternativas a los sistemas basados en reglas.

Una vez que las empresas decidan invertir en ML, deberán establecer cuidadosamente planes de implantación, aprovechando la experiencia externa para garantizar el cumplimiento y el éxito de la integración operativa. Si se siguen estos pasos correctamente, es probable que el beneficio potencial en la prevención del fraude merezca la inversión.

El futuro de la prevención del fraude con Machine Learning

No cabe duda de que el ML va a seguir siendo parte integral de la prevención del fraude en el futuro. A medida que más sectores maduren en sus programas de prevención del fraude, cabe la posibilidad de que el intercambio de datos entre organizaciones y regiones (manteniendo la privacidad) se generalice. Este intercambio global de datos se conoce como inteligencia colectiva y podría llevar nuestra aplicación actual de ML a la prevención del fraude al siguiente nivel.

La incorporación de cantidades tan grandes de datos permitiría una mayor precisión en la detección del fraude. En teoría, esto podría llegar a eliminar el fraude, ya que se identificarían todas las formas posibles de cometerlo y se añadirían al modelo global de prevención del fraude. Aunque esto pueda parecer poco realista, el potencial de la inteligencia colectiva está claro. El sentimiento de los consumidores hacia el intercambio de datos también está mejorando a medida que se comprenden mejor las ventajas para la seguridad asociadas al intercambio de datos con empresas de confianza.

Según nuestra investigación global entre más de 6.000 consumidores de todo el mundo, el **56% INDICÓ** que estarían dispuestos a permitir que distintas empresas compartieran sus datos personales entre sí para garantizar una mayor seguridad en línea y evitar proactivamente ser víctimas de un fraude.

Dado que el nivel de sofisticación y la organización de los sindicatos del fraude en línea avanza, la mejor defensa reside en tecnologías como la identificación del fraude con ML y la colaboración. El intercambio colectivo de inteligencia entre empresas podría ayudarlas a anticiparse a los estafadores y reducir el impacto del fraude.

¿Cómo puede ayudar Experian a tu empresa a detectar el fraude?

Como proveedor líder de datos, análisis avanzados y software de prevención del fraude, Experian puede ayudar a tu empresa a desarrollar e implantar un modelo de ML diseñado específicamente para tus circunstancias. Operamos en 45 países y contamos con la experiencia y los conocimientos necesarios para ayudarte en cada etapa del establecimiento y mantenimiento de tu proceso de prevención del fraude con ML. Nos aseguramos de que tu modelo de prevención del fraude sea totalmente transparente y de que los resultados sean explicables para garantizar el cumplimiento de la normativa local.

Experian dispone de una gama de soluciones de prevención del fraude, diseñadas para ayudar a los clientes a encontrar el equilibrio óptimo entre la prevención del fraude y una experiencia del cliente sin fisuras. Nuestra última solución contra el fraude, Aidrian, mejora continuamente gracias al Machine Learning, con perfiles de dispositivos integrados y un motor de reglas flexible. Ayuda a los clientes a aumentar sus ingresos reduciendo los falsos positivos. Combinando nuestro modelo de ML personalizado con un centro de reglas de alto rendimiento, podemos clasificar las transacciones con mayor precisión que nunca.

CONTACTA PARA MÁS INFORMACIÓN

Glosario: Terminología sobre fraude y Machine Learning

Echemos un vistazo a la terminología asociada con el ciberfraude y cómo se aplica a la prevención del fraude con ML.

¿Qué son los algoritmos?
Son una secuencia claramente definida de procedimientos utilizados para resolver un problema específico. En la prevención del fraude se utilizan diversos algoritmos para identificar comportamientos fraudulentos, como árboles de decisión, *gradient boosting* y *random forests*. Sirven para analizar datos de clientes para identificar fraudes.

¿Qué son las API?
Una interfaz de programación de aplicaciones es una herramienta de código que se utiliza entre dos programas para permitir conexiones e interacciones en la nube. Predominan las API de REST, o API de transferencia de estado representacional, porque utilizan menos ancho de banda.

¿Qué es un falso positivo?
Cuando un cliente de buena fe es clasificado erróneamente como sospechoso de fraude.

¿Qué es la tasa de falsos positivos?
Esta métrica permite evaluar la precisión de un modelo de ML al clasificar los clientes y es crítica en la evaluación del proceso de prevención del fraude.

¿Qué son las características en ML?
Toda transacción en línea tiene una serie de atributos asociados, como valor monetario, ubicación y frecuencia. La combinación de uno o más atributos nos da una característica, que puede usarse para entrenar el algoritmo. Al identificar las características con mayor poder predictivo podemos crear modelos de ML eficaces. La ingeniería de características es

una especialidad que requiere una combinación exacta de atributos y hace que el ML basado en características sea muy superior a los sistemas basados en reglas de sí o no.

¿Qué es el Machine Learning?
Este término genérico puede entenderse de manera general como derivar conocimiento de la experiencia. El ML es un tipo de sistema de IA que aprende a partir de ejemplos e identifica patrones con ayuda de algoritmos. Proporcionando al modelo suficientes datos de alta calidad como ejemplos, se puede conseguir un nivel de precisión incomparable, del 99%. Lo bueno del ML en la prevención del fraude es que proporciona una puntuación de probabilidad en lugar de una decisión de sí o no, y esta puntuación de probabilidad de fraude permite a las empresas establecer con precisión su nivel de apetito de riesgo en función de la naturaleza de su oferta.

¿Qué es un conjunto de reglas?
Las reglas son descripciones claramente definidas de los criterios y parámetros que dan una respuesta binaria de sí o no. Con frecuencia se describen como una lógica si-entonces, y la combinación de todas las reglas que conducen a una decisión se conoce como conjunto de reglas. Experian dispone de un conjunto estándar de más de cien reglas que utiliza para crear conjuntos individuales en función del cliente.

¿Qué es un centro de reglas?
Es el software que utiliza la lógica de decisión de un conjunto de reglas para controlar automáticamente el proceso antifraude. Permite cambiar las reglas según sea necesario para adaptarse constantemente a las nuevas amenazas de fraude.

¿Qué es reentrenar un modelo de ML?
Una vez configurado un sistema de ML antifraude, los usuarios pueden introducir nuevos datos en el modelo a intervalos regulares. Esto permite entrenar constantemente el modelo con las últimas técnicas que los estafadores utilizan para intentar burlar los sistemas de prevención del fraude. Esta formación continua garantiza que el modelo esté siempre actualizado y ofrezca una precisión cada vez mayor.

¿Qué es una puntuación de riesgo?
Es un número de 0 a 100 que indica la probabilidad de que un cliente potencial sea un estafador. Los algoritmos que analizan las características determinan la puntuación. La precisión de una puntuación de riesgo depende de la calidad de los datos utilizados para entrenar los algoritmos. Comprender las sutilezas de los datos del conjunto de entrenamiento es la clave para producir una puntuación de riesgo precisa.

¿Qué es un umbral?
Un umbral de decisión es el punto desencadenante de una acción, como el uso de una regla. El valor umbral o límite es la puntuación que eliges como punto de inflexión para aceptar, rechazar o revisar una transacción.

Apéndice: Diferentes tipos de fraude en línea

Hay varios tipos de fraude relevantes para esta guía, así que vamos a verlos para comprender mejor cómo actúan los estafadores.

Robo de identidad

Es uno de los tipos de fraude más frecuentes. Consiste en que un estafador se hace pasar por un cliente real asumiendo la identidad de esa persona. Los estafadores utilizan varias técnicas para robar una identidad, como:

- **Phishing –** un individuo incauto proporciona voluntariamente datos personales a través de un correo electrónico o sitio web que imita a una empresa legítima.
- **Pharming –** se utiliza un virus o troyano desde una aplicación o sitio web para robar datos personales.
- **Whaling –** un estafador se hace pasar por un líder empresarial para atacar a ejecutivos y robar datos de la empresa.

Una vez que un estafador ha robado una identidad, puede utilizarla para llevar a cabo otros tipos de fraude, como el fraude limpio, la apropiación de cuentas y el fraude de fidelización.

Fraude limpio

Se trata de transacciones fraudulentas que parecen válidas porque el estafador tiene acceso a los datos de pago exclusivos de la víctima. No hay nada sospechoso en estas transacciones, salvo el hecho de que el verdadero propietario de los datos no está realizando el pedido, por lo que normalmente son capaces de eludir los controles de seguridad del comerciante o proveedor de servicios.

Apropiación de cuentas

Es una forma de robo de identidad en la que el estafador consigue acceso no autorizado a una o varias cuentas en línea de la víctima y las utiliza para realizar transacciones fraudulentas. Las apropiaciones de cuentas pueden darse con cualquier cuenta, desde bancaria o de otro método de pago hasta de correo electrónico o redes sociales.

Fraude de fidelización

Muchas empresas ofrecen programas de fidelización y, una vez que un estafador se ha hecho con una cuenta con datos de identidad robados, puede explotar estas ventajas en su propio beneficio.

Comprobación de tarjetas

Para verificar si la tarjeta de crédito o los datos de pago robados siguen estando disponibles, los estafadores realizan una pequeña transacción para ver qué tarjetas se han cancelado ya antes de pasar a transacciones más grandes. Cuanto menor sea el importe, menos posibilidades hay de que el propietario de la tarjeta se dé cuenta.

Fraude de afiliados

Este tipo de fraude implica una actividad falsa, a menudo llevada a cabo por bots, que genera comisiones fraudulentas para marketing de afiliación. Existen diferentes esquemas en función del modelo de pago a los afiliados, entre los que se incluyen los leads o impresiones falsos y los clics automatizados.

Reenvío

La primera fase de esta estafa consiste en que el estafador roba los datos de la tarjeta de crédito y pide productos en línea. En lugar de pedir que se envíen los productos a su propia dirección, utiliza a un intermediario para que reciba y vuelva a empaquetar los productos antes de enviarlos al estafador. Estos intermediarios no suelen ser conscientes del delito y los reclutan con la promesa de una oportunidad legítima de trabajo desde casa.

Botnets

Se trata de redes de ordenadores infectados con malware que están controlados por estafadores. Utilizando varios ordenadores y datos de pago e identidad robados, pueden burlar con frecuencia los controles de seguridad para que parezca que una transacción se originó en el mismo lugar que la tarjeta de crédito robada.

Fraude de triangulación

Consiste en que un estafador anuncia productos a bajo precio en un sitio web de subastas en línea. En cuanto recibe un pedido de un comprador incauto, compra los productos un comerciante en línea utilizando los datos de la identidad y la tarjeta de crédito robados y se los envían directamente al comprador. En cuanto el propietario de la tarjeta de crédito denuncie la transacción fraudulenta, el comerciante original tendrá que reembolsar la compra, con la consiguiente pérdida de los bienes.

Visita nuestro sitio web para saber más y cómo podemos ayudarte:
www.experian.es

O contacta con nosotros a través de:
marketingcsda.es@experian.com

La información contenida en este informe se ha preparado utilizando datos de Experian y también de fuentes de datos externas, además de estudios de mercado. Todas las fuentes, a menos que se haga referencia a ellas, proceden de Experian Insights.