TransUnion

TransUnion 2023 Informe Sobre el Estado del Fraude Omnicanal

Tendencias y estrategias para aumentar la confianza en el comercio

Introducción

El fraude volvió en 2022 a niveles similares a los que observamos antes de la pandemia, sin embargo, debido al aumento de las transacciones digitales, los riesgos a los que se someten tanto empresas como individuos son ahora mayores que nunca.

Los cibercriminales y los defraudadores siguen evolucionando y muestran mayor sofisticación en las operaciones que llevan a cabo, ahora con el robo de información sobre identidades como máxima prioridad en sus estrategias. Los consumidores, por su parte, son conscientes del riesgo de utilizar canales online y juzgan, por ello, cómo protegen sus datos las empresas con las que interactúan.

En este escenario, las organizaciones que liderarán el mercado serán aquellas que pongan en marcha estrategias de prevención de fraude más inteligentes y que apuesten por la confianza de sus clientes, demostrando que las transacciones que se realizan a través de cualquier canal son seguras.

El Informe sobre el Estado del Fraude Omnicanal 2023 de TransUnion muestra las tendencias que hemos observado, así como la experiencia que tiene la compañía para optimizar la prevención del fraude en la industria. Incluye análisis y recomendaciones para los responsables de la prevención del fraude y muestra experiencias online para mejorar los resultados de negocio.

Con este informe, podrá evaluar los programas de prevención de fraude actuales en el contexto del mercado. Es importante que comparta la información de este documento si quiere mejorar la satisfacción de sus clientes, reducir el fraude y mejorar el rendimiento del negocio.

Todos los datos de este informe proceden de la red de inteligencia global de TransUnion, así como de un estudio realizado para TransUnion en 18 países y regiones de todo el mundo.

CONCLUSIONES MÁS DESTACADAS

El crecimiento digital aumenta la exposición a riesgos

El **4,6%**
de las transacciones digitales fueron fraudes potenciales en 2022

El **80%**
de las transacciones digitales realizadas entre 2019 y 2022 fueron sospechosas de fraude

Los datos se están convirtiendo en armas

83%
Las brechas de datos crecieron en EE.UU. un 83% entre 2020 y 2022

4.600 millones
Se estima en 4.600 millones de dólares el saldo correspondiente a posibles identidades sintéticas* en EE.UU. para la solicitud de créditos para la compra de vehículos, en tarjetas de crédito, en tarjetas de compras o en créditos personales no garantizados en 2022. Se trata del nivel más alto de la historia, con un crecimiento del 27% desde 2020

*Identidades dintéticas: Perfil construido por los cibercriminales con información real y falsa

Los defraudadores se aprovechan de cualquier canal

El **62%**
de las llamadas de alto riesgo a centros de atención al usuario en 2022 en EE.UU. procedían de líneas VoIP no fijas

El **52%**
de los consumidores afirma haber sido objetivo de un intento de fraude, ya sea online, a través del correo electrónico, de llamadas de teléfono o de mensajes de texto, entre septiembre y diciembre de 2022

TransUnion

Índice

Tendencias globales sobre fraude digital

El crecimiento en el volumen de transacciones digitales incrementa el riesgo de fraude

Según TransUnion, el 4,6% de las transacciones digitales de sus clientes analizadas fueron intentos sospechosos de fraude en 2022. Esta cifra supone volver a los niveles de fraude previos a la pandemia: aunque el número de transacciones digitales realizadas globalmente creció un 80% entre 2019 y 2022, los intentos sospechosos de fraude digital crecieron también un 80% en muchos de los países analizados.

Por ejemplo, las transacciones originadas en EE.UU. crecieron un 89% y los intentos sospechosos de fraude digital en ese país crecieron un 122%. Esto representa un importante incremento en la exposición al fraude que sufren empresas e individuos. Los patrones de fraude más utilizados fueron los relacionados con la identidad y con el fraude financiero: el fraude cometido con identidades sintéticas fue el que experimentó un mayor aumento (un 76% más) entre los cinco tipos de fraude digital que analiza TransUnion desde 2019.

El número de transacciones digitales realizadas globalmente creció en un 80% entre 2019 y 2022

Las industrias afectadas buscan el compromiso digital de sus clientes

Con la pandemia aprendimos que los delincuentes y los defraudadores centran sus esfuerzos en empresas e instituciones que tienen acceso directo a dinero o a productos y servicios que se pueden transformar de forma muy sencilla en valor dinerario.

Los programas de recuperación de muchos gobiernos sufrieron importantes fraudes, de la misma manera que las industrias más relacionadas con el consumo digital. Los delincuentes incrementaron los intentos de fraude digital especialmente en empresas relacionadas con los viajes, la logística y los servicios financieros, con un aumento del impacto del 117%, del 63% y del 39%, respectivamente. Estas industrias también se vieron favorecidas por un incremento en el volumen de transacciones debido a los cambios de comportamiento de los consumidores durante la pandemia.

Cómo mide el fraude digital TransUnion
La tasa o el porcentaje de intentos de fraude digital reflejan tanto las transacciones que los clientes de TransUnion denegaron en tiempo real debido a indicadores de fraude como los intentos que se consideraron fraudulentos después de una revisión, comparados con el total de transacciones analizadas.

Intentos de fraude digital global por industrias en 2022

- **Tasa de intentos sospechosos de fraude en 2022**
- **Tipo de fraude más común en 2022**
- **Variación de la tasa en los intentos sospechosos de fraude entre 2019 y 2022**

Juego
(apuestas online, poker, etc.)

2022
7,5%
Abuso de promociones

2019-2022
-21%

Retail

2022
7,2%
Abuso de promociones

2019-2022
7%

Videojuegos

2022
5,4%
Gold farming

2019-2022
-82%

Servicios financieros

2022
4,2%
Fraude de identidad legítima

2019-2022
39%

Comunidades en línea
(aplicaciones de citas, foros, etc.)

2022
4%
Perfiles falsos

2019-2022
-8%

Viajes y ocio

2022
2,1%
Fraude en tarjeta de crédito

2019-2022
117%

Telecomunicaciones

2022
2,1%
Fraude en tarjeta de crédito

2019-2022
-51%

Seguros

2022
1,7%
Fraude con terceros

2019-2022
22%

Logística

2022
1,3%
Fraude en envíos

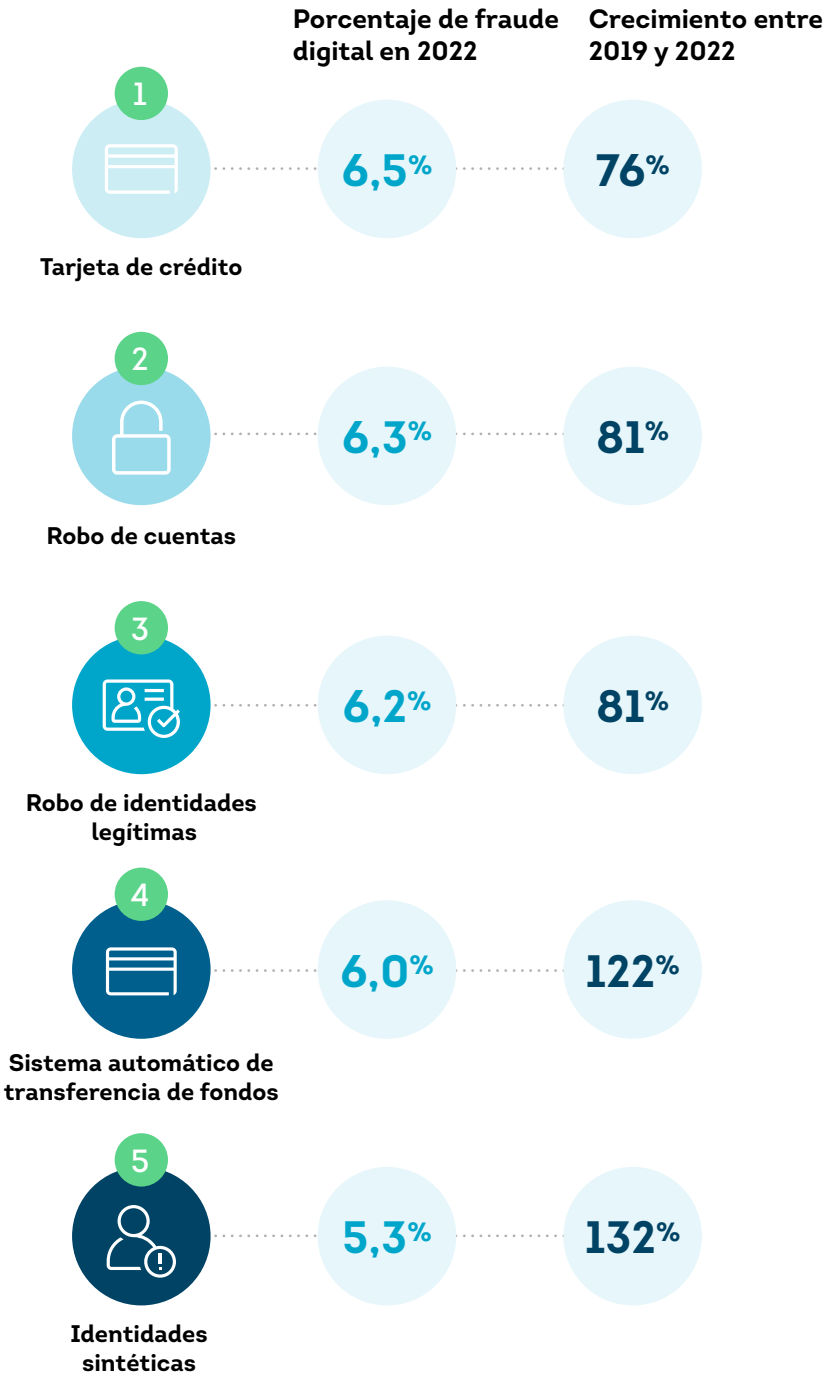
2019-2022
63%

Fuente: TruValidate de TransUnion

El fraude basado en identidad incrementa el riesgo de empresas y consumidores

El incremento en la sofisticación de las actividades que llevan a cabo los defraudadores se hace más evidente aún en ciertos tipos de patrones de fraude. El robo de identidades o las estafas a partir de identidades (ya sea phishing, vishing o smishing, con los que pretenden acumular información sobre la identidad) conllevan un aumento, lo que implica también el robo de cuentas, el fraude en pagos o la creación de nuevas cuentas falsas con identidades sintéticas.

Tipos más importantes de fraude y crecimiento



Fuente: TruValidate de TransUnion

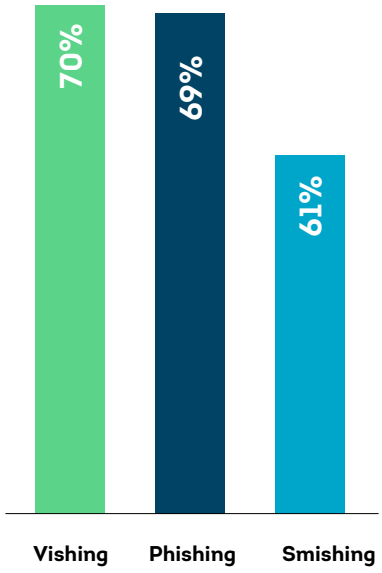
Los consumidores son conscientes de que sus identidades están en riesgo

Como ya hemos comentado, el número de transacciones analizadas por TransUnion casi se ha doblado en los últimos cuatro años. Con una dependencia cada vez mayor sobre los canales digitales, los consumidores son conscientes de los peligros a los que se enfrentan especialmente en lo que se refiere a robo de identidades y fraude digital. Aunque las preocupaciones son diferentes según la región o el país, la inquietud relacionada con la protección de la identidad es universal.

Principales preocupaciones relacionadas con el fraude

Porcentaje de consumidores que admite tener miedo a ser víctima del tipo de fraude mencionado

COLOMBIA



BRASIL

Vishing: **69%**
Robo de identidad: **57%**
Phishing: **51%**

CANADÁ

Robo de identidad: **57%**
Robo de la tarjeta de crédito: **56%**
Phishing: **46%**

CHILE

Vishing: **72%**
Phishing: **64%**
Robo de identidad: **58%**

ESPAÑA

Vishing: **62%**
Phishing: **56%**
Robo de identidad: **49%**

EEUU

Robo de identidad: **51%**
Robo de tarjetas de crédito: **48%**
Phishing: **38%**

FILIPINAS

Vishing: **67%**
Robo de identidad: **63%**
Estafas con terceros: **58%**

HONG KONG

Vishing: **58%**
Phishing: **53%**
Robo de identidad: **49%**

INDIA

Phishing: **38%**
Estafas con terceros: **36%**
Robo de identidad: **35%**

KENIA

Phishing: **59%**
Robo de cuentas: **58%**
Robo de identidad: **58%**

MÉXICO

Vishing: **68%**
Phishing: **59%**
Robo de identidad: **49%**

NAMIBIA

Robo de cuentas: **69%**
Robo de identidad: **65%**
Robo de tarjetas de crédito: **64%**

PUERTO RICO

Phishing: **69%**
Robo de identidad: **67%**
Vishing: **67%**

REINO UNIDO

Robo de identidad: **52%**
Robo de tarjetas de crédito: **45%**
Robo de cuentas: **41%**

REPÚBLICA DOMINICANA

Vishing: **76%**
Phishing: **73%**
Robo de la tarjeta de crédito: **57%**

RUANDA

Estafas con terceros: **42%**
Robo de cuentas: **38%**
Robo de tarjetas de crédito: **37%**

SUDÁFRICA

Robo de identidad: **62%**
Robo de tarjetas de crédito: **57%**
Robo de cuentas: **55%**

ZAMBIA

Robo de cuentas: **67%**
Robo de identidad: **64%**
Estafas con terceros: **63%**

Fuente: Estudio sobre fraude al consumidor de TransUnion

Tendencias en las brechas de datos

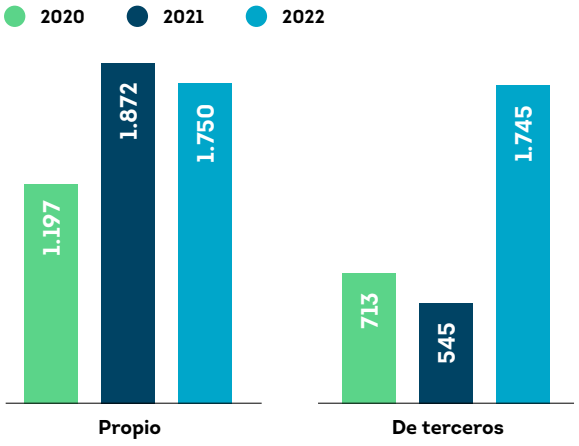
Las brechas de datos en EE.UU. crecen en volumen y gravedad, indicadores de fraudes futuros

Según los datos analizados por Sontiq, una compañía TransUnion, el número de brechas de datos sufridas en EE.UU. entre 2020 y 2022 creció un 83% (1.910 en 2020; 2.417 en 2021; y 3.495 en 2022). Además, entre 2020 y 2022, la gravedad de dichas brechas, según el Score de Riesgos relacionados con Brechas de Sontiq, se incrementó un 6%.

Aumento de brechas en terceros

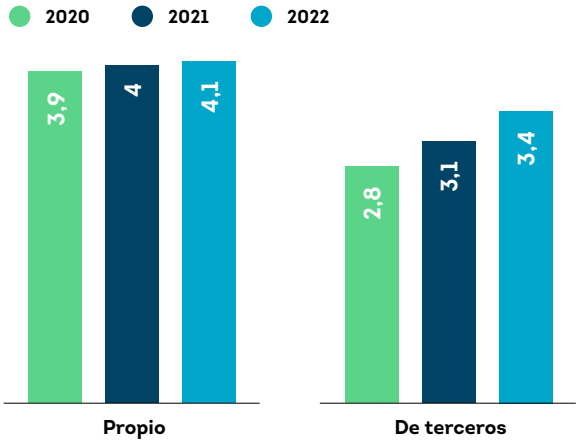
Sontiq también confirma que el número de brechas relacionadas con terceros aumentó un 145% entre 2020 y 2022. Un ataque a terceros, también conocido como ataque a la cadena de valor, ataque a la cadena de suministro o brecha de puerta trasera, consiste en que un atacante accede a la red a través de un proveedor que tiene acceso legítimo. El Score de Sontiq sobre brechas en terceros también creció un 23%, frente al 4% de aumento en brechas propias. En el futuro, las empresas sufrirán probablemente ataques relacionados con fraude más numerosos y más sofisticados y esto provocará que los consumidores tengan más preocupaciones sobre su bienestar financiero.

Volumen de brechas de datos en EE.UU. Propias y de terceros en el período 2020–2022



Fuente: Sontiq, una compañía TransUnion

Promedio de la puntuación de riesgo de brechas de datos en EE.UU.



Fuente: Sontiq, una compañía TransUnion

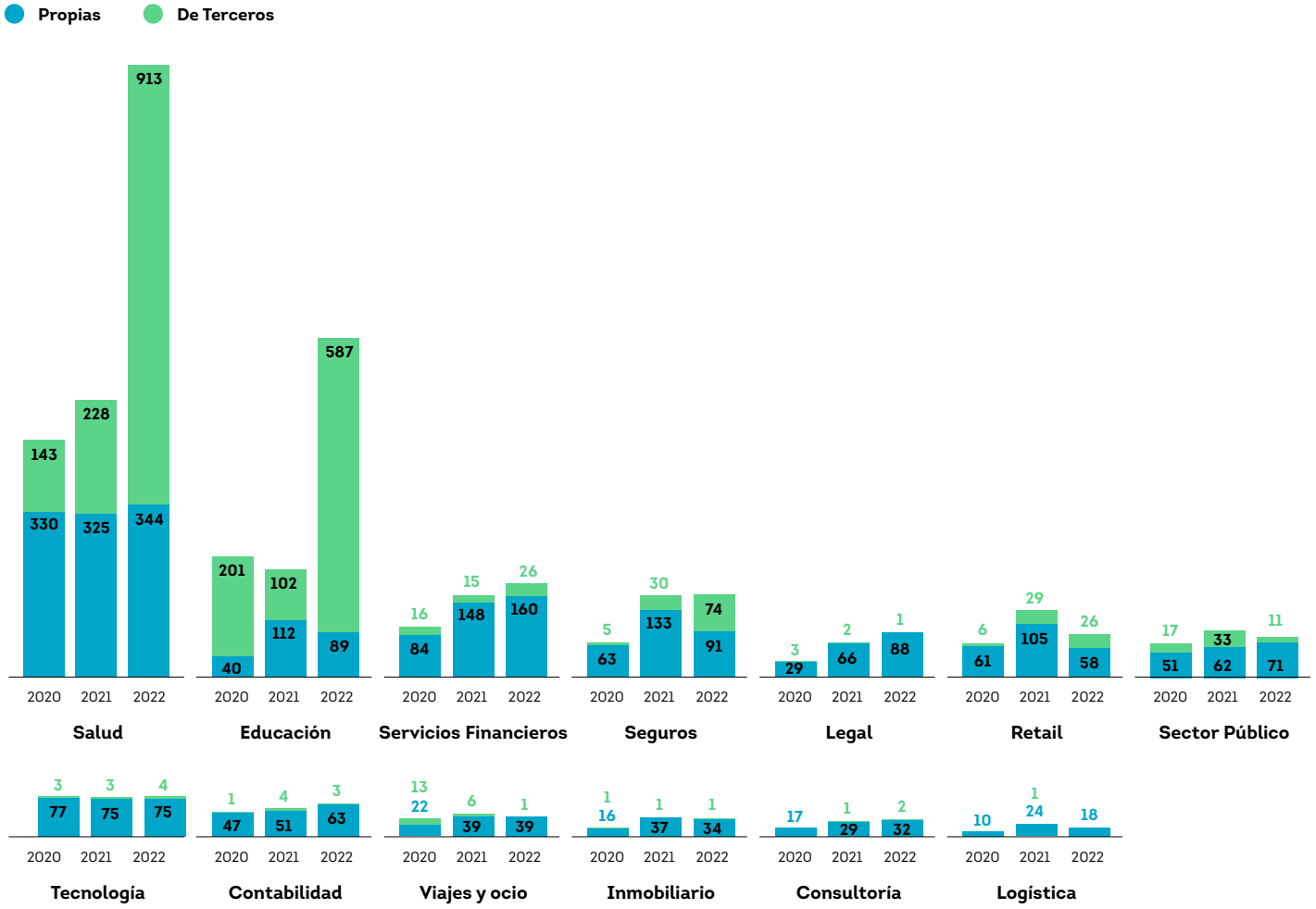
El Score de Riesgos relacionados con Brechas de Sontig se basa en la cantidad y gravedad de las credenciales particulares que una entidad afectada por una brecha considera que han sido perjudicadas. El algoritmo de Inteligencia Artificial de Sontiq, que cuenta con 1.300 elementos de análisis, observa 60 atributos relacionados con las credenciales para ofrecer un score de riesgos y un patrón, así como una recomendación de acciones para el consumidor. El Score utiliza una escala de 1 a 10 en la que el 1 supone la menor gravedad y el 10, la mayor. Se puede acceder a la herramienta para comprobar el Score de alguna brecha concreta, así como las recomendaciones de Sontiq para los usuarios afectados, en **sontiq.com/breachiq/#search-breached-organizations**.

Las brechas de datos sobre ingenieria de identidades impactan a todas las industrias

Como vemos, las brechas de datos están creciendo en volumen y gravedad, por lo que es esencial diferenciar los riesgos que ciertos tipos de brechas suponen para las estrategias de prevención de fraude. Los delincuentes pueden acceder a mucha información sobre identidades disponible en la dark web, aunque algunos de los datos más valiosos, como documentos de identidad o números de las cuentas bancarias, no se suelen encontrar ahí. Los criminales atacan a ciertas industrias, que son las que más sufren las brechas de datos, para conseguir datos con los que crear identidades sintéticas o para desarrollar ataques de ingeniería social más sofisticados. Por ejemplo, cuando consiguen ciertos datos personales, los ciberdelincuentes pueden acceder a cuentas de servicios financieros, ya sean bancos o emisores de tarjetas, para realizar compras en otros sitios.

La industria relacionada con la salud es la que más brechas sufre normalmente: más de 1.250 en 2022 y más de 2.300 en los últimos tres años, lo que supone el 36% y el 29%, respectivamente, del total de brechas de datos en el conjunto de la economía estadounidense. Otros sectores afectados suelen ser el legal o el de la logística, con un Score de 4,7, seguidos de las asesorías de contabilidad (Score de 4,6), inmobiliarias (Score de 4,6) y servicios financieros (Score de 4,4). En muchas ocasiones, se trata de empresas pequeñas o medianas que no cuentan con las infraestructuras o los procedimientos necesarios para proteger sus redes.

Volumen de brechas de datos por industrias en EE.UU., propias y de terceros



Fuente: Sontiq, una compañía TransUnion

Fraudes globales al consumo y sentimiento sobre la experiencia de usuario

Las experiencias que muestran una protección a la identidad, claves en las estrategias ganadoras

El 36% de los consumidores encuestados por TransUnion en todo el mundo afirma que realiza más de la mitad de sus transacciones online. Es decir: los riesgos de hacer negocios online están bastante claros. Más de la mitad de los ciudadanos que participaron en el estudio admite haber sido objetivo de un fraude entre septiembre y diciembre de 2022.

Por ello, los compradores suelen valorar más a las organizaciones que protegen sus cuentas online y sus identidades. Esto significa que aquellos que no sean capaces de proteger los datos de sus clientes de forma correcta perderán negocio: más de la mitad de los encuestados (59%) asegura que estarían dispuestos a cambiar de empresa para conseguir una experiencia digital mejor.

El miedo por la seguridad y a ser víctima de un fraude inhiben el comercio

El **63%**
de los compradores no volvería a una web si cree que puede ser víctima de un fraude

El **55%**
admite haberse echado atrás a la hora de abrir una cuenta desde el móvil debido al miedo por la seguridad. En el caso de los dispositivos de sobremesa, la cifra se reduce al 48%

El **48%**
de los compradores abandonó su carrito debido a las preocupaciones relacionadas con la seguridad

Fuente: Estudio sobre fraude al consumidor de TransUnion

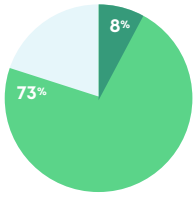
Los consumidores se enfrentan a ataques contra su identidad de forma regular

Más de la mitad (52%) de los compradores que formaron parte del estudio de TransUnion admite haber sido objetivo de un fraude entre septiembre y diciembre de 2022, ya sea a través del correo electrónico, actividades online, llamadas de teléfono o mensajes de texto. El 9% llegó a ser víctima del fraude. Las tasas de fraude son más altas en África, con un 81% de keniatas considerados objetivo de un fraude o un 14% de los sudafricanos llegando a ser víctimas del fraude. Las experiencias de fraude más comunes globalmente fueron estafas a partir de ingeniería social, como phishing, vishing o smishing.

Denuncias por fraude entre septiembre y diciembre de 2022 por país o región

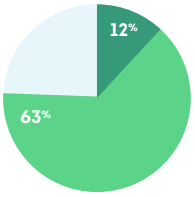
- Objetivo pero no víctima
- Objetivo y víctima
- Tipo de fraude más común
- No fue objetivo

KENIA



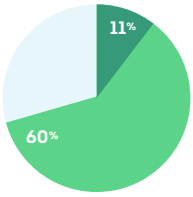
Vishing

ZAMBIA



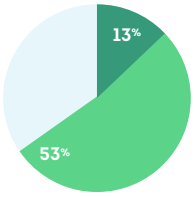
Smishing

FILIPINAS



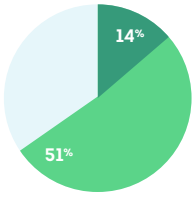
Phishing

NAMIBIA



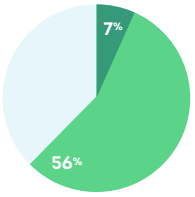
Phishing

SUDÁFRICA



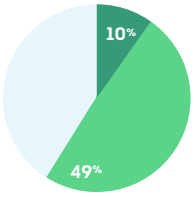
Smishing

RUANDA



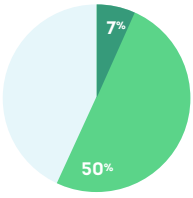
Estafas con terceros y mulas de dinero

INDIA



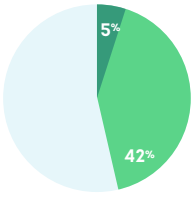
Phishing

CANADÁ



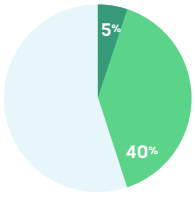
Phishing

REINO UNIDO



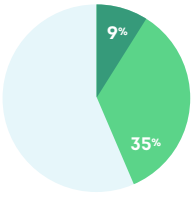
Phishing

HONG KONG



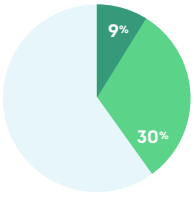
Phishing

PUERTO RICO



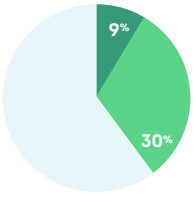
Vishing

BRASIL



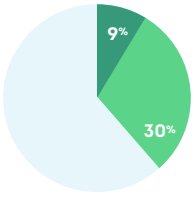
Robo de tarjeta

MÉXICO



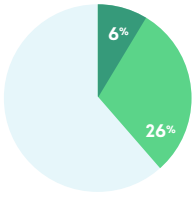
Robo de tarjeta

CHILE



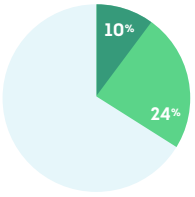
Vishing

ESPAÑA



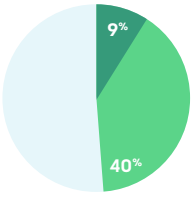
Phishing

REPÚBLICA DOMINICANA



Robo de tarjeta

ESTADOS UNIDOS



Phishing

Fuente: estudio sobre fraude al consumidor de TransUnion

TransUnion

Los consumidores eligen organizaciones que protegen sus datos personales

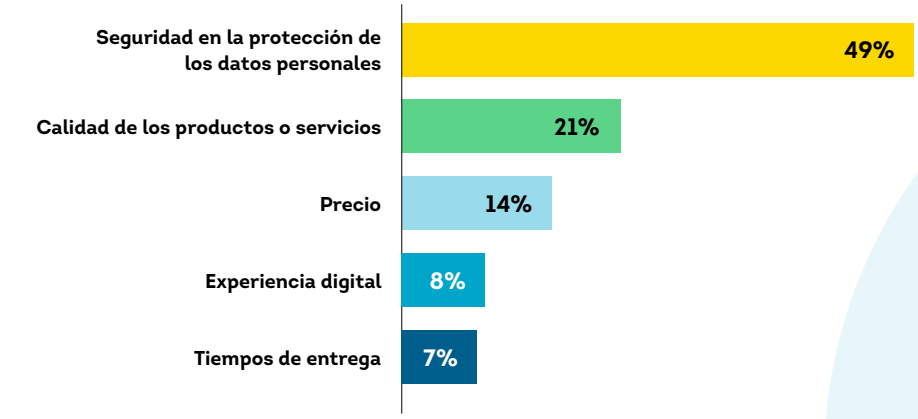
Teniendo en cuenta que los consumidores sufren fraude potencial demasiado a menudo, el valor que otorgan a las organizaciones que protegen correctamente los datos personales es muy alto. La mayoría de los encuestados en el estudio de TransUnion (78%) admite que prefieren elegir empresas que protegen la información. Además, el 49% colocó la seguridad de los datos personales como la cualidad primordial que esperan de una empresa con la que realizan transacciones online. Esto es más del doble de la segunda cualidad esperada: buenos productos o servicios (21%); y el triple de la tercera: el precio (14%).

¿Cuáles son las cualidades más importantes a la hora de elegir una empresa con la que realizará transacciones online?

Muy importante

Expectativas o cualidades que se buscan en compañías online

Mejores respuestas



Fuente: estudio sobre fraude al consumidor de TransUnion

Implicación de los responsables de prevención de fraudes

Reducir la fricción para mejorar las tasas de conversión

La respuesta instintiva al incremento de las brechas de datos y al persistente fraude digital podría ser incrementar la verificación de la identidad o realizar comprobaciones de autenticación. Sin embargo, en la transición hacia un mundo "siempre conectado" con experiencias digitales casi permanentes, los responsables de la prevención del fraude deben anteponer en muchas ocasiones una experiencia de usuario óptima sin perder de vista los riesgos.

Unos buenos resultados en el negocio se consiguen mediante la conversión de ventas: que los clientes potenciales se conviertan en reales y que los clientes existentes incrementen las transacciones que realizan. Esto supone reducir la fricción tanto para los clientes potenciales como para los actuales. Si no pensamos en la conversión, reducir la fricción para los clientes mejora la confianza y la conveniencia: se darán cuenta de que pueden confiar en la empresa con la que realizan las transacciones porque protegen sus datos, pero a la vez, ofrecen la experiencia digital que están esperando.

Pero, lamentablemente, muchos clientes no otorgan su confianza tan fácilmente. Más de la mitad de los consumidores preguntados por TransUnion (53%) admite haber abandonado una solicitud online o un formulario para solicitar información sobre un producto financiero; y el 42% dice que abandonó el proceso porque temía por la seguridad de sus datos personales. Además, el 48% afirma que ha abandonado su carrito de compra debido a miedos relacionados con la seguridad. Para mejorar las tasas de conversión y reducir la fricción en las transacciones, los responsables de prevención de fraude deberían considerar dos estrategias:

Estrategia para incrementar las tasas de conversión:

- Conseguir que los clientes nuevos confíen en la organización

Estrategia para reducir la fricción:

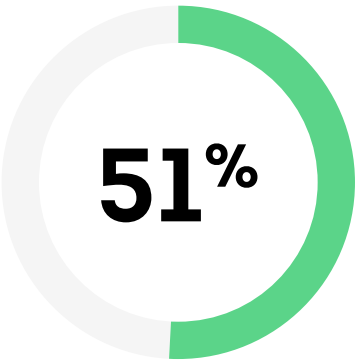
- Alinear las técnicas de autenticación con las preferencias de los clientes

El **53%**

admite haber abandonado una solicitud online o un formulario para solicitar información sobre un producto financiero

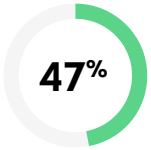
Razones principales por las que un consumidor abandona una solicitud online o un formulario para solicitar información sobre un producto financiero

COLOMBIA



Falta de confianza sobre la protección de los datos personales

BRASIL

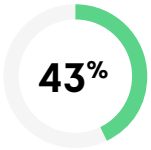


Falta de confianza sobre la protección de los datos personales

CANADÁ

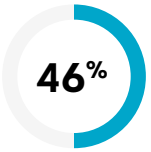
Se solicitaba demasiada información

CHILE



Falta de confianza sobre la protección de los datos personales

ESPAÑA

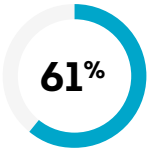


Se solicitaba demasiada información

EEUU

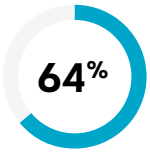
Se solicitaba demasiada información

FILIPINAS



Se solicitaba demasiada información

HONG KONG

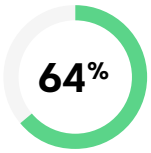


Se solicitaba demasiada información

INDIA

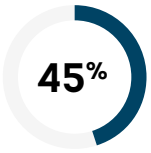
Se solicitaba demasiada información

KENYA



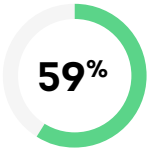
Falta de confianza sobre la protección de los datos personales

MÉXICO



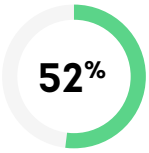
El sitio era demasiado lento

NAMIBIA



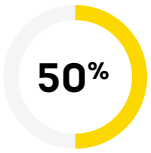
Falta de confianza sobre la protección de los datos personales

PUERTO RICO



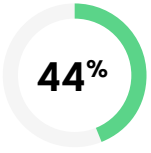
Falta de confianza sobre la protección de los datos personales

REINO UNIDO



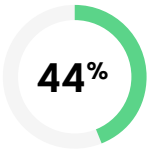
El proceso resultó frustrante

REPÚBLICA DOMINICANA



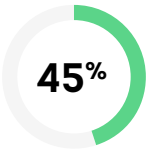
Falta de confianza sobre la protección de los datos personales

RUANDA



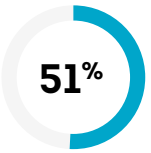
Falta de confianza sobre la protección de los datos personales

SUDÁFRICA



Falta de confianza sobre la protección de los datos personales

ZAMBIA



Se solicitaba demasiada información

Fuente: estudio sobre fraude al consumidor de TransUnion

TransUnion

Estrategia para incrementar las tasas de conversión: Conseguir que los clientes nuevos confíen en la organización

Es fácil imaginar que un cliente puede abandonar una web si observa que no se utiliza tecnología de cifrado (se puede comprobar fácilmente con el candado que aparece en la línea de navegación), sobre todo cuando se está ofreciendo información personal. En realidad, para un negocio profesional y legítimo, ofrecer ese nivel de seguridad es muy básico.

Los procesos de verificación de identidad con los que se protege a los clientes y a la empresa pueden matizarse más, pero siguen siendo fundamentales si se busca la confianza del consumidor. La verificación de la identidad es clave, tal y como lo demuestra el hecho de que existen consumidores en todo el mundo que admiten la voluntad de modificar sus identidades digitales cuando solicitan un crédito o crean una nueva cuenta. Esto podría ser tan simple como usar una dirección de correo recién creada, informar de un domicilio antiguo o cambiar ligeramente la filiación.

Formas más comunes con las que un consumidor altera su identidad a la hora de contratar un servicio

El **31%** abrió una cuenta de correo nueva

El **22%** utiliza un número de teléfono nuevo

El **19%** modifica expresamente su nombre

El **18%** utiliza un domicilio diferente al real

Fuente: estudio sobre fraude al consumidor de TransUnion

Si unimos estos comportamientos a las identidades sintéticas creadas por los defraudadores, las empresas pueden verse sobrepasadas a la hora de verificar la legitimidad de un individuo, por lo que necesitan de capas adicionales con las que verificar la identidad. Para superar estos desafíos, los equipos de prevención de fraude deben utilizar un validador de identidades con datos y capacidades de resolución muy robustos.

Combinando atributos digitales procedentes de múltiples dispositivos o cuentas de un mismo usuario la organización puede saber con quién está tratando y mejorar la experiencia del usuario en las transacciones que lleve a cabo.

Próximos pasos

Para mejorar la confianza de las identidades con el objetivo de reducir la necesidad de verificaciones adicionales, los responsables de prevención de riesgos deben utilizar grafos de identidad. Es necesario utilizar una solución que ofrezca acceso a atributos robustos, tales como filiación, domicilio, dirección de correo electrónico o número de teléfono. Los datos de la identidad se pueden combinar con inteligencia artificial y técnicas de Machine Learning para crear los grafos dinámicos que conecten de forma permanente y continua los atributos relacionados con la identidad. Aprovechar los grafos de identidad para verificar identidades puede ayudar enormemente a la conversión de nuevos clientes ya que se reducen los pasos de verificación en los momentos más críticos de la experiencia de usuario.

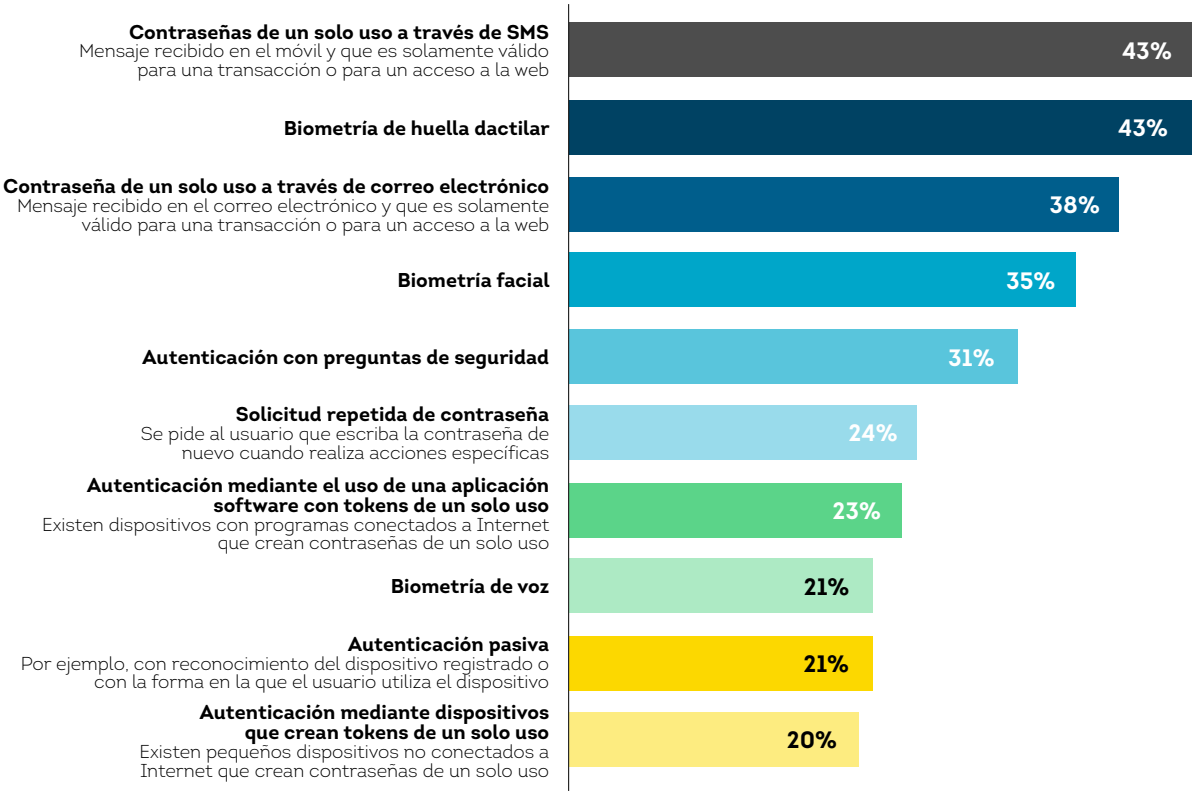
Estrategia para reducir la fricción: alinear las técnicas de autenticación con las preferencias de los clientes

Los consumidores esperan que sus cuentas estén protegidas. Y aunque entienden que para garantizar la seguridad es necesario autenticarse correctamente, lo que no quieren es encontrarse con un proceso con mucha fricción. De hecho, el 63% de los encuestados en el estudio de TransUnion confirmó que prefieren pasar por una autenticación explícita cuando acceden a servicios online. Y la mayoría (70%) admite que para ello prefieren que la autenticación ocurra en el inicio de la sesión. Por el contrario, el 64% no quiere pasar por procesos de reautenticación, por ejemplo a la hora de realizar un pago o cambiar la contraseña. Una clara mayoría (el 78%) afirma que prefiere la autenticación multifactor.

Los responsables de prevención de fraude deben escuchar a sus clientes para incorporar los procesos que aseguren la integridad de los procesos, al mismo tiempo, deben ser capaces de reducir la fricción aplicando técnicas adicionales de autenticación solamente a aquellas cuentas que presenten un comportamiento sospechoso.

Medidas de seguridad adicionales preferidas por los consumidores

Porcentaje de las tres respuestas mayoritarias



Fuente: estudio sobre fraude al consumidor de TransUnion

Próximos pasos

Los responsables de prevención de fraude deben centrar sus esfuerzos en la autenticación basada en riesgos (con un análisis continuo de la sesión del usuario) con el objetivo de poder preguntar al usuario en cualquier momento si se percibe un aumento del riesgo. Deben poner en marcha procesos de autenticación multifactor, tales como contraseñas OTP seguras de un solo uso (como SMS) o a través de aplicación push, o autenticación biométrica, ya sea mediante el uso de la huella dactilar o el reconocimiento facial. También pueden considerar el uso de procesos de autenticación a través de dispositivos en cuentas de mayor confianza.

El **63%**
de los consumidores admite que prefiere pasar por una autenticación explícita cuando acceden a servicios online

EXPERIENCIAS EN EL MUNDO REAL

Cómo los procesos de verificación mejorada de la identidad y de autenticación redujeron el abandono de las solicitudes

Una entidad emisora de tarjetas de crédito sufría un 63% de abandono en las solicitudes debido a los procesos excesivos de autenticación. Una vez que aplicó un nuevo proceso de autenticación y verificación de identidades más robusto consiguió:

50%
Una reducción en las solicitudes fraudulentas del 50%, lo que le permitió ahorrar aproximadamente 1,4 millones de euros al año

13%
Una reducción del 13% en las solicitudes abortadas, con lo que aumentó el número de solicitudes en 51.000, con un negocio potencial de más de 11,5 millones de euros

Mejorar la detección de fraude para reducir los falsos positivos

Para los responsables de prevención de fraude, los falsos positivos que paralizan las transacciones legítimas debido a procesos adicionales de autenticación son propuestas perdedoras. La autenticación adicional no solo molesta a los clientes legítimos hasta el punto de poder perderlos, sino que además, las revisiones manuales son costosas y exigen de una gran cantidad de recursos que se podrían utilizar para descubrir fraude real.

Lamentablemente para muchas empresas grandes, tales como las que ofrecen servicios financieros, comercios o incluso en el sector público, en las que se utilizan diversos canales, las operaciones pueden almacenarse en silos independientes en los que se generan sistemas de datos de clientes no conectados y muy diferentes. Es decir, cuando un cliente existente realiza una operación a través de un canal de compra diferente al habitual se puede producir un falso positivo simplemente porque no se le reconozca correctamente. Para mejorar la detección del fraude reduciendo a la vez los falsos positivos, los responsables de prevención de fraude deben considerar dos tipos de estrategia:

Estrategia para reducir los falsos positivos:

- Generar un enfoque multicanal para la prevención de riesgos

Estrategia para mejorar la detección de fraude:

- Optimizar la verificación de la identidad con el análisis del dispositivo

Los falsos positivos que paralizan las transacciones legítimas debido a procesos adicionales de autenticación son propuestas perdedoras

Estrategia para reducir los falsos positivos: generar un enfoque multicanal para la prevención de riesgos

A pesar de que muchas entidades animan a sus usuarios a gestionar por sí mismos la información de sus cuentas (cambios en las contraseñas, actualización de la dirección fiscal…), los consumidores utilizan el canal que más les conviene en cada momento. De hecho, el 60% de los encuestados en el estudio de TransUnion dijo que gestiona online menos de la mitad de su cuenta; y el 15% confirmó que no realiza ningún tipo de gestión de su cuenta. Es decir, los clientes utilizan el servicio de atención al cliente o incluso visitan físicamente la tienda para realizar ciertas transacciones. Esto significa que los responsables de prevención de riesgos necesitan trabajar con equipos en todos los canales de relación con clientes, incluido el servicio de atención
al cliente, para eliminar los silos de información y garantizar que los procesos de autenticación coherentes se llevan a cabo en todos los canales de comunicación.

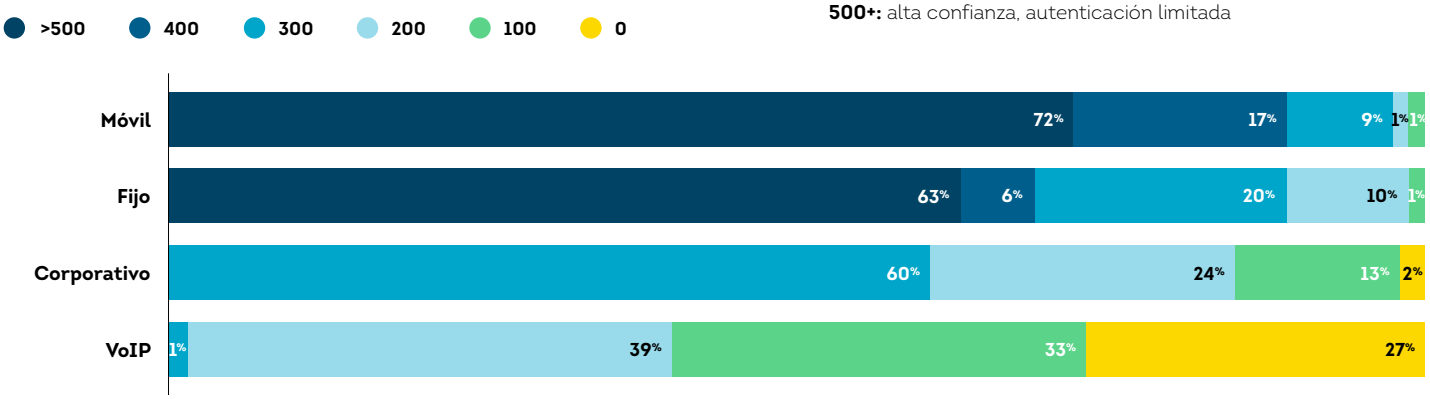
Según el estudio de TransUnion, la gran mayoría (el 85%) de las llamadas recibidas en los centros de atención al cliente de las entidades financieras de EE.UU. en 2022 se realizaron desde un teléfono móvil y menos del 2% de esas llamadas se identificaron como de alto riesgo; sin embargo, las llamadas de alto riesgo realizadas desde un teléfono móvil el año pasado fueron el 14% del total.

El canal que presenta mayor riesgo para un servicio de atención al cliente es el de las llamadas VoIP, es decir, un número de teléfono que no está asociado a ninguna dirección física. Ese canal solamente representó el 3% de las llamadas, pero el 60% fue identificado como de alto riesgo para el fraude. El 62% de las llamadas de alto riesgo procedió de llamadas VoIP.

Volumen de riesgos total y por canal en servicios de atención al cliente en EEUU

Score de riesgos en servicios de atención al cliente

0–199: el más alto, con autenticación en la configuración
200–499: autenticación usual
500+: alta confianza, autenticación limitada



Fuente: TruValidate de TransUnion

Próximos pasos

Los responsables de prevención de fraude deben trabajar codo con codo con los centros de atención al cliente para poner en marcha tecnologías integradas de autenticación de llamadas entrantes basadas en la reputación del dispositivo o móvil desde el que se realiza la llamada. Esto permitiría a los clientes utilizar tanto los canales digitales como los de voz sin el riesgo de ser molestados para llevar a cabo procesos de autenticación adicionales que eviten falsos positivos.

En los servicios de atención al cliente, las llamadas de alto riesgo pueden ser derivadas inmediatamente a los equipos de fraude para que sean autenticadas correctamente. De esta forma, se ayuda a que las llamadas legítimas puedan ser respondidas desde soluciones de respuesta interactiva o con personas físicas sin necesidad de autenticación adicional.

Estrategia para mejorar la detección de fraude: optimizar la verificación de la identidad con el análisis del dispositivo

El crecimiento del fraude basado en la identidad exige que se mejoren las herramientas que se utilizan para prevenir fraude. Usar tecnologías de rastreo de la reputación del dispositivo (es decir, la huella digital que deja el dispositivo) puede ayudar al análisis del riesgo reduciendo la fricción e incrementando la conversión. Pero confiar solamente en la reputación del dispositivo puede ser también arriesgado: los delincuentes son capaces en ocasiones de emular dispositivos y ocultar la información de trazabilidad. Los dispositivos desconocidos pueden también generar dudas en las soluciones de huella digital, con lo que es posible que se incremente el riesgo de fraude, los falsos positivos o las fricciones innecesarias. Sin señales adicionales de riesgo, no hay forma de determinar si el usuario que hay detrás de un dispositivo nuevo se merece una cálida bienvenida o un escrutinio adicional.

Utilizar señales adicionales de riesgo o verificaciones de dispositivo determina la confianza del dispositivo y de la identidad antes de que se inicien los procesos de autenticación, reduciendo la necesidad de peticiones adicionales de autenticación. La verificación del dispositivo extiende la comprobación de la identidad en experiencias digitales analizando los riesgos de la identidad que opera el dispositivo. La verificación del dispositivo mejora los enfoques multidimensionales con los que analizar el riesgo: huella digital del dispositivo, conexiones entre dispositivos e identidades, análisis del comportamiento del usuario… Todo esto puede ayudar a reducir los falsos positivos en clientes que utilizan un nuevo dispositivo o en nuevos clientes que generan una cuenta por primera vez.

Crecimiento del fraude digital basado en identidad

81%
Robo de identidades reales

132%
Identidades sintéticas

Source: TransUnion TruValidate

Próximos pasos

Los responsables de prevención de fraude deben buscar la manera de reducir los falsos positivos mejorando los programas de fraude con capacidades de verificación del dispositivo. Poner en marcha estas funciones basadas en el dispositivo facilita el hecho de que los clientes legítimos puedan realizar transacciones a la vez que se alerta sobre clientes sospechosos de fraude, a los que se les puede demandar un proceso adicional de verificación. Las soluciones ideales incluyen una amplia gama de dispositivos y de métricas relacionadas con la identidad y con el comportamiento que pueden aplicarse en los modelos de detección de fraude.

EXPERIENCIAS EN EL MUNDO REAL

Una verificación de identidad robusta reduce el fraude en solicitudes

Una entidad **europea de préstamos buscaba** crecer a la vez que reducía la fricción en las solicitudes de sus clientes. La entidad puso en funcionamiento una solución de verificación de identidades más robusta y basada en el dispositivo del cliente, con lo que consiguió:

Un **40%** menos de solicitudes fraudulentas, con lo que ahorró aproximadamente 16 millones de euros al año

Las identidades sintéticas pueden impactar en el fraude más allá de los servicios financieros

Los responsables de riesgos y de prevención del fraude han centrado sus esfuerzos en combatir las identidades sintéticas durante años. Las identidades sintéticas representan un riesgo financiero real para las entidades financieras y de crédito. Estas identidades modificadas o completamente falsas se utilizan para abrir cuentas, crear historial de crédito y acceder y utilizar créditos, así como para lavar capitales ilícitos.

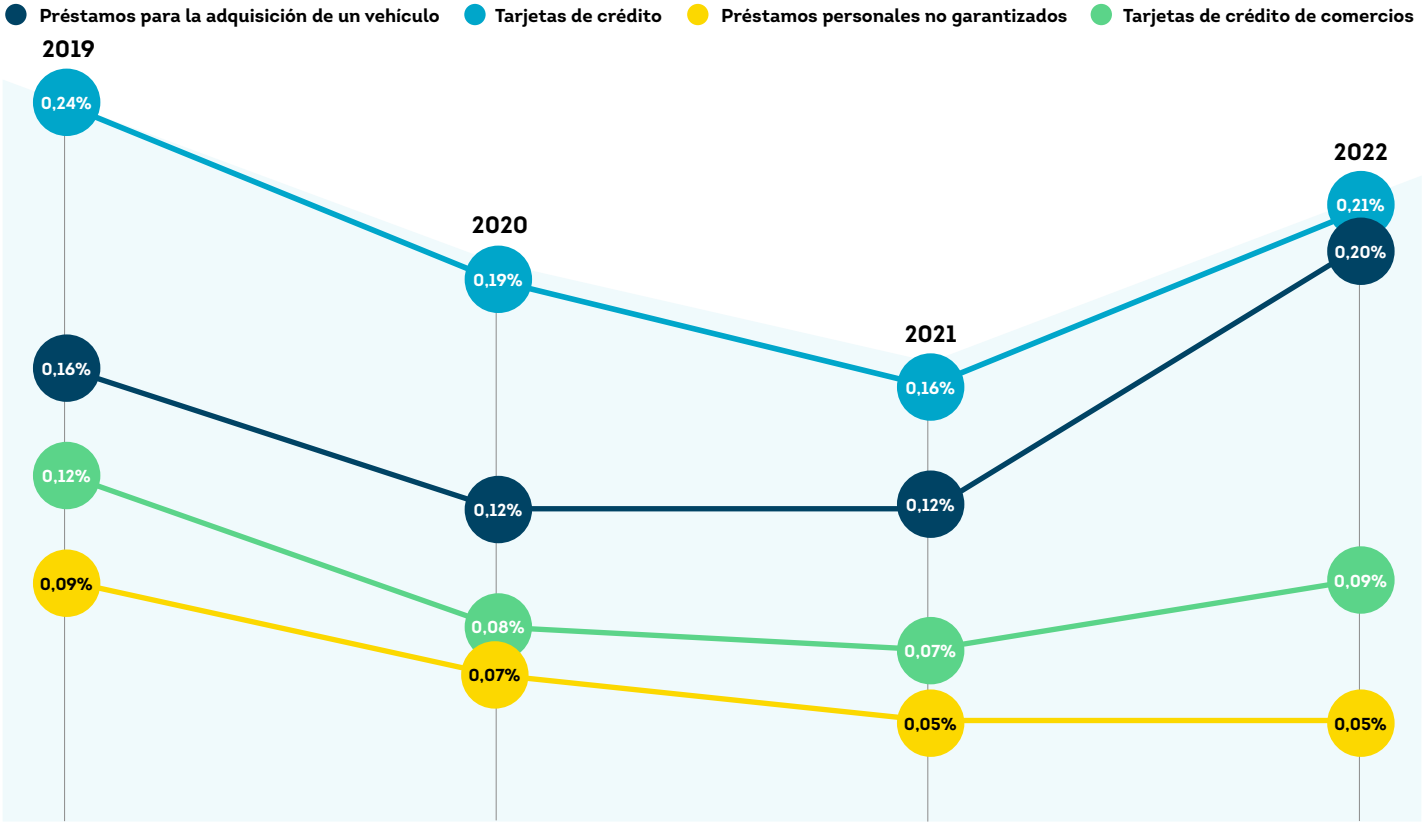
Los saldos pendientes[1] atribuidos a las identidades sintéticas y referidos a créditos personales, de tarjetas de compra o de crédito y a préstamos para la adquisición de un vehículo en EE.UU. alcanzaron un récord en 2022, según un informe de TransUnion, llegando a 1.200 millones de euros en el último trimestre de 2022 y a los 4.300 millones de euros en todo el año 2022.

Y aunque hasta ahora las identidades sintéticas han supuesto un problema para las entidades financieras, sobre todo por el hecho de que los defraudadores buscaban contar con historial de crédito, la realidad es que cualquier tipo de empresa puede ser un objetivo de este tipo de fraude.

Estrategia: aplicar analítica avanzada para detectar identidades y cuentas sintéticas

Aunque el uso de identidades sintéticas disminuyó durante la pandemia, el fraude relacionado con este patrón ha vuelto a crecer desde principios de 2021. Ya sean personalidades modificadas o completamente ficticias, las identidades sintéticas suponen una amenaza al negocio y a los resultados de cualquier empresa que invierte en conseguir clientes para su organización. Como no suelen aparecer hasta que se cancela la cuenta, es importante que los responsables de prevención de fraude las detecten en el momento de comenzar la relación, o al menos que se les cace en alguna de las revisiones que se realizan utilizando modelos de detección de fraude (por ejemplos, los compatibles con el Acta FCRA).

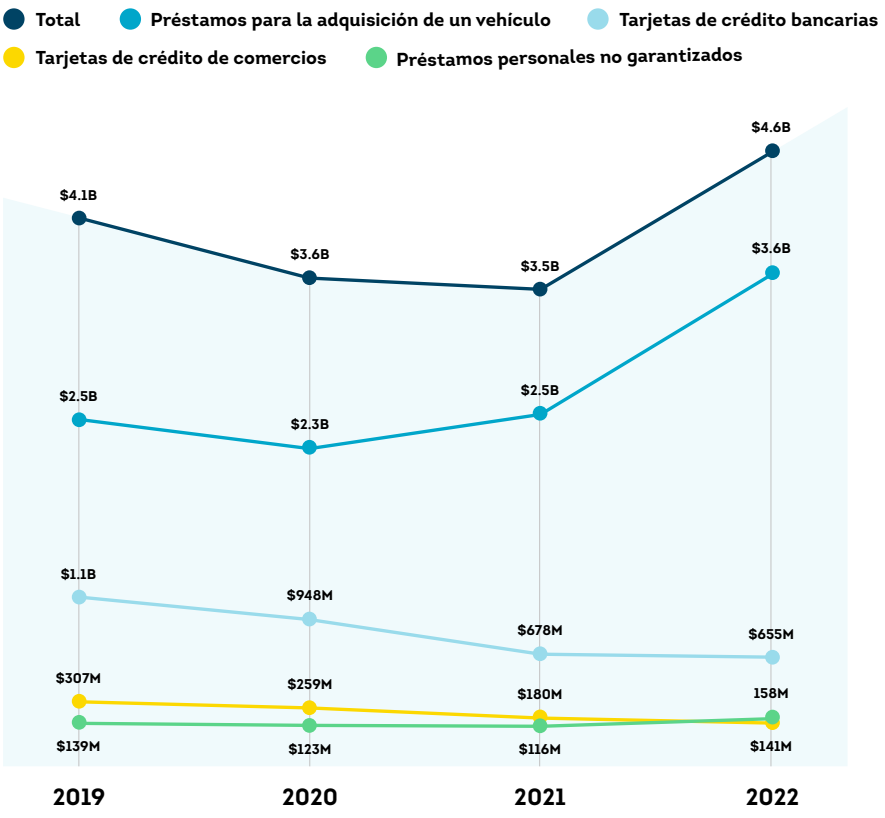
Incidencias relacionadas con identidades sintéticas en entidades financieras de EEUU en el momento de crear nuevas cuentas



Fuente: TruValidate de TransUnion

1 Un saldo pendiente es la cantidad que un consumidor debe abonar en una fecha concreta

Saldos pendientes en cuentas de crédito sospechosas de haber utilizado una identidad sintética en EEUU



Fuente: TruValidate de TransUnion

Próximos pasos

Aprovechar los modelos de detección de fraude creados para detectar identidades sintéticas en todos los pasos del ciclo de vida del cliente. Esto incluye el momento de adquisición del cliente, la toma de decisiones sobre la concesión del crédito o el análisis del conjunto de clientes. Utilizar modelos dedicados también ayuda a priorizar cuentas según los riesgos que presentan, con lo que se mejora el cumplimiento de los inventarios por fecha y las regulaciones relacionadas con el conocimiento de los clientes.

Además, en EEUU, poner en marcha la verificación electrónica del número de la Seguridad Social (eCBSV), que permite a las entidades verificar los datos de la Seguridad Social y combinarlos con la filiación y la fecha de nacimiento del cliente, puede ayudar de forma eficaz a prevenir el fraude.

EXPERIENCIAS EN EL MUNDO REAL

Poner en marcha un modelo de fraude sintético reduce las cancelaciones potenciales

Una **entidad financiera** estadounidense quería proteger la adquisición online de clientes y evitar el riesgo de atraer identidades sintéticas a su modelo de negocio. La entidad puso en marcha un modelo de fraude sintético en los procesos de toma de decisión para la concesión de créditos con lo que:

10%–15%

Redujo entre un 10% y un 15% lascancelaciones y un 0,7% las pérdidas estimadas

Conclusión

Si miramos a este 2023 y un poco más allá, los responsables de prevención de fraude deben preparar sus empresas para sufrir ataques cada vez más sofisticados. En un mundo en el que lo digital se ha impuesto, los datos relacionados con la identidad son vitales para los defraudadores que quieren desarrollar esquemas de fraude, por lo que generar reputación en las identidades es clave para ellos.

Por su parte, los consumidores exigen plataformas de comercio electrónico seguras en las que puedan llevar a cabo sus transacciones con confianza. Y quieren disfrutar de la experiencia digital en todo momento sin fricciones, pero sabiendo que están protegidos.

Dicho esto, los responsables de prevención de fraude deben proponer enfoques globales que prevengan el fraude y que generen confianza para los clientes. Y, para ello, precisan de estrategias de innovación continua que aprovechen los datos, la tecnología y la analítica de la forma más precisa posible para detectar el fraude sin impactar en la experiencia de los clientes legítimos.

Los consumidores exigen plataformas de comercio electrónico seguras en las que puedan llevar a cabo sus transacciones con confianza

Metodología de los datos

Este informe utiliza datos propios de la red de inteligencia global de TransUnion, así como de un estudio llevado a cabo para la compañía. La solución TruValidate de TransUnion incluye productos de fraude y de identidad que protegen las experiencias de los consumidores en cualquier canal y sin fisuras.

Centro de atención al cliente

Los resultados relacionados con centros de atención al cliente se han generado a partir de 5.000 millones de transacciones analizadas a lo largo de 2022 en entidades financieras de todos los tamaños con sede en EE.UU. Las tasas y porcentajes de llamadas de alto riesgo se determinan a partir del análisis de múltiples factores de riesgo.

Estudio sobre consumidores

Dynata ha realizado un estudio para TransUnion en el que se preguntó online a 13.383 adultos mayores de edad entre el 8 y el 23 de diciembre de 2022 residentes en 18 países (Brasil, Canadá, Chile, Colombia, España, Estados Unidos, Filipinas, Hong Kong, India, Kenia, México, Namibia, Puerto Rico, Reino Unido, República Dominicana, Ruanda, Sudáfrica y Zambia). Se utilizó un panel de datos online con una combinación de dispositivos (tablet, PC y móvil). Se preguntó en chino (en Hong Kong), en inglés y francés (en Canadá), en portugués (en Brasil) y en español (en Colombia, España, México, Puerto Rico y República Dominicana). Para asegurar la representatividad demográfica, el estudio incluyó cuotas que equilibraran las respuestas en cuanto a edad, género e ingresos. Es posible que algunos porcentajes no sumen 100 debido al redondeo o a que se aceptaban respuestas múltiples.

Brechas de datos

Sontiq es una compañía TransUnion que obtiene datos sobre brechas gracias a su acuerdo con el Identity Theft Resource Center (ITRC). El ITRC analiza diferentes fuentes en las que se publican eventos públicos relacionados con brechas de datos en EEUU, entre los que se incluyen los del Fiscal General del Estado, notas de prensa, publicaciones de despachos de abogados y de expertos en ciberseguridad, entre otros. Sontiq combina los datos con un algoritmo de inteligencia artificial que cuenta con 1.300 elementos y genera un score de riesgo, una lista de riesgos y consejos para los consumidores.

Fraude digital

TransUnion utiliza la inteligencia que otorga el análisis de miles de millones de transacciones llevadas a cabo en las 40.000 webs y apps que protegen sus soluciones. La tasa o porcentaje de intentos sospechosos de fraude reflejan las transacciones denegadas en tiempo real debido a los indicadores de compromiso y aquellas que fueron categorizadas como riego después de una revisión frente al total de transacciones analizadas. Los análisis por país o región analizan las transacciones en las que tanto el consumidor como el defraudador estaban en dicho país o región.

Fraude sintético

Los hallazgos relacionados con fraude sintético se basan en los datos analizados por TransUnion entre los créditos al consumo solicitados en EE.UU. y proceden del estudio de más de 50 años de datos relacionados con los créditos al consumo. Contienen toda la información de aproximadamente 400 millones de clientes.

Más información sobre TruValidate de TransUnion

TruValidate organiza el análisis de comportamientos, dispositivos e identidades para ayudar a las empresas a fidelizar clientes de forma segura a través de cualquier canal y en cualquier momento del ciclo de vida, mejorando la conversión, reduciendo las pérdidas por fraude y ofreciendo experiencias de usuario mejoradas y sin fisuras.

www.transunion.co/solucion/truvalidate

Sobre TransUnion

TransUnion es una organización global de información y análisis con más de 12.000 profesionales que operan en más de 30 países. Conseguimos generar confianza asegurando que cada persona se vea representada legítimamente en el mercado. Y lo hacemos con una imagen verdadera de cada individuo que permite tomar decisiones con cuidado. Gracias a las últimas adquisiciones de la compañía y a las inversiones en tecnología, hemos desarrollado soluciones innovadoras que se extienden más allá de nuestros fundamentos en el crédito, tales como marketing, riesgos de fraude o analítica avanzada. Como resultado de ello, tanto clientes como empresas pueden realizar transacciones con confianza y conseguir grandes avances. Nosotros lo llamamos "Information for Good", "Información para hacer el bien" y ayuda a aprovechar las oportunidades económicas, a generar grandes experiencias y a dar el poder a millones de personas en todo el mundo.

www.transunion.co/empresas