stripe

El estado del fraude en línea

Introducción

Este informe ofrece una descripción completa del estado del fraude en línea. Analizamos miles de millones de intentos de pago en millones de empresas en Stripe durante un período de dos años y trabajamos con Milltown Partners (en colaboración con focaldata) para encuestar a más de 2.500 líderes empresariales en 9 mercados de todo el mundo (Australia, Canadá, Francia, Alemania, Japón, Países Bajos, Singapur, Reino Unido y Estados Unidos).

Al combinar nuestro propio análisis de Stripe con los resultados de esta encuesta, podemos identificar las mayores tendencias de fraude en el último año, como el aumento de disputas relacionadas con productos en 2020 y que las empresas de pagos recurrentes están especialmente preocupadas por los impactos financieros del fraude. También destacamos cómo puede adaptarse con éxito a estas tendencias de fraude con consejos a lo largo del informe basados en los datos que descubrimos. Concluimos este informe con cuatro mejores prácticas generales basadas en nuestras predicciones sobre el rumbo de las practicas de fraude.

Clasificamos este informe en cuatro secciones:

- Por qué ha aumentado el fraude
- Cómo se diferencia el fraude según la región y el tamaño de la empresa
- El impacto comercial del fraude
- Nuestras predicciones para la industria del fraude

Resumen ejecutivo

- Según nuestra encuesta, el 64% de los líderes empresariales globales afirman que, desde el inicio de la pandemia, se ha vuelto más difícil para sus compañías luchar contra el fraude. Creemos que esto se debe, en parte, a un aumento en los tipos de fraude y el volumen general del mismo.
- Al comienzo de la pandemia, observamos un aumento temporal del 156% en las disputas relacionadas con productos, como los códigos de disputa de “producto no recibido” y “producto no aceptable”. Suponemos que los clientes solicitaban devoluciones de pago después de que los vendedores tardaban semanas, o incluso meses, en cumplir con los pedidos debido a interrupciones en la cadena de suministro.
- También vimos que un 40% más de empresas experimentaron intentos de ataques de prueba de tarjetas. Se crearon miles de nuevos negocios de comercio electrónico durante la pandemia, y creemos que este crecimiento dio paso a nuevas oportunidades para los estafadores.
- Si bien los intentos de fraude han aumentado para las empresas de todo el mundo, las de América Latina eran, y continúan siendo, particularmente susceptibles a ataques de este tipo. Observamos que las empresas de América Latina tenían una tasa de fraude un 70% más alta en comparación con las de América del Norte y un 143% más alta que las de Asia-Pacífico.
- Las empresas que ofrecen subscripciones o pagos recurrentes con tarjeta tokenizada fueron las que más lucharon contra el fraude, específicamente las empresas al consumidor (B2C). Más del 75% de las empresas en Norteamérica, Europa y la región Ásia Pacífico de suscripción B2C informaron que su carga de revisión manual aumentó y que tuvieron que desviar más recursos para combatir el fraude en el último año. Creemos que estas empresas orientadas al consumidor tienen más reconocimiento de marca, lo que significa que sus productos son más fáciles de revender. Como resultado, es más probable que los estafadores se dirijan a ellos.
- El impacto comercial del fraude va más allá de las pérdidas financieras. Según el análisis que realizamos en Stripe, cuanto más fraude intenta prevenir una empresa, más probable es que también bloquee los cargos legítimos, lo que reduce sus tasas de conversión de pagos. En un esfuerzo por reducir estos falsos positivos, las empresas pueden revisar manualmente los pagos marcados, pero esto agrega una sobrecarga operativa adicional.
- Predecimos que las empresas se adaptarán a estas tendencias de cuatro maneras: 1) Las intervenciones, como 3DS, jugarán un papel más importante; 2) fuentes de datos más completas ayudarán a las empresas a tomar decisiones más rápidas y precisas; 3) los emisores y las empresas colaborarán más para agilizar las disputas y reducir los falsos rechazos; y 4) las preferencias de pago de los consumidores seguirán cambiando, lo cual modificará el panorama del fraude.

Por qué ha aumentado el fraude

El COVID-19 marcó el comienzo de una ola histórica de crecimiento del comercio electrónico. Las empresas en Stripe procesaron globalmente más de **USD 640 mil millones** en pagos en 2021, un 60% más que el año anterior. Estos pagos proceden de un grupo de empresas en rápido crecimiento: **1.400** nuevas empresas se unieron a Stripe cada día el año pasado. Este crecimiento, especialmente en los nuevos negocios, creó más oportunidades para los estafadores.

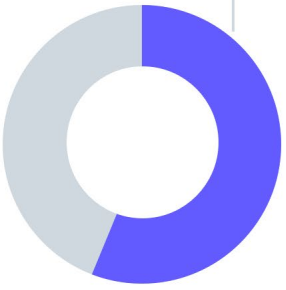
Muchos estaban iniciando negocios por primera vez y carecían de las herramientas o los recursos para lidiar con el fraude, o bien, estaban más concentrados en establecer su empresa y volverse rentables que en crear una estrategia para prevenir ataques de este tipo. Pero estos desafíos no estaban reservados solo para los nuevos negocios; incluso las empresas establecidas encontraron más difícil prevenir el fraude debido a ataques más complejos o mayores volúmenes de fraude en comparación con los tiempos previos a la pandemia.

Al mismo tiempo, los estafadores continúan volviéndose más sofisticados. Encuentran nuevas formas de dirigirse a las empresas, a menudo organizándose en grupos y conectándose con otros estafadores para compartir las “mejores prácticas”.

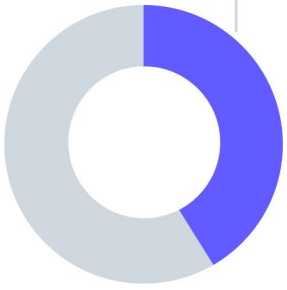
> “A medida que más clientes compran en línea en nuestras tiendas, el volumen de pagos fraudulentos ha aumentado. Es difícil revisar manualmente todas las transacciones, por lo que nos centramos en unas pocas porque no [hay] suficientes [recursos].
>
> - Profesional de fraude en una empresa de comercio electrónico en Singapur

64 % de los encuestados dicen que desde el inicio de la pandemia de COVID-19, **se ha vuelto más difícil para sus negocios prevenir el fraude**

Entre los que dicen que prevenir el fraude se ha vuelto más difícil:



56 % dice que es porque su negocio enfrenta **tipos de fraude más complejos** que antes de la pandemia



41 % dice que es porque su negocio enfrenta **mayores volúmenes de fraude** que antes de la pandemia

Específicamente, vimos aumentos en disputas relacionadas con productos y ataques de prueba de tarjetas:

Las disputas relacionadas con productos se duplicaron en 2020 en comparación con 2019

Desde marzo de 2020 hasta mayo del mismo año, nuestro análisis de Stripe encontró que los pagos tenían más del doble de probabilidades de generar códigos de motivo no fraudulentos, como disputas de "producto no recibido" y "producto no aceptable", en comparación con 2019. Nuestra hipótesis es que los clientes solicitaban más devoluciones de cargo después de que los vendedores tardaban semanas, o incluso meses, en cumplir con los pedidos debido a interrupciones en la cadena de suministro.

América Latina aparentemente experimentó las tasas más bajas de disputas relacionadas con productos, pero creemos que este hallazgo se debe al comportamiento de los emisores. En México, las disputas tienen siete veces más probabilidades de reportarse sin un código de motivo que en todos los países combinados, y en Brasil, las disputas tienen un 50% más de probabilidades de reportarse como fraude.

Mejores prácticas para prevenir disputas relacionadas con productos:

- ☐ Haga que su política de devolución sea clara, transparente y razonable. Por ejemplo, inicie la ventana de devolución cuando un cliente recibe el producto en lugar de cuando se envía el producto.
- ☐ Agregue el nombre de su empresa directamente en la descripcion de su tarjeta de crédito.
- ☐ Establezca un proceso formal de disputa.
- ☐ Notifique a los clientes antes de procesar su pago. Para las empresas de suscripción, asegúrese de que los clientes reciban al menos un recordatorio de su próximo pago.
- ☐ Para las empresas de comercio electrónico, solicite la firma de un cliente al entregar su pedido.

Intentos de ataques probando tarjetas se han dirigido a 40% más empresas

Los ataques probando diferentes tarjetas ocurren cuando alguien intenta determinar si la información de la tarjeta robada está activa para poder usarla para realizar compras. Un estafador puede hacer esto comprando información de tarjetas de crédito robadas y luego intentando validar o hacer compras con esas tarjetas para determinar qué tarjetas siguen siendo válidas.

Durante el primer año de la pandemia, vimos un aumento del 40% en la proporción de empresas que experimentaron intentos de ataques con tarjetas. Aquellas que se habían registrado en Stripe dentro de los 90 días representaron una parte mayor de lo habitual de las empresas probadas con tarjetas.

Los ataques con tarjetas pueden afectar negativamente a las empresas de varias maneras. La afluencia de transacciones debido a un ataque con tarjeta puede generar mayores costos de procesamiento de pagos y el riesgo de tiempo de inactividad (si una empresa no puede manejar el aumento en el tráfico, su sitio web puede colapsar). Además, los ataques exitosos de prueba de tarjetas dañan el ecosistema financiero global. Es más probable que las empresas procesen pagos con tarjetas robadas, lo que en última instancia genera más disputas. Debido al riesgo para el ecosistema financiero, los emisores y las redes de tarjetas pueden penalizar a las empresas por permitir ataques.

Otro **análisis de Stripe,** realizado en noviembre de 2021, encontró que las organizacions sin fines de lucro se ven particularmente afectadas por los ataques de prueba de tarjetas: El 11 % de todos los ataques de prueba de tarjetas que observamos estaban dirigidos a ellas. ¿Por qué? Muchas organizaciones benéficas permiten a los donantes (o, en este caso, a los estafadores) elegir una cantidad de donación muy pequeña, como USD 1.00 o USD 5.00. Es menos probable que el verdadero titular de la tarjeta note las transacciones pequeñas en un estado de cuenta. Además, es más probable que las organizaciones benéficas tengan equipos de fraude más pequeños y carezcan de los recursos para bloquear transacciones. Las organizaciones benéficas (y cualquier negocio objetivo de prueba de tarjetas) no solo pierden el dinero, sino que también son penalizados por los bancos por permitir que ocurran estos ataques con tarjetas.

Mejores prácticas para prevenir ataques con tarjetas:

- ☐ Optimice su integración con su proveedor de pagos. Muchos proveedores de pagos aplicarán diferentes controles para mitigar un ataque de prueba de tarjeta, pero el éxito de esos controles depende de la calidad de su integración y las señales que envíe al proveedor. En general, cuantos más datos proporcione su integración, más exitosa puede ser la prevención de validación de tarjetas.
- ☐ Mantenga seguras sus claves API. Su clave de API secreta se puede utilizar para realizar cualquier llamada de API en nombre de su cuenta, como crear pagos o realizar reembolsos. Trate su clave API secreta como lo haría con cualquier otra contraseña y solo otorgue acceso a quienes lo necesiten.
- ☐ Habilite CAPTCHA en su flujo de pago para diferenciar entre clientes legítimos y bots de prueba de tarjetas.
- ☐ Establezca límites de velocidad para controlar la cantidad de tráfico entrante y saliente. Por ejemplo, si los probadores de tarjetas validan las tarjetas adjuntándolas a nuevos clientes, podría limitar la cantidad de nuevos clientes que provienen de una sola dirección IP en un día.
- ☐ Considere solicitar a los clientes que inicien sesión en su cuenta para realizar un pago.

Cómo se diferencia el fraude por región, país, y tamaño de empresa

La importancia de combatir el fraude es universal: El 90% de los líderes que encuestamos en Norteamerica, Europa y región Asia Pacífico dicen que prevenir el fraude en el comercio electrónico es importante para su negocio. Sin embargo, existen diferencias sutiles en la actividad de fraude según la industria y la ubicación de la empresa, lo que sugiere un panorama complejo.

Fraude por región y país

Stripe tiene la mayor cantidad de datos de volumen de pago para empresas en América del Norte, por lo que usaremos esta región como referencia para otras en el análisis de esta sección.

Todos los negocios en línea tienen que gestionar el fraude; sin embargo, nuestro análisis de Stripe mostró que las empresas en América Latina eran particularmente susceptibles al aumento de las tasas de fraude.

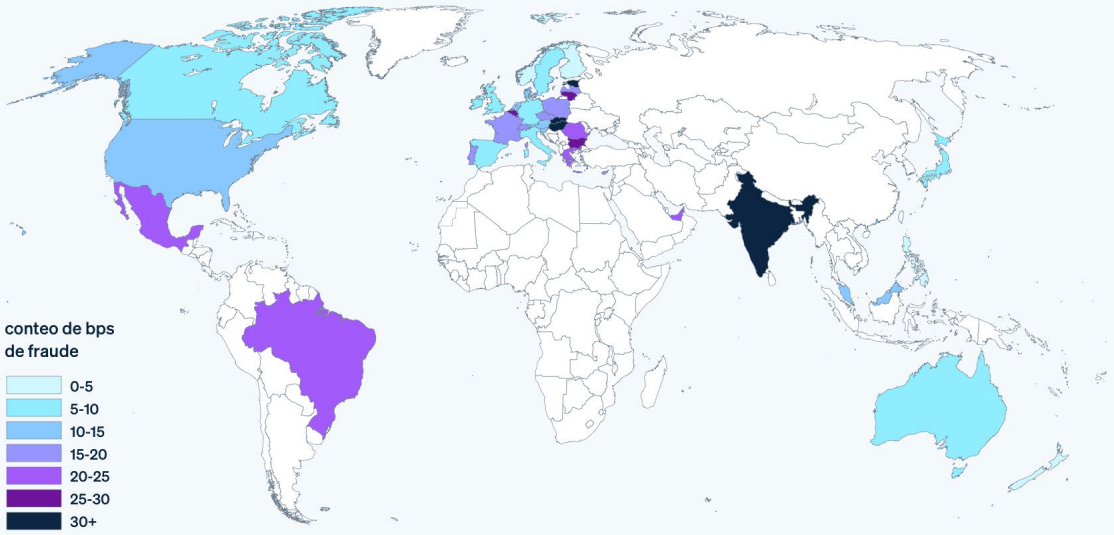
Nuestros datos mostraron que América Latina tuvo las tasas de fraude con tarjetas más altas del mundo durante nuestro período de tiempo estudiado: 97% más que en América del Norte y 222% más que en la región de Asia y el Pacífico. Las reglas también tienden a favorecer a los titulares en el proceso de disputa, lo que hace que las empresas sean especialmente vulnerables al fraude. Además de estos factores locales, el mercado se está moviendo cada vez más en línea (observamos un aumento del **518%** en los nuevos negocios iniciados en Stripe en América Latina en 2021), lo que crea aún más oportunidades para que los estafadores ataquen.

Las empresas de Europa, Oriente Medio y África tuvieron tasas de fraude sustancialmente más bajas en comparación con América del Norte, lo que probablemente refleja el impacto de las regulaciones de **Autenticación Reforzada del Cliente (SCA, Strong Customer Authentication)** que exigen que las empresas agreguen la autenticación de dos factores a su flujo de pago.

También hubo una variación considerable entre países. Por ejemplo, Francia tuvo casi el doble de la tasa de fraude de Alemania, mientras que Singapur experimentó la mitad de la tasa de fraude de la región de Asia-Pacífico en su conjunto. Esta variación en el fraude entre países puede dificultar aún más que las empresas globales luchen contra este problema. Como resultado, nunca existe un enfoque único para la gestión del fraude.

Tasas de fraude por país identificadas por Radar

Stripe Radar utiliza machine learning para detectar y bloquear diferentes tipos de fraude.



Recomendaciones:

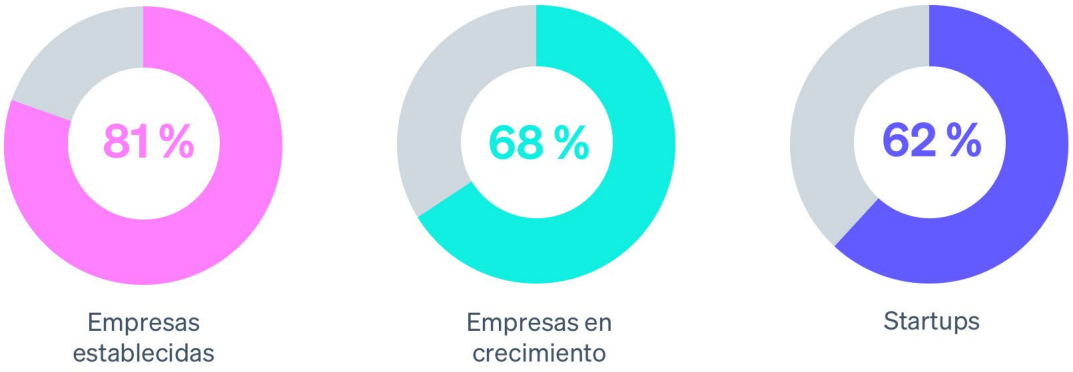
Si tiene la capacidad y los recursos , le recomendamos analizar el comportamientode sus clientes, las tendencias del mercado y las regulaciones en cada país en el que opera para comprender mejor los ataques y vectores de fraude más probables que podría experimentar. Sin embargo, a medida que las empresas crecen, esta complejidad puede convertirse rápidamente en algo difícil de administrar, lo que subraya la importancia de aprovechar una herramienta de fraude automatizada y sofisticada.

Fraude por tamaño de empresa y modelo de negocio

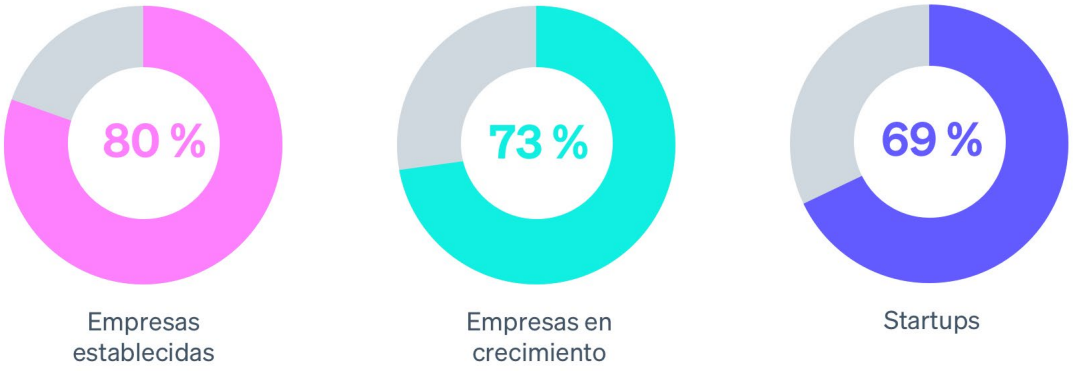
Los líderes empresariales perciben el riesgo de fraude de manera diferente según el tamaño de la empresa y el modelo de negocio. Por ejemplo, nuestra encuesta con usuarios de América del Norte, Europa y Asia Pacífico mostró que la prevención del fraude se vuelve más importante con la escala y, como era de esperar, las empresas más grandes tienen más recursos para invertir en una estrategia para prevenirlo, en comparación con las empresas más pequeñas. Sin embargo, los recursos por sí solos no previenen el fraude. De acuerdo con nuestra encuesta, los líderes empresariales con grandes equipos de fraude tenían más probabilidades de enfrentar desafíos operativos al administrar el fraude y es más probable que reporten mayores pérdidas por fraude.

Estas tendencias pueden representar oportunidades para las empresas más pequeñas: las empresas en crecimiento pueden optar por desarrollar una estrategia de fraude en profundidad ahora, cuando son más pequeñas, para adelantarse al problema. Sin embargo, desviar tiempo y recursos para luchar contra el fraude puede ser a expensas del crecimiento del negocio, y las empresas más pequeñas deben considerar cuidadosamente las compensaciones.

Es más probable que los líderes de las empresas más grandes consideren que el fraude en el comercio electrónico es muy importante



Es más probable que los líderes de las empresas más grandes estén de acuerdo en que esperan destinar más recursos a la prevención del fraude este año que el año pasado



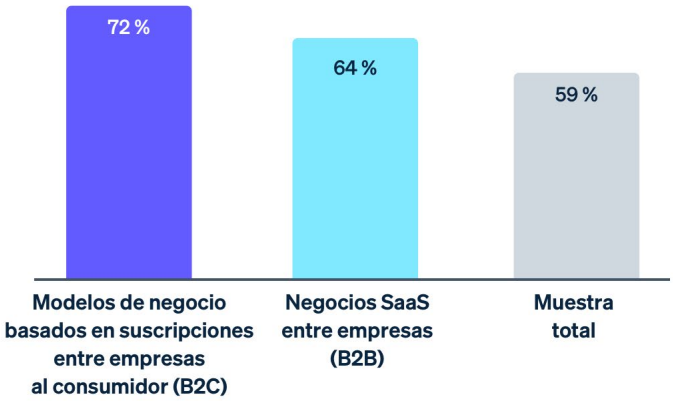
Empresas establecidas: Ganancias de negocio y USD 2 millones en ingresos anuales.
Empresas en crecimiiento: Negocios que ganan entre USD 2 y USD 60 millones en ingresos anuales.
Startups: Negocio con ingresos y USD 60 millones en ingresos anuales.

También analizamos los resultados de nuestra encuesta según el modelo de negocio, clasificando a las empresas de la siguiente manera:

- Software como servicio (SaaS)
- Empresas de suscripciones hacia el consumidor (B2C)
- Marketplaces y plataformas
- Comercio electrónico

Descubrimos las empresas que ofrecen susbcripciones o pagos recurrentes eran los más preocupados por el impacto financiero del fraude. En comparación con otros modelos comerciales que encuestamos, los líderes de fraude en las empresas de pagos recurrentes estaban más preocupados por perder dinero a causa del fraude y era más probable que pensaran que perdieron una mayor proporción de sus ingresos a causa del fraude en 2021, en comparación con la época anterior a la pandemia. Estas preocupaciones pueden ser el resultado de su modelo de negocio: Debido a que generan ingresos en un cronograma establecido (como mensual o trimestralmente) y a que han visto aumentar sus tasas de fraude en el último año, es más probable que piensen que esa tendencia solo continuará a medida que crezca su negocio.

Es más probable que las empresas de ingresos recurrentes digan que les preocupa perder más dinero por fraud e en 2022 que en 2021



En particular, las empresas de suscripción B2C en Norteamérica, Europa y APAC lucharon más con la carga operativa del fraude. Era más probable que informaran que sus casos de revisión manual aumentaron en 2021, que desviaron más recursos para combatir el fraude y que tuvieron que retrasar inversiones o planes de expansión para gestionar el fraude.

Sugerimos como hipótesis que las empresas B2C experimentaron más fraudes porque es más probable que sean marcas familiares, lo que facilita que los estafadores revendan los bienes o servicios robados (como comprar una suscripción digital con una tarjeta de crédito robada y luego venderla a un precio más bajo).

El impacto comercial del fraude

El fraude es caro. De hecho, el 59% de los encuestados espera que su negocio pierda más ingresos por fraude este año que el anterior.

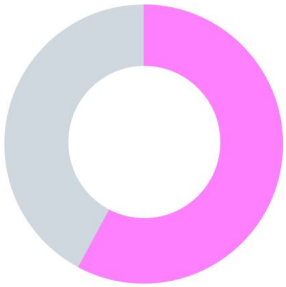
Las empresas pierden dinero tanto por disputas fraudulentas como por tratar de prevenir ese fraude. Por ejemplo, si su negocio pierde una disputa, usted es responsable de pagar más que el monto original de la transacción. El fraude a menudo conduce a tarifas de devolución de cargo (el costo asociado con el banco que revierte el pago con tarjeta) y tarifas de red más altas por disputas.

Sin embargo, nuestra encuesta encontró que el impacto comercial del fraude va más allá de las pérdidas financieras. Muchas empresas tienen que expandir su equipo de fraude o desviar productos o recursos de ingeniería para administrar los gastos generales operativos, desviando recursos valiosos de su producto principal.

El impacto comercial del fraude va más allá de las pérdidas financieras

72 %

de los negocios globales han tenido **que desviar productos o recursos de ingeniería para luchar contra el fraude**



58 %

de los líderes empresariales globales han tenido que **retrasar planes de expansión o inversión debido a fraude**

Tasas de conversión de pago más bajas

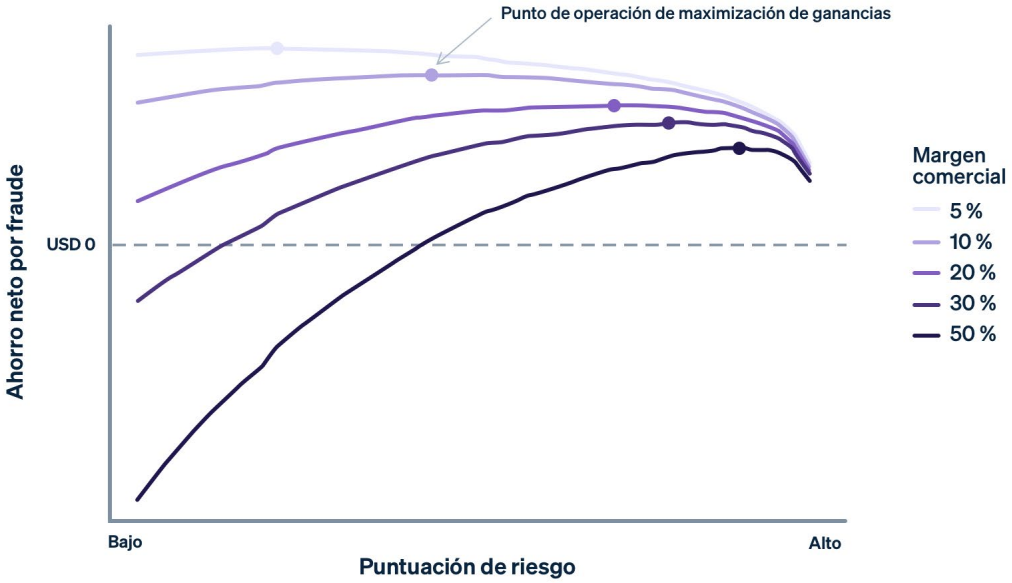
En nuestro análisis de Stripe, descubrimos que cuanto más fraude trata de prevenir una empresa, más probable es que también bloquee los cargos legítimos.

Los falsos positivos, o los falsos rechazos, se dan cuando un cliente legítimo intenta realizar una compra, pero se le impide hacerlo. Los falsos rechazos pueden hacer que la empresa tenga un impacto tanto en la ganancia bruta como en su reputación. De hecho, 33% de los consumidores dijeron que no volverían a comprar en una empresa después de un falso rechazo.

> “ Incluso un solo problema de fraude [puede] causar muchos problemas y puede hacernos perder a un comprador legítimo debido a revisiones de seguridad adicionales.
>
> - Profesional de fraude en una empresa SaaS en Canadá

Existe una equivalencia entre evitar más disputas y reducir la cantidad de clientes legítimos bloqueados. Cuando evite más fraudes, aumentará la cantidad de buenos clientes bloqueados. Por otro lado, reducir la cantidad de buenos clientes indebidamente bloqueados a menudo aumenta la probabilidad de que se escapen más fraudes reales. Esta compensación también depende de su solución contra el fraude: Siempre tendrá que gestionar esta compensación si su solución antifraude es estática y no invierte en recursos continuos para mejorarla. Por otro lado, si los modelos de su solución de fraude se adaptan y cambian continuamente en función de los vectores de fraude, esta compensación puede ser un desafío menor.

Dada la compensación entre la prevención de disputas y el bloqueo de pagos legítimos, las empresas pueden seleccionar el umbral en el que bloquear los pagos para maximizar las ganancias. Este punto de maximización de ganancias es donde la diferencia entre los costos de fraude prevenidos y las buenas ganancias bloqueadas es mayor.



La puntuación de riesgo es el umbral en el que se bloquean las transacciones utilizando Stripe Radar (la configuración predeterminada bloquea las transacciones cuando superan una puntuación de riesgo de 75).

El ahorro neto por fraude es el resultado de los costos totales de fraude evitados menos la ganancia legítima bloqueada.

El punto operativo de maximización de ganancias es el punto exacto en el que una empresa ha maximizado los ahorros netos por fraude, optimizando el bloqueo de transacciones fraudulentas y el bloqueo de transacciones buenas.

Cómo leer está gráfica: A medida que aumenta el umbral de riesgo a lo largo del eje x, existe una mayor probabilidad de que una transacción sea fraudulenta. Cuanto mayor sea el umbral de riesgo, menos transacciones serán bloqueadas. A medida que bloquea más transacciones, aumentan sus ahorros netos por fraude, pero también es más probable que bloquee transacciones legítimas.

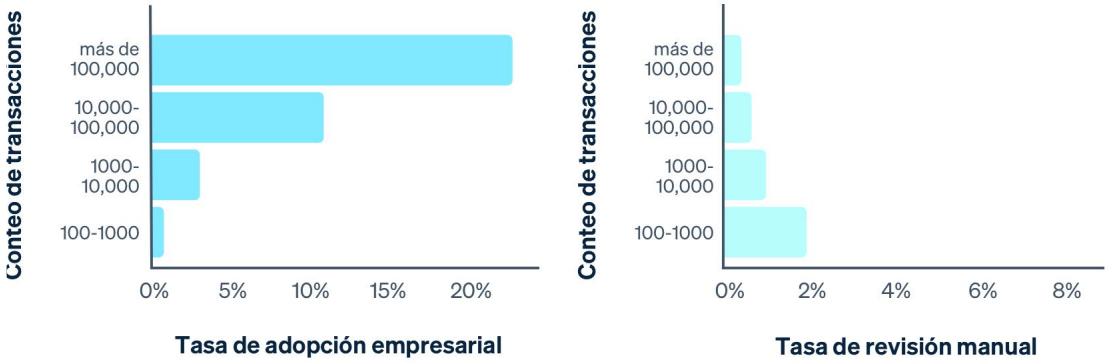
La compensación entre la prevención del fraude y el bloqueo de transacciones legítimas depende del margen por transacción. Por ejemplo, es más probable que las empresas con transacciones de alto margen (50%) a lo largo de la línea azul oscuro del gráfico permitan más transacciones y tengan un umbral de riesgo más alto porque cada transacción individual legítima es mucho más valiosa (en comparación con una empresa de menor margen, por ejemplo).

Las empresas deben administrar esta compensación en función de sus márgenes, perfil de crecimiento y otros factores. Si los márgenes de una empresa son pequeños, por ejemplo, si vende alimentos en línea, es posible que el costo de una transacción fraudulenta deba compensarse con cientos de buenas transacciones, lo que hace que cada falso negativo sea muy costoso. Las compañías con este perfil pueden inclinarse por lanzar una red amplia cuando intentan detener un posible fraude. Por otro lado, si los márgenes de una empresa son altos, por ejemplo, para una empresa SaaS, ocurre lo contrario. La pérdida de ingresos de un cliente legítimo bloqueado puede compensar el costo del aumento del fraude. También es importante tener en cuenta que las empresas pueden elegir cómo optimizar sus tasas de fraude hasta cierto punto; si el fraude alcanza ciertos niveles, las redes de tarjetas impondrán tarifas y multas.

Gastos generales operativos

En un esfuerzo por reducir los falsos positivos, las empresas pueden revisar manualmente algunos pagos marcados para confirmar si son realmente fraudulentos. Esto es bastante laborioso; las empresas necesitan un equipo de analistas de fraude para evaluar el riesgo en función de una variedad de factores, como los detalles de la transacción y el historial del cliente.

> Es realmente frustrante porque significa que tengo que desviar recursos para acomodarlo o siento que la situación se va a salir de control.
>
> - Profesional de fraude en una empresa de SaaS en Australia



Proporción de empresas activas elegibles de Stripe que usan revisiones manuales (tasa de adopción comercial) y la proporción promedio de transacciones revisadas manualmente (tasa de revisión manual) por número de transacciones en el último año (los números listados son los límites superiores de los segmentos)

Descubrimos que las empresas más grandes tienen más probabilidades de adoptar revisiones manuales, pero cuanto más grandes son, menor es la fracción de transacciones que revisan. Por ejemplo, más del 20% de las empresas que realizaron más de 100.000 transacciones en el último año usaron revisiones manuales, pero revisaron menos del 1% de sus transacciones totales. Las grandes empresas tienen los recursos para revisar manualmente las transacciones, pero guardan esas revisiones manuales para transacciones de mayor importancia.

Recomendaciones para reducir los gastos generales operativos:

- ☐ Para las medianas y grandes empresas de comercio electrónico, una solución antifraude de aprendizaje automático (machine learning) puede ayudar a combatir el fraude a gran escala, sin necesidad de recursos de ingeniería adicionales.
- ☐ Las grandes empresas a menudo usan un puñado de soluciones puntuales (como herramientas específicas para admitir CAPTCHA o escaneo de tarjetas) junto con software de fraude o como entradas en sus propios modelos de fraude.

Nuestras predicciones para la industria del fraude

El fraude evoluciona constantemente con el tiempo, y 2021 no fue la excepción. De hecho, los estafadores se volvieron aún más sofisticados el año pasado y se dirigieron a las empresas en línea de nuevas formas. Hemos abarcado una serie de desafíos en este informe, pero ¿qué significa esto para su empresa? Creemos que las compañías deben adaptarse al panorama actual del fraude de cuatro maneras:

1. Las intervenciones, como 3DS, jugarán un papel más importante

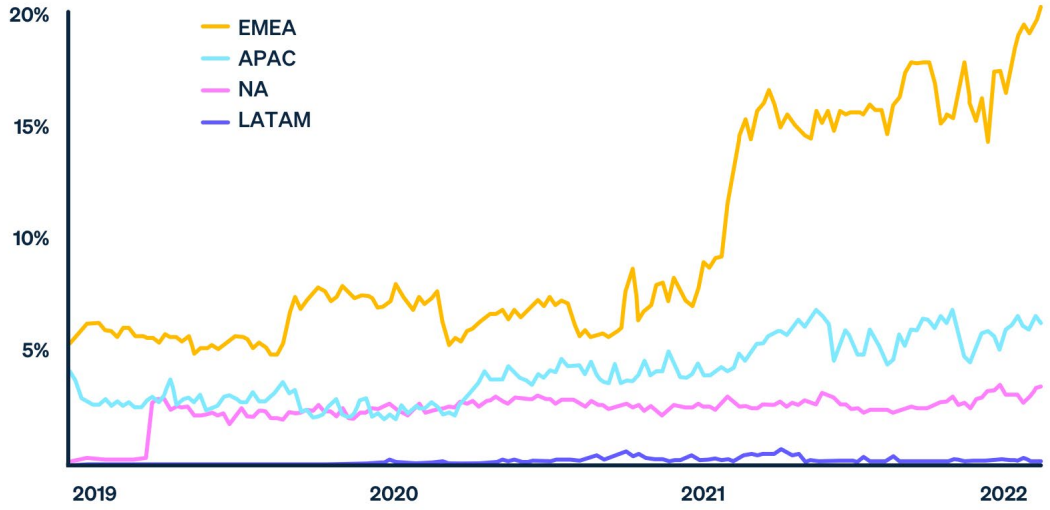
Las intervenciones le permiten bloquear o permitir transacciones con mayor confianza cuando cree que son sospechosas al emitir un "desafío" a los clientes (como pedirles que ingresen un código único que se envía por mensaje de texto).

Las intervenciones pueden tomar muchas formas, incluyendo:

- 3DS, que requiere que los clientes completen la autenticación de dos factores para realizar un pago. Es el principal método de autenticación de tarjeta utilizado para cumplir con los requisitos de Autenticación Reforzada del Cliente (SCA) en Europa y un mecanismo clave para que las empresas soliciten permisos a SCA.
- Escaneos de tarjetas para confirmar que el cliente tiene su tarjeta física en su poder en el momento de la transacción.
- Herramientas CAPTCHA que requieren que los visitantes del sitio web resuelvan un rompecabezas simple, como transcribir una serie de números o letras de una imagen distorsionada.

Las intervenciones ya están ganando popularidad. Analizamos la actividad de una intervención específica, 3DS, entre las empresas usuarias de Stripe en 2021 y descubrimos que la adopción de 3DS aumentó en todos los ámbitos, con las mayores ganancias fuera de América del Norte. Como era de esperar, las empresas europeas experimentaron el mayor aumento en la adopción de 3DS (esto fue el resultado de la aplicación total de los requisitos de SCA en casi todos los países europeos elegibles el año pasado). La regulación similar a la SCA también está creciendo en popularidad fuera de Europa, aumentando más rápido en India.

Cobertura 3DS de cargos por región a lo largo del tiempo



En un experimento, Stripe descubrió que reducir el umbral en el que se activa 3DS generó una disminución del 74% en su tasa de disputas fraudulentas. Además, en comparación con el bloqueo total de los cargos, 3DS todavía permite que la mayoría de los pagos sean exitosos (67% en todos los niveles de riesgo, 5% para el nivel de riesgo elevado). Sin embargo, el rendimiento de 3DS puede variar entre emisores.

En el futuro, esperamos que aumente el uso de intervenciones. Las empresas aplicarán intervenciones a una mayor parte de su volumen de transacciones y utilizarán tipos más diversos de éstas, especialmente aquellas que reducen la cantidad de fricción en el proceso de pago.

Consejos para el uso de intervenciones:

- ☐ Reemplace las transacciones que bloquea actualmente con intervenciones para aumentar la conversión y evitar el bloqueo de cargos legítimos.
- ☐ Las intervenciones pueden introducir fricción en la experiencia del cliente, lo que puede afectar negativamente la conversión. Optimice y pruebe cuidadosamente cómo desea activar las intervenciones para asegurarse de que no está afectando negativamente a los clientes legítimos.
- ☐ Cada intervención tiene una tasa de aprobación diferente y un impacto diferente en la reducción del fraude. Por ejemplo, si bien las claves de seguridad son extremadamente efectivas para prevenir estafadores, pueden perjudicar la conversión. Elija la intervención adecuada en función del riesgo de la acción que realiza su cliente y su tolerancia al riesgo/conversión.
- ☐ Ejecute intervenciones donde tengan el sentido más lógico en el desplazamiento del usuario (como solicitar un escaneo de tarjeta física cuando un cliente está agregando los detalles de su tarjeta).

2. Fuentes de datos más completas ayudarán a las empresas a tomar decisiones más rápidas y precisas

La gestión del fraude solía ser muy manual y requería un equipo de analistas para revisar todas y cada una de las transacciones. Hoy en día, la mayoría de las empresas utilizan algún nivel de automatización y modelos de aprendizaje automático para combatir el fraude a gran escala, además de revisiones manuales cuando es necesario (este enfoque híbrido varía según las industrias y los modelos comerciales). Los modelos de aprendizaje automático aprenden a distinguir las transacciones legítimas de aquellas que son potencialmente fraudulentas, y algunos incluso pueden entrenarse a sí mismos, lo que los hace más escalables y eficientes.

Los modelos de aprendizaje automático alguna vez se consideraron tecnología de punta para combatir el fraude, pero ahora están en juego. De hecho, las capacidades de aprendizaje automático por sí solas ya no son suficientes para mitigar los riesgos de fraude en constante evolución. Nuestros encuestados en America del Norte, Europa y APAC opinan lo mismo: más de la mitad de los encuestados, cuyo proceso de revisión está mayormente automatizado, dijeron que el tipo y la cantidad de fraude que enfrentan está evolucionando demasiado rápido para que su negocio se mantenga al día.

> “ Las oportunidades de fraude financiero se han vuelto más diversas y complejas con el tiempo. Necesitamos adaptarnos constantemente a los nuevos patrones y oportunidades de fraude.
>
> - Profesional de fraude en una empresa de servicios profesionales en Alemania

Creemos que la próxima fase en la evolución de la gestión del fraude se centrará en datos más completos para perfeccionar los modelos de fraude. Las herramientas y la tecnología para recopilar esta información están disponibles en la actualidad, pero a menudo se encuentran en sistemas aislados y dispares; las empresas pueden tener herramientas separadas para la verificación de identidad y la biometría, por ejemplo. En el futuro, predecimos que las empresas podrán aprovechar una mejor tecnología e integraciones para consolidar esta información en un solo lugar, brindando un enfoque holístico para hacer que los modelos de fraude sean más eficientes.

Al observar los datos relevantes de todo el recorrido del cliente, incluidos datos de comportamiento, biométricos y de terceros enriquecidos relacionados con números de teléfono, direcciones de correo electrónico, el depósito sin explotar de datos del emisor e incluso plataformas de redes sociales, las empresas pueden alcanzar nuevos niveles de precisión de detección de fraude.

Si bien este nivel de datos es muy útil para mejorar los modelos de fraude, las empresas deben tener cuidado al recopilar y almacenar esta información para garantizar el cumplimiento de las leyes globales de privacidad y seguridad de datos.

3. Los emisores y las empresas colaborarán más para agilizar las disputas y reducir los falsos rechazos

Cuando un cliente completa una compra en su sitio, su proveedor de pagos toma los detalles del pago y los envía a través de las redes de tarjetas, como Visa o Mastercard, al banco emisor (el banco del cliente) como una solicitud de pago. Los bancos emisores son quienes toman las decisiones finales al aprobar o rechazar una transacción durante la **fase de autorización**. Calculan el riesgo de fraude en función de las señales que reciben durante la autorización, que son bastante limitadas.

Las empresas, por otro lado, tienen una gran cantidad de datos de clientes y transacciones, como el correo electrónico y las direcciones de facturación de un cliente. La combinación de estos datos con la información que ya tiene el emisor puede llevar a que se acepte un mayor porcentaje de transacciones.

Las tasas mejoradas de autorización y fraude son mutuamente beneficiosas: el banco emisor puede reducir las pérdidas por fraude, ahorrar en costos operativos y aumentar el volumen de transacciones al reducir la cantidad de consultas de clientes sobre falsos rechazos. Al mismo tiempo, las empresas disfrutan de mayores tasas de conversión de pagos y una mejor retención de clientes. Sin embargo, la mayoría de las empresas aún no comparten estos datos con los emisores, lo que genera una asimetría de información que contribuye a los **USD 443.000 millones** de falsos bloqueos en 2021.

Ahora vemos un cambio, ya que los emisores invierten en la creación de API de autorización mejoradas, como la **API de datos de toma de decisiones mejorados** de Capital One y la **API de autorización mejorada de Amex**. Las grandes empresas, para las que cada aumento de punto porcentual en la autorización se manifiesta en millones de dólares, también comprenden la importancia del intercambio de datos y están comenzando a invertir en la integración con los emisores. Sin embargo, existe una brecha para los millones de otras empresas que no tienen la capacidad técnica o un volumen de pagos significativo para justificar el ROI de las integraciones con emisores. Para estas empresas, esperamos que socios financieros como Stripe y otros proveedores de pagos ayuden a facilitar este intercambio aprovechando su tamaño y sus asociaciones con emisores ya integrados.

4. Las preferencias de pago de los consumidores seguirán cambiando, modificando el panorama del fraude

Los métodos de pago como **Compre ahora, pague después**, las billeteras digitales y métodos locales de pagos como transferencias bancarias y OXXO están en aumento. Los servicios Compre ahora, pague después han aumentado particularmente en adopción: **más de la mitad de los clientes de EE. UU**. han utilizado un servicio Compre ahora, pague después, y fue el método de pago de más rápido crecimiento en 2020 en **India** y **el Reino Unido**.

Todos los métodos de pago utilizados para las transacciones en línea presentan cierto nivel de riesgo de fraude, y los métodos sin tarjeta no son diferentes. Por ejemplo, los métodos de pago como Compre ahora, pague después conllevan un menor riesgo de fraude de transacciones, pero pueden ser más susceptibles al fraude de cuentas nuevas (donde los estafadores crean nuevas identidades para abrir cuentas fraudulentas durante el flujo de onboarding, que pueden estar mal protegidos) y adquisiciones de cuentas (en las que un tercero malintencionado obtiene acceso a las credenciales de la cuenta de un cliente y utiliza su información de pago para realizar compras fraudulentas).

Sin embargo, las empresas pueden mitigar estos riesgos centrándose en estrategias de prevención de fraude en una etapa más temprana del ciclo de vida del cliente. En lugar de centrarse en la transacción en sí, las empresas pueden detectar actividades fraudulentas antes en el recorrido del cliente para realizar una evaluación antes de que el cliente (o el estafador) incluso realice una compra. Por ejemplo, las empresas deben confirmar la identidad de un cliente durante la incorporación, verificar si hay cuentas duplicadas y aplicar medidas de verificación de identidad (como la autenticación de dos factores) al iniciar sesión.

Cómo puede ayudar Stripe

Stripe es un conjunto totalmente integrado de productos que impulsa los pagos para minoristas en línea y en persona, empresas de suscripciones, plataformas de software y mercados, y mucho más. Desde combatir el fraude hasta verificar identidades, millones de empresas usan Stripe para:

Optimizar la experiencia de pago

- **Recopilar información más relevante durante el pago:** Pedirles a los clientes que proporcionen información más relevante al finalizar la compra lo ayudará a verificar mejor su legitimidad. Por ejemplo, asegúrese de conseguir el nombre y la dirección de correo electrónico del cliente. Esta información adicional se puede pasar a Stripe Radar, lo que resulta en una mejor detección de fraude mediante aprendizaje automático y le brinda más evidencia para enviar durante una posible disputa.
- **Explorar otros métodos de pago:** El conjunto correcto de métodos de pago puede ofrecer flexibilidad a los clientes y reducir el riesgo de fraude. Las billeteras digitales, como Apple Pay o Google Pay, requieren una verificación adicional del cliente (como datos biométricos, SMS o un código de acceso) para completar un pago, lo que da como resultado tasas de disputa más bajas. Asimismo, la mayoría de los débitos bancarios, donde extrae fondos directamente de la cuenta bancaria de un cliente, requieren que los clientes acepten un mandato o verifiquen la propiedad de la cuenta, lo que agrega una barrera adicional de seguridad y reduce la posibilidad de disputas.

Prevenga el fraude durante el pago

- **Aproveche la detección de fraudes mediante el aprendizaje automático:** La detección de fraudes basada en reglas, que opera con una lógica de "si sucede x, entonces haga y", nunca se diseñó para las empresas modernas de Internet y puede provocar la pérdida de ingresos. Stripe Radar funciona con aprendizaje automático adaptativo, con algoritmos que evalúan cada transacción y asignan una puntuación de riesgo, y luego bloquean o permiten transacciones en función del riesgo de fraude. Los algoritmos de Radar se adaptan rápidamente a los patrones de fraude cambiantes y a su negocio único.
- **Prevenir el fraude y aumentar la autorización a través de asociaciones con emisores:** La asociacion de Stripe con diferentes bancos emisores proporciona el intercambio de datos de riesgo, cuando es posible, para ayudar a los emisores a bloquear transacciones fraudulentas mientras aprueban las legítimas. La integración con los emisores crea valor tanto para el titular de la tarjeta como para la empresa: Los clientes pueden comprar más con mayor confianza, mientras que las empresas obtienen una mayor cantidad de transacciones aprobadas sin un aumento de las disputas fraudulentas.
- **Aplicar dinámicamente la autenticación de dos factores:** Stripe Checkout puede manejar los requisitos SCA europeos y aplicar autenticación dinámicamente, como 3DS, cuando lo requiera el banco del titular de la tarjeta o cuando se sospeche de fraude. Stripe Checkout también es compatible con el método más simple de validación de PCI con un SAQ A precargado, y activa CAPTCHA solo cuando sospechamos ataques de prueba de tarjetas, para evitar fraudes.

Gestionar el fraude con su equipo

- **Crear reglas para personalizar el fraude:** Con Radar for Fraud Teams, puede crear reglas personalizadas para administrar cómo su empresa maneja los pagos entrantes, bloqueando los que considere sospechosos o colocándolos en revisión. Por ejemplo, podría reducir la puntuación de riesgo requerida para activar revisiones manuales o revisar pedidos grandes de clientes nuevos. Radar for Fraud Teams también proporciona perspectivas de riesgo sobre pagos particulares, lo que le permite comprender los factores más importantes que contribuyen a una puntuación de riesgo alta. Puede utilizar esta información para crear reglas adicionales más específicas.
- **Revisar manualmente los pagos de alto riesgo:** Radar for Fraud Teams incluye un proceso adicional de revisión que le permite marcar ciertos pagos para su revisión (aunque estos pagos aún se procesan y se cobran a la tarjeta de crédito). Si bien Radar for Fraud Teams es comúnmente utilizado por organizaciones más grandes, la capacidad de revisar pagos manualmente es útil, independientemente del tamaño de su empresa (aunque las empresas más pequeñas han encontrado que las revisiones manuales son especialmente útiles). Revisar manualmente los pagos sospechosos puede ayudarlo a tomar medidas con mayor precisión, antes de que ocurra una posible disputa. Por ejemplo, si no está seguro acerca de un pago cuando lo está revisando, puede comunicarse con el cliente por teléfono o correo electrónico. O, si sospecha que un pago es fraudulento, puede reembolsarlo.

Consejos adicionales para la prevención del fraude

- **Acceder a información más detallada sobre las tendencias de fraude:** Stripe Sigma le permite analizar rápidamente sus datos de Stripe a través de consultas SQL predefinidas o personalizadas en el panel de control de Stripe. Responda sus preguntas comerciales complejas, desde comprender por qué los clientes disputan los pagos hasta qué porcentaje de disputas usted impugna. También puede usar Stripe Data Pipeline para enviar datos de Stripe actualizados a su almacén de datos de Snowflake o Amazon Redshift. Esto le permite combinar fácilmente sus puntajes de riesgo de fraude de Stripe con otros datos de fraude para obtener informes de fraude más completos.
- **Optimizar la conversión y recuperar más ingresos:** Stripe Card Image Verification ayuda a reducir la cantidad de transacciones bloqueadas por error. En lugar de bloquear transacciones potencialmente de alto riesgo, les brinda a los usuarios la oportunidad de confirmar que tienen la tarjeta que dicen tener al pedirles que escaneen una imagen de su tarjeta (lanzamiento en 2022).

Para obtener más información sobre cómo Stripe Radar puede ayudar a su empresa a combatir el fraude, lea nuestros documentos o regístrese para obtener una cuenta.

Recursos adicionales

Aquí hay recursos adicionales para ayudarlo a administrar el fraude y proteger su empresa:

- Introducción a los pagos en línea
- Mejores prácticas para prevenir el fraude
- Introducción al aprendizaje automático para la detección de fraudes
- Radar for fraud teams: Aspectos básicos de las reglas
- Acerca de Stripe Radar
- Acerca de Radar for Fraud Teams

Metodología

Stripe analizó miles de millones de intentos de pago de millones de empresas entre 2019 y 2021. En esos pagos y empresas, analizamos las disputas y sus motivos, las predicciones de nuestros modelos de aprendizaje automático, el uso de 3DS y la actividad de revisión manual de las empresas. Para las tasas de fraude a nivel de país, excluimos de nuestro análisis los países con menos de 10.000 pagos en 2021 porque tenían muy pocas transacciones para calcular las tasas de fraude de manera confiable.

A principios del 2022, Stripe también trabajó con Milltown Partners (en asociación con su proveedor de datos, focaldata) para encuestar a más de 2.500 líderes empresariales en 9 mercados de todo el mundo (Australia, Canadá, Francia, Alemania, Japón, los Países Bajos, Singapur, el Reino Unido y los Estados Unidos) que estiman que sus empresas obtienen al menos el 10% de sus ingresos de las ventas en línea.