SIETE PRINCIPALES RETOS DE FRAUDE EN AMÉRICA LATINA

Y ESTRATEGIAS COMPROBADAS PARA AFRONTAR EL RIESGO QUE PLANTEAN

Defiéndase contra el ciberdelito a la vez que mejora la experiencia digital del cliente.

LexisNexis®
RISK SOLUTIONS

CONTENIDO

INTRODUCCIÓN

Este ebook se basa en las perspectivas del estudio de LexisNexis® Risk Solutions El verdadero costo del fraude en América Latina – informe regional 2021. Provee orientación a empresas que buscan crecer su negocio con seguridad en un entorno de fraude siempre cambiante.

TENDENCIAS ACTUALES DE FRAUDE EN COMERCIO MINORISTA, COMERCIO ELECTRÓNICO Y SERVICIOS FINANCIEROS

El fraude digital aumenta en la medida que las ventas en línea crecen y los defraudadores apuntan a comerciantes que están recién llegados al comercio electrónico o carecen de recursos para implementar medidas de seguridad avanzadas.

Este ebook se basa en las perspectivas del estudio de LexisNexis® Risk Solutions El verdadero costo del fraude en América Latina – informe regional 2021. Provee orientación a empresas que buscan crecer su negocio con seguridad en un entorno de fraude siempre cambiante.

Utilizando datos recolectados desde febrero a abril de 2021 de 454 ejecutivos de riesgo y fraude encuestados, ofrece una imagen veraz de las actuales tendencias de fraude en los mercados de comercio minorista, comercio electrónico y servicios financieros de América Latina.

En particular, examina los retos de seguridad asociados a:

- realización de transacciones a través de canales en línea y móviles;
- adición de mecanismos de pago nuevos;
- expansión internacional;
- entrega de una experiencia de cliente omnicanal óptima.

El estudio es único en el sentido que los datos recolectados incluyen las inusuales circunstancias creadas por la COVID-19. Al haber más consumidores haciendo compras en línea que nunca, los defraudadores hallaron nuevas oportunidades de esconderse entre la gente y explotar vulnerabilidades del comercio y la banca. El resultado fue un auge en el fraude del lado del consumidor, lo cual obligó a muchas empresas a replantear sus estrategias de prevención de fraude para el futuro.

CONCEPTO #1

RETO | RÁPIDO AUMENTO DE COSTOS DE FRAUDE

Los consumidores de hoy exigen transacciones fluidas y sencillas en todos los canales. Pero al agregar mecanismos de pago nuevos y expandir los canales a sectores móviles, internacionales y en línea, los minoristas y vendedores de comercio electrónico no se dan cuenta de que crean nuevas oportunidades para los defraudadores.

Los ataques de fraude aumentaron debido a diversos factores, entre ellos:

- **más focalización en entidades financieras con fines de apropiación de cuentas y clonación de tarjetas[1];**
- **mayor uso de métodos de pago digitales y sin contacto por parte de los consumidores, lo cual aumentó las pérdidas por fraude;**
- **un volumen más alto de transacciones por el canal móvil, lo cual generó problemas relacionados con identidades y cuentas.**

El promedio mensual de ataques de fraude exitosos aumentó a 624, siendo Colombia y Argentina los países que tuvieron la mayor cantidad de ataques. A la par con ese aumento de volumen, los minoristas y vendedores de comercio electrónico observaron un aumento en los costos de fraude. El costo de fraude creció fuertemente para comerciantes y entidades financieras en América Latina. Hoy en día, cada transacción fraudulenta cuesta en promedio 3,68 veces el valor de la transacción perdida, comparado con 3,46 veces en 2019, lo cual refuerza la importancia de la prevención.

Hoy en día, cada transacción fraudulenta cuesta en promedio 3,68 veces el valor de la transacción perdida, comparado con 3,46 veces en 2019, lo cual refuerza la importancia de la prevención.

SOLUCIÓN | MANTENERSE EXPECTANTE

Con la escalada en intentos de fraude y ataques exitosos, ninguna empresa se puede dar el lujo de ignorar el riesgo de fraude.

Debe mantenerse vigilante y preparada para un aumento de fraude en el futuro previsible. Equipe a su organización de soluciones de protección contra el fraude a la vez que minimiza la fricción del cliente en un entorno competitivo de canales en línea y móviles.

[1] https://www.globenewswire.com/fr/news-release/2021/05/03/2221375/0/en/Latin-America-Fraud-Detection-and-Prevention-Market-to-Reach-USD-2-945-3-Million-by-2028-Increasing-Incidence-of-Data-Fraud-to-Stimulate-Growth-Fortune-Business-Insights.html

CONCEPTO #2

RETO | ACELERACIÓN DE LA MIGRACIÓN DIGITAL

Aumento de actividad en canales móviles y en línea, lo cual incrementa los riesgos y costos de fraude. América Latina es uno de los mercados móviles de más rápido crecimiento, siendo el móvil el principal medio de conectividad a internet para gran parte de la población. La cantidad de comerciantes e instituciones financieras que ofrecen comercio móvil ha crecido significativamente. El 84 % de las empresas ofrecen comercio móvil, un aumento del 22 % respecto al 2019.

La pandemia de COVID-19 aceleró en gran medida la transformación digital con el desplazamiento de los compradores hacia transacciones en línea/por navegador y por canales móviles. Pero los defraudadores también se pusieron en línea. Desarrollaron nuevas habilidades durante la pandemia y buscaron vulnerabilidades. Los comerciantes y las instituciones financieras no estaban preparados para el aumento de volumen de transacciones digitales. Carecían de soluciones de detección de fraude que pudieran evaluar identidades digitales y riesgos de transacciones.

- El porcentaje de costos de fraude atribuidos al canal móvil aumentó para vendedores de comercio electrónico.
- El aumento en el uso de billeteras móviles/digitales y pagos sin contacto se alinea con un aumento en el porcentaje de costos de fraude atribuidos a estos métodos de pago.
- El fraude relacionado con identidades y cuentas, tal como la apropiación y la creación fraudulenta de cuentas, es especialmente problemático para entidades financieras y comerciantes que permiten el comercio móvil, y representa una porción significativa de las pérdidas por fraude.
- América Latina es uno de los mercados móviles de más rápido crecimiento, siendo el dispositivo móvil el principal medio de conectividad a internet para muchos.
- Para responder a esa necesidad, el 84 % de las empresas actualmente ofrecen comercio móvil, un aumento del 22 % respecto al 2019.

América Latina es uno de los mercados móviles de más rápido crecimiento, siendo el dispositivo móvil el principal medio de conectividad a internet para muchos.

SOLUCIÓN | LA TECNOLOGÍA ES CLAVE

Para minimizar el fraude, las organizaciones ya no pueden seguir dependiendo de procesos manuales o tecnologías limitadas para reducir tasas de desafíos, revisiones manuales y costos. Necesitan una robusta plataforma tecnológica para fraude y seguridad que les permita adaptarse a un entorno digital cambiante, que provea una sólida gestión de fraude y ofrezca una experiencia sin fricción para clientes confiables.

CONCEPTO #3

RETO | FRAUDE SOFISTICADO MÁS COMPLEJO Y DIFÍCIL DE DETECTAR

A medida que ha aumentado el volumen de fraude, también se ha vuelto más sofisticado, lo cual crea nuevos desafíos para los minoristas en línea y las instituciones financieras.

- Redes de fraude organizadas y conectadas globalmente comparten información de identidad robada y colaboran en la ejecución de ataques de fraude. Utilizando múltiples dispositivos vinculados, pueden esconder la fuente y la localización de la transacción original.
- El alto volumen de ataques de *botnets*, incluidos los *botnets* móviles, incrementa el número de ataques exitosos. Estos ataques de fraude automatizados aumentaron un 66 % en relación con el año pasado. Argentina, Brasil y Chile sufrieron la mayor cantidad de ataques.
- Las identidades sintéticas compuestas de información personal real y/o falsa se están volviendo más comunes. Son difíciles de detectar utilizando herramientas tradicionales de mitigación de riesgos.

SOLUCIÓN | UNA ESTRATEGIA MULTICAPA DE AUTENTICACIÓN

La prevención eficaz del fraude requiere diferentes soluciones para diferentes canales y tipos de transacciones. No hay una solución única que pueda autenticar los criterios tanto digitales como físicos, así como el riesgo de identidad y transacción. Las organizaciones requieren una estrategia de defensa fuerte y multicapa para la autenticación, con el fin de evitar el rápido crecimiento de los costos y el impacto del fraude sobre los ingresos.

- El fraude no se puede detener con una solución universal.
- La utilización conjunta de varias soluciones proporciona la mejor protección, a la vez que garantiza una experiencia de cliente positiva y de baja fricción.
- Se deben aplicar soluciones diferentes para canales y tipos de transacciones diferentes.
- Los minoristas y los vendedores de comercio electrónico/móvil deben invertir proactivamente en soluciones para evitar amenazas digitales y móviles.

La prevención eficaz del fraude requiere diferentes soluciones para diferentes canales y tipos de transacciones.

CONCEPTO #4

RETO | VERIFICACIÓN DE IDENTIDAD

El fraude relacionado con identidad representa una porción significativa de las pérdidas por fraude. Incluye la apropiación y creación fraudulenta de cuentas. Para los minoristas y las entidades de servicios financieros con canales móviles y en línea fue difícil verificar identidades y distinguir clientes legítimos de *bots* maliciosos sin implementar medidas de seguridad onerosas.

- La verificación de la identidad del cliente fue considerada el reto de fraude #1 que afrontan las empresas latinoamericanas, pasando de 21 % en 2019 a 44 % en 2021.
- El fraude de primera instancia y el fraude amigo también están entre las principales preocupaciones.
- Los proveedores de pagos no bancarios terceros ofrecen transparencia limitada de las identidades que están detrás de complejas cadenas de pago y perfiles de cliente final.
- Muchos minoristas y vendedores de comercio electrónico tienen una capacidad limitada para confirmar la localización de un pedido, la cual es un indicador útil de fraude.

SOLUCIÓN | UNA DEFENSA FORMIDABLE

Para fortalecer la seguridad se requieren numerosas formas de protección:

- Una solución de prevención de fraude eficaz debe validar identidades en todos los canales. Debe estar en capacidad de obtener respuestas a las siguientes preguntas a lo largo de la jornada del cliente:
  - Apertura de cuentas - **¿Quién es el cliente?**
  - Gestión continuada de cuentas - **¿El cliente es quien dice ser?**
  - Pagos - **¿La transacción es fraudulenta o se trata de un falso positivo?**
- Las herramientas de rastreo de transacciones en tiempo real deben evaluar identidades individuales, el riesgo de transacción y la congruencia con patrones de comportamiento anteriores del comprador - y todo en tiempo real.
- Debido a que las redes de *bots* y las identidades sintéticas imitan personas y transacciones reales, se necesita una visión completa del cliente para determinar si son reales o falsas.
- Una visión completa combina datos de identidad físicos y digitales. Abarca la inteligencia relacionada con dispositivos, ubicaciones, identidades, vínculos y comportamientos previos para distinguir correctamente entre usuarios confiables y fraudulentos.
- Combine estos diferentes elementos para crear una defensa formidable y acoja el aprendizaje automático con el fin de prevenir el fraude antes de que suceda.

CONCEPTO #5

RETO | FRICCIÓN DE CLIENTE

Los clientes utilizan numerosos canales y dispositivos a lo largo del día. Fluyen de uno a otro, y esperan una experiencia uniforme y sin tropiezos en todos los canales.

A medida que se desplazan más transacciones a los canales en línea y móviles, los consumidores tienen más opciones, entre ellas abandonar una transacción que sea onerosa o genere demoras.

No toda transacción conlleva el mismo nivel de riesgo; las empresas necesitan inteligencia para saber cuándo aplicar más o menos medidas de seguridad con los clientes. Los clientes nuevos podrían valorar inicialmente las medidas adicionales tomadas para verificar su identidad, tales como preguntas tipo reto o claves de acceso de uso único. Los clientes que retornan podrían cansarse de estas medidas de seguridad, basándose en la expectativa de que la empresa debería conocerlos.

Su empresa puede personalizar automáticamente el nivel de autenticación según la pertinencia de señales de riesgo e inteligencia de identidad, minimizando así la fricción para los clientes valiosos

SOLUCIÓN | INTELIGENCIA COMPARTIDA

Al aprovechar la inteligencia global compartida de la LexisNexis® Digital Identity Network®, LexisNexis Risk Solutions está en capacidad de suministrar una completa solución integral que ayuda a minoristas y entidades financieras a reconocer en forma instantánea a clientes confiables y autenticar sus transacciones.

El resultado es una experiencia de usuario optimizada y exitosa. A la vez, dichas soluciones deben mantener tasas de falsos positivos bajas y detectar con precisión transacciones de alto riesgo, minimizando así la exposición al fraude.

Con herramientas de validación de identidad flexibles y adaptables, los riesgos de fraude se pueden segmentar, de tal forma que los controles de seguridad se puedan ajustar hacia arriba o hacia abajo según la transacción. Su empresa puede personalizar automáticamente el nivel de autenticación según la pertinencia de señales de riesgo e inteligencia de identidad, minimizando así la fricción para los clientes valiosos.

CONCEPTO #6

RETO | COOPERACIÓN CON OTROS

Es probable que las empresas estén combatiendo muchos de los mismos tipos de fraude. De hecho, los patrones y riesgos de fraude tienen muchas similitudes en diversos sectores y geografías. Además, los defraudadores rara vez limitan sus intentos a un solo comerciante. Cooperar con otros en su sector, incluso con competidores, podría ser de beneficio mutuo.

SOLUCIÓN | CONSORCIOS

Busque alianzas dentro de su industria para compartir perspectivas de fraude e información. La construcción de una alianza específica a un sector para que haya intercambio de información importante puede mantener a los miembros al día sobre patrones y tácticas de fraude en dicho sector.

Usted puede ir más allá de su propia inteligencia para identificar y rastrear con mayor precisión individuos y dispositivos riesgosos.

Tal información puede incluir:

- histórico de dispositivos en lista negra
- cuentas mula y estrategias de fraude asociadas
- riesgos específicos relacionados con sector/caso de uso/geografía

CONCEPTO #7

RETO | PREPARACIÓN PARA EL FUTURO

El mundo minorista postcovid probablemente nunca retornará a los niveles precovid. Es arriesgado asumir una actitud de esperar a ver qué pasa.

Es probable lo siguiente en el futuro inmediato:

- aumento de volumen de ataques de fraude
- amenazas más sofisticadas y complejas
- ciberdelitos más audaces y maliciosos

SOLUCIÓN | INTEGRACIÓN DE LAS SOLUCIONES DE FRAUDE CON LA CIBERSEGURIDAD Y LA EXPERIENCIA DE CLIENTE

Comerciantes y entidades de servicios financieros de América Latina pueden reducir los costos y riesgos de fraude mediante una buena práctica: la integración de las operaciones de ciberseguridad, experiencia digital de cliente y fraude para:

- Mejorar las decisiones y la experiencia de cliente con aprendizaje automatizado e integración de sistemas/recursos que gestionan el riesgo en todo el negocio y todos los extremos.
- Predecir las amenazas en lugar de reaccionar a ellas, utilizando funciones ampliadas de datos y analítica, provistas por herramientas tales como inteligencia artificial, aprendizaje automático, ciberalertas, inteligencia de medios sociales y *crowdsourcing*.
- Integrar estas herramientas con soluciones basadas en identidad digital para brindar protección a lo largo de la jornada del cliente con fricción mínima.

CONCLUSIÓN

El panorama del fraude es complejo y cambia constantemente. Desafía a su empresa a lograr el equilibro entre la seguridad robusta y una experiencia sin tropiezos en cada etapa de la jornada del cliente.

Sus clientes exigen interacciones digitales rápidas, fluidas y seguras, ya sea que estén en línea o en un móvil. Depende de usted entregar experiencias óptimas o de lo contrario, no dudarán en abandonar la transacción y acudir a su competidor.

LexisNexis® Risk Solutions ofrece soluciones de identificación y autenticación que ayudan a prevenir el fraude. Modulares y adaptables, nuestras soluciones se pueden personalizar para satisfacer las necesidades específicas de gestión de identidad y flujos de trabajo de su empresa. Contáctenos para conocer más sobre prevención de fraude y a la vez, la entrega de experiencias óptimas de cliente, lo cual no solo protege a su organización, sino que le da una ventaja competitiva en el congestionado mercado digital de hoy.

Para conocer más sobre las estrategias para reducir el fraude y sobre el costo real del fraude en América Latina, descargue el informe completo en risk.lexisnexis.com/TCoFLATAM

LexisNexis®
RISK SOLUTIONS

Acerca de LexisNexis® Risk Solutions

LexisNexis Risk Solutions aprovecha el poder de los datos y la analítica avanzada para entregar conocimiento que ayuda a las empresas y las entidades gubernamentales a reducir el riesgo y mejorar las decisiones para el beneficio de las personas en todo el mundo. Ofrecemos soluciones de información y tecnología para una amplia gama de sectores, entre ellos: seguros, servicios financieros, salud y gobierno. Con sede principal en el área metropolitana de Atlanta, Georgia, EE.UU. tenemos oficinas en todo el mundo y somos parte de RELX (LSE: REL/NYSE: RELX), un proveedor mundial de herramientas de analítica y toma de decisiones para clientes profesionales y empresariales basadas en información. Para más información, visite www.risk.lexisnexis.com y www.relx.com.

Nuestras soluciones para servicios financieros ayudan a las organizaciones a prevenir el delito financiero, lograr el cumplimiento regulatorio, mitigar el riesgo de negocios, mejorar las eficiencias operativas y aumentar la rentabilidad.