TransUnion

ACTUALIZACIÓN H2 2024

INFORME DEL FRAUDE OMNICANAL

Tendencias y estrategias para proteger a las organizaciones y a los consumidores

Introducción

Los líderes empresariales reconocen que cada año se enfrentan potencialmente a pérdidas significativas de ingresos y a un aumento de los costos operativos debido al fraude. Los ciberdelincuentes están robando más información de identidad de organizaciones e individuos para abrir nuevas cuentas a nombre de los consumidores, creando cuentas fraudulentas, incluido un número récord de cuentas sintéticas, o engañando a los consumidores para que compartan el acceso a sus cuentas. Al adoptar una postura de amenaza que asume que la información del consumidor está comprometida, las organizaciones que construyen confianza en el consumidor mediante la mejora de sus experiencias omnicanal con capacidades de detección y prevención de fraudes sin fricciones, tienen la posibilidad de ganar. Es decir, emplear datos mejorados de identidad y señales de riesgo, reglas de fraude centralizadas y tecnología integrada para garantizar la confianza en la autenticidad de las personas con las que tratan, independientemente del canal.

Todos los datos de este informe combinan conocimientos exclusivos de la red global de inteligencia de TransUnion, una encuesta empresarial encargada especialmente por TransUnion en Canadá, India, Reino Unido y Estados Unidos, y una encuesta al consumidor encargada especialmente por TransUnion en 18 países y regiones de todo el mundo. A lo largo de este informe, H1 (la primera mitad del año) corresponde del 1 de enero al 30 de junio, y H2 (la segunda mitad del año) corresponde del 1 de julio al 31 de diciembre.

PRINCIPALES CONCLUSIONES

El costo del fraude representó un riesgo financiero significativo para las organizaciones

6.5%
de los ingresos equivalentes en promedio se perdió debido al fraude, lo que representa USD$ 359 mil millones en pérdidas por fraude en el último año, entre 801 líderes empresariales encuestados en Canadá, India, Estados Unidos y Reino Unido.

75%
de los líderes empresariales indicaron que el fraude aumentó o se mantuvo igual en el último año.

La preocupación por el fraude sigue siendo alta para las empresas y los consumidores

5.2%
de todas las transacciones digitales a nivel mundial fueron sospechosas de Fraude Digital en el primer semestre de 2024, según la red de inteligencia global de TransUnion.

49%
de los consumidores en 18 países y regiones seleccionadas informaron haber sido objeto de intentos de fraude por correo electrónico, en línea, llamadas telefónicas y mensajes de texto en el segundo trimestre de 2024, según una encuesta de consumidores de TransUnion.

La creación de nuevas cuentas representó el mayor riesgo de fraude

6.5%
de todos los intentos de apertura de cuentas digitales a nivel mundial fueron sospechosos de Fraude Digital, según la red de inteligencia global de TransUnion; esta cifra fue la más alta en el recorrido del cliente.

USD$ 3.200 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 julio de 2024 (nivel más alto jamás registrado). El porcentaje de identidades sintéticas entre las cuentas abiertas en el primer semestre de 2024 también es el más alto de la historia, según la red de inteligencia global de TransUnion.

Contenidos

Experiencias de fraude de los líderes empresariales

El costo del fraude

Proteger a los clientes y sus negocios del fraude es esencial para la salud y el éxito de las organizaciones. Los líderes empresariales encuestados en Canadá, India, Estados Unidos y Reino Unido informaron que, en promedio, sus empresas perdieron el equivalente al 6.5% de los ingresos debido al fraude en el último año. Esto representa un total de USD$359 mil millones en pérdidas por fraude entre los 801 líderes empresariales encuestados.

Casi un tercio (31%) de los líderes empresariales mencionó el fraude por estafa/fraude autorizado como la causa más significativa de las pérdidas por fraude reportadas, seguidos por el fraude de terceros (17%). Mientras que el 75% informó que todos los tipos de fraude medidos se mantuvieron igual o aumentaron en el último año, casi la mitad (49%) señaló que el fraude por estafa/fraude autorizado aumentó más: 10 puntos porcentuales más que cualquier otro tipo de fraude.

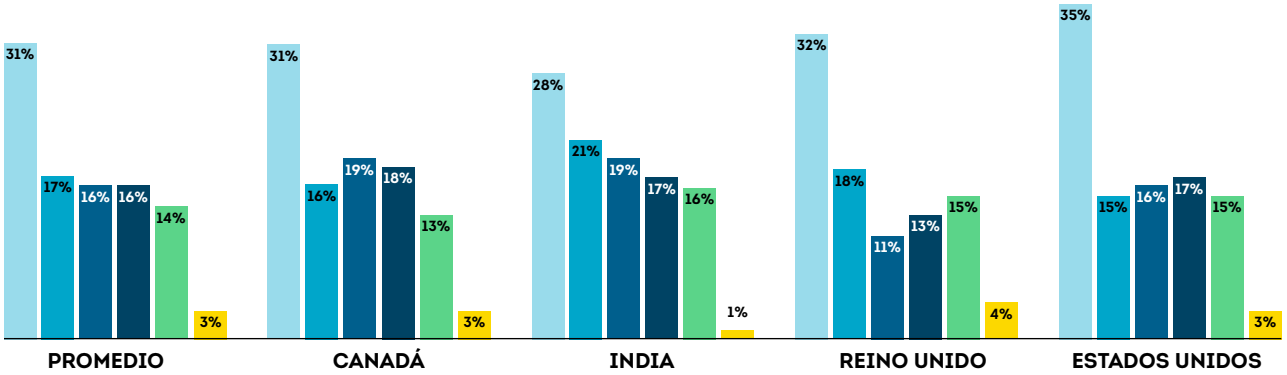
Costo total del fraude

Los líderes empresariales indicaron el porcentaje de ingresos que sus empresas perdieron debido al fraude en el último año y la cantidad monetaria correspondiente.

*La conversión a USD se basa en el valor de cambio del 5 de agosto de 2024

Causa más prominente de pérdidas por fraude

- **Fraude por estafa/fraude autorizado**
  Esquema deshonesto destinado a engañar a una persona para que renuncie a algo de valor (por ejemplo, acceso a cuentas, dinero, información).
- **Fraude de terceros**
  El uso de una identidad robada para abrir una cuenta
- **Apropiación de cuentas**
  Individuos no autorizados tomando el control de una cuenta en línea de alguien (por ejemplo, banca, redes sociales, correo electrónico) sin su permiso
- **Fraude de identidad sintética**
  Uso de una combinación de información de identificación personal para fabricar una persona o entidad con el fin de cometer un acto deshonesto para obtener un beneficio financiero o personal
- **Fraude en primera persona**
  Representación incorrecta de identidad o falsificación de información con el propósito de obtener beneficios financieros.
- **Otro**



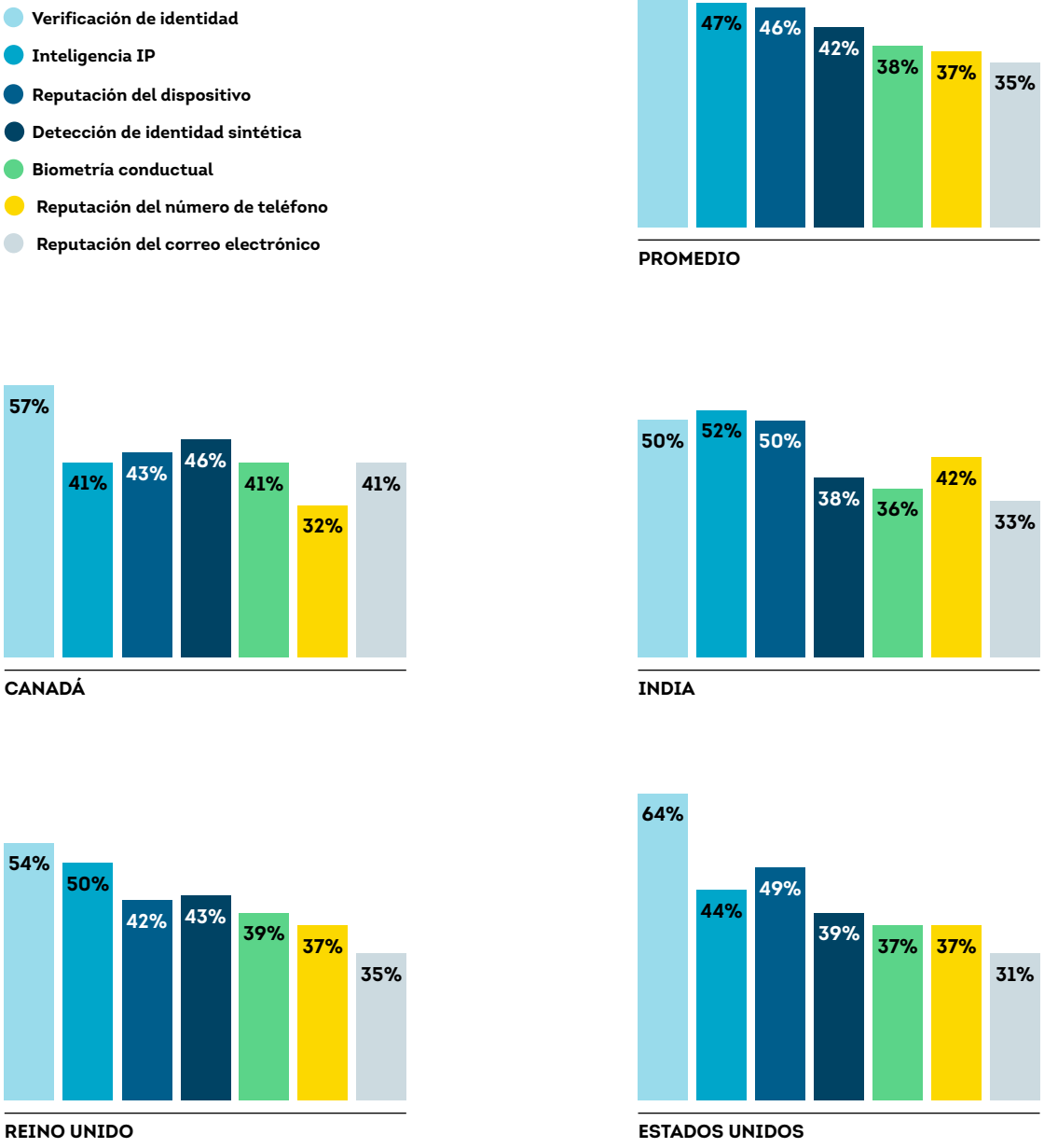
Fuente: Encuesta empresarial de TranUnion

TransUnion

Tecnología más efectiva para la prevención de fraude

Dada la complejidad del fraude y el riesgo que entrañan las identidades comprometidas de los consumidores, las organizaciones utilizan una variedad de datos, señales de riesgo, tecnología y herramientas para prevenir el fraude. Más de la mitad (56%) de los líderes empresariales encuestados en general clasificaron la verificación de identidad como la tecnología más eficaz para prevenir el fraude, y casi dos tercios (64%) de los líderes empresariales estadounidenses dijeron lo mismo (ambos con el porcentaje declarado más alto).

Tecnología clasificada como la más efectiva para prevenir el fraude

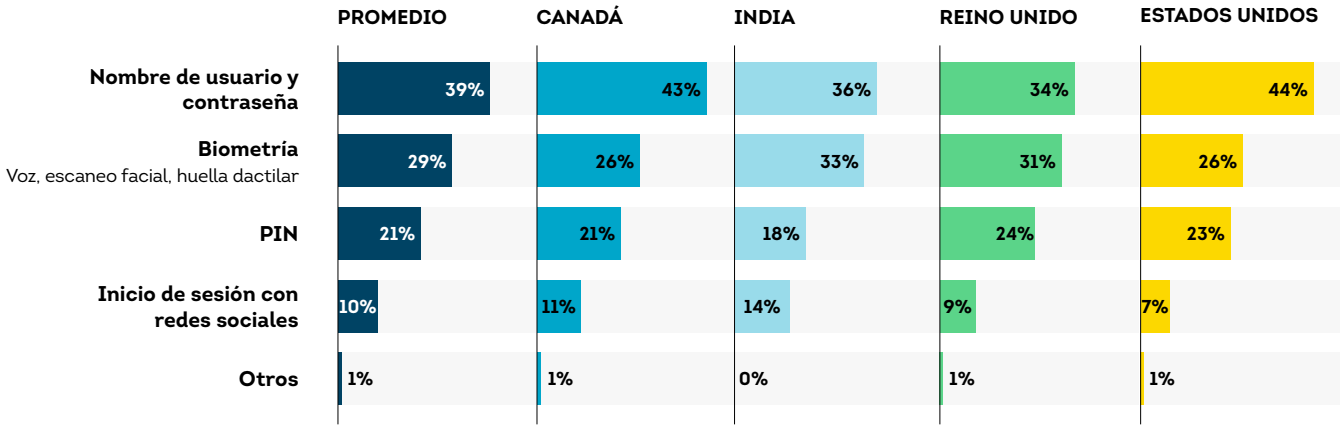


Fuente: Encuesta empresarial de TransUnion

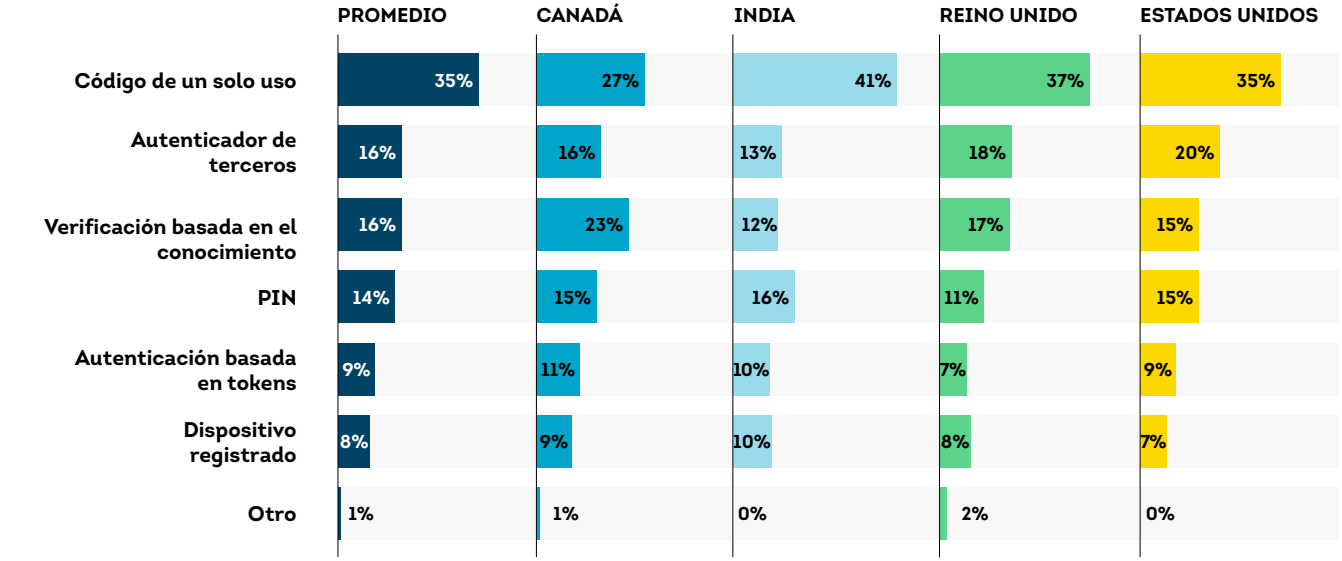
Utilización de métodos de autenticación de identidad

Mientras las credenciales de los usuarios estaban amenazadas por filtraciones de datos y estafas dirigidas a consumidores, el 39% de los líderes empresariales indicó que utilizan nombres de usuario y contraseñas como sus métodos principales de autenticación de clientes, siendo este el porcentaje más alto. Otro 29% indicó que la biometría es el método principal de autenticación. Los códigos de un solo uso fueron el segundo método más popular para la autenticación de clientes, con un 35% de los líderes empresariales indicando que los utilizan.

Método principal utilizado para autenticar a los clientes



Método secundario utilizado para autenticar a los clientes



Fuente: Encuesta empresarial de TransUnion

Tendencias de la exposición de datos de identidad

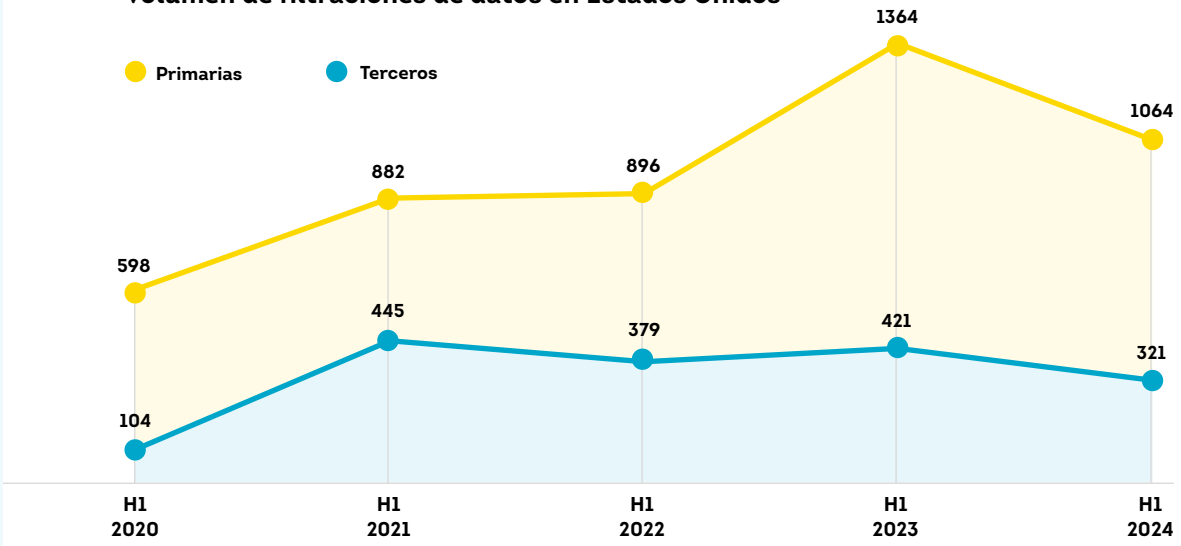
Los criminales siguieron decididos a adquirir datos de identidad de los consumidores, dirigiéndose a organizaciones y consumidores para alimentar esquemas de fraude. Aproximadamente la mitad (49%) de todos los consumidores encuestados en 18 países y regiones en el segundo trimestre de 2024 afirmaron haber sido objeto de estafas fraudulentas a través de correos electrónicos, en línea, llamadas telefónicas y mensajes de texto en los últimos tres meses. Además, la gravedad de las filtraciones de datos en Estados Unidos alcanzó niveles históricos en la primera mitad de 2024.

Las violaciones de datos en EE. UU. alcanzaron una gravedad récord.

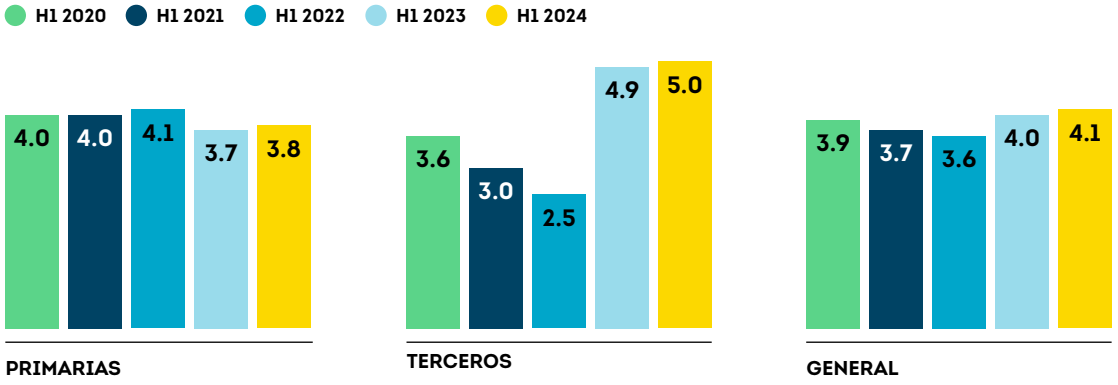
Dado que las violaciones de datos son un indicador adelantado de futuros fraudes, las organizaciones estadounidenses informaron de cientos de violaciones digitales y físicas en la primera mitad del año. Mientras que el volumen de filtraciones de datos en Estados Unidos disminuyó un 22% año contra año en el primer semestre de 2024, la gravedad media del riesgo de filtración (la capacidad de una filtración para permitir el fraude de identidad), medida por el Puntaje de Riesgo de Filtración (BRS, por sus siglas en inglés) TruEmpower™ de TransUnion®, aumentó un 3% año contra año durante ese periodo. Esta fue la cifra más alta medida en un período H1 desde que TransUnion comenzó a analizar en 2020.

Los criminales continúan enfocándose en los proveedores de servicios de terceros como fuente de múltiples credenciales de consumidores. Según datos de TransUnion, las filtraciones de terceros fueron más graves en el primer semestre de 2024, con un Puntaje de Riesgo de Filtración (BRS) promedio un 32% más alto que el de las filtraciones primarias.

Volumen de filtraciones de datos en Estados Unidos



Puntaje promedio de riesgo de filtración de datos en Estados Unidos



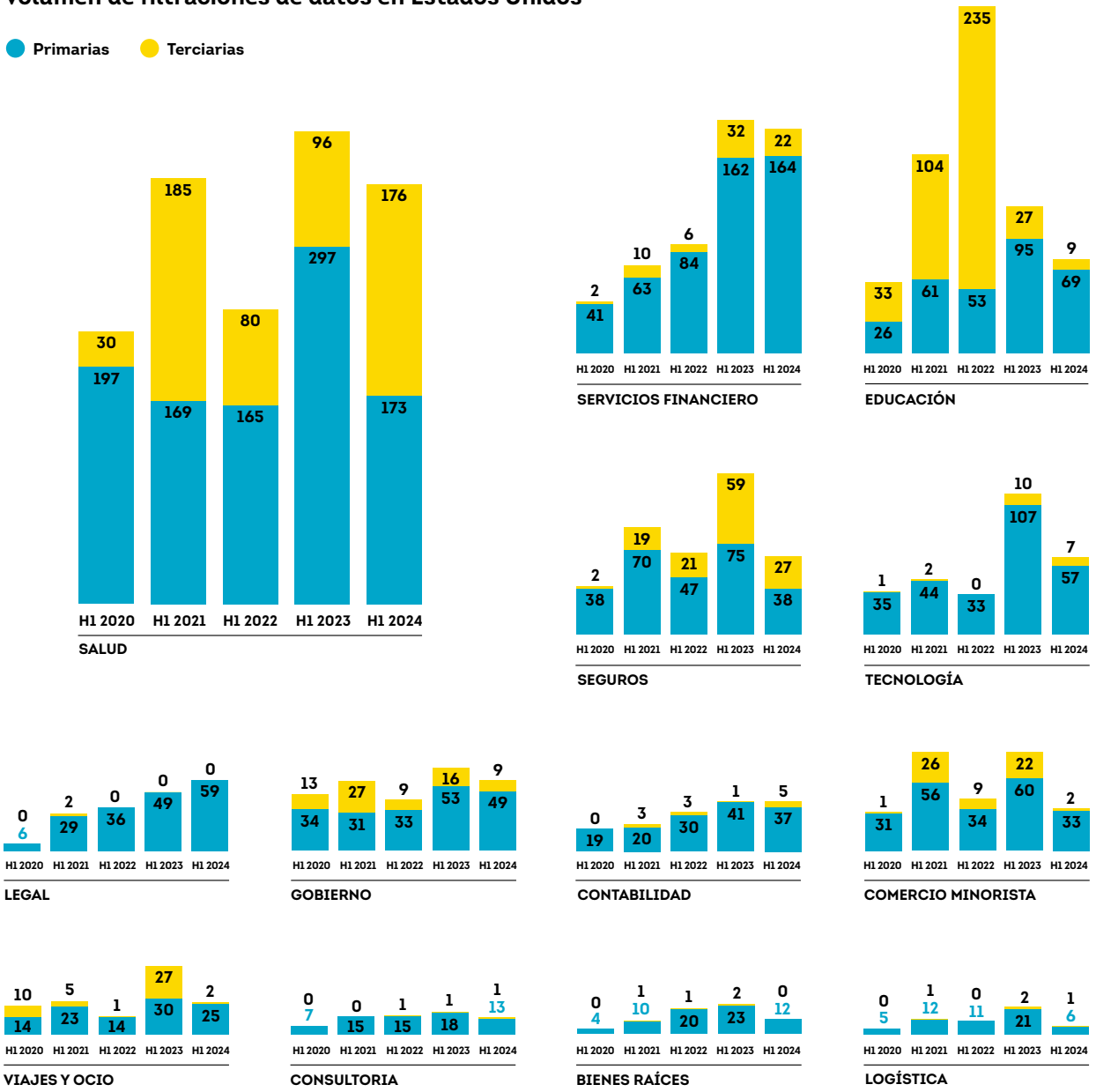
Una violación de datos primaria representa un ataque directo a una organización. Una violación de datos de terceros, también conocida como ataque a la cadena de suministro, ataque a la cadena de valor o violación de puerta trasera, se produce cuando un atacante accede a la red de una entidad a través de terceros vendedores o proveedores. Por ejemplo, procesamiento de nóminas o facturación médica.

Fuente: TransUnion TruEmpower

Los sectores de salud y servicios financieros experimentaron la mayoría de las filtraciones de datos

Según TransUnion, en el primer semestre de 2024 el sector salud fue el que experimentó el mayor número de filtraciones, seguido por servicios financieros y educación. La salud no solo registró el mayor volumen de filtraciones, sino que TransUnion descubrió que también fueron las más graves durante ese periodo, con un BRS de 5,4, seguidas de contabilidad (4,0) y administración pública (4,0).

Volumen de filtraciones de datos en Estados Unidos



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

Fuente: TransUnion TruEmpower

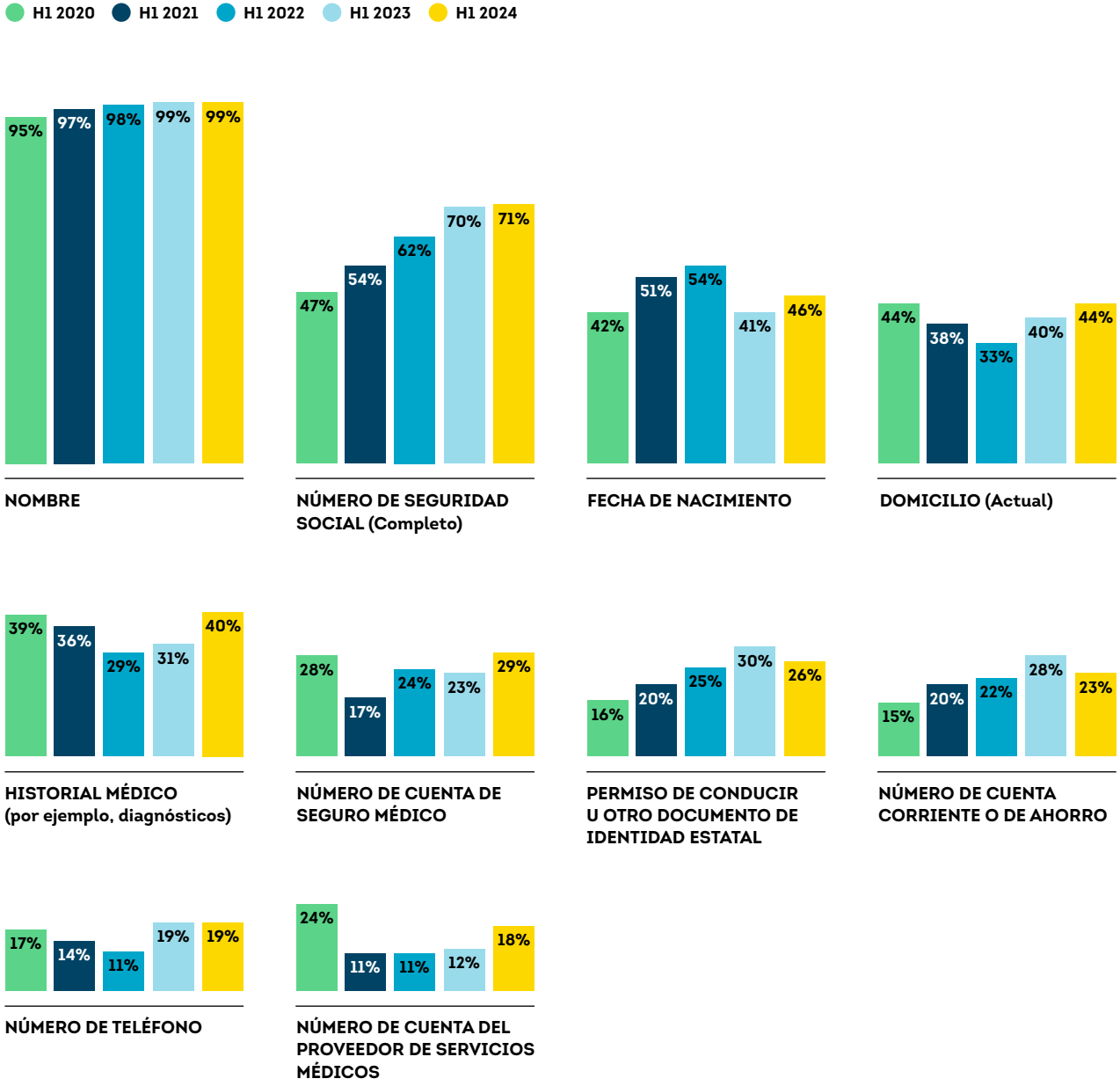
Las credenciales de identidad fueron el objetivo principal de las filtraciones de datos

Los delincuentes vulneraron los sistemas de las organizaciones para robar las credenciales de identidad de los consumidores necesarias para abrir cuentas fraudulentas y crear identidades sintéticas. En el primer semestre de 2024, TransUnion descubrió que en el 71% de las violaciones de datos se expusieron los números completos de la Seguridad Social, en el 46% las fechas de nacimiento y en el 44% las direcciones particulares.

La exposición de datos del sector salud experimentó un crecimiento significativo en el primer semestre de 2024. Los historiales médicos se incluyeron en el 40% de las filtraciones, un aumento año contra año del 29%, y en el 71% de las filtraciones a terceros, un aumento del 58%. De igual forma, se observó un aumento en el robo de los datos de la industria de tarjetas de pago (PCI, por sus siglas en inglés) de las organizaciones de servicios financieros: la exposición de número de tarjeta de crédito o débito aumentó un 69%, las fechas de caducidad un 136%, los códigos de seguridad un 79% y el nombre del titular de la tarjeta un 85%.

Las 10 credenciales de identidad más expuestas en las violaciones de datos en Estados Unidos H1 2024

Porcentaje de credenciales expuestas en una filtración de datos



Fuente: TransUnion TruEmpower

TransUnion

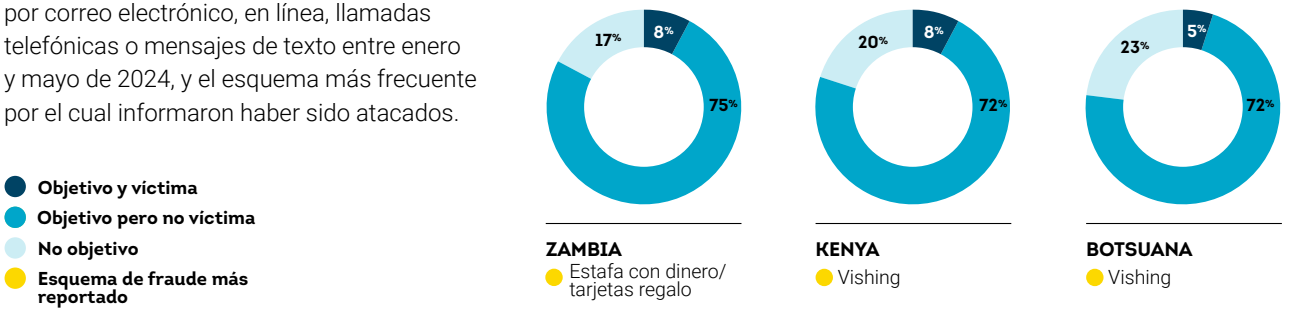
Los consumidores informaron ser blanco de estafas de fraude de manera regular

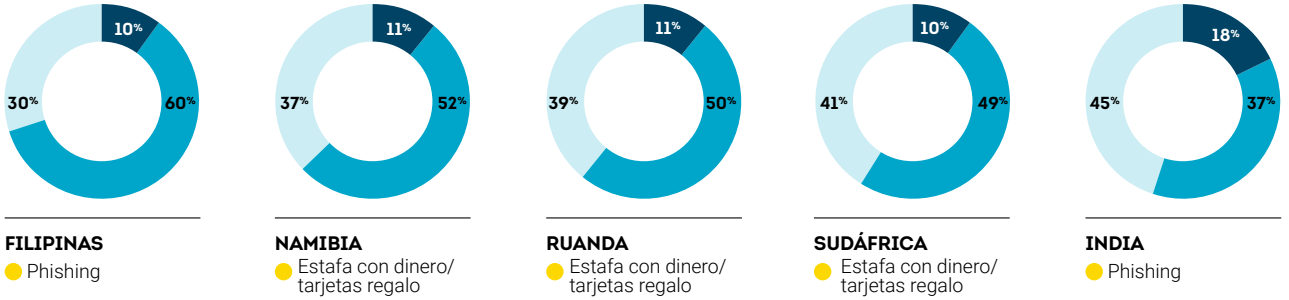
Casi la mitad (49%) de los consumidores informaron haber sido blanco de estafas de fraude por correo electrónico, en línea, llamadas telefónicas o mensajes de texto, y el 9% dijo haber sido víctima entre enero y mayo de 2024, según la Encuesta Consumer Pulse de TransUnion del segundo trimestre de 2024. Sin embargo, una parte significativa de la población no reconoció el fraude potencial: el 51% dijo no estar consciente de haber sido objeto de esquemas fraudulentos. Entre quienes afirmaron haber sido objeto de fraude, el smishing (37%), el phishing (34%) y el vishing (33%) fueron los tipos de fraude más comunes experimentados a nivel mundial.

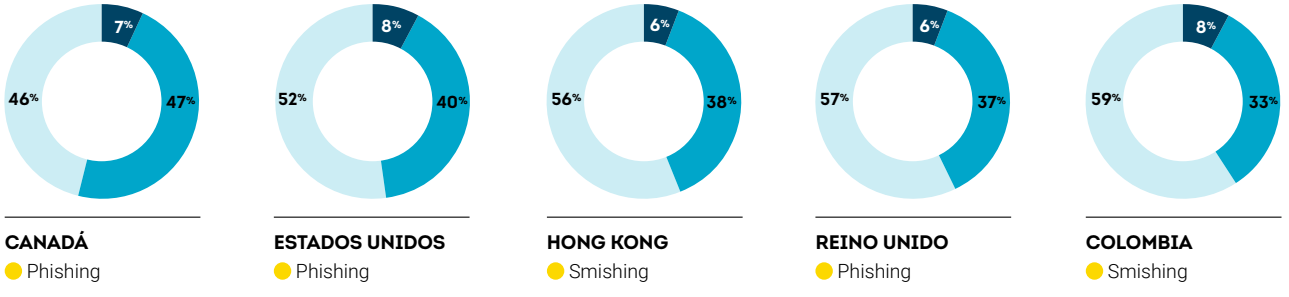
Consumidores objetivo de fraude

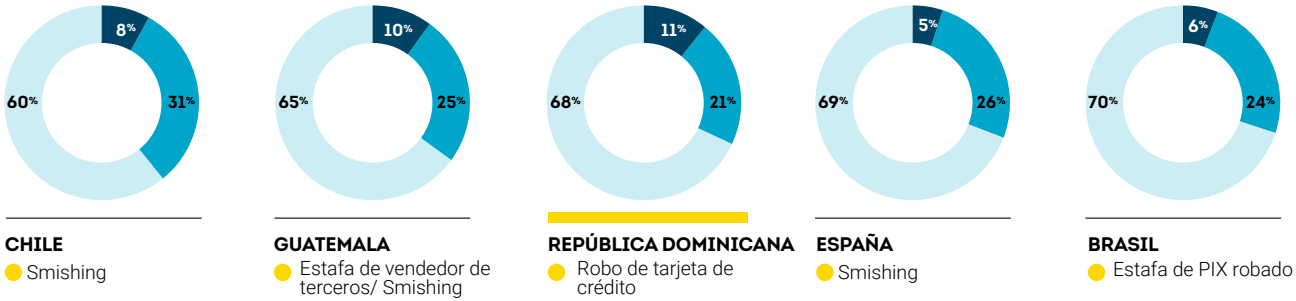
Porcentaje de consumidores que dijeron haber sido objetivo de intentos de fraude por correo electrónico, en línea, llamadas telefónicas o mensajes de texto entre enero y mayo de 2024, y el esquema más frecuente por el cual informaron haber sido atacados.

- **Objetivo y víctima**
- **Objetivo pero no víctima**
- **No objetivo**
- **Esquema de fraude más reportado**









Fuente: Encuesta consummer Pulse de TransUnion del segundo trimestre de 2024

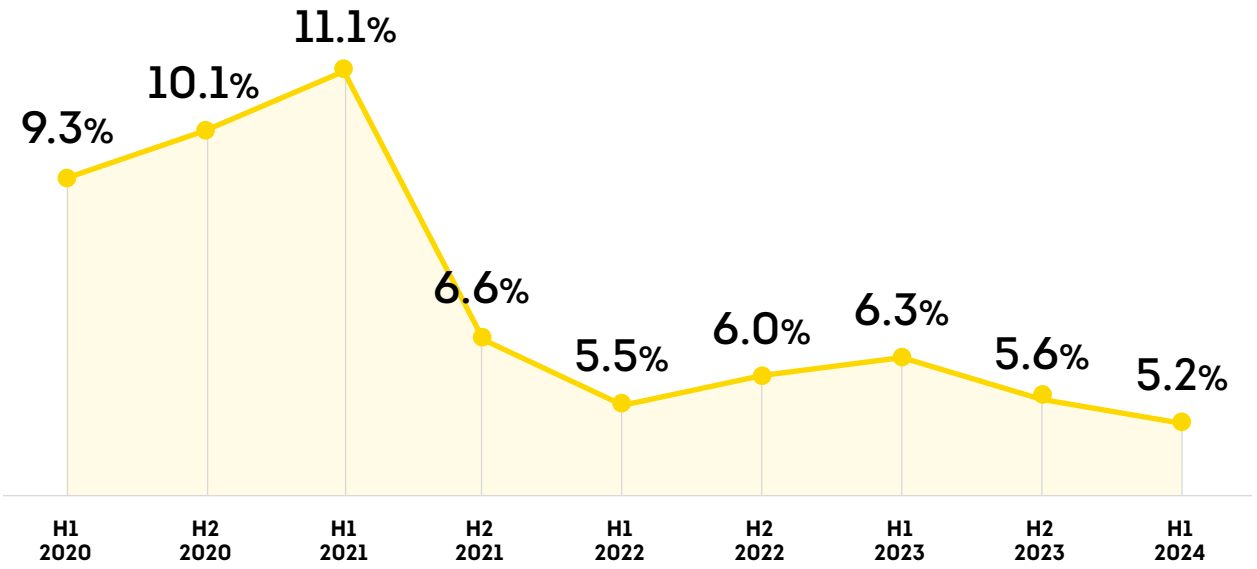
Tendencias globales de Fraude Digital

El riesgo de Fraude Digital sospechoso se mantuvo elevado

El Fraude Digital continuó su patrón histórico de oleadas, sin embargo, se mantiene alto. La tasa de Fraude Digital sospechoso a nivel global entre los clientes de TransUnion TruValidate™ cayó al 5.2% en el primer semestre de 2024, desde el 5.6% en el segundo semestre de 2023 y el 6.3% en el primer semestre de 2023. Como se observó en informes anteriores, el riesgo de fraude digital difiere según el país en el que se encontraba el consumidor al intentar realizar una transacción, la industria y el tipo de transacción.

De los 19 mercados, siete (Brasil, Canadá, Chile, Colombia, India, México y Filipinas) experimentaron un aumento en la tasa de Fraude Digital sospechoso año contra año en el primer semestre de 2024. Además, siete mercados (Brasil, Canadá, Colombia, República Dominicana, Hong Kong, India y Filipinas) tuvieron tasas de Fraude Digital sospechoso superiores al promedio global del 5.2% en el primer semestre de 2024.

Tasa de sospecha de Fraude Digital

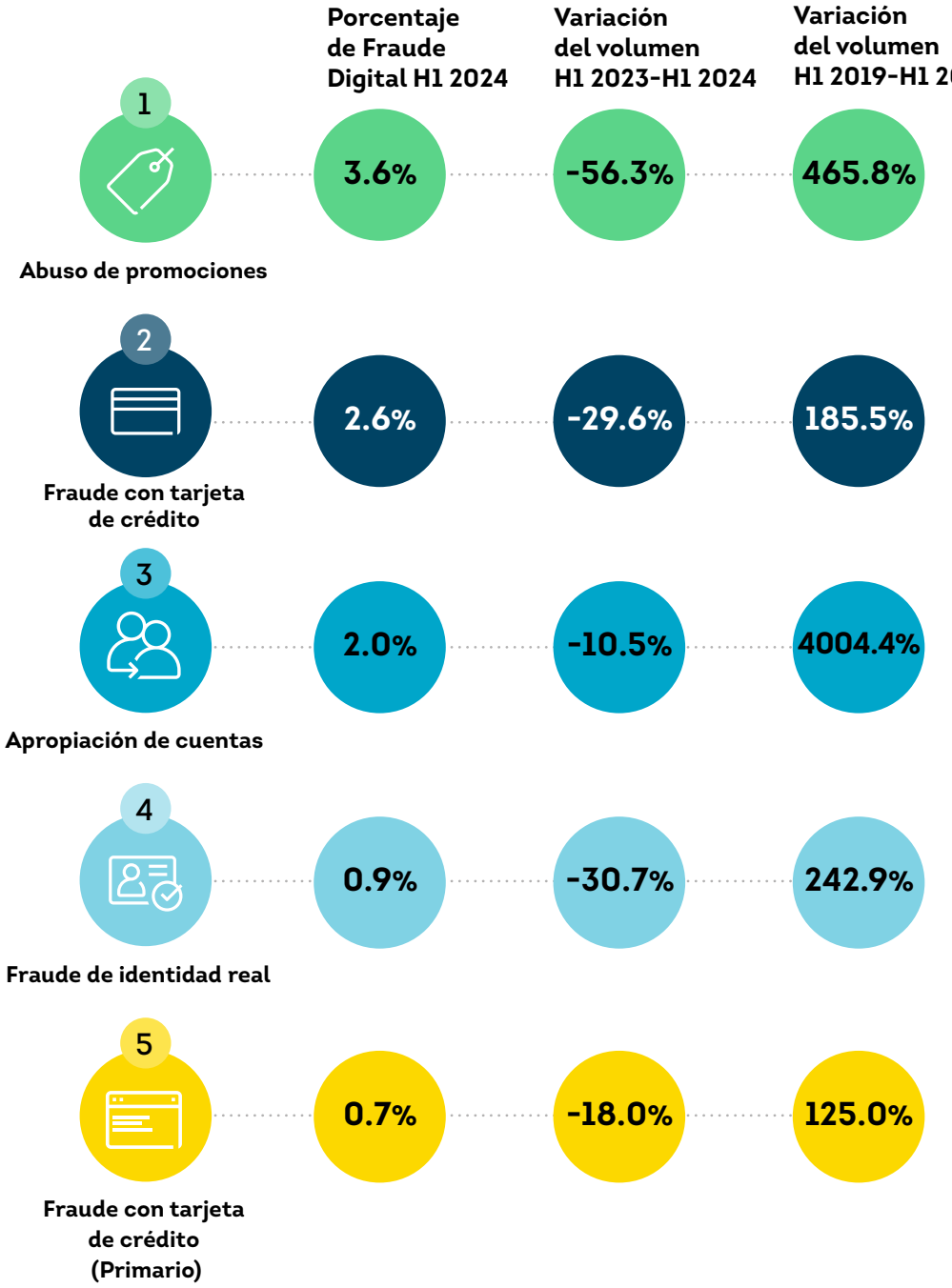


Fuente: TransUnion TruValidate

El abuso de promociones encabezó la lista de los tipos de fraude más comunes

Con un 3.6%, el abuso de promociones (consumidores o estafadores que aprovechan ofertas de marketing para recibir incentivos financieros no intencionados) fue el tipo principal de Fraude Digital reportado a TransUnion por sus clientes a nivel global en el primer semestre de 2024, aproximadamente un tercio más que el fraude con tarjetas de crédito (2.6%). Sin embargo, el fraude de identidad sintética (aumento del 153%) fue el tipo de Fraude Digital de más rápido crecimiento en términos de volumen desde el segundo semestre de 2023 hasta el primer semestre de 2024, y el fraude en pagos ACH/débito (aumento del 113%) fue el de más rápido crecimiento año contra año en el primer semestre de 2024, según los clientes de TransUnion.

Principales tipos de fraude y su crecimiento



Fuente: TransUnion TruValidate

La industria de comunidades experimentó las tasas más altas de Fraude Digital

La industria de comunidades, que incluye propiedades web como foros en línea y sitios web de citas, experimentó el mayor porcentaje (11.5%) de Fraude Digital sospechoso a nivel global en el primer semestre de 2024, según datos de TruValidate por TransUnion, lo que representa un aumento del 23% en la tasa y del 22% en el volumen de Fraude Digital sospechoso en comparación con el primer semestre de 2023. Los usuarios de comunidades en línea dependen de las organizaciones para proporcionar confianza y seguridad mientras utilizan sus plataformas. Sin embargo, los clientes de comunidades de TransUnion informaron que la falsificación de perfiles fue el tipo de Fraude Digital más frecuente que presenciaron en el primer semestre de 2024.

Intentos de Fraude Digital global por industria

- **Tasa de intentos de Fraude Digital sospechosos H1 2024**
- **Principal tipo de fraude H1 2024**
- **Variación en el volumen de sospecha de Fraude Digital H1 2023- H1 2024**

Comunidades
(citas en línea, foros, etc.)

H1 2024
11.5%
Falsificación de perfil

H1 2023-H1 2024
+22.3%

Videojuegos

H1 2024
11.4%
Estafa/Solicitud

H1 2023-H1 2024
-6.3%

Comercio minorista

H1 2024
7.3%
Abuso de promoción

H1 2023-H1 2024
-61.1%

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

H1 2024
7.2%
Abuso de promoción

H1 2023-H1 2024
-9.2%

Servicios financieros

H1 2024
4.6%
Apropiación de cuenta

H1 2023-H1 2024
-3.6%

Logística

H1 2024
2.9%
Fraude de envío

H1 2023-H1 2024
+120.7%

Telecomunicaciones

H1 2024
2.4%
Fraude de identidad real

H1 2023-H1 2024
-89.2%

Seguros

H1 2024
1.8%
Broker fantasma

H1 2023-H1 2024
-32.4%

Gobierno

H1 2024
1.6%
n/a*

H1 2023-H1 2024
+13.3%

*N/A - El número de clientes que informaron sobre tipos de Fraude Digital no fue lo suficientemente significativo desde el punto de vista estadístico como para ser reportado.

Viajes y ocio

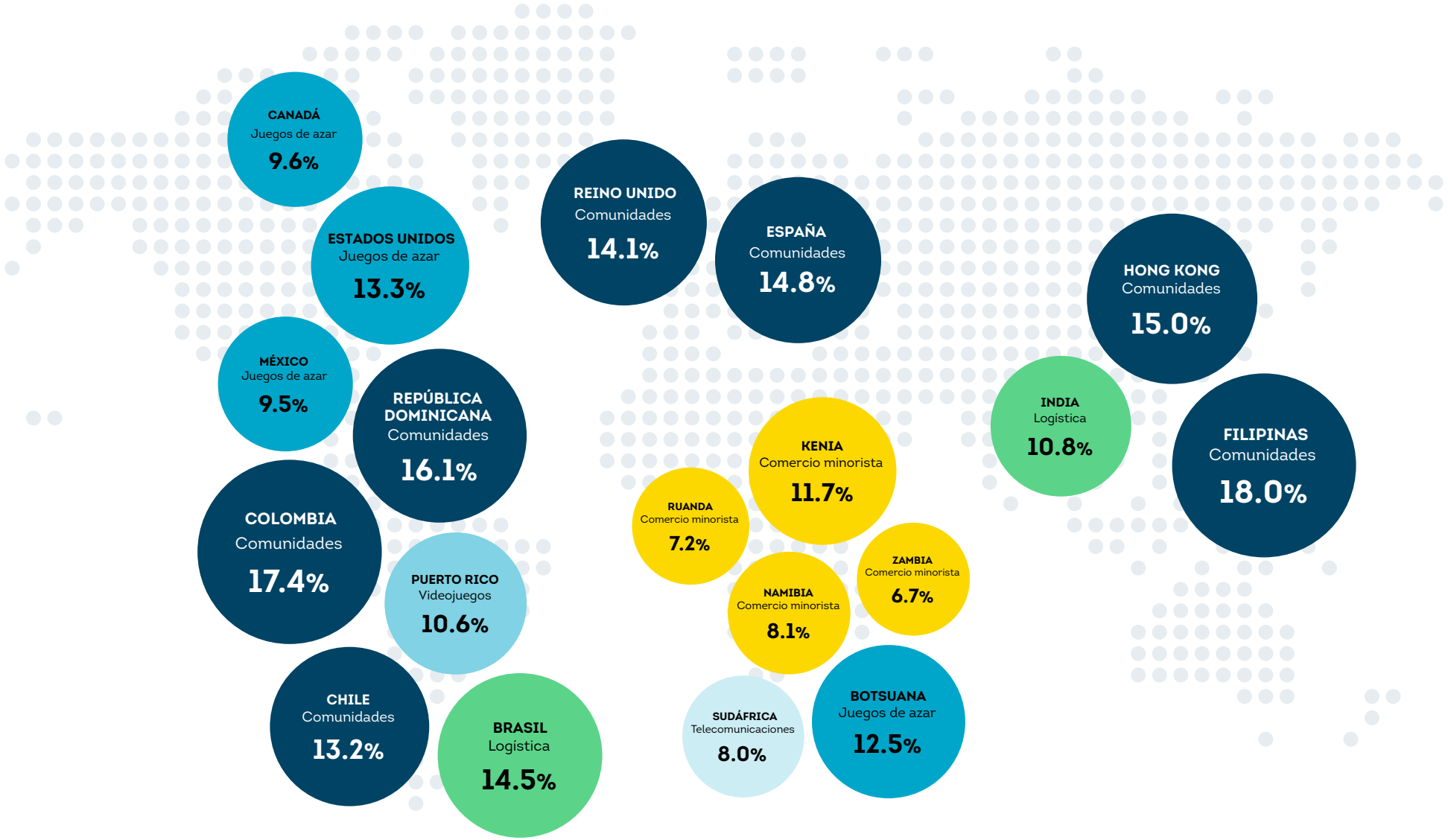
H1 2024
1.0%
Fraude con tarjeta de crédito

H1 2023-H1 2024
-33.2%

Fuente: TransUnion TruValidate

Intentos de Fraude Digital por región e industria H1 2024

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 desempeñan un papel importante en una experiencia omnicanal para el cliente, representando un punto de contacto de alta confianza para los consumidores que están siendo explotados de múltiples formas. Entre los líderes empresariales en la encuesta patrocinada por TransUnion afirmaron estar muy o extremadamente informados sobre actividades relacionadas con el fraude en sus Centros de Atención Telefónica, el 43% indicó que los estafadores aumentaron sus ataques a los Centros de Atención Telefónica en el último año. Además, más de la mitad de esos líderes empresariales señalaron que la información personal robada para pasar la autenticación basada en el conocimiento (59%), el uso de suplantación de identidad para hacerse pasar por un cliente (54%) y los servicios de llamadas virtuales para ser anónimos o inubicables (53%) han aumentado en el último año.

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

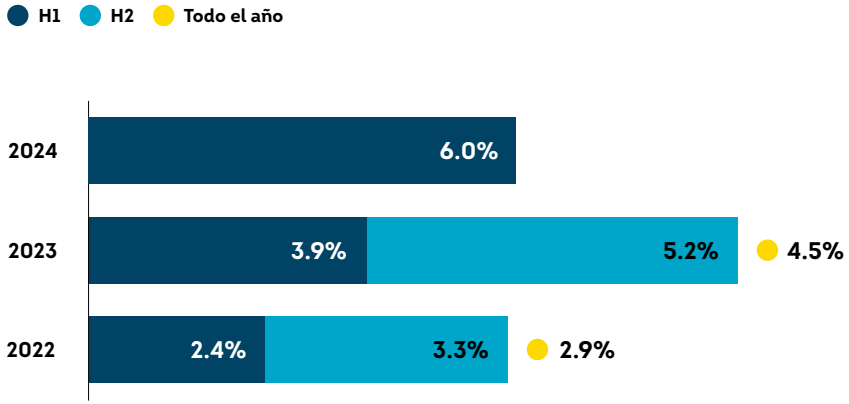
TransUnion documentó un aumento del 54% en el porcentaje de llamadas de alto riesgo a los Centros de Atención Telefónica de Estados Unidos de H1 2023 a H1 2024, pasando del 3.9% al 6.0%.

Aumento de la frecuencia de los ataques de fraude a los Centros de Atención Telefónica

El cambio en la frecuencia de ataques de fraude en los Centros de Atención Telefónica durante el último año, según los líderes empresariales que afirmaron tener un conocimiento muy o extremadamente alto sobre la actividad relacionada con el fraude en sus Centros de Atención Telefónica.

Fuente: Encuesta empresarial de TransUnion

Llamadas de alto riesgo a Centros de Atención Telefónica



Fuente: TransUnion TruValidate

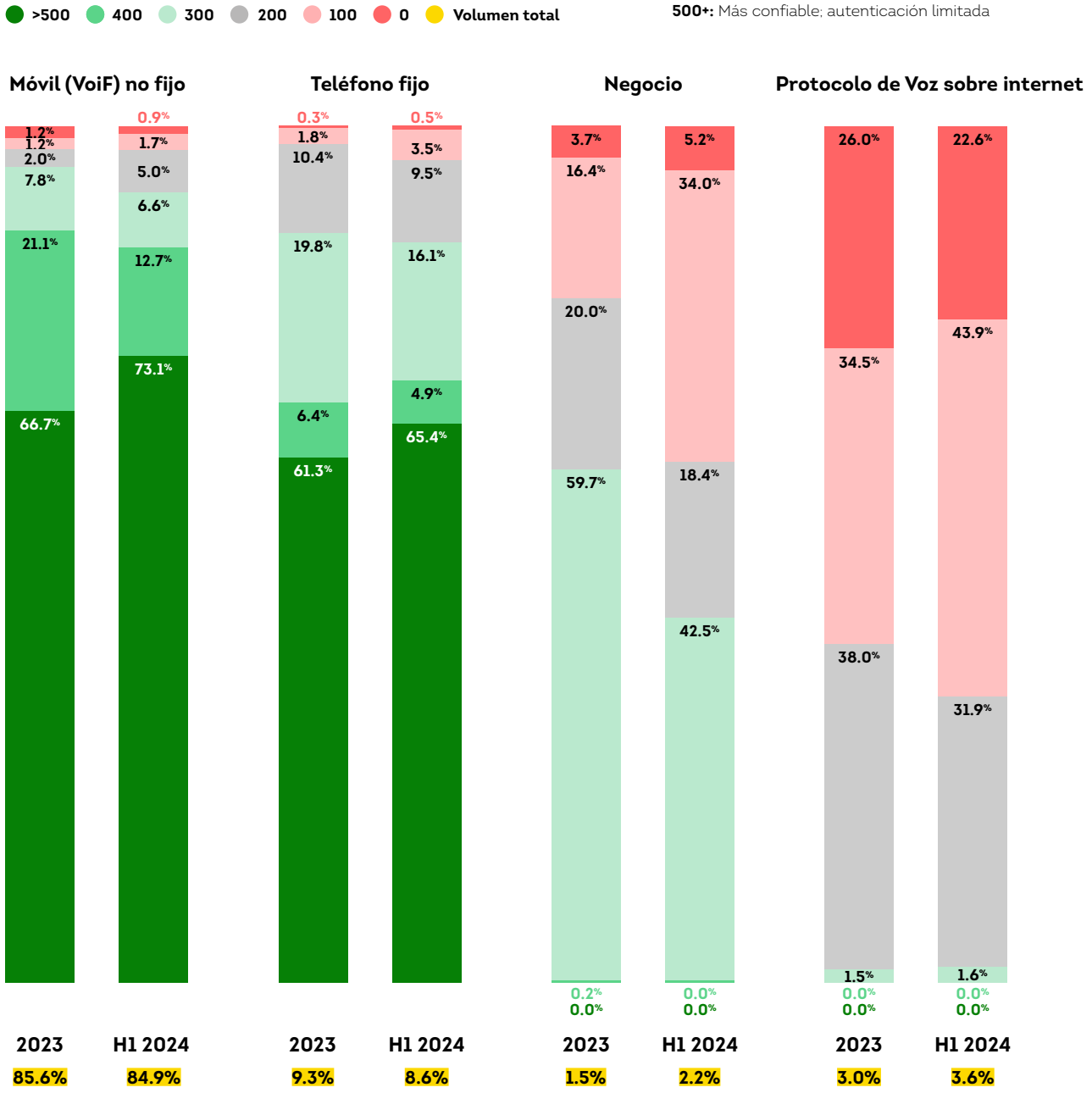
TransUnion

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

Si bien TransUnion documentó que la gran mayoría (86%) de las llamadas recibidas por sus clientes de Centros de Atención Telefónica en Estados Unidos en el primer semestre de 2024 provinieron de teléfonos móviles, solo el 2.6% de esas llamadas se identificaron de alto riesgo de fraude. El porcentaje de llamadas móviles de riesgo aumentó del 2.4% en todo 2023. El canal más riesgoso el 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 3.6% del volumen total de llamadas, el 67% de esas llamadas se identificaron como de alto riesgo de fraude, un aumento con respecto a todo 2023.

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



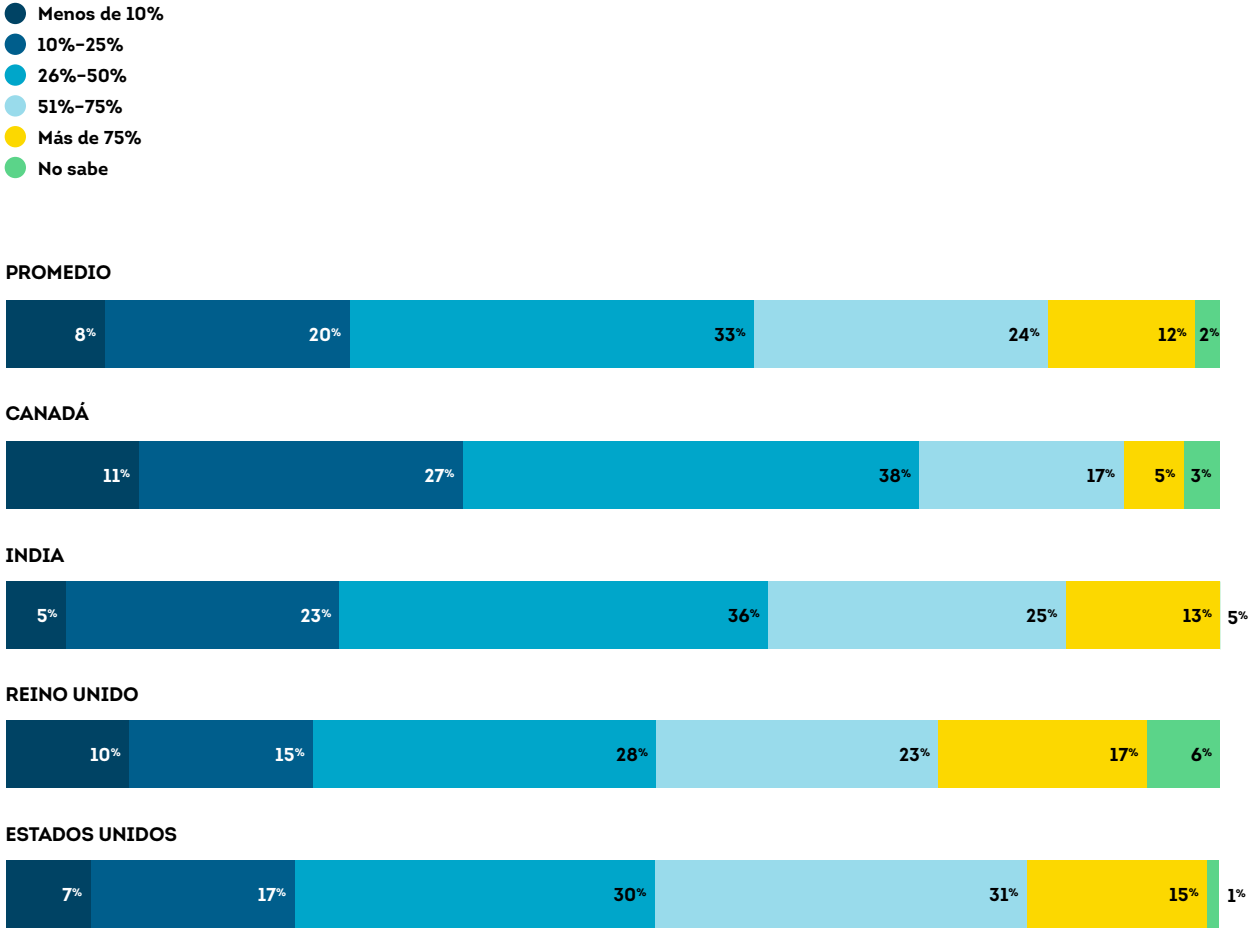
Fuente: TransUnion TruValidate

El riesgo de Fraude Digital en la creación de nuevas cuentas amenaza las experiencias digitales

A medida que las organizaciones dependen más de los canales digitales y móviles para ofrecer experiencias rápidas y convenientes a los clientes, la creación de nuevas cuentas en línea plantea un riesgo creciente. Más de dos tercios de los líderes empresariales encuestados por TransUnion indicaron que al menos el 25% de las nuevas cuentas de sus organizaciones se realizan en línea, más de un tercio indicó que era el 51% o más. Si bien el 72% de los líderes empresariales indicaron que una alta tasa de detección es extremadamente o muy importante para sus soluciones contra el fraude, con tanta información de identidad comprometida en el mercado, a menudo luchan por proteger sus negocios mientras aseguran experiencias rápidas y fluidas para los clientes, especialmente en la apertura de cuentas.

Nuevas cuentas abiertas en línea

Porcentaje de nuevas cuentas de clientes abiertas en línea



Fuente: Encuesta empresarial de TransUnion

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

Al analizar el riesgo por etapa del recorrido del cliente, resulta especialmente preocupante el riesgo asociado a la creación de nuevas cuentas, impulsado por actores malintencionados que utilizan identidades sintéticas o robadas para abrir cuentas. De todas las transacciones globales de creación de cuentas digitales de TransUnion TruValidate en el primer semestre de 2024 (que representan el 7% de todo el volumen de tráfico), TransUnion encontró que el 6.5% eran sospechosas de Fraude Digital, la tasa de riesgo más alta de cualquier etapa del recorrido del cliente.

Ejemplos de las etapas del recorrido del cliente

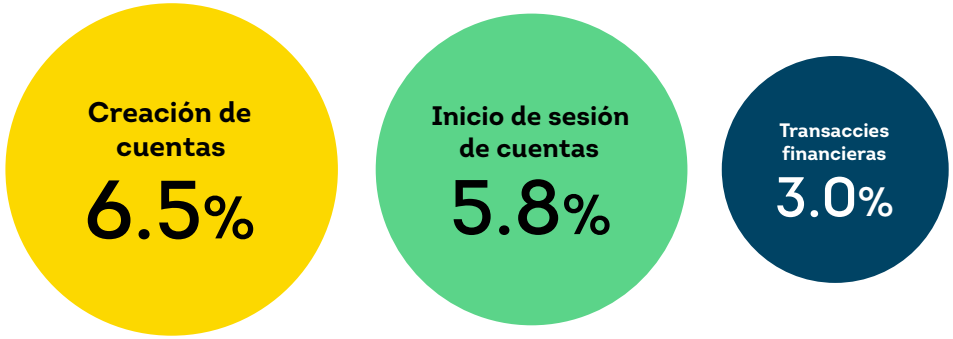
Creación de cuenta: Registro de cuenta, inscripción y originación de créditos.

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

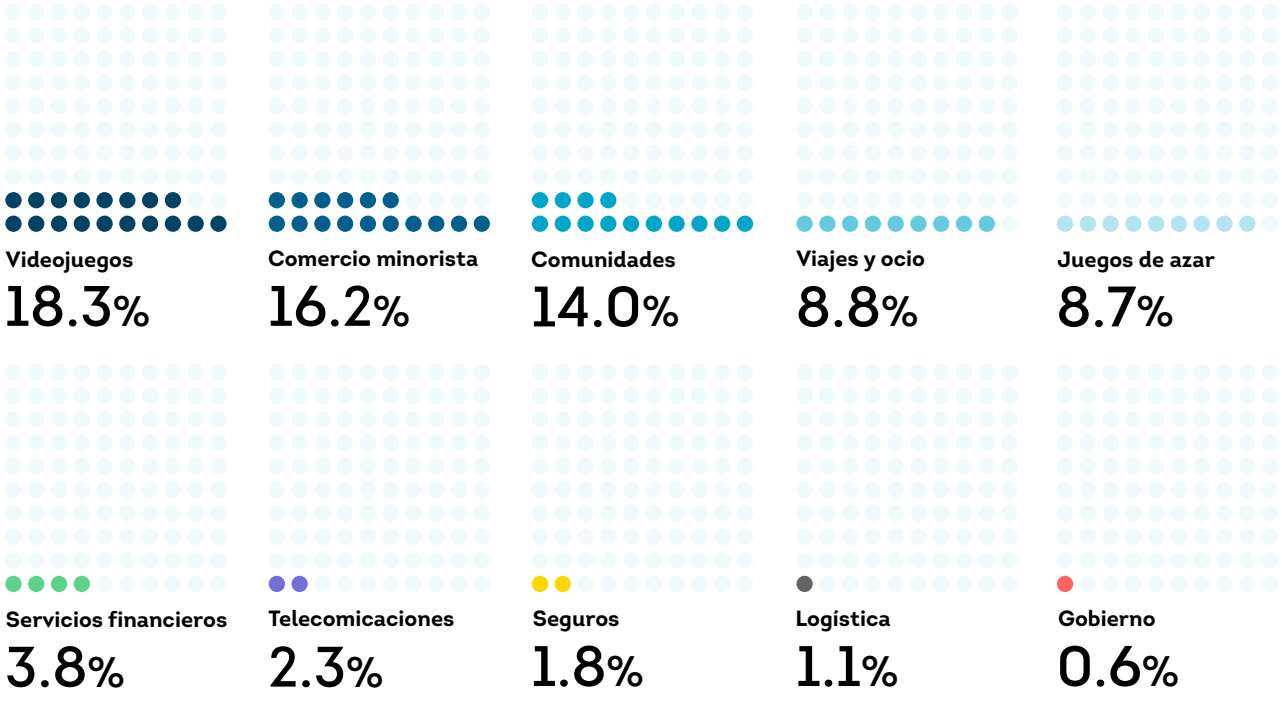
Porcentaje de cada tipo de transacción sospechosa de ser Fraude Digital a nivel mundial en H1 2024



Fuente: TransUnion TruValidate

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 H1 2024



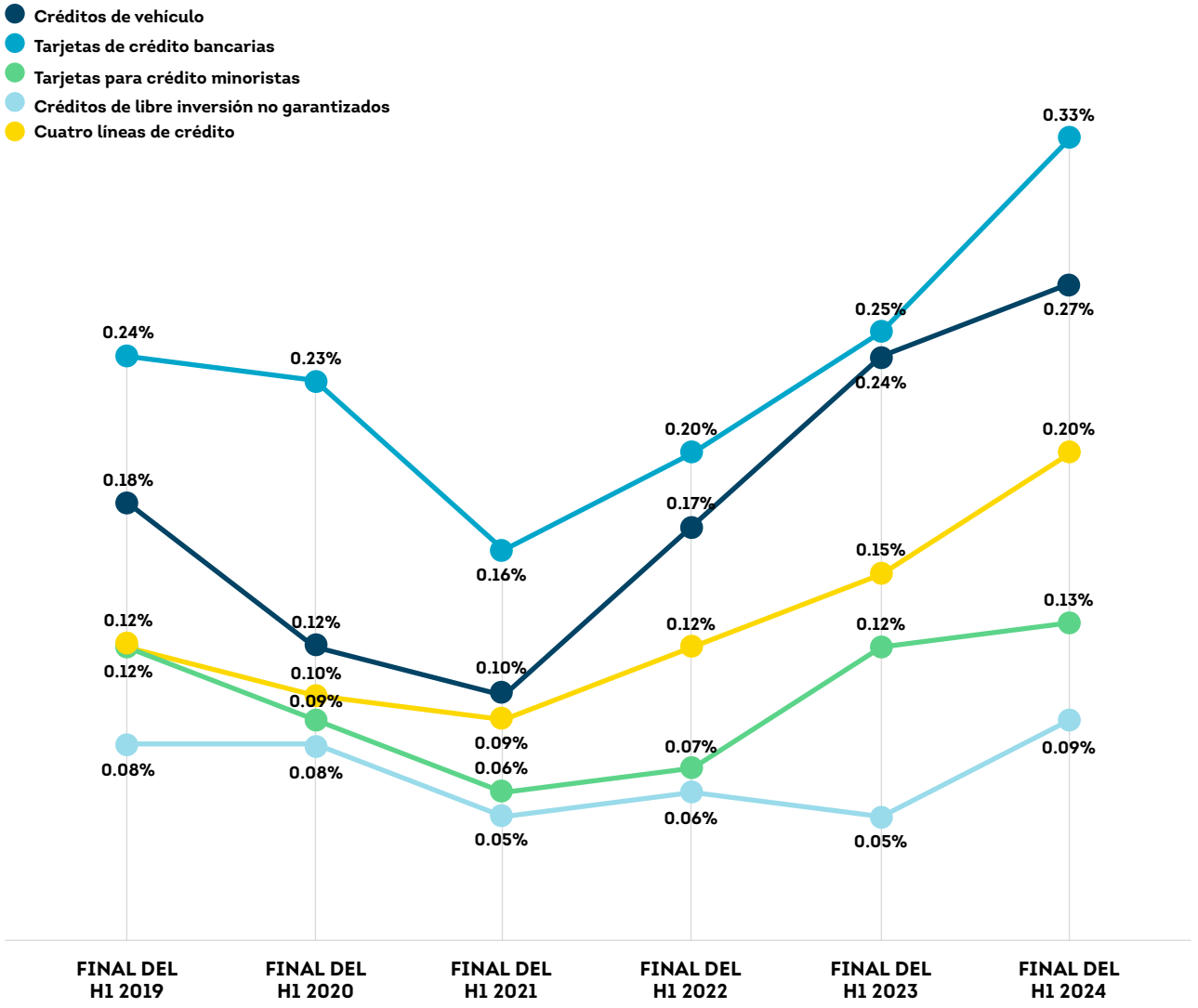
Fuente: Encuesta de fraude al consumidor de TransUnion

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

Con una gran cantidad de credenciales de identidad robadas fácilmente disponibles, TransUnion descubrió que los delincuentes se están volviendo muy hábiles en la creación de identidades falsas. Según los datos de crédito a los consumidores de TransUnion, el porcentaje de identidades sintéticas entre las cuentas abiertas por entidades de crédito en Estados Unidos para créditos de vehículo, tarjetas de crédito bancarias, tarjetas de crédito para minoristas y créditos de libre inversión no garantizados alcanzó un máximo histórico al final del primer semestre de 2024, dejando a las entidades de crédito expuestas a pérdidas potenciales de 3.2 mil millones de dólares, también una cifra récord y un 7% más que a finales del primer semestre de 2023. Las identidades sintéticas entre cuentas abiertas aumentaron un 18% (alcanzando el 0.20%) en el primer semestre de 2024 en comparación con el primer semestre de 2023. Según el porcentaje de intentos de apertura de cuentas con identidades sintéticas, el mercado enfrenta una amenaza creciente de futuras cancelaciones. La aplicación de identidades sintéticas a créditos de vehículo parece particularmente atractiva para los defraudadores que buscan acumular saldos. La exposición total de las entidades de crédito a identidades sintéticas en créditos de vehículo fue aproximadamente el doble de la del sector de tarjetas de crédito bancarias, que ocupó el segundo lugar entre los tipos de crédito analizados.

Identidades sintéticas en la apertura de cuentas

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



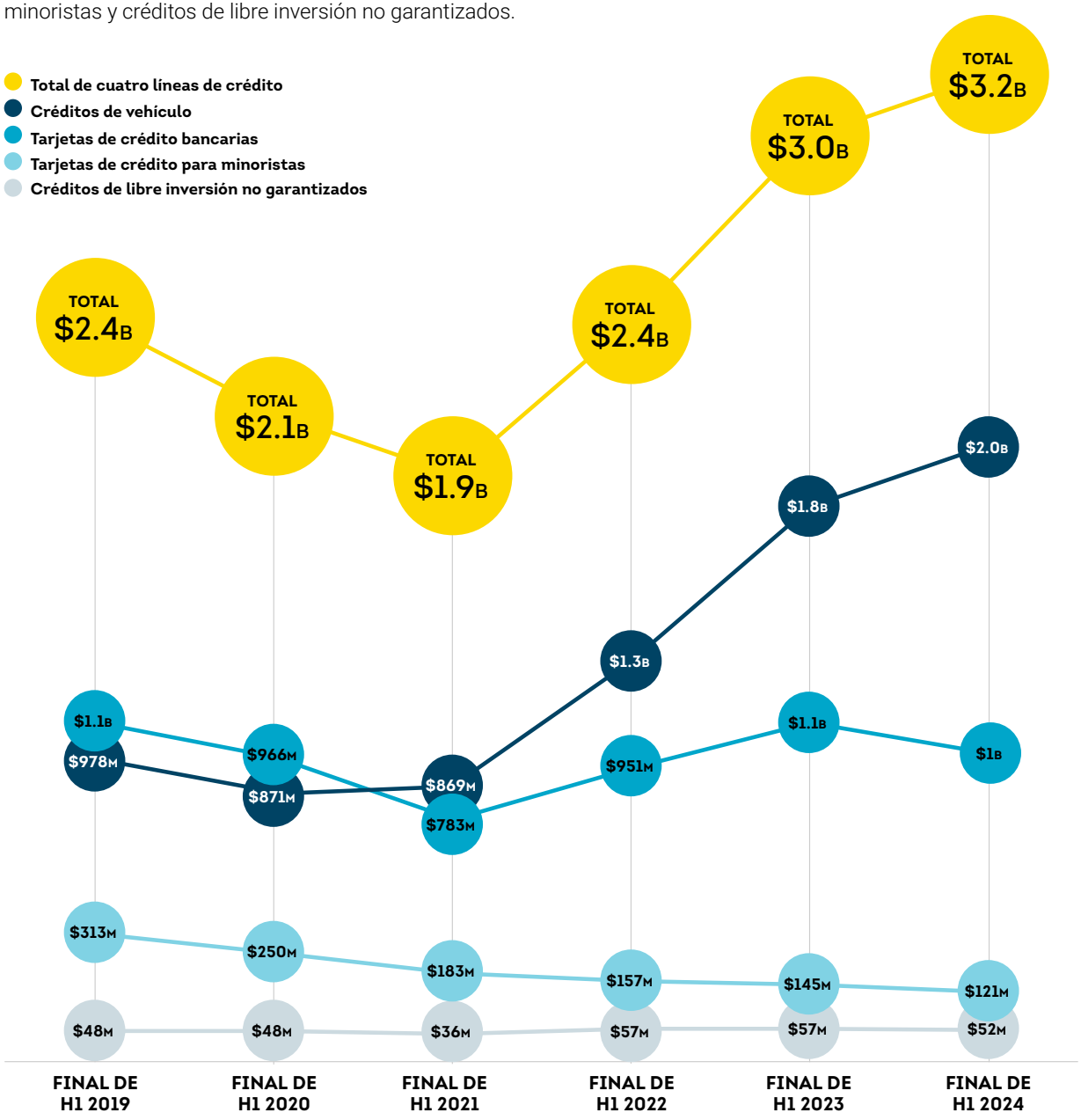
Fuente: TransUnion TruValidate

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 de deudas en el futuro. Entre las cuentas abiertas utilizando identidades sintéticas, los créditos de vehículo parecían ser los más atractivos para que los estafadores acumularan saldos. Al final del primer semestre de 2024, la exposición total de las entidades de crédito a identidades sintéticas en créditos para vehículo tenía saldos un 100% más altos que el sector de tarjetas créditos bancarias.

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

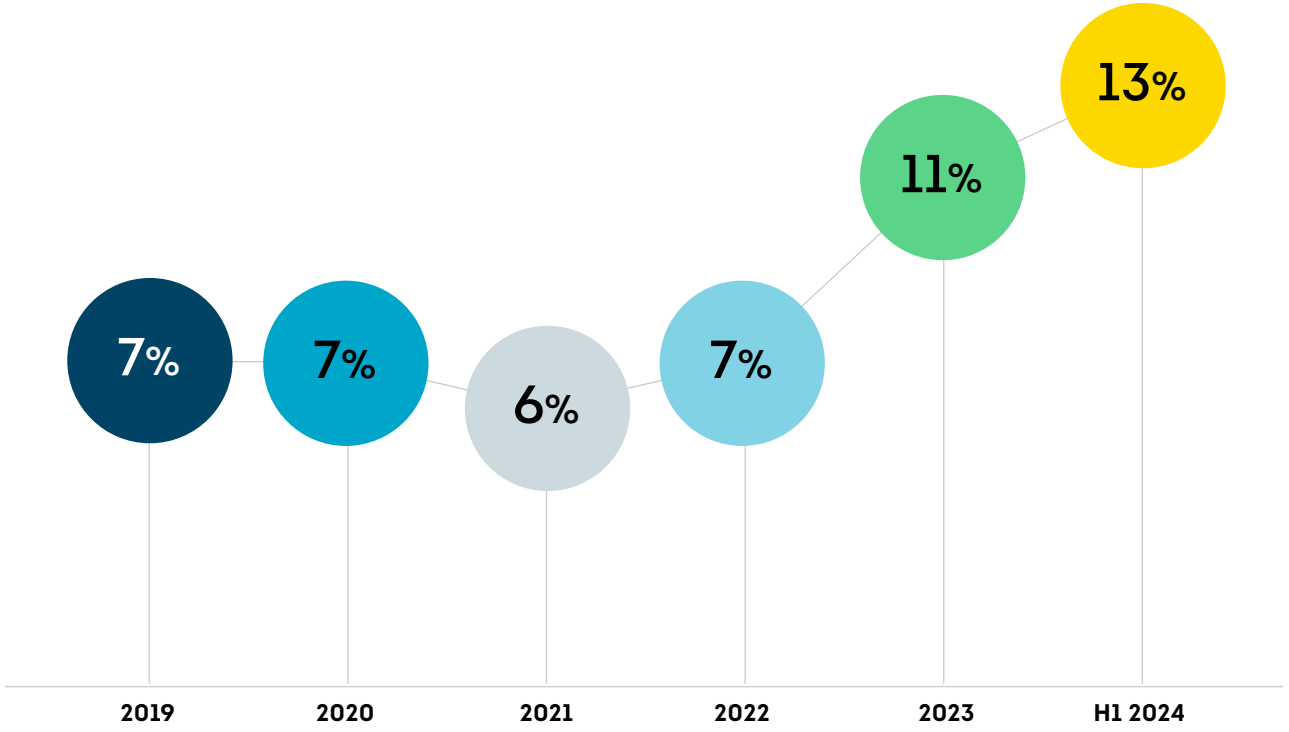
TransUnion

El lavado de crédito (Credit Washing) amplió 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 intentar reciclar una identidad mediante el lavado de crédito, una estafa de manipulación crediticia para eliminar información negativa del historial crediticio de una identidad al presentar reclamaciones falsas 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 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 el primer semestre de 2024, las disputas en los Estados Unidos debido a reclamaciones de fraude representaron el 13% de todas las disputas, el porcentaje más alto en el período de cinco años que TransUnion analizó.

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: Crédito a los Cosumidores de TransUnion

Conclusión

El Fraude Digital sube y baja, pero las tendencias en filtraciones de datos y estafas a consumidores son claras. Ahora y en el futuro, las organizaciones enfrentan a ciberdelincuentes más sofisticados que utilizan datos de identidad a gran escala para llevar a cabo esquemas de fraude primarios y de tercera persona. No solo deberán lidiar con estafas persistentes de hackeo de cuentas, sino que los delincuentes seguirán construyendo identidades falsas pero confiables, habilitadas por la tecnología, para operar a una escala y velocidad sin precedentes.

En cuanto a los líderes empresariales, desean proteger tanto a los clientes como a sus organizaciones. El fraude les cuesta a las organizaciones pérdidas significativas de ingresos y beneficios cada año. A medida que los líderes observan un aumento del riesgo de fraude en todos los canales, la prevención del fraude se convierte en un costo necesario que debe ser lo más eficiente posible. Los responsables de la lucha contra el fraude deben adoptar un enfoque integral a nivel empresarial para prevenir el fraude y generar confianza en los clientes. Es clave emplear una estrategia de innovación continua mediante mejores datos y señales de riesgo, análisis avanzados y tecnología integrada para detectar el fraude de manera más efectiva, sin aumentar las pérdidas comerciales ni los costos adicionales derivados de falsos positivos.

Metodología de obtención de datos

Este informe combina datos propios de la red global de inteligencia de TransUnion y encuestas especialmente encargadas a empresas y consumidores.

Encuesta empresarial

Esta encuesta en línea se realizó en Canadá (200 encuestados), India (200 encuestados), Reino Unido (201 encuestados) y Estados Unidos (200 encuestados) del 14 al 29 de mayo de 2024 por TransUnion en colaboración con el proveedor de investigación de terceros, Dynata. La encuesta estuvo dirigida a roles gerenciales con responsabilidad en riesgo y/o fraude en empresas cuyos principales clientes eran consumidores, y cuyos ingresos superaban los CA$300 millones en Canadá, 1B en India, £200 millones en el Reino Unido y USD$200 millones en los Estados Unidos. Las personas fueron encuestadas utilizando un método de panel de investigación en línea a través de una combinación de dispositivos de escritorio, móviles y tabletas. Estos resultados de investigación no están ponderados y son estadísticamente significativos a nivel de país individual con un margen de error de ± 6.9 puntos porcentuales a un nivel de confianza del 95%. Tenga en cuenta que algunos porcentajes en los gráficos pueden no sumar 100% debido a redondeos o a que se aceptaron múltiples respuestas.

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 15.372 adultos fue realizada del 29 de abril al 20 de mayo de 2024 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 (Botsuana, Brasil, Canadá, Chile, Colombia, República Dominicana, Guatemala, Hong Kong, India, Kenia, Namibia, Filipinas, Ruanda, Sudáfrica, España, Reino Unido, Estados Unidos 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 (Chile, Colombia, República Dominicana, Guatemala 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 digitales y físicas 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.

Metodología de obtención de datos

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

Los hallazgos de fraude sintético 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. El análisis de fraude sintético abarca la actividad crediticia de Estados Unidos registrada entre el 1 de enero de 2009 y el 30 de junio de 2024. Las medidas de exposición para las entidades de crédito se basaron en la fórmula patentada de TransUnion para capturar la posible pérdida total en riesgo para las entidades de crédito.

Acerca de TransUnion TruValidate

TruValidate 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.

transunion.do/solucion/truvalidate

TransUnion