LexisNexis®
RISK SOLUTIONS

LexisNexis® Financial Crime Digital Intelligence

Mejore sus procesos de conocimiento de clientes en canales digitales y mitigue potenciales riesgos

La inteligencia de identidad digital, así como la información de georeferenciación, puede ayudar a identificar mejor riesgos relacionados con entidades sancionadas, pero sobre todo mejorar la experiencia del cliente.

En estos tiempos inéditos, los consumidores y las empresas están recurriendo cada vez más a las transacciones digitales como parte de la “nueva normalidad”—sin embargo, también lo hacen los delincuentes. Los delitos financieros en general están a la alza. Los canales digitales no son la excepción y cada día vemos como esto atrae la atención de autoridades y entidades reguladoras.

El crecimiento del volumen de transacciones en línea ha generado un incremento de delitos financieros digitales. Los canales digitales siguen representando la mayor porción de los costos del fraude para las empresas de comercio electrónico así como instituciones financieras en América Latina.[1] Además de la verificación de identidad, la capacidad de distinguir entre clientes legítimos y *bots* maliciosos es crítica, pero no se puede hacer a costa de una experiencia sin fricción del cliente, por lo cual equilibrar la prevención de delitos financieros, mientras se mejora la experiencia del cliente, es una tarea cada vez más difícil.

Todo esto ocurre en un momento en que las transacciones e interacciones digitales en los mercados se aceleran en forma vertiginosa. **Se espera que las ventas minoristas del comercio electrónico pasen de 2,84 billones de dólares en 2018 a 4,88 billones de dólares en 2021.**[2] Según una encuesta realizada en 2020, el 53 % de los clientes prefieren abrir una cuenta bancaria nueva utilizando una aplicación móvil, sitio web u otro canal que no implique presencialidad.[3] A medida que continúa la adopción explosiva de la revolución digital, los delincuentes se están aprovechando del anonimato de los canales digitales, escondiéndose detrás de transacciones sin rostro y presentando una identidad física alterna que saben seguramente vulnerará los controles internos de las diferentes instituciones. Esto es especialmente cierto en el caso de entidades sancionadas, las cuales saben que no deben someter sus identidades reales al filtrado de listas de control y en caso de haber herramientas robustas como el bloqueo de IP, saben que pueden ocultar su verdadera ubicación con una VPN o *proxy* para eludirlas.

Los reguladores se están percatando de estas técnicas de evasión emergentes, tal como se evidencia en la reciente serie de medidas de cumplimiento de la OFAC y directrices de FinCEN y GAFI relacionadas con inteligencia de identidad y ubicación digital, las cuales indican que hay un creciente reconocimiento de que los controles tradicionales para identificar entidades sancionadas no son suficientes en la lucha contra el delito financiero en la era digital.

La evolución de los canales digitales y las actuales vulnerabilidades, han ocasionado que los retos se incrementen.

Las instituciones financieras y otras empresas se esfuerzan por equilibrar los beneficios de la transformación digital acelerada con el aumento del riesgo de delitos financieros y escrutinio regulatorio. Algunos de los principales problemas a los que se enfrentan los equipos de cumplimiento son:

- Los delincuentes aprovechan tecnologías tales como VPN y proxies que ocultan su verdadera ubicación.
- El volumen de alertas sigue creciendo cada año—se requieren cuatro horas (en promedio) para resolver una alerta de sanciones.[3]
- Los analistas están abrumados—cada año se pierde más de una semana de productividad debido a insatisfacción laboral.[4]

El resultado es que algunas empresas e instituciones financieras pueden estar, sin quererlo, no cumpliendo con las regulaciones e incurriendo multas exorbitantes, daño reputacional y una afectación significativa de sus operaciones en general. Muchas empresas no han modificado sus estrategias para mitigar el delito financiero que se perpetúa por medio de identidades falsas o prestadas, de tal forma que dichas estrategias incluyan una evaluación exhaustiva del riesgo de la identidad digital que puede estar detrás de las identidades físicas suministradas. Todo esto sucede mientras sigue aumentando la presión por parte de los reguladores, y las consecuencias de no cumplir pueden ser catastróficas.

La OFAC promulgó recientemente una serie de medidas de cumplimiento relacionadas con la omisión del bloqueo de transacciones originadas en países sancionados cuando una organización penalizada tenía alguna inteligencia de dirección IP o ubicación que podría haber utilizado para evaluar donde se originó una transacción.

Multa de la OFAC en febrero de 2020 > 7,8 millones de dólares relacionada con una empresa de telecomunicaciones.[5]

Una compañía de tecnología estadounidense fue sancionada por no bloquear transacciones en billeteras digitales basadas en dirección IP.[6]

En abril de 2021, una empresa de software fue multada por vender soluciones ofrecidas por sus clientes en un país sancionado.

A medida que el delito financiero sigue evolucionando rápidamente en la era digital, la adaptabilidad es clave. La detección de la evasión digital requiere soluciones digitales. Las compañías deben determinar rápidamente y casi en tiempo real, si el comprador en una transacción anónima representa un verdadero riesgo de sanciones—sin aumentar falsos positivos, incrementar cargas de trabajo manual o generar fricción injustificada a clientes leales. Lamentablemente, los métodos tradicionales de mitigar estos riesgos, que implican más que todo procesos retrospectivos manuales que dependen en gran medida de la identidad física únicamente, solo agregan fricción a la experiencia del cliente. Las buenas prácticas y las herramientas de cumplimiento contra el delito financiero simplemente no se han mantenido a la par de la evolución del riesgo de la transformación digital—hasta ahora.

Se requiere una solución innovadora para el cambiante delito financiero digital.

Al seguir acelerándose los cambios en las técnicas de evasión en los delitos financieros y en el comportamiento del consumidor, el enfoque del *statu quo* hacia el cumplimiento ya no es suficiente en nuestra nueva normalidad digital. Es hora de emplear el rastro digital, único y en tiempo real, que dejan los consumidores al recorrer el mundo digital, y así ganarle a los delincuentes financieros en su propio terreno.

Presentamos **LexisNexis® Financial Crime Digital Intelligence,** una innovadora solución para el cumplimiento contra el delito financiero digital que utiliza la potencia de la inteligencia global compartida de identidad y ubicación digital de LexisNexis® ThreatMetrix® para que juntos combatamos el delito financiero. LexisNexis® Financial Crime Digital Intelligence permite a las organizaciones identificar mejor y casi en tiempo real el verdadero riesgo de sanciones utilizando políticas hechas a la medida y flujos de trabajo automatizados que corresponden a su apetito de riesgo. LexisNexis® Financial Crime Digital Intelligence permite:

Identificar mejor el verdadero riesgo de sanciones basadas en ubicación dentro del canal digital, utilizando la inteligencia colaborativa de identidad y ubicación digital de la red de identidad digital de LexisNexis ThreatMetrix para detectar entidades que han estado asociadas previamente con transacciones originadas en una ubicación sancionada.

Reconocer entidades existentes que podrían estar intentando evadir controles como bloqueo de IP, al ocultar su verdadera ubicación con tecnologías tales como *proxies* o VPN.

Combinar la inteligencia de identidad y ubicación digital con datos tradicionales de delitos financieros para crear flujos de trabajo automatizados que reducen falsos positivos y generan eficiencias.

Acelerar investigaciones y cumplir requisitos regulatorios emergentes relacionados con identidad y ubicación digital utilizando herramientas dinámicas de visualización de identidad.

Al trabajar con el equipo de LexisNexis® Risk Solutions, usted puede crear políticas hechas a la medida y flujos de trabajo automatizados que reflejan su tolerancia al riesgo, para identificar mejor el riesgo real de sanciones y crear eficiencias en su proceso actual. Aunque esta solución no es un reemplazo para su proceso de filtrado estándar, provee otra barrera sólida para detener a los delincuentes, reduciendo la exposición de su organización tanto al riesgo para el cumplimiento como al daño reputacional.

Para más información visite risk.lexisnexis.com/cumplimiento

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 la ciudad 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 ayudan a las organizaciones a prevenir los delitos financieros, lograr el cumplimiento regulatorio, mitigar el riesgo de negocios, mejorar las eficiencias operativas y aumentar la rentabilidad.

[1] El verdadero costo del fraude en América Latina 2021, LexisNexis Risk Solutions

[2] 99Firms, Ecommerce Statistics, 99firms.com/blog/ecommerce-statistics/

[3] 2020 Accenture Global Banking Study, accenture.com/_acnmedia/PDF-144/Accenture-Infographic-Banking-Consumer-Study-2020.pdf#zoom=50

[4] El verdadero costo del cumplimiento contra los delitos financieros - edición América Latina 2020

[5] home.treasury.gov/system/files/126/20200226_sita.pdf

[6] home.treasury.gov/system/files/126/20201230_bitgo.pdf