10 tendencias que ayudarán a enfrentar el panorama de fraude en 2022

LexisNexis® RISK SOLUTIONS

Para muchas organizaciones, la detección y prevención de fraude es una ardua tarea. Los consumidores siguen migrando rápidamente a los canales digitales, a la vez que las organizaciones también se desplazan hacia la digitalización de productos y servicios para aumentar la rentabilidad, aunque todo tiene un costo. Tras el aumento de transacciones, los defraudadores están buscando nuevas oportunidades para explotar y así obtener las mayores ganancias con el menor riesgo.

Presentamos nuestras predicciones sobre las 10 tendencias más importantes a considerar, ya que tienen la mayor probabilidad de impactar los presupuestos y las acciones contra el fraude durante este año.

01 Es poco probable que la transformación digital se desacelere

La digitalización de las interacciones de los clientes se aceleró varios años por causa de la pandemia. A la vez que las empresas siguen llevando sus servicios al ambiente digital, los clientes también se sienten más cómodos y confiados al consumir estos servicios en línea.

Aunque la transformación digital estaba en alza antes de la pandemia, adquirió una nueva urgencia al desatarse la misma. Esto generó un cambio fundamental en la forma en que las personas interactúan con las empresas, poniendo a disposición de los defraudadores una serie de usuarios digitales sin experiencia.

A nivel mundial, el promedio de la porción de interacciones digitales de los clientes aumentó 22 %[1].

21 % Asia Pacífico

23 % Europa

24 % EE.UU.

02 Mayor automatización

La automatización es un arma de doble filo. Aunque agiliza la jornada del cliente al ofrecer campos de llenado automático y otras ventajas, también facilita los ataques de los defraudadores, lo cual eleva el volumen de ataques. Las metodologías automatizadas también pueden hacer más daño más rápido.

1.200 millones
Número de ataques de bots durante el primer semestre de 2021

lo cual representa un crecimiento de
41 %
año a año a nivel mundial

El volumen de ataques de bots aumentó
28 %
año contra año en servicios financieros

El sector de medios fue duramente golpeado con un aumento de
174 %
en el volumen de bots

Los ataques de bots a lo largo de la jornada del cliente también están en alza:

Inicios de sesión	Pagos	Creación de cuentas nuevas
aumento de 52 % en intentos de apropiación de cuentas	aumento de 18 % (probablemente haciendo prueba de credenciales de tarjetas de crédito robadas)	tasa de ataques de 8.9 % la más alta de todos los casos de uso[2]

03 Adopción de nuevos pagos y métodos digitales

Sector de pagos digitales:

2019: Transacciones por valor de $ 4.700 billones de dólares
2020: $ 5.400 billones de dólares
2021: $ 6.700 billones de dólares
2022: $ 7.800 billones de dólares
para el 2025: $ 10.700[3] billones de dólares

Las nuevas opciones de pagos digitales ofrecen creación fácil de cuentas y acceso rápido a crédito, abriendo así la puerta al abuso por parte de defraudadores con credenciales robadas.

A los consumidores les encanta el Buy Now Pay Later (BNPL)...

Más de 17 millones
Número de consumidores que han utilizado el BNPL en el Reino Unido[4]

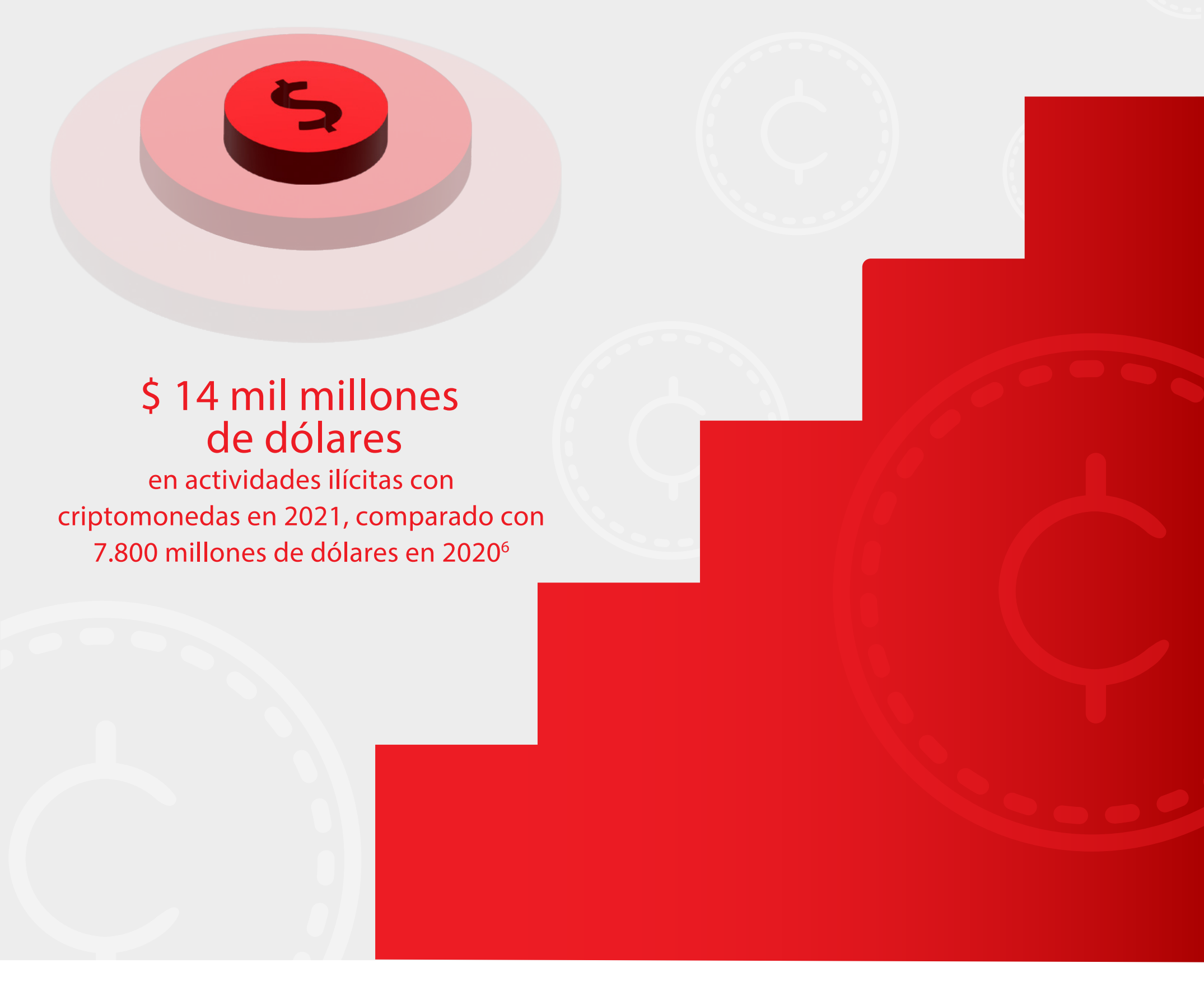
Más de 400 %
Aumento de BNPL en EE. UU. de 2020 a 2021

U.S. $ 1 billón
Volumen global bruto esperado de mercancía en la industria de BNPL en 2025[5]

...pero a los defraudadores también.

Las plataformas de BNPL más grandes reportaron un aumento significativo de fraude, principalmente por creación de cuentas nuevas, apropiación de cuentas y pagos con tarjetas de crédito robadas

Las criptomonedas también representan una amenaza creciente. La falta de transparencia de las criptomonedas hace que sean la moneda preferida para estafas, pago de rescates, lavado de activos y otras actividades ilícitas.



$ 14 mil millones de dólares en actividades ilícitas con criptomonedas en 2021, comparado con 7.800 millones de dólares en 2020[6]

04 Creciente riesgo de fraude en pagos

A los consumidores les encantan las transacciones digitales. A nivel mundial, se proyecta que el mercado de pagos digitales llegará a más de 236 mil millones de dólares para 2028, con una tasa de crecimiento anual compuesto de 19.4 %.[7]

Sin embargo, el aumento de actividad de transacciones digitales también actúa como imán para los defraudadores, ya que la consciencia de la importancia de la seguridad en los datos no crece a la misma velocidad que las actividades digitales. Por ejemplo, los intentos de fraude digital en servicios financieros aumentaron casi 150 %.[8]

Pérdidas estimadas del comercio electrónico mundial debido al fraude en pagos digitales en 2021
$ 20 mil millones de dólares
un crecimiento del 14 % respecto al 2020[9]

El 70 % de las transacciones fraudulentas de banca digital en el segundo trimestre de 2021 se originaron en el canal móvil, comparado con el 63 % en el trimestre anterior. El mayor aumento se presentó en el fraude con aplicaciones de banca móvil[10]

No obstante que las pérdidas por fraude se presentan a lo largo de la jornada del cliente, la creación de cuentas nuevas y el punto de distribución parecen ser los más susceptibles a fraude en EE. UU.[11]

05 Aumento en frecuencia de estafas

La apropiación de cuentas y las estafas de ingeniería social, que incluyen el fraude de pago push autorizado (APP) de romance, inversión y suplantación, están entre los delitos financieros de más rápido crecimiento. De hecho, el 98 %[12] de los ataques cibernéticos se basan en la ingeniería social. Debido a la dificultad para detectarlas, estas estafas constituyen un desafío global emergente.

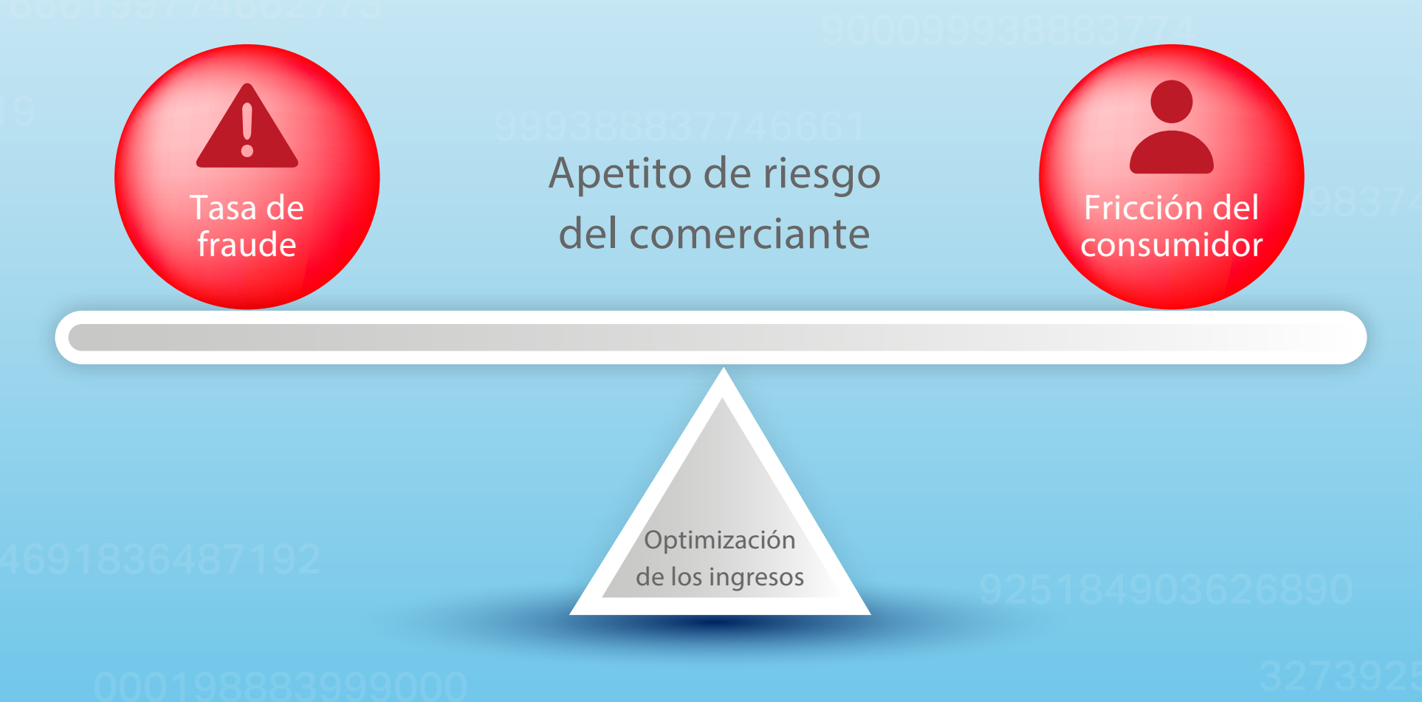
Reino Unido
El fraude de APP aumentó 71 % en la primera mitad de 2021, con pérdidas por más de 482 millones de dólares[13]. En comparación, en todo el 2020 fue de 648 millones de dólares.[14]

Australia
Más de $ 126 millones de dólares perdidos solo en estafas de inversión, la mayor cifra de cualquier categoría.[15]

EE. UU.
Cerca de $ 1.200 millones de dólares perdidos por estafas de suplantación en 2020, impactando aproximadamente a una de cada cinco personas.[16]

06 Continúa el reto de equilibrar fraude y fricción

Las empresas luchan continuamente por hallar el equilibrio óptimo entre oportunidad y riesgo. Aunque cada pieza adicional de información personal proporcionada por los consumidores puede ayudar a reducir el fraude, también añade fricción a la jornada digital del usuario, lo cual lo puede alejar de la transacción. El equilibrio entre fraude y fricción es aún más difícil de lograr en numerosos canales (p.ej., móvil, web, punto de venta).



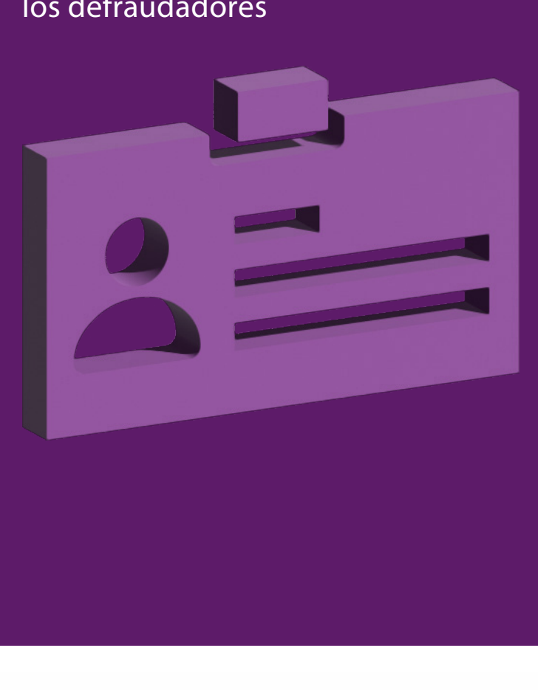
Acoplar incorrectamente métodos de autenticación al riesgo de la transacción puede generar fricción en la jornada digital del cliente, causando una reducción de las conversiones. Para seguir manteniendo bajo el fraude y ofrecer la cantidad correcta de fricción, los comerciantes y emisores están buscando soluciones de autenticación alternas para maximizar la experiencia del cliente y minimizar la fricción innecesaria durante los procesos de incorporación y pago.

07 Auge de identidades sintéticas

La creación de identidades nuevas combinando elementos de información real y falsificada es uno de los delitos digitales de más rápido crecimiento en EE. UU.[17] Impulsado por el crecimiento de la banca en línea y otros servicios financieros digitales, el fraude de identidad sintética se ha convertido en un problema multimillonario. También es uno de los tipos de robo de identidad más difíciles de detectar porque no hay una persona real que pueda reportar el fraude.

Cómo funciona la identidad sintética

Fragmentos de datos legítimos tomados por los defraudadores + información ficticia = creación de nueva identidad



Acumule información de datos legítimos
- Solicite tarjetas de crédito
- Obtenga préstamos
- Abra cuentas bancarias
- Solicite beneficios gubernamentales

08 Creciente costo de fraude

A raíz de la pandemia se registró la mayor cantidad de consumidores en los canales móviles y en línea. Con esto, no tardaron en llegar los defraudadores lo que provocó un aumento del volumen de ataques y, en consecuencia, del costo del fraude. Actualmente ambos indicadores son significativamente más elevados que antes del inicio de la pandemia.

$ 5.4 billones de dólares
costo global del fraude[18]

9.9 %
aumento en el costo del fraude para firmas de servicios financieros estadounidenses. Cada dólar en pérdidas por fraude les cuesta 4 dólares a las firmas financieras estadounidenses (comparado con 3,25 dólares en 2019 y 3,64 en 2020).[19]

En Asia Pacífico , una transacción fraudulenta cuesta hasta 3,87 veces el valor de la transacción perdida, en comparación con 3,40 en 2019.[20]

En Latinoamérica, una transacción fraudulenta cuesta hasta 3,68 veces el valor de la transacción perdida, en comparación con 3,46 en 2019.[21]

Las pérdidas por fraude en el Reino Unido se estiman en
$ 185 mil millones de dólares[22]

09 Mayor necesidad de evaluación de fraude multicapa

Hoy en día, los defraudadores lanzan ataques complejos con múltiples vectores, continuamente desarrollan nuevas estrategias para eludir controles y explotar debilidades. Un enfoque multicapa que incluya identidad física, inteligencia de identidad digital y biometría del comportamiento es una de las mejores defensas para mitigar el riesgo de fraude.

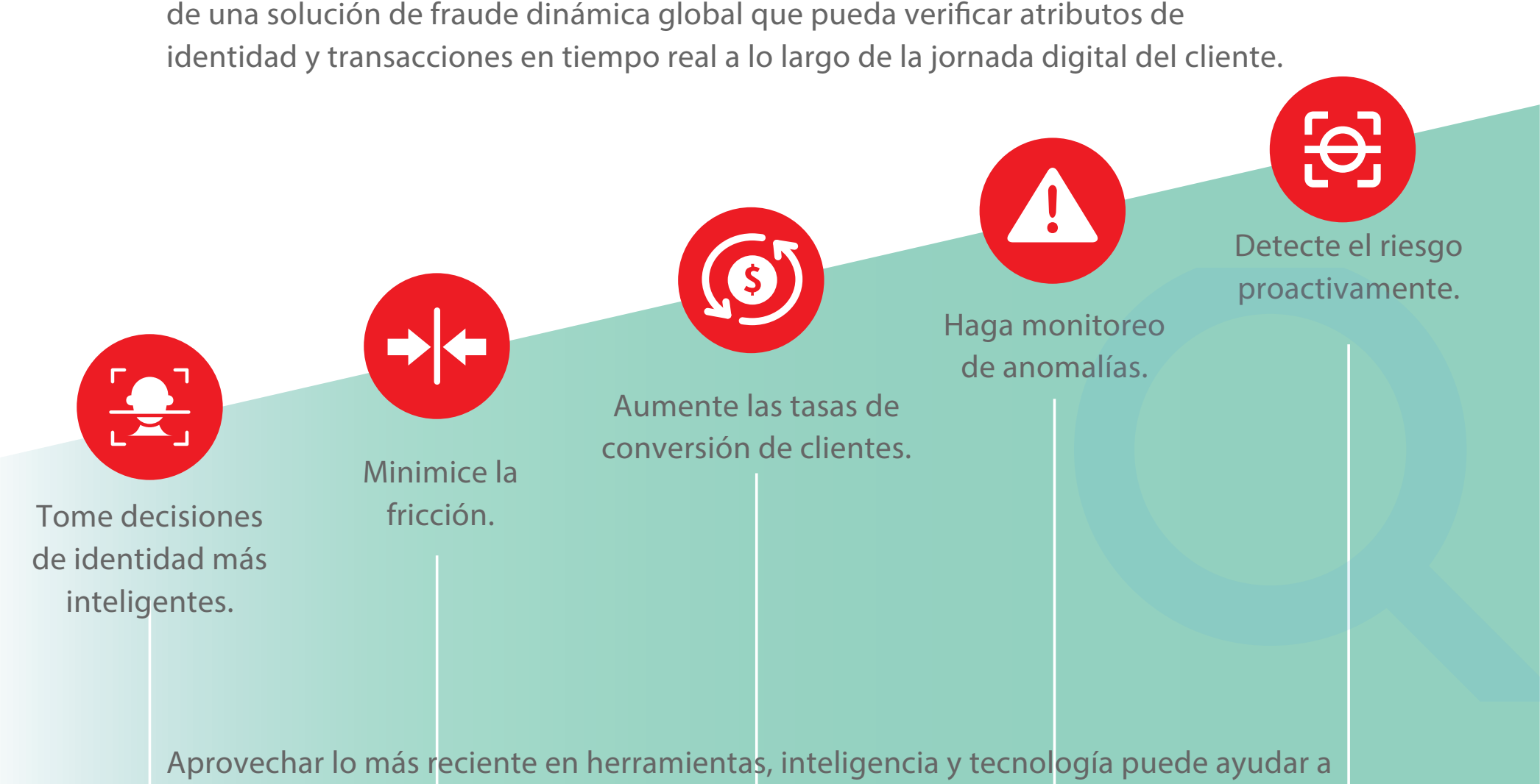
La biometría del comportamiento analiza cómo un usuario:

La biometría del comportamiento se puede utilizar para:

- detectar bots y suplantadores;
- identificar perfiles de clientes “buenos”;
- perfilar estafadores en forma confiable;
- reconocer interacciones inusuales;
- fortalecer la confianza de los clientes buenos.

10 Se acentúa la necesidad de evaluar los riesgo en tiempo real

La tendencia ascendente de las actividades móviles y en línea destaca la necesidad de una solución de fraude dinámica global que pueda verificar atributos de identidad y transacciones en tiempo real a lo largo de la jornada digital del cliente.



Aprovechar lo más reciente en herramientas, inteligencia y tecnología puede ayudar a las organizaciones a minimizar el riesgo de fraude y mantenerse un paso adelante de los rápidos cambios en las estrategias de los criminales.

Descubra cómo LexisNexis® Risk Solutions reúne gestión de fraude, verificación de identidad y perspectivas de riesgo aprovechando la inteligencia en red, el monitoreo global confiable y la propiedad intelectual para permitir a su empresa distinguir con certeza entre un cliente legítimo y una amenaza, manteniendo a la vez una experiencia de cliente fluida.

risk.lexisnexis.com/fraude

LexisNexis® RISK SOLUTIONS

Sources:

[1] https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
[2] https://f.datasrvr.com/fr1/521/90994/0031_Financial_Cost_of_Fraud_2021_v5.pdf
[3] https://www.statista.com/outlook/dmo/fintech/digital-payments/worldwide#transaction-value
[4] https://www.bbc.com/news/business-59433904
[5] https://www.cbinsights.com/research/report/buy-now-pay-later-outlook/#today
[6] https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/
[7] https://www.businesswire.com/news/home/20211124006042/en/Global-Digital-Payment-Market-Report-2021-Transactions-Worth-7-Trillion-is-Expected-to-Shift-from-Cash-to-Card-and-Digital-Payments-by-2023---Forecast-to-2028---ResearchAndMarkets.com#:~:text=The%20global%20digital%20payment%20market,the%20fintech%20sector's%20technological%20developments
[8] https://www.propertycasualty360.com/2021/06/22/fraudsters-targeting-financial-services-more-than-any-other-industry-in-2021-414-204577/?slreturn=20220117094312
[9] https://www.businesswire.com/news/home/20210425005002/en/Juniper-Research-eCommerce-Losses-to-Online-Payment-Fraud-to-Exceed-20-Billion-Annually-in-2021/
[10] https://www.outseer.com/wp-content/uploads/Outseer-Fraud-Report-Q32021.pdf
[11] https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#financialservices
[12] https://purplesec.us/resources/cyber-security-statistics/
[13] https://www.finextra.com/newsarticle/38884/app-fraud-losses-overtake-card-crime-in-h1-2021
[14] https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf
[15] https://www.scamwatch.gov.au/scam-statistics
[16] https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf
[17] https://www.fbi.gov/audio-repository/ftw-podcast-synthetic-ids-010220.mp3/view
[18] https://f.datasrvr.com/fr1/521/90994/0031_Financial_Cost_of_Fraud_2021_v5.pdf
[19] https://risk.lexisnexis.com/about-us/press-room/press-release/20220106-annual-true-cost-of-fraud-study
[20] https://risk.lexisnexis.com/global/en/insights-resources/research/apac-true-cost-of-fraud-study#:~:text=Depending%20on%20the%20market%2C%20the,other%20APAC%20markets%20at%203.40
[21] https://www.prnewswire.com/news-releases/true-cost-of-fraud-study-reveals-fraud-costs-3-75-times-the-lost-transaction-value-for-each-fraudulent-transaction-in-mexico-301403618.html#:~:text=Every%20fraudulent%20transaction%20now%20costs,digital%20transactions%20during%20the%20pandemic
[22] https://f.datasrvr.com/fr1/521/90994/0031_Financial_Cost_of_Fraud_2021_v5.pdf

---

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 la zona 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 risk.lexisnexis.com, relx.com