TransUnion

TransUnion 2024 Informe sobre el estado de Fraude Omnicanal

Tendencias y perspectivas para hacer posible un comercio confiable

Introducción

Ahora más que nunca, conocer la identidad de las personas con las que se está tratando es clave para las estrategias de prevención de fraude de cualquier empresa. Aprovechándose del crecimiento continuo de las transacciones digitales a nivel mundial después de la pandemia, el fraude alcanzó niveles sin precedentes en 2023. Los ciberdelincuentes están robando más información de identidad de las organizaciones y de los individuos para cometer apropiación de cuentas (Account takeover - ATO, en inglés), provocando fraudes de terceros o creando cuentas fraudulentas —incluyendo un número récord de cuentas sintéticas— para perpetrar fraudes directos.

Los consumidores, en reacción a esta amenaza real, están confiando en las empresas para proteger sus datos personales, seleccionando marcas con base en la seguridad percibida. Las organizaciones que demuestran seguridad y conveniencia en sus experiencias omnicanal, mediante capacidades de detección y prevención de fraude, tienen la oportunidad de ganarse la confianza de los consumidores.

En el Informe sobre el Estado del Fraude Omnicanal 2024, TransUnion reúne tendencias, referencias y experiencias en identidad y fraude de toda nuestra organización. Ofrecemos información a aquellos responsables de prevenir el fraude y optimizar las experiencias de los clientes para obtener mejores resultados comerciales. Utilice este informe para evaluar los programas actuales de prevención de fraudes en el contexto del mercado en general. Comparta esta información en toda su organización con el objetivo de aumentar la satisfacción del cliente, reducir el fraude y mejorar el rendimiento empresarial.

Todos los datos en este informe combinan información obtenida de la red de inteligencia global de TransUnion y la encuesta Consumer Pulse realizada por TransUnion en 18 países y regiones a nivel mundial.

PRINCIPALES HALLAZGOS

La suplantación de identidad aumentó el riesgo de fraude

15%
aumentaron las filtraciones de datos en Estados Unidos de 2022 a 2023 y +157% de 2020 a 2023. La gravedad de las filtraciones aumentó un 11% de 2022 a 2023.

54%
de los consumidores en 18 países y regiones seleccionados informaron haber sido objeto de intentos de fraude en línea, correo electrónico, llamadas telefónicas o mensajes de texto entre septiembre y diciembre de 2023.

El Fraude Digital superó el crecimiento de las transacciones

5%
de todas las transacciones digitales a nivel mundial fueron sospechosas de Fraude Digital en 2023, con un aumento del 14% en el volumen sospechoso respecto a 2022.

105%
creció el volumen de Fraude Digital sospechoso de 2019 a 2023, superando el aumento del 90% de las transacciones digitales en general.

La creación de cuentas representó un alto riesgo en todos los canales

13.5%
de todas las transacciones globales para la creación de cuentas digitales en 2023 fueron sospechosas de Fraude Digital.

USD $3.100 millones
en pérdidas potenciales de las entidades de crédito por las identidades sintéticas sospechosas para créditos de vehículo, tarjetas de crédito bancarias, tarjetas de crédito para minoristas y créditos de libre inversión no garantizados en Estados Unidos originados a finales de 2023 (nivel más alto jamás registrado; el porcentaje de identidades sintéticas en las cuentas abiertas también es el más alto jamás registrado).

Contenidos

TransUnion

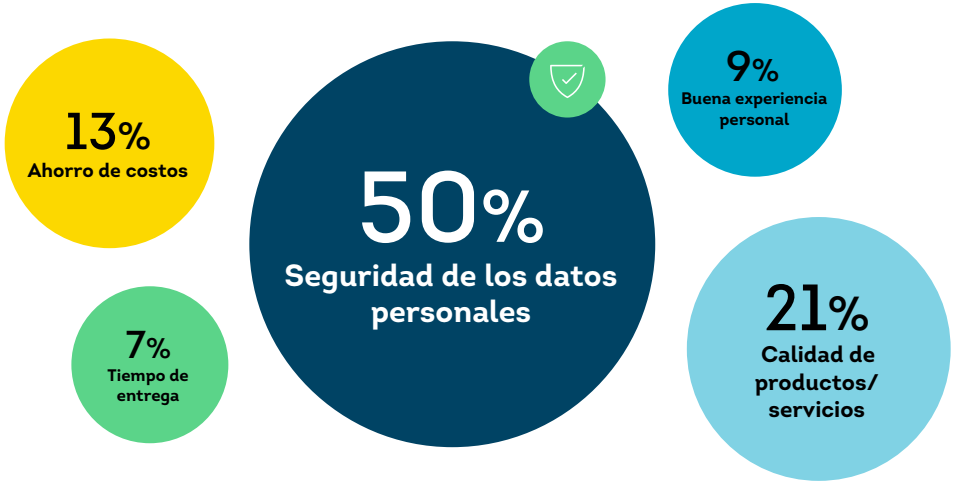
Perspectiva del consumidor

Cumplir con las expectativas de seguridad y conveniencia es una estrategia ganadora

Los consumidores tienen grandes expectativas de que las organizaciones protejan sus identidades mientras ofrecen experiencias convenientes. De hecho, el 59% de los consumidores informaron que es probable que cambien de empresa para obtener una mejor experiencia digital. Sin embargo, los consumidores clasificaron la seguridad de los datos personales (50%) como la principal razón para hacer negocios con una empresa en línea. Además, el 93% dijo que la confianza en que sus datos personales no serán comprometidos es lo más importante al elegir con quién hacer transacciones en línea, con un 79% que dijo que es muy importante.

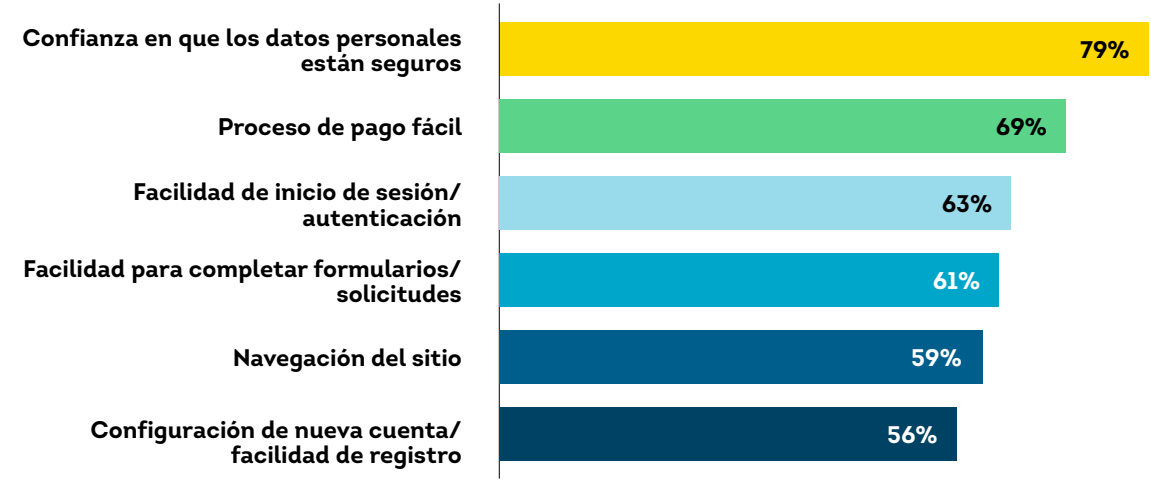
Clasificación de expectativas o cualidades en las empresas en línea preferidas

Principal respuesta elegida



Características importantes declaradas al elegir con quién hacer transacciones en línea

Muy importante



Fuente: Encuesta de fraude al consumidor de TransUnion

TransUnion

La confianza y la seguridad son fundamentales para las tasas de conversión en línea

Las organizaciones deben asegurarse que las experiencias omnicanal sean percibidas como seguras o corren el riesgo de perder clientes. Menos consumidores (34%) informaron realizar más del 50% de sus transacciones en línea en 2023, frente al 36% en 2022 y al 45% en 2021. Si bien la disminución puede deberse a que más ubicaciones físicas estén abiertas después de la pandemia mundial, también puede ser en respuesta a un mayor conocimiento del riesgo de fraude.

Dos tercios de los consumidores (65%) informaron que las preocupaciones por el fraude fueron la principal razón por la que no volverían a usar un sitio, un aumento frente al 63% en 2022. La mitad de los consumidores informaron haber abandonado un carrito de compras en línea debido a preocupaciones sobre el fraude y/o la seguridad. Mientras que la mayoría de las personas (52%) han abandonado solicitudes en línea de servicios financieros y de seguros, sus razones abarcaron la seguridad y la facilidad: Demasiada información solicitada (48%), no confiaban en que sus datos personales estuvieran seguros (41%) y demasiado tiempo para completar (37%) fueron las principales razones para el abandono

La principal razón por la que los consumidores abandonaron una solicitud en línea o un formulario para un producto financiero o de seguros

Fuente: Encuesta de fraude al consumidor de TransUnion

Tendencias de la exposición de datos de identidad

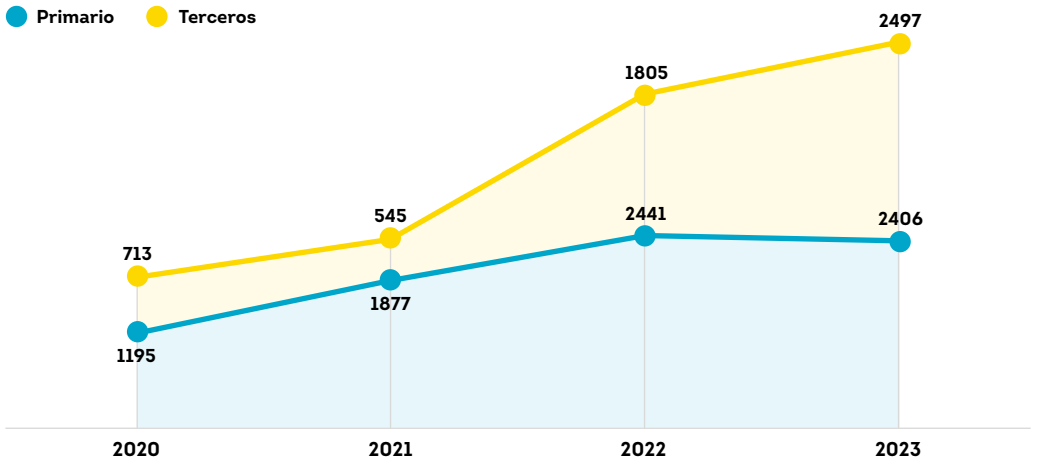
Los datos de identidad o la información de identificación personal (PII, por sus siglas en inglés) son un objetivo principal de los ciberdelincuentes. Están utilizando todos los medios posibles, apuntando tanto a organizaciones como a consumidores, para obtener credenciales de identidad y alimentar esquemas de fraude. Más de la mitad de todos los consumidores (54%) dijeron que fueron blanco de fraude por correo electrónico, en línea, llamadas telefónicas o mensajes de texto en los últimos tres meses. Además, las filtraciones de datos reportadas y su gravedad alcanzaron máximos históricos en Estados Unidos.

Las filtraciones de datos en Estados Unidos alcanzaron un volumen y una gravedad récord

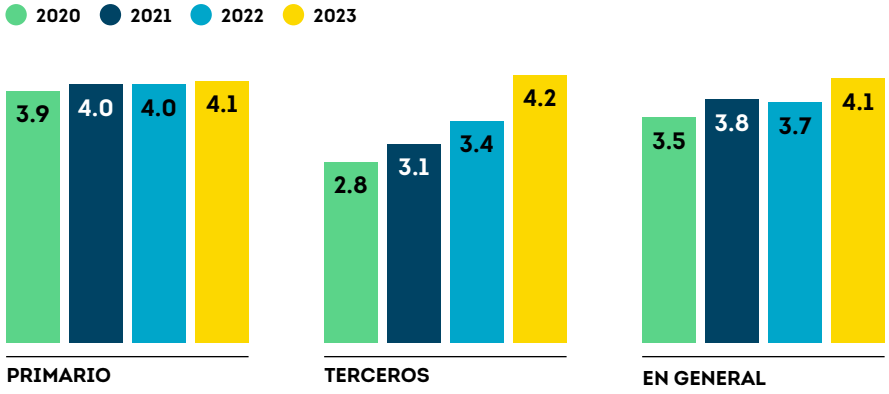
Las filtraciones de datos son un indicador principal de futuros fraudes, ya que los ciberdelincuentes roban credenciales en cantidades sin precedentes. Las filtraciones de datos en Estados Unidos aumentaron un 15% año tras año en 2023, alcanzando un volumen nunca visto, impulsado por un aumento del 38% año tras año en violaciones de terceros. Además, la gravedad promedio del riesgo de filtración (la capacidad de una filtración para facilitar el fraude de identidad), medida por el Puntaje de Riesgo de Filtración (BRS, por sus siglas en inglés) TruEmpower™ de TransUnion, aumentó un 11% año tras año a 4.1 en 2023, también el más alto jamás medido.

Los ciberdelincuentes se centraron en los proveedores de servicios de terceros como el vector de filtración de datos más grande, superando a las filtraciones primarias por primera vez en 2023. No solo hubo más filtraciones de terceros, sino que también fueron más severas, con un Puntaje de Riesgo de Filtración (BRS) promedio un 24% más alto que en 2022.

Volumen de filtraciones de datos en Estados Unidos



Puntuación promedio del riesgo de filtración de datos en las filtraciones de datos en Estados Unidos



Una filtración de datos primaria representa un ataque directo a una organización. Una filtración de datos de terceros, también conocida como un ataque a la cadena de suministro, ataque a la cadena de valor o filtración por puerta trasera, ocurre cuando un atacante accede a la red de una entidad a través de proveedores o suministradores externos, como el procesamiento de nóminas o la facturación médica.

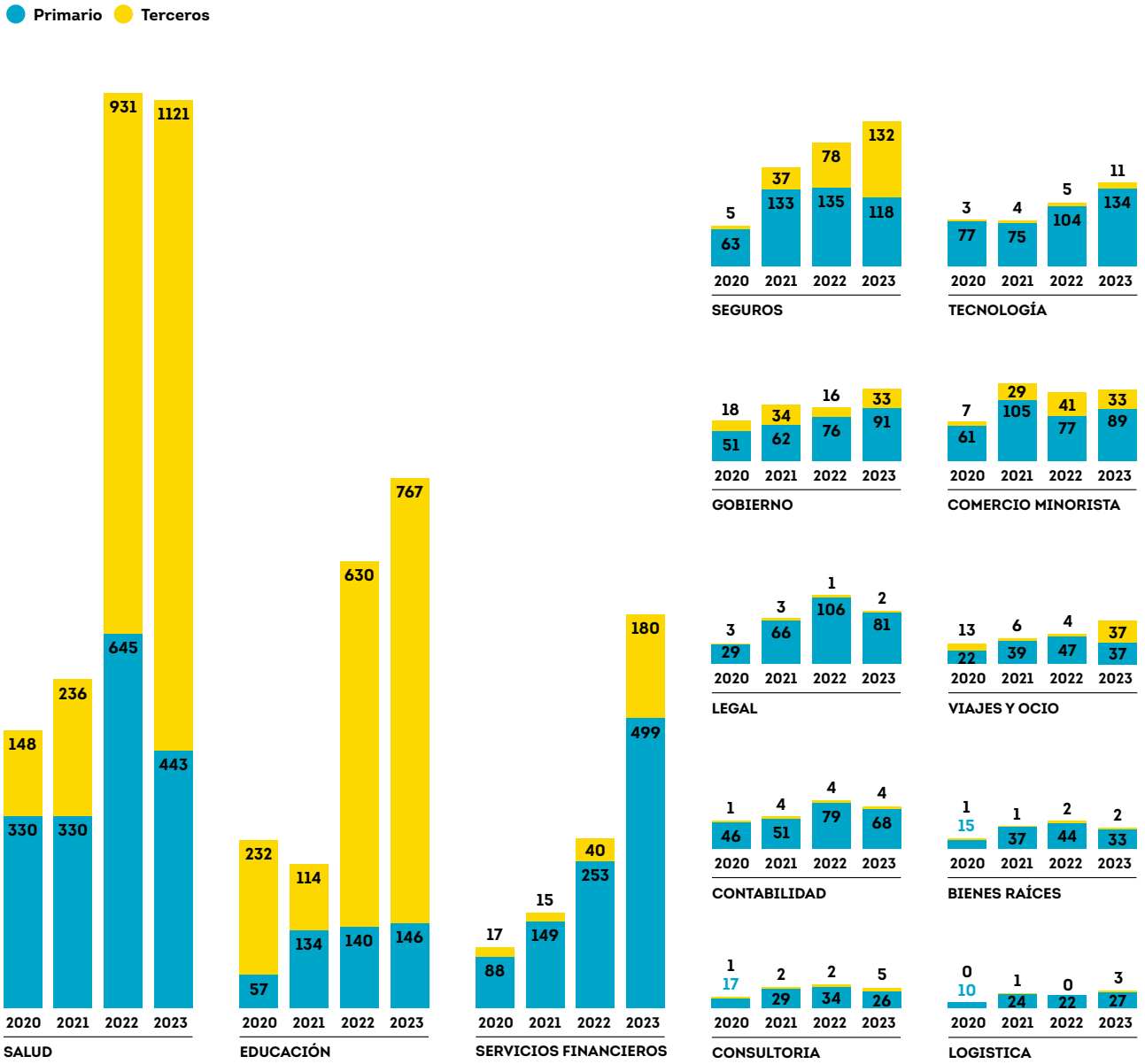
Fuente: TransUnion TruEmpower

TransUnion

El sector de la salud y la educación experimentaron la mayoría de las filtraciones de datos

Por segundo año consecutivo, el sector de la salud experimentó el mayor número de filtraciones de datos, seguido por el sector educativo. A pesar de que el mayor volumen ocurrió en el sector de la salud, las filtraciones más graves ocurrieron en el sector educativo (5.6 BRS) y en el sector de seguros (4.9 BRS).

Volumen de filtraciones de datos en Estados Unidos por industria en 2023



Nota: Los cambios en los informes en la Oficina del Fiscal General del Estado de Nueva York aumentaron el número de filtraciones reportadas en servicios financieros en 2023.

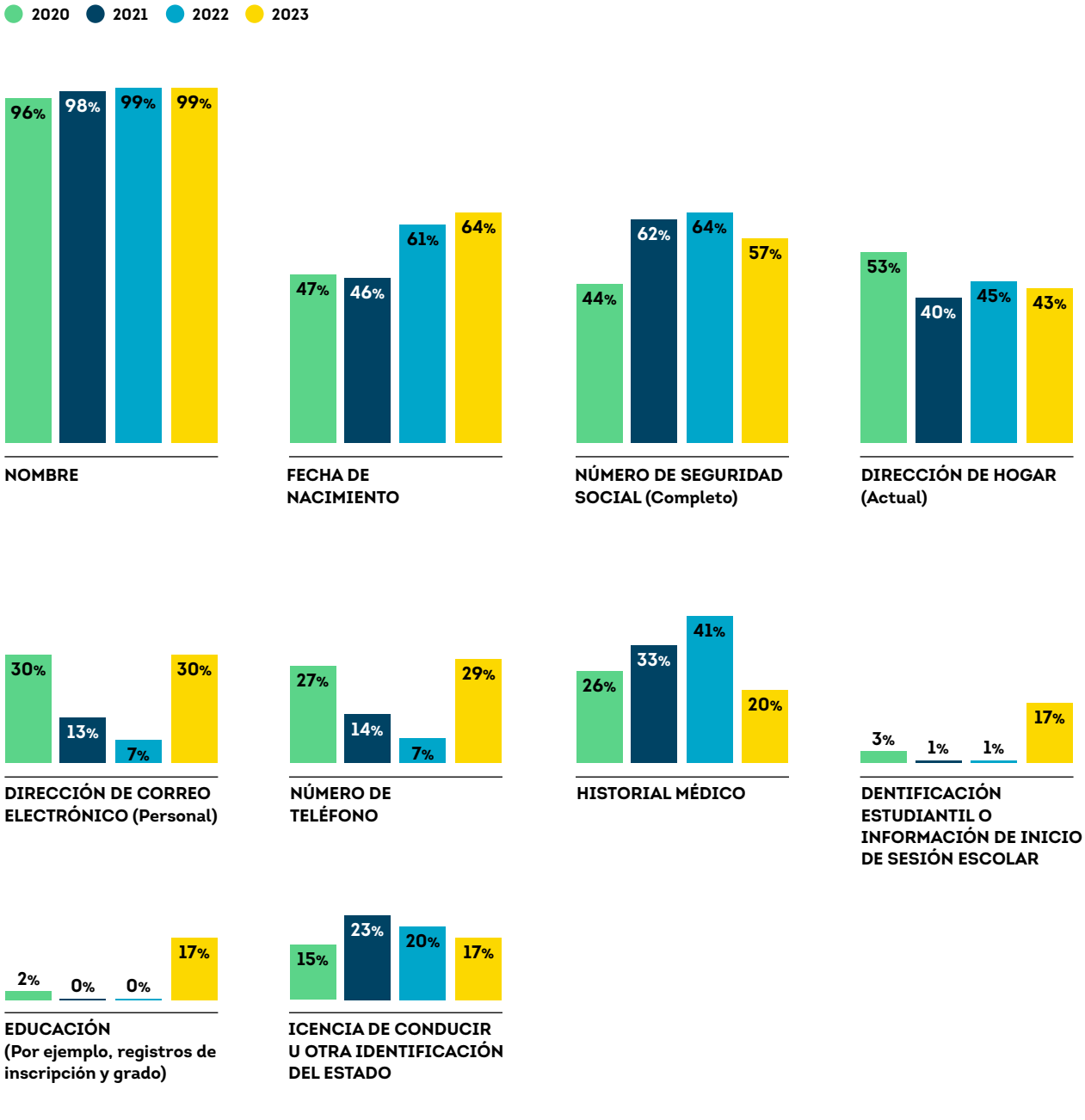
Fuente TransUnion TruEmpower

TransUnion

Las credenciales de identidad son el objetivo de las filtraciones de datos

Los ciberdelincuentes continuaron violando los sistemas de las organizaciones para robar las credenciales de identidad de los consumidores, incluyendo la fecha de nacimiento, el número completo de la seguridad social y la dirección del hogar, necesarios para abrir cuentas fraudulentas y crear identidades sintéticas. También buscaron credenciales como la dirección de correo electrónico, el número de teléfono y la identificación estudiantil o la información de inicio de sesión escolar para posiblemente facilitar la apropiación de cuentas (ATO – Account takeover en inglés) y las estafas al consumidor.

Las 10 credenciales de identidad expuestas más comunes en las filtraciones de datos de EE. UU. en 2023



Fuente: TransUnion TruEmpower

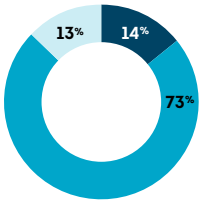
Los consumidores son regularmente blanco de estafas para obtener acceso a cuentas o de engaños para robar fondos

Más de la mitad de los consumidores (54%) informaron haber sido blanco de un esquema de fraude por correo electrónico, en línea, llamada telefónica o mensaje de texto, y el 11% dijo que fueron víctimas entre septiembre y diciembre de 2023. Entre aquellos que dijeron haber sido blanco, el phishing (correos electrónicos fraudulentos, sitios web, publicaciones en redes sociales, códigos QR, etc. destinados a robar datos) al 33%; el smishing (mensajes de texto fraudulentos destinados a engañarlo para que revele datos) al 29%; y el vishing (llamadas telefónicas fraudulentas destinadas a engañarlo para que revele datos) al 27% fueron los principales tipos de fraude los consumidores informaron haber experimentado.

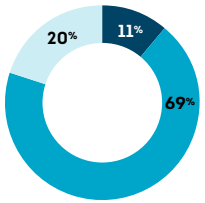
Consumidores blanco de fraude

Porcentaje de consumidores que dijeron que los estafadores los atacaron con intentos de fraude por correo electrónico, en línea, llamada telefónica o mensaje de texto de septiembre a diciembre de 2023, y el esquema más frecuente por el cual informaron haber sido atacados.

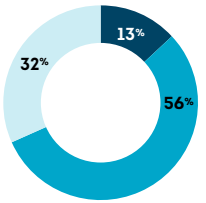
- **Blanco y fueron víctimas**
- **Blanco pero no fueron víctimas**
- **No fue blanco**
- **Esquema de fraude más reportado**



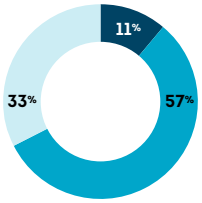
KENIA
Smishing



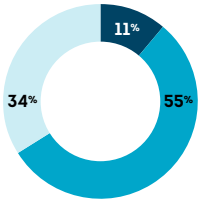
ZAMBIA
Smishing



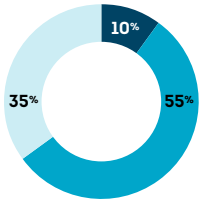
SUDÁFRICA
Mula de dinero



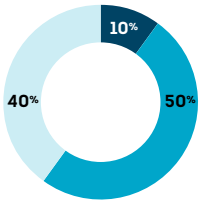
FILIPINAS
Phishing



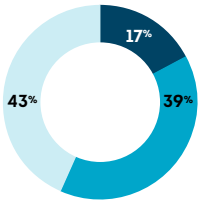
RUANDA
Mula de dinero



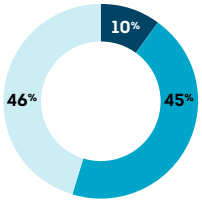
NAMIBIA
Phishing



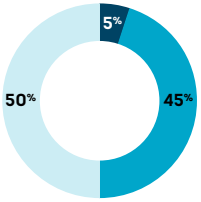
CANADÁ
Phishing



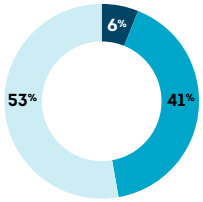
INDIA
Phishing



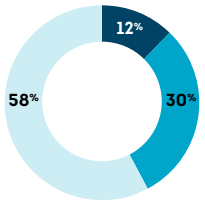
ESTADOS UNIDOS
Phishing



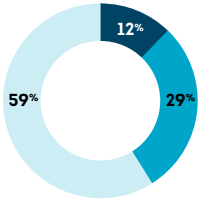
HONG KONG
Phishing



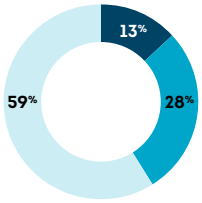
REINO UNIDO
Phishing



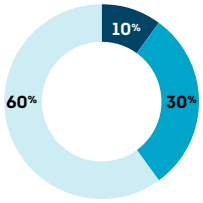
MÉXICO
Robo de tarjeta de crédito



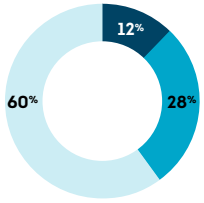
CHILE
Vishing



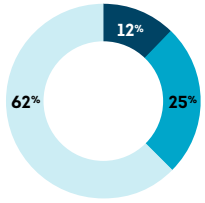
PUERTO RICO
Robo de tarjeta de crédito



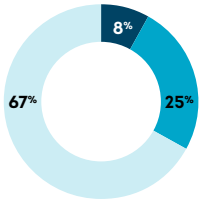
BRASIL
Robo de tarjeta de crédito



COLOMBIA
Vishing



REPÚBLICA DOMINICANA
Robo de tarjeta de crédito



ESPAÑA
Robo de tarjeta de crédito

Fuente: Encuesta de fraude al consumidor de TransUnion

TransUnion

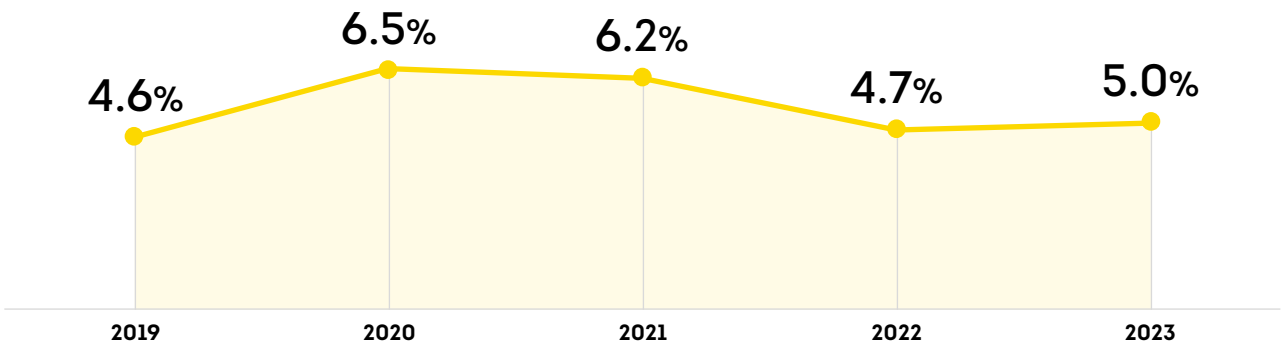
Tendencias globales de Fraude Digital

Las tasas de sospecha de Fraude Digital aumentaron junto con el volumen de transacciones digitales

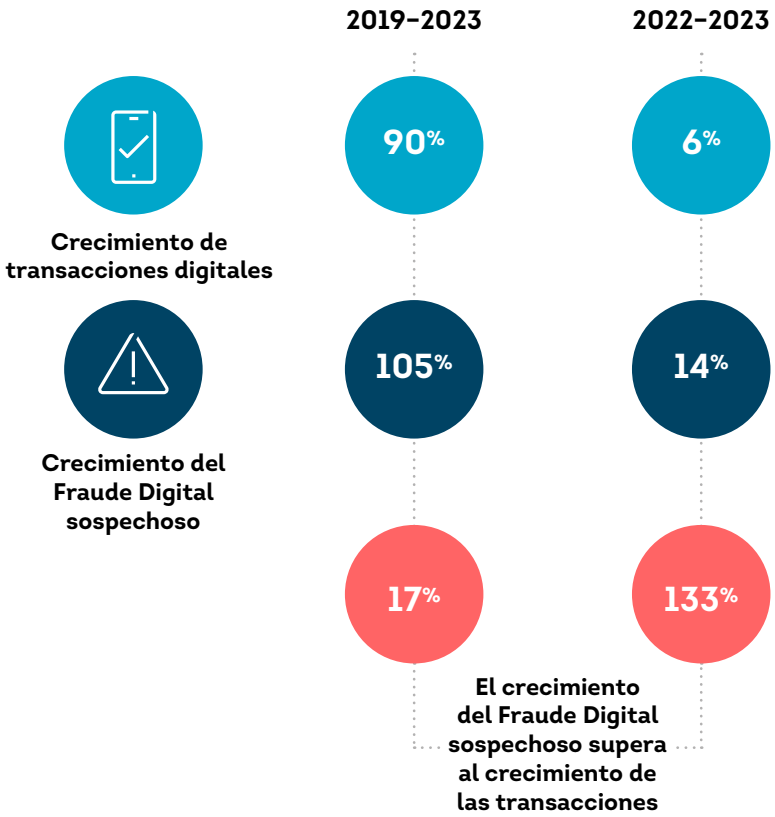
El Fraude Digital continuó creciendo mientras que la tasa de fraude fue ligeramente más alta que los niveles previos a la pandemia a nivel mundial. La tasa de transacciones digitales sospechosas de fraude a nivel mundial aumentó al 5% en 2023, un 6% más que en 2022. El volumen de Fraude Digital sospechoso a nivel mundial creció más rápido que el número de transacciones en todo el mundo. En 2023, el volumen de Fraude Digital sospechoso aumentó un 14% en comparación con 2022 (+6% para todas las transacciones) y un 105% en comparación con 2019 (+90% para todas las transacciones). El crecimiento del Fraude Digital superó el de las transacciones digitales en un 133% de 2022 a 2023 y un 17% de 2019 a 2023.

Para las transacciones en las que el consumidor o el estafador estaban en Estados Unidos, la tasa y el volumen de transacciones digitales sospechosas se mantuvo relativamente sin cambios de 2022 a 2023 (-1% y +1%, respectivamente), pero aumentaron significativamente desde los niveles previos a la pandemia de 2019 a 2023 (+16% y +124%, respectivamente). De los 19 mercados incluidos en el análisis de este año, aproximadamente la mitad (Brasil, Botsuana, Canadá, Colombia, República Dominicana, India, Namibia, Ruanda, España y Zambia) experimentaron una tasa de Fraude Digital sospechoso superior año tras año en 2023. Sin embargo, solo cinco mercados (Brasil, Canadá, Hong Kong, India y Filipinas) tuvieron tasas de Fraude Digital sospechoso por encima del promedio mundial de 5% en 2023.

Tasa de Fraude Digital sospechoso



Crecimiento en volumen de Fraude Digital sospechoso comparado con las transacciones digitales a nivel global



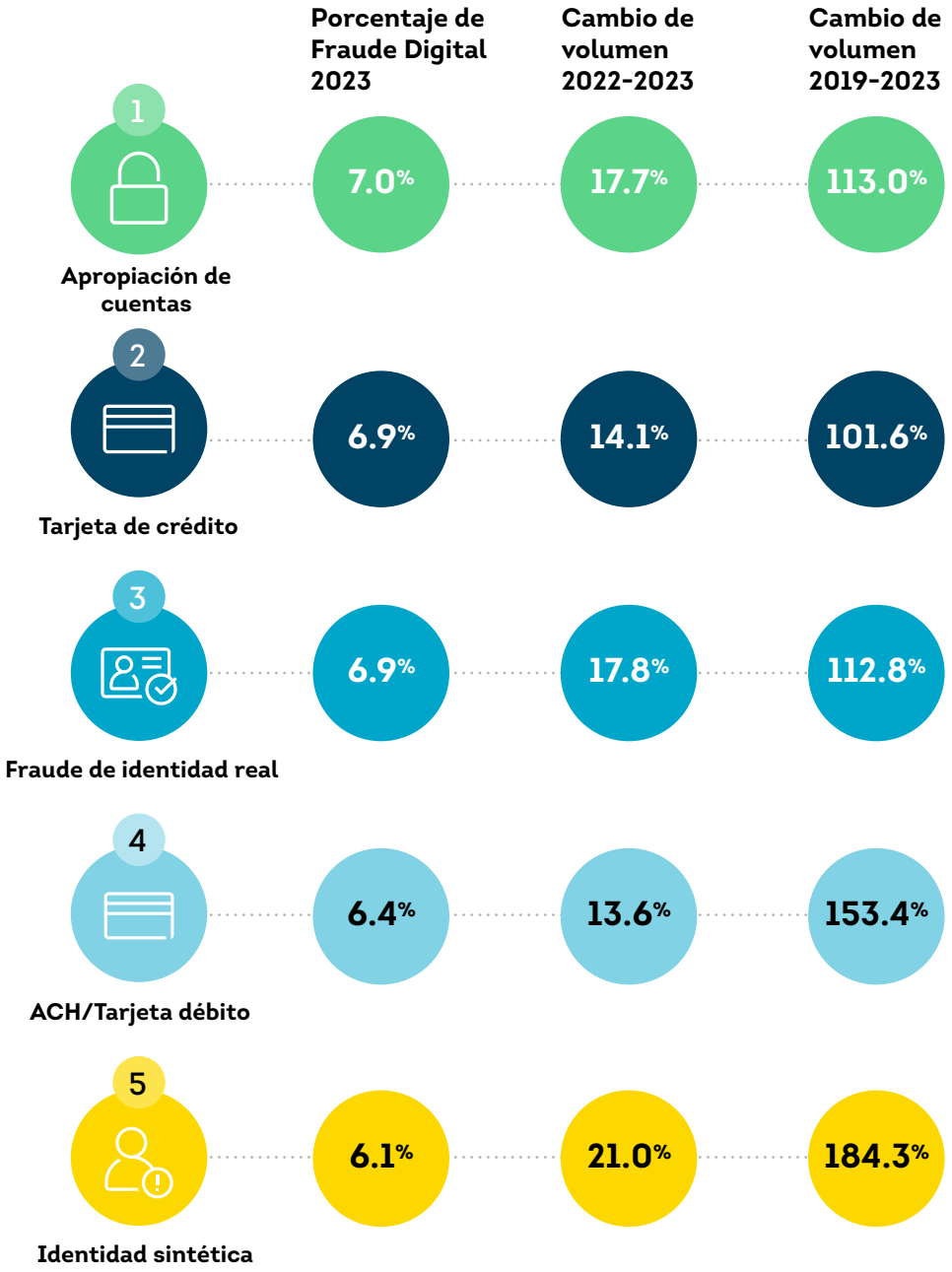
Fuente: TransUnion TruValidate™

TransUnion

La apropiación de cuentas (ATO) encabezó la lista de los tipos de fraude más comunes

La apropiación de cuentas (ATO) representó el 7% del Fraude Digital a nivel mundial en 2023, superando ligeramente al fraude con tarjeta de crédito, que fue el tipo de Fraude Digital más reportado a TransUnion por sus clientes en 2022. Sin embargo, el fraude de identidad sintética fue el tipo de Fraude Digital de más rápido crecimiento en 2023, aumentando al 6.1% a nivel mundial desde el 5.3% en 2022; y en cuanto a volumen el 21% año contra año y el 184% de 2019 a 2023.

Tipos de fraude principales y su crecimiento



Fuente: TransUnion TruValidate

El comercio minorista experimentó las tasas más altas de Fraude Digital

La industria del comercio minorista experimentó el mayor porcentaje (8.7%) de transacciones digitales sospechosas de fraude a nivel mundial en 2023, un aumento del 21% respecto a 2022, y un crecimiento del 34% en el volumen de Fraude Digital sospechoso año contra año. El abuso de promociones fue el tipo de Fraude Digital más reportado en las transacciones minoristas. A pesar de la exposición general al fraude en el comercio minorista, la industria de juegos (juegos de azar en línea) experimentó la tasa más alta de transacciones sospechosas de fraude en 2023 en la mayoría (seis) de los mercados analizados: Colombia, República Dominicana, Kenia, Puerto Rico, España y Estados Unidos.

Intentos de Fraude Digital global por industria

- Tasa de intentos de Fraude Digital sospechosos 2023
- Principal tipo de fraude 2023
- Variación en el volumen de sospecha de Fraude Digital 2022–2023

Comercio minorista

2023
8.7%
Abuso de promciones
2022-2023
+33.5%

Videojuegos

2023
7.6%
Producción fraudulenta de recursos
2022-2023
+32.6%

Juegos de azar
(juegos de azar en línea, póker, etc.)

2023
5.3%
Abuso de promciones
2022-2023
+2.9%

Comunidades
(citas en línea, fotos, etc.)

2023
4.6%
Falcificación de perfil
2022-2023
+9.3%

Telecomunicaciones

2023
4.5%
Fraude con tarjeta de crédito
2022-2023
-7.6%

Servicios financieros

2023
4.3%
Fraude de identidad real
2022-2023
+5.8%

Viajes y ocio

2023
2.3%
Fraude con tarjeta de crédito
2022-2023
+25.0%

Seguros

2023
1.5%
Violación de la política
2022-2023
+18.8%

Gobierno

2023
1.4%
Apropiación de cuentas
2022-2023
+144.9%

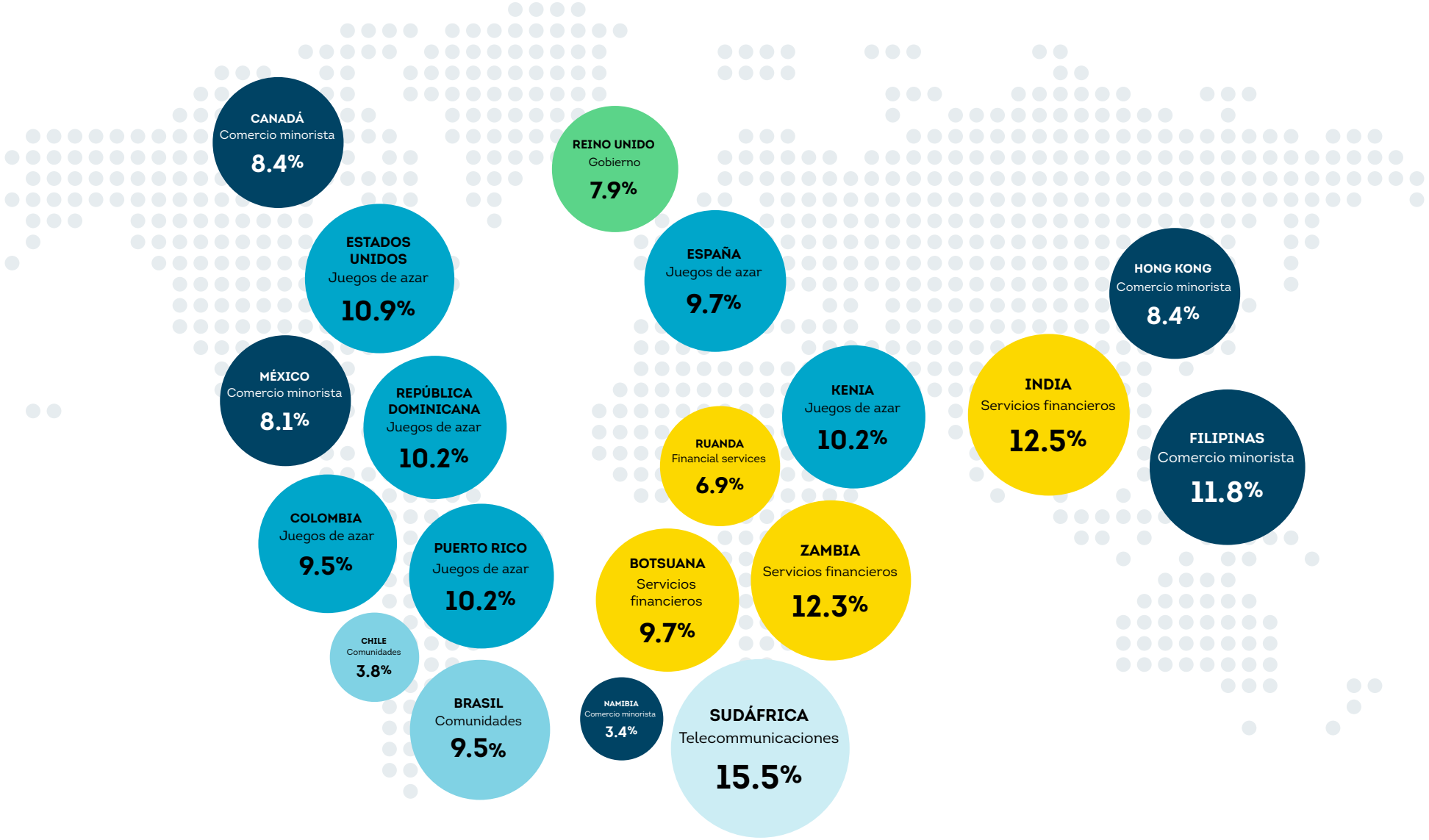
Logística

2023
0.9%
Fraude de envío
2022-2023
-43.9%

Fuente: TransUnion TruValidate

Intentos de Fraude Digital por región e industria 2023

La industria con la tasa más alta de Fraude Digital sospechoso donde el consumidor se encuentra en esa región durante la transacción



Fuente: TransUnion TruValidate

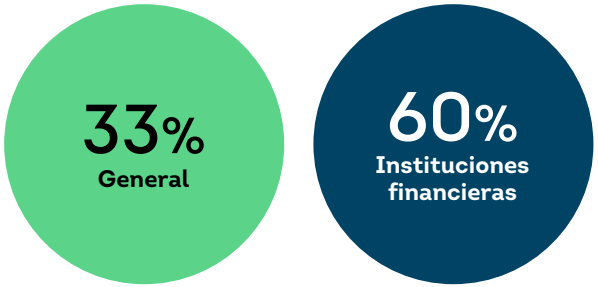
Tendencias de fraude en Centros de Atención Telefónica

Los Centros de Atención Telefónica juegan un papel importante en la experiencia del cliente omnicanal: representan un punto de contacto de alta confianza para los consumidores que están siendo explotados de múltiples formas. Los estafadores han aumentado sus ataques a los Centros de Atención Telefónica para acceder a credenciales y tomar el control de las cuentas de los clientes. Los estafadores también están facilitando la apropiación de cuentas (ATO) utilizando la suplantación de llamadas salientes para engañar a los consumidores y hacer que entreguen sus credenciales de cuenta. No sorprendentemente, un tercio (33%) de las organizaciones encuestadas por TransUnion consideraron a los Centros de Atención Telefónica como una de las principales fuentes de apropiación de cuentas (ATO), aumentando al 60% para las instituciones financieras.

Las llamadas de alto riesgo a los Centros de Atención Telefónica aumentaron rápidamente

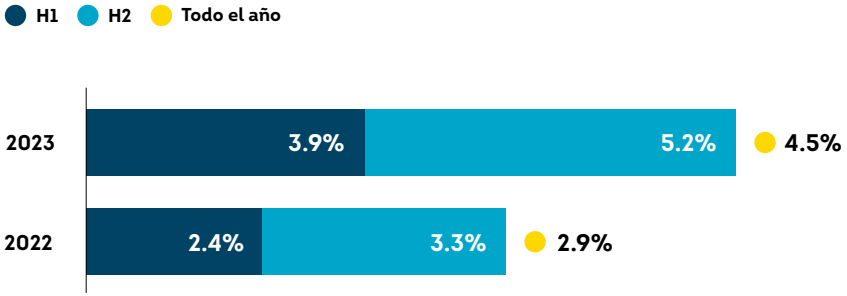
TransUnion documentó un aumento del 55% en el porcentaje de llamadas de alto riesgo a los Centros de Atención Telefónica de Estados Unidos de 2022 a 2023, de 2.9% a 4.5%. En solo medio año, TransUnion encontró que las llamadas de alto riesgo a los Centros de Atención Telefónica de Estados Unidos aumentaron un 33%, de 3.9% en el primer semestre a 5.2% en el segundo semestre de 2023.

Porcentaje de organizaciones en Estado Unidos que creían que la apropiación de cuentas comienza en los Centros de Atención Telefónica



Fuente: Informe sobre el Estado de la Autenticación Omnicanal de TransUnion en 2023

Llamadas de alto riesgo a Centros de Atención Telefónica



H1 es del 1 de enero al 30 de junio y H2 es del 1 de julio al 31 de diciembre

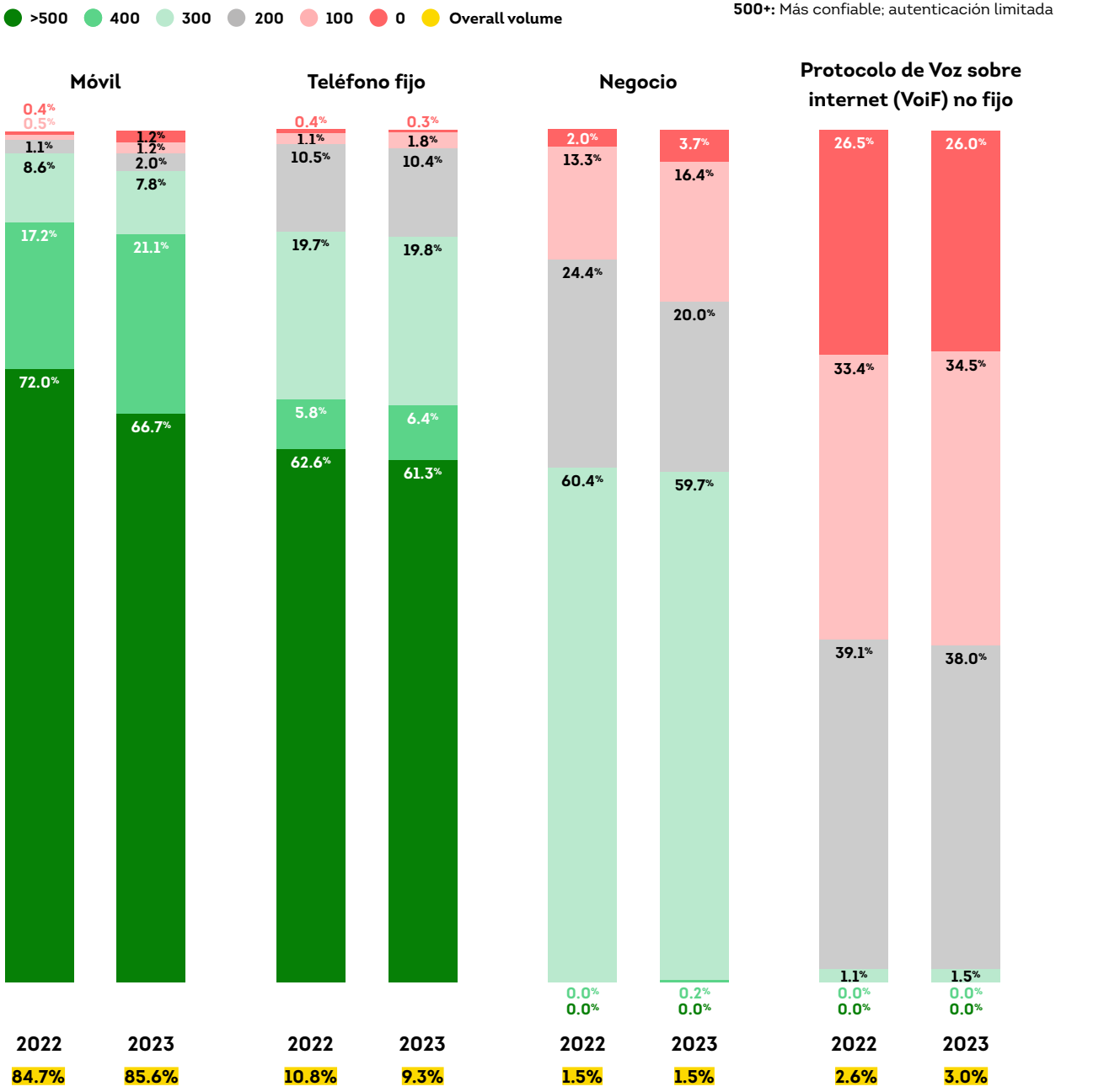
Fuente: TransUnion TruValidate

Las llamadas virtuales representan los mayores riesgos para los Centros de Atención Telefónica

Si bien TransUnion documentó que la gran mayoría (86%) de las llamadas recibidas por los clientes en los Centros de Atención Telefónica en Estados Unidos provenían de teléfonos móviles en 2023, solo el 2.4% de esas llamadas fueron identificadas como de alto riesgo de fraude. El porcentaje de llamadas riesgosas realizadas desde teléfonos móviles a los Centros de Atención Telefónica de Estados Unidos aumentó desde 2022, cuando fue del 0.9%, en 2023. El canal más riesgoso para los Centros de Atención Telefónica fue el Protocolo de Voz sobre Internet (VoIP) no fijo, un número de teléfono que no está asociado con un dispositivo físico. Aunque ese canal representó solo el 3% del volumen total de llamadas en 2023, el 61% de esas llamadas fueron identificadas como de alto riesgo de fraude. Casi el mismo porcentaje de VoIP no fijo fue considerado de alto riesgo en 2022.

Riesgos en los Centros de Atención Telefónica de Estados Unidos por canal y por volumen total

Niveles de puntuación de riesgo de llamadas
0–100: Más alto; autenticación reforzada
200–400: Funcionamiento habitual con autenticación
500+: Más confiable; autenticación limitada



Fuente: TransUnion TruValidate

TransUnion

Riesgo de Fraude Digital en la creación de nuevas cuentas

La creación de cuentas representa la etapa de mayor riesgo en el recorrido del cliente

Las organizaciones y los consumidores enfrentan riesgos, tanto de fraude como impulsados por políticas, en toda la experiencia omnicanal. Al analizar el riesgo por etapa en el recorrido del cliente, una preocupación particular es el riesgo en la creación de nuevas cuentas. De todas las transacciones de creación de cuentas digitales a nivel mundial en 2023 (que representan el 6% del volumen total de tráfico), se encontró que el 13.5% eran sospechosas de Fraude Digital. El alto porcentaje de Fraude Digital en la creación de cuentas contrastaba con las transacciones más típicamente asociadas con el comportamiento fraudulento digital. De hecho, fue más de cuatro veces mayor que el Fraude Digital al inicio de sesión en una cuenta, que puede llevar al de la apropiación de cuentas (ATO), y más de cinco veces mayor que las transacciones financieras en las que realmente se intercambiaba dinero. Esto indica que los estafadores simplemente pasan por alto las cuentas existentes para crear otras nuevas que controlan

Ejemplos de las etapas del recorrido del cliente

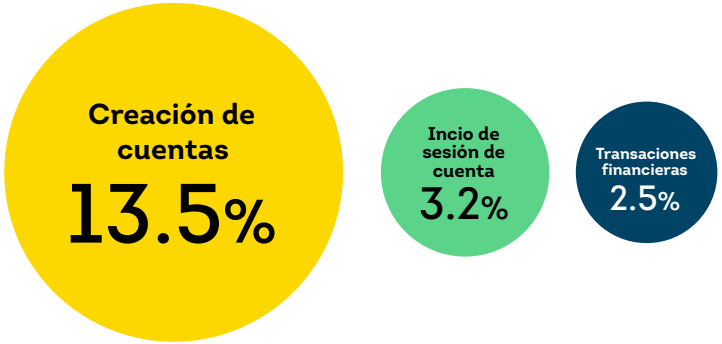
Creación de cuenta: Registro de cuenta, inscripción y originación de créditos.

Inicio de sesión de cuenta: Inicio de sesión y eventos de inicio de sesión fallidos.

Transacciones financieras: Compras, retiros y depósitos.

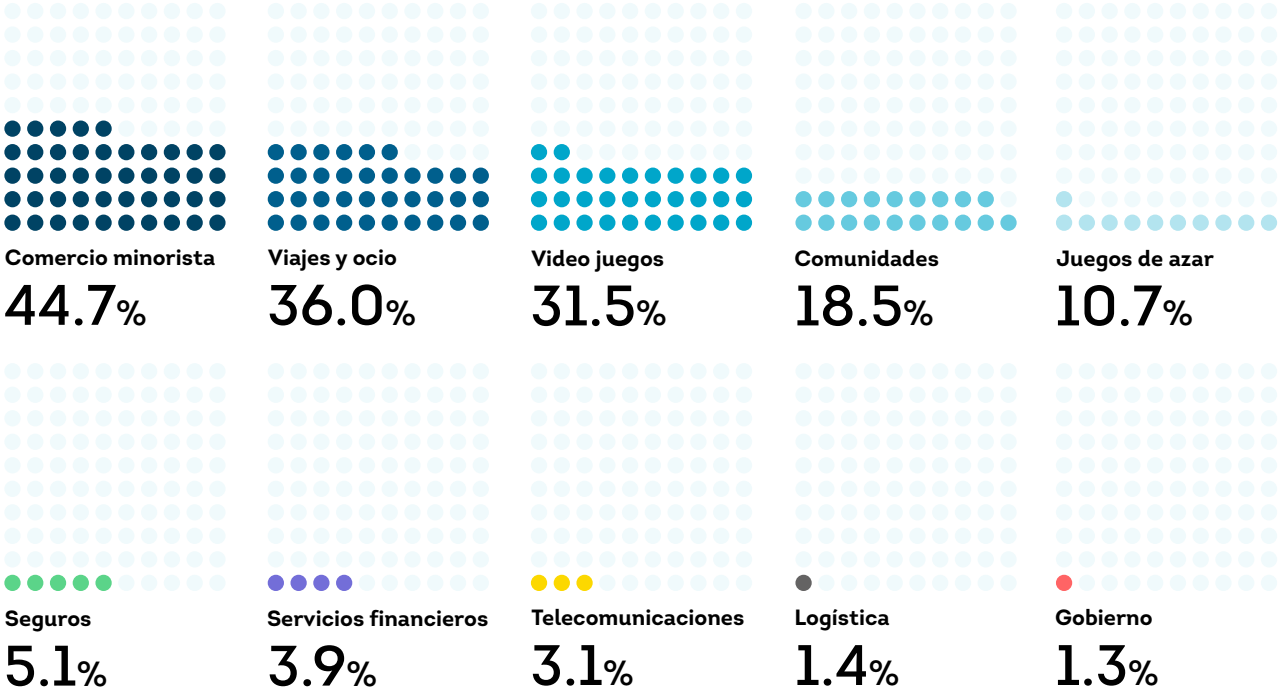
Riesgo de Fraude Digital por tipo de transacción durante el recorrido del cliente

Porcentaje de cada tipo de transacción sospechosa de ser Fraude Digital a nivel mundial en 2023



Fraude Digital en la creación de cuentas por industria

Porcentaje de transacciones de creación de cuentas digitales en cada industria a nivel mundial que fueron sospechosas de Fraude Digital en 2023



Fuente: TransUnion TruValidate

TransUnion

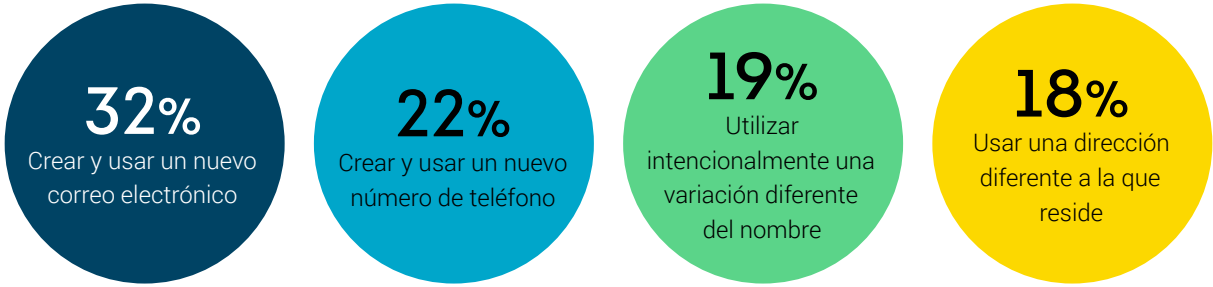
Los consumidores modifican fácilmente su identidad al crear cuentas

Los consumidores de todo el mundo informaron estar dispuestos a modificar sus identidades digitales al establecer nuevas cuentas o solicitar créditos. Muchos minoristas, comunidades en línea, empresas de medios y organizaciones de servicios requieren que los usuarios creen una cuenta, y los consumidores que buscan anonimato pueden ocultar sus identidades al registrarse. Esto podría ser tan simple como usar una dirección de correo electrónico recién creada, informar vivir en una dirección antigua o modificar ligeramente su nombre.

La exposición a los créditos de identidades sintéticas alcanza su máximo histórico

Con una gran cantidad de credenciales de identidad robadas disponibles, los delincuentes están volviéndose muy hábiles en la fabricación de identidades. El porcentaje de identidades sintéticas entre las cuentas abiertas por las entidades de crédito estadounidenses para créditos de vehículo, tarjetas de crédito bancarias, tarjetas de crédito minoristas y créditos de libre inversión no garantizados alcanzó un máximo histórico a finales de 2023, dejando a las entidades de crédito expuestas a pérdidas potenciales de $3.100 millones, también un máximo histórico y un 11% más que a finales de 2022. Las identidades sintéticas entre las cuentas abiertas para las cuatro líneas de crédito aumentaron un 17% en el cuarto trimestre de 2023 en comparación con el tercer trimestre de 2023, alcanzando el 0.19% al final de 2023.

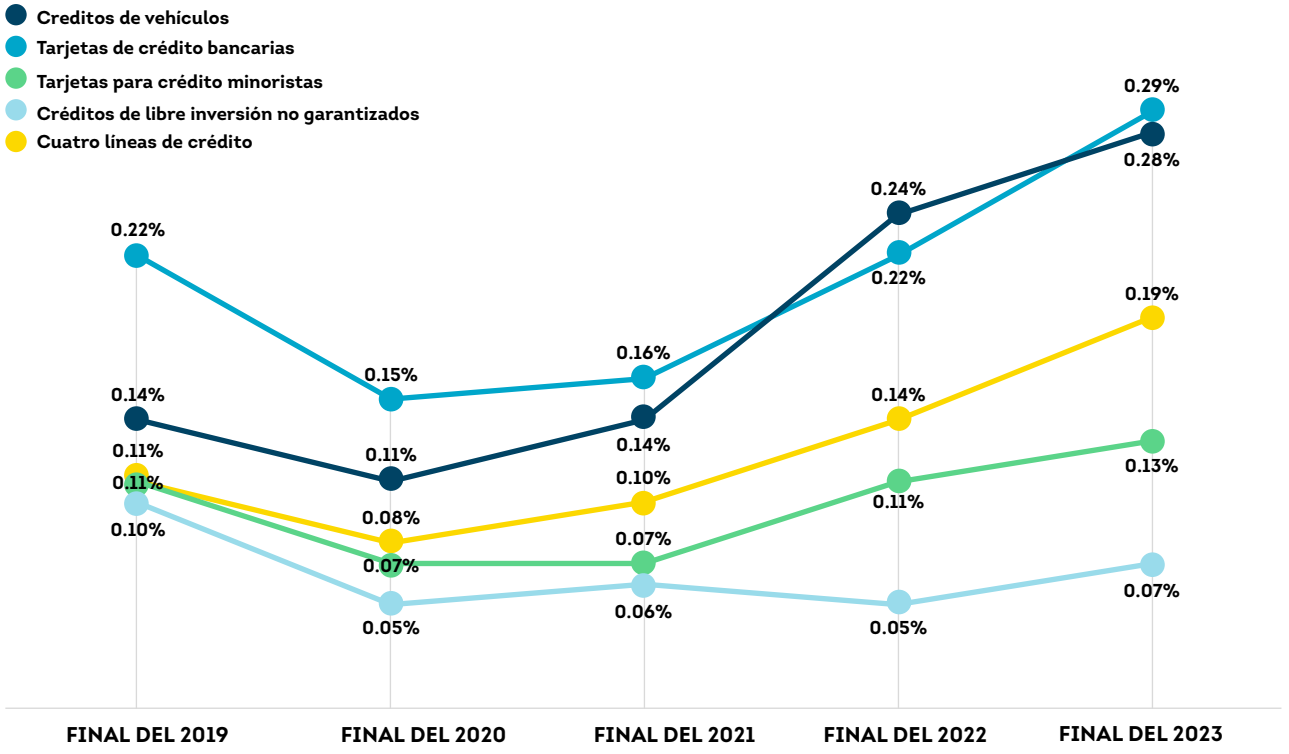
Principales formas en que los consumidores dijeron que modificarían sus atributos de identidad al registrarse para un producto o servicio



Fuente: Encuesta de Fraude al Consumidor de TransUnion

Identidades sintéticas en la apertura de cuentas

Porcentaje de cuentas recién abiertas en Estados Unidos asociadas con identidades sintéticas



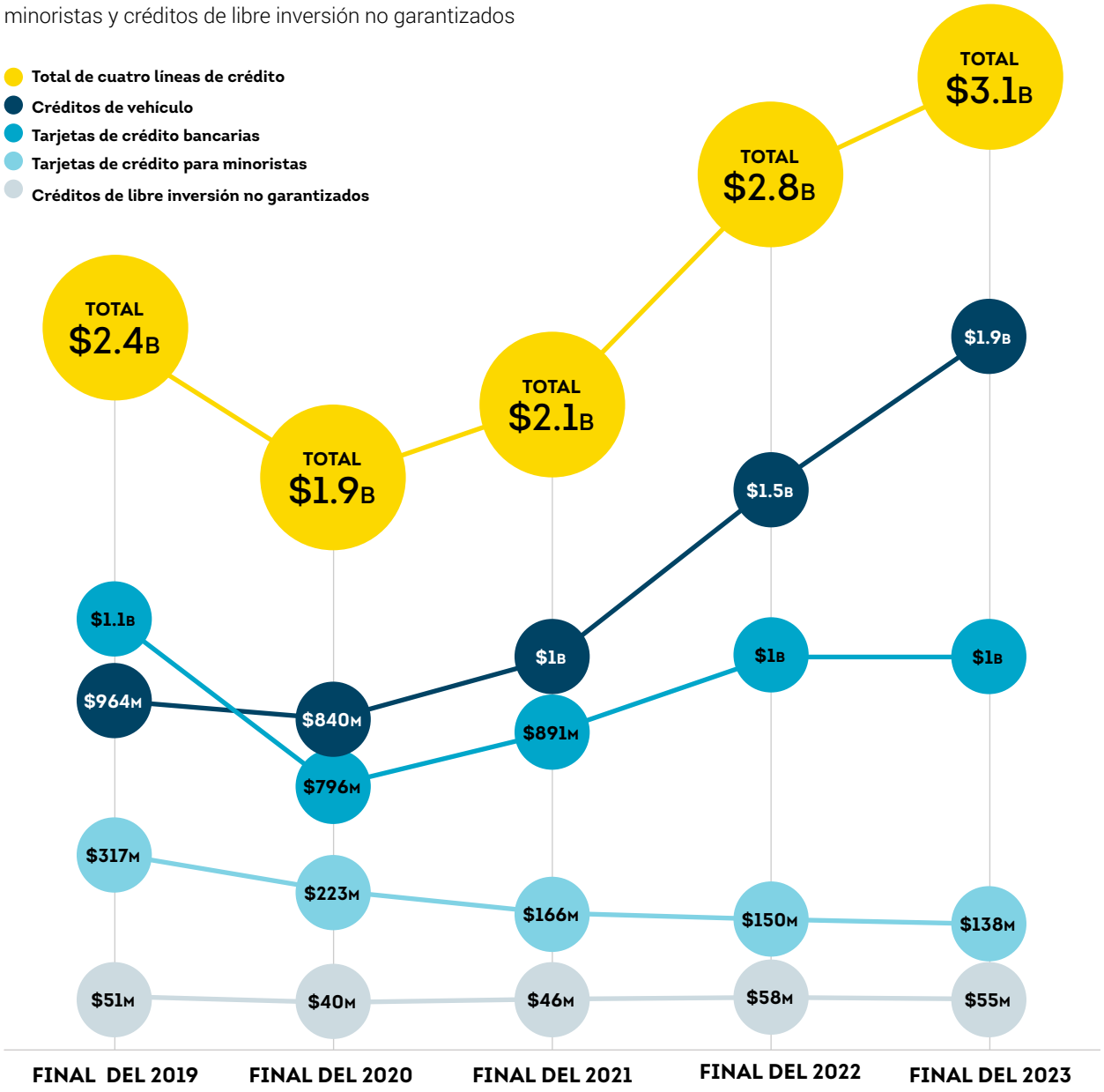
Fuente: TransUnion TruValidate

Los créditos de vehículo de alto valor atraen a los estafadores

Basado en el porcentaje de intentos de apertura de cuentas con identidades sintéticas, el mercado enfrenta una creciente amenaza de cancelaciones en el futuro. Entre las cuentas abiertas utilizando identidades sintéticas, los créditos de vehículo parecían ser los más atractivos para los estafadores para acumular saldos. A finales de 2023, la exposición total de las entidades de crédito a identidades sintéticas para créditos de vehículo tenía saldos un 90% más altos que el sector de tarjetas bancarias, el cual ocupa el segundo lugar entre los tipos de crédito analizados.

Identidades sintéticas: Exposición total de las entidades de crédito

La cantidad total de crédito a la que tienen acceso las identidades sintéticas en Estados Unidos para créditos de vehículo, tarjetas de crédito bancarias, tarjetas de crédito para minoristas y créditos de libre inversión no garantizados



Fuente: TransUnion TruValidate

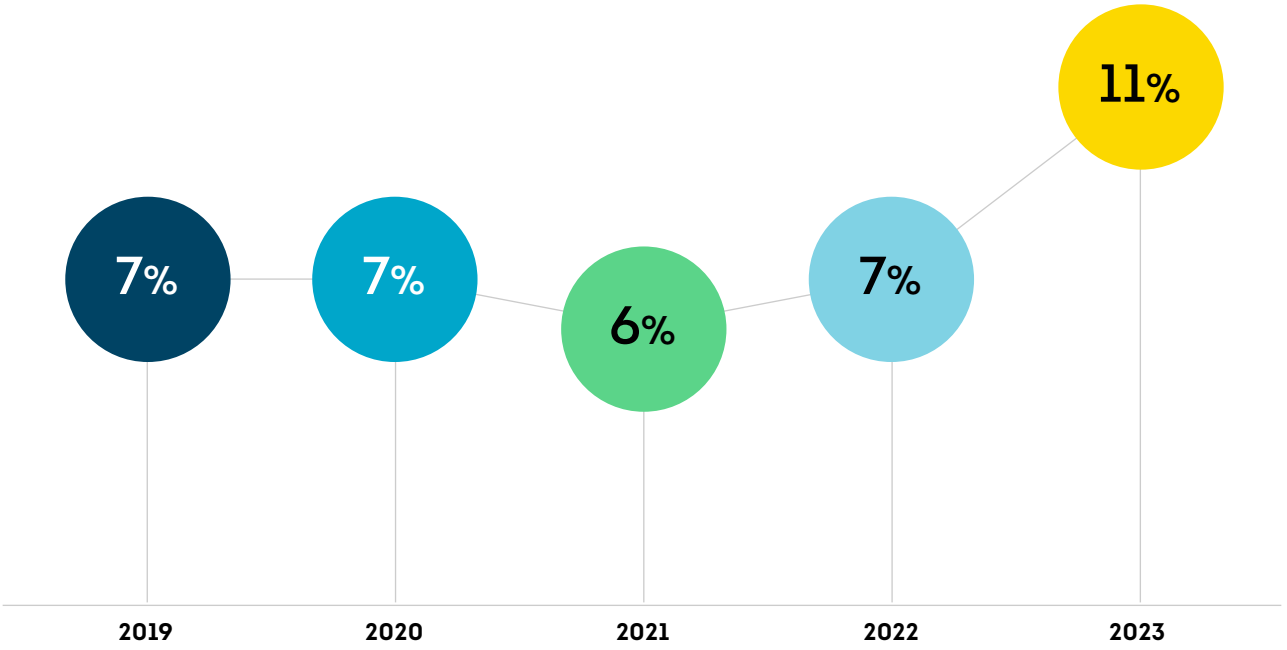
TransUnion

El lavado de crédito (Credit Washing) amplía el riesgo de fraude en la apertura de nuevas cuentas

A medida que aumenta el fraude de identidad, los delincuentes que cometen fraude directo con identidades robadas o sintéticas pueden buscar reciclar una identidad mediante el lavado de crédito, una estafa de manipulación de crédito para eliminar información negativa del historial crediticio de una identidad al presentar falsas reclamaciones de fraude de identidad. Estas disputas falsas en los informes de crédito podrían hacerse contra cuentas abiertas utilizando la identidad de un consumidor robada o una identidad sintética, o transacciones no autorizadas en la cuenta de crédito legítima de un consumidor.

Los consumidores en los Estados Unidos (o sus representantes autorizados) tienen el derecho legal de disputar los registros en sus informes de crédito, y TransUnion sigue un proceso de resolución de disputas altamente regulado. En 2023, las disputas en los Estados Unidos debido a una reclamación de fraude representaron el 11% de todas las disputas, la cifra más alta en cinco años.

Disputas en los informes de crédito de los consumidores de Estados Unidos debido a una reclamación por fraude como porcentaje del total de disputas



Fuente: TransUnion Crédito al Consumidor

Conclusión

En adelante, las organizaciones se enfrentan a técnicas más sofisticadas utilizadas por los ciberdelincuentes que apuntan a los datos de identidad con el fin de llevar a cabo esquemas de fraude directos y a terceros a gran escala. No solo las organizaciones tendrán que lidiar con el hackeo persistente de cuentas, sino que los estafadores seguirán construyendo identidades falsas pero confiables que la tecnología permitirá operar con un alcance y una velocidad sin precedentes.

En cuanto a los consumidores, desean experiencias digitales seguras que fomenten la confianza al realizar transacciones. Y quieren que esas experiencias sean convenientes en cada etapa del recorrido del cliente. Dicho esto, los consumidores también desean controles de autenticación sólidos para garantizar su seguridad, pero no tanto como para convertirse en una molestia. Los líderes en prevención de fraudes deben adoptar un enfoque que abarque a toda la empresa para prevenir el fraude y construir la confianza del cliente. Emplear una estrategia de innovación continua a través de mejores datos, análisis y tecnología para detectar posibles fraudes con mayor precisión y, al mismo tiempo, reducir la fricción para los buenos clientes.

Metodología de obtención de datos

Este informe combina datos exclusivos de la red de inteligencia global de TransUnion y una investigación de consumidores especialmente encargada. La suite TruValidate de TransUnion comprende productos de identidad y fraude que garantizan la confianza en todos los canales y ofrecen experiencias de consumo sin problemas.

Centro de Atención de Llamadas

Los hallazgos del Centro de Atención de Llamadas de TransUnion se basaron en datos de instituciones financieras grandes y pequeñas con sede en Estados Unidos. La tasa o el porcentaje de llamadas de alto riesgo se determinó mediante la evaluación de múltiples factores de riesgo.

Disputas en los informes de crédito de los consumidores

Los hallazgos de disputas en los informes de crédito de los consumidores de TransUnion se basaron en datos de crédito de los consumidores de Estados Unidos, sus estados, territorios, protectorados y bases militares estadounidenses y extranjeras. Estos datos son obtenidos rutinariamente de más de 50 años de información crediticia del consumidor y contienen información crediticia de aproximadamente 400 millones de consumidores.

Encuesta a los consumidores

Esta encuesta en línea a 13,923 adultos fue realizada del 5 al 23 de diciembre de 2023 por TransUnion en colaboración con el proveedor de investigación de terceros, Dynata. Se encuestó a adultos de 18 años en adelante que residían en 18 mercados globales (Brasil, Canadá, Chile, Colombia, República Dominicana, Hong Kong, India, Kenia, México, Namibia, Filipinas, Puerto Rico, Ruanda, Sudáfrica, España, Reino Unido, EE. UU. y Zambia) utilizando un método de panel de investigación en línea a través de una combinación de dispositivos de escritorio, móviles y tabletas. Las preguntas de la encuesta se administraron en chino (Hong Kong), inglés, francés (Canadá), portugués (Brasil) y español (Colombia, República Dominicana, México, Puerto Rico y España). Para garantizar una representación equilibrada en cuanto a la demografía de los residentes, la encuesta incluyó cuotas para equilibrar las respuestas en cuanto a las principales características demográficas como la edad, el género y el ingreso. Por favor, tenga en cuenta que algunos porcentajes en los gráficos pueden no sumar 100% debido al redondeo o la aceptación de múltiples respuestas.

Filtraciones de datos

TransUnion TruEmpower obtiene sus datos exclusivos sobre filtraciones cibernéticas en colaboración con el Identity Theft Resource Center (ITRC). El personal de ITRC rastrea todos los eventos de exposición de datos públicamente reportados en Estados Unidos, provenientes de fuentes que incluyen comunicados de prensa de entidades filtradas de fiscales generales estatales, bufetes de abogados, expertos en ciberseguridad y más. TransUnion amplía los datos de ITRC con un proceso que calcula los riesgos principales de cada filtración, pasos de acción apropiados para los consumidores y el Puntaje de Riesgo de Filtración (BRS). El BRS se basa en la cantidad y la gravedad de los datos de identidad particulares que la entidad afectada determinó que fueron expuestos. De entre 60 opciones posibles de credenciales de identidad, cada filtración se somete al Perfil de Amenazas de Identidad de TruEmpower para producir un puntaje y un patrón de riesgo, y acciones recomendadas para los consumidores. El Puntaje de Riesgo de Filtración utiliza una escala del 1 al 10, donde 1 representa el menos grave y 10 representa el más grave.

Fraude Digital

TransUnion utiliza inteligencia de miles de millones de transacciones originadas en más de 40.000 sitios web y aplicaciones para proteger las transacciones digitales. La tasa o el porcentaje de intentos de Fraude Digital sospechosos refleja aquellos que los clientes de TransUnion determinaron que cumplían con una de las siguientes condiciones: 1) negación en tiempo real debido a indicadores de fraude, 2) negación en tiempo real por violaciones de la política corporativa, 3) fraudulenta tras la investigación del cliente, o 4) una violación de política corporativa tras la investigación del cliente, en comparación con todas las transacciones evaluadas. Los análisis por país y región examinaron las transacciones en las que el consumidor o el presunto estafador estaban ubicados en un país o región seleccionado al realizar una transacción. La estadística global representa todos los países del mundo y no solo los países y regiones seleccionados.

Fraude sintético

TransUnion's synthetic fraud findings were based on US consumer credit data from the US states, territories, protectorates, and US and overseas military bases. It's routinely sourced from more than 50 years of consumer credit data and contains credit information from approximately 400 million consumers. The synthetic fraud analysis encompasses US credit activity recorded between Jan. 1, 2009 and June 30, 2023. The lender exposure measures were based upon TransUnion's proprietary formula to capture potential total loss at risk for lenders.

Acerca de TransUnion TruValidate

Tru Validate organiza información de identidad, dispositivos y comportamiento para ayudar a las organizaciones a interactuar con confianza y seguridad con los consumidores en todos los canales y en cada etapa del recorrido del cliente, mejorando las conversiones, reduciendo las pérdidas por fraude y ofreciendo experiencias de usuario mejoradas y sin fricciones.

https://www.transunion.do/solucion/truvalidate

TransUnion