LexisNexis®
RISK SOLUTIONS

LexisNexis® Financial Crime Digital Intelligence

Reduza o risco crescente de compliance contra crimes financeiros em operações digitais

Identidade digital e inteligência de localização podem ajudá-lo a melhor identificar riscos de sanções ao mesmo tempo em que aprimora a experiência do cliente.

Nesses tempos sem precedentes, não são só os clientes e as empresas que recorrem, cada vez mais, às operações digitais como parte do seu "novo normal", mas também os criminosos. As atividades de crimes financeiros estão em ascensão e indicadores de alto risco estão sendo encontrados em diversos vetores de ameaças em operações digitais, chamando a atenção dos reguladores.

O aumento no volume das operações online gerou crescimento dos crimes financeiros digitais, já que os canais digitais continuam representando a maior parcela dos custos de fraudes para os comerciantes dos Estados Unidos e Canadá.[1] Além da verificação de identidade, é fundamental ter a capacidade de distinguir clientes legítimos, de *bots* nocivos, mas isso não pode ser às custas da experiência do cliente, o que torna mais desafiador do que nunca o equilíbrio entre prevenção de crimes financeiros e atritos.

Tudo isso acontece em um momento em que as operações e as interações digitais entre os mercados estão se acelerando a uma velocidade impressionante. **Espera-se que as vendas do comércio eletrônico global, que em 2018 somaram US$ 2.84 trilhões, cheguem a US$ 4.88 trilhões em 2021.**[2] Em 2020, 53% dos clientes entrevistados preferiram abrir uma nova conta bancária através de um aplicativo móvel, website ou outro canal sem interação presencial.[3] À medida que a revolução digital continua sendo altamente adotada, os criminosos tiram proveito do anonimato dos canais digitais, escondendo-se por trás de operações sem rosto, evitando serem detectados e apresentando identidade física alternativa, que sabem que será aprovada pelas verificações de compliance tradicionais para screening de nomes. Isso é especialmente verdade para as sanções. Entidades sob sanções sabem que não devem apresentar a sua identidade verdadeira para o screening de nome de lista de inspeção e, caso ferramentas contundentes, como bloqueio de IP, estiverem implementadas, que para contorná-las, também devem ocultar a sua localização verdadeira com uma VPN ou proxy.

Os reguladores estão ficando mais espertos com relação a essas técnicas de evasão e vetores de ameaças em ascensão, conforme ficou provado por uma recente onda de fiscalizações da OFAC e orientações da FinCEN e do GAFI relacionadas a identidade digital e inteligência de localização, que indicam um reconhecimento emergente de que os controles tradicionais de sanções do passado não são suficientes para combater os crimes financeiros na era digital.

Os desafios de compliance transbordam à medida que os criminosos invadem o ambiente dos clientes

As instituições financeiras (IFs) e outras empresas enfrentam dificuldades para equilibrar os benefícios da acelerada transformação digital, com maior risco de crimes financeiros e investigação regulatória. Algumas das principais condições enfrentadas pelas equipes de compliance incluem:

- Os criminosos aproveitam tecnologias como VPNs e proxies que escondem a sua localização verdadeira.
- Os volumes de alertas continuam crescendo todo ano—e um alerta de sanções leva, em média, quatro horas para ser esclarecido.[3]
- As análises são desgastantes—perde-se meia semana de produtividade por ano devido a insatisfação no trabalho.[4]

Como resultado, algumas empresas e IFs podem inadvertidamente se encontrar descumprindo as regulamentações e sofrer multas exorbitantes, danos à reputação e interrupção significativa das operações comerciais. Muitas organizações não dinamizaram as suas abordagens de mitigação de crimes financeiros perpetuados por trás de identidades falsas ou emprestadas em canais digitais, incluindo uma avaliação de risco meticulosa da identidade digital que pode estar por trás das identidades físicas fornecidas. Tudo isso acontece enquanto o escrutínio do vigilante continua crescendo e as consequências do não cumprimento podendo ser terríveis.

A OFAC promulgou recentemente uma série de ações de execução relacionadas à falha no bloqueio de operações originadas de países sob sanções, quando a organização penalizada exibia um endereço IP ou inteligência de localização que poderia ter sido usado para avaliar o local de origem da operação.

Uma multa aplicada pela OFAC em fevereiro de 2020 > US$ 7.8 milhões envolvendo uma empresa de telecomunicações.[5]

Uma empresa de tecnologia dos EUA foi penalizada por não bloquear operações em carteiras digitais com base em endereço IP.[6]

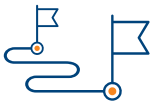
Em abril de 2021, uma empresa de software foi multada por vender soluções que seus clientes disponibilizavam em países sob sanções.

À medida que crimes financeiros continuam evoluindo rapidamente na era digital, a adaptabilidade se torna fundamental. A detecção de evasão digital exige soluções digitais. As empresas devem determinar rapidamente, em tempo quase real, se um comprador em uma operação sem rosto apresenta um risco verdadeiro de sanções, sem gerar falsos positivos, aumentar a carga de trabalho manual ou criar atrito indevido para clientes fiéis. Infelizmente, os métodos tradicionais de mitigação desses riscos, que costumam envolver processos manuais de retrovigilância, altamente dependentes apenas da identidade física, somente acrescentam atrito à experiência do cliente. As melhores práticas e ferramentas de compliance contra crimes financeiros simplesmente não acompanharam o risco crescente da mudança digital—até agora.

A evolução dos crimes financeiros digitais exige uma solução digital revolucionária

À medida que continuamos vendo mudanças cada vez mais rápidas nas técnicas de evasão de crimes financeiros e no comportamento do consumidor, a abordagem do *status quo* em relação ao compliance de sanções não é mais suficiente para o nosso novo normal digital. Está na hora de aproveitar a pegada digital exclusiva que os consumidores deixam em tempo real, enquanto estes cruzam pelo mundo digital, para derrotar os criminosos financeiros em seu próprio jogo.

Apresentamos o LexisNexis® Financial Crime Digital Intelligence, uma solução revolucionária para o compliance contra crimes financeiros digitais que usufrui do poder da identidade digital global compartilhada e da inteligência de localização do LexisNexis® ThreatMetrix,® para que, juntos, possamos superar os crimes financeiros. O Financial Crime Digital Intelligence permite que organizações identifiquem o real risco de sanções de forma melhor e em tempo quase real, usando políticas personalizadas e fluxos de trabalho automatizados que correspondem ao seu apetite de risco. O Financial Crime Digital Intelligence possibilita:



Identificar melhor o verdadeiro risco de sanções com base na localização no canal digital, usando a identidade digital e a inteligência de localização colaborativas da rede LexisNexis ThreatMetrix para identificar entidades que foram previamente associadas a operações originadas de um local sob sanções.

Reconhecer entidades que retornam, que podem estar tentando escapar dos controles de bloqueio de IP ao disfarçarem a sua verdadeira localização com tecnologias como proxy ou VPN.

Combinar identidade digital e inteligência de localização a dados tradicionais sobre crimes financeiros para a criação de fluxos de trabalho automatizados, reduzindo falsos positivos e aprimorando a eficiência.

Acelere investigações e atenda aos requisitos regulatórios emergentes relacionados à identidade digital e à localização utilizando ferramentas dinâmicas de visualização de identidade.

Trabalhar com a equipe da LexisNexis® Risk Solutions permite que você crie políticas personalizadas e fluxos de trabalho automatizados que atendem à sua tolerância de risco para uma melhor identificação do verdadeiro risco de sanções e resultem em eficiência no seu processo atual. Embora essa solução não seja um substituto do seu processo padrão de screening, ela fornece mais um grande obstáculo para combater criminosos, reduzindo a exposição da sua organização tanto ao risco de compliance como aos danos à reputação.

Para mais informações visite risk.lexisnexis.com/complianceBR

LexisNexis®
RISK SOLUTIONS

Sobre a LexisNexis Risk Solutions

A LexisNexis® Risk Solutions aproveita o poder dos dados e das análises avançadas para fornecer informações que ajudam empresas e governos a reduzir risco e melhorar a tomada de decisões, beneficiando pessoas no mundo todo. Fornecemos soluções de dados e de tecnologia para uma grande variedade de setores, inclusive de seguros, serviços financeiros, assistência médica e governos. Com sede na área metropolitana de Atlanta, Geórgia, contamos com escritórios por todo o planeta e fazemos parte do RELX (LSE: REL/NYSE: RELX), fornecedor global de análises baseadas em informações e ferramentas de tomada de decisão para clientes profissionais e empresas. Para mais informações, acesse www.risk.lexisnexis.com e www.relx.com.

As nossas soluções auxiliam organizações a prevenir crimes financeiros, alcançar o cumprimento de regulamentações, mitigar riscos comerciais, aprimorar eficiência operacional e aumentar a rentabilidade.

[1] risk.lexisnexis.com/insights-resources/research/2020-true-cost-of-fraud-retail

[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] pesquisa O real custo do compliance 2019, da LexisNexis Risk Solutions – Edição EUA e Canadá

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

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

O Financial Crime Digital Intelligence, fornecido pela LexisNexis, não é fornecido por “agências de informação de crédito”, conforme a definição do termo pela lei federal americana Fair Credit Reporting Act (15 U.S.C. Non FCRA § 1681, et seq.) (“FCRA”) ”) e não constitui “relatório sobre consumidores”, conforme a definição do termo pela FCRA. O Financial Crime Digital Intelligence não pode ser usado, em seu todo ou em parte, como fator de determinação de elegibilidade para crédito, seguro, emprego ou qualquer outro propósito com os quais um relatório sobre consumidor pode ser usado sob a FCRA. Devido à natureza e à origem das informações de registros públicos, estes e as fontes de dados comercialmente disponíveis usados em relatórios podem conter erros. A LexisNexis e a logomarca Knowledge Burst são marcas comerciais registradas da RELX Inc. A ThreatMetrix é uma marca comercial registrada da ThreatMetrix, Inc. Copyright © 2021 LexisNexis Risk Solutions. NXR14970-00-0621-PT-LA