LexisNexis®
RISK SOLUTIONS

LexisNexis® Financial Crime Digital Intelligence

Reduce growing financial crime compliance risk in digital transactions

Digital identity and location intelligence can help you better identify true sanctions risk while improving customer experience.

In these unprecedented times, consumers and businesses are increasingly turning to digital transactions as part of their "new normal"—but so are criminals. Financial crime activity is on the rise and high-risk indicators are being seen across numerous threat vectors in digital transactions, drawing the attention of regulators.

Increasing online transaction volumes have spawned a surge in financial crime as digital channels continue to represent the largest share of fraud costs for U.S. and Canadian retailers.[1] In addition to identity verification, the ability to distinguish legitimate customers from malicious bots is critical, but doing so cannot come at the expense of elegant customer experience, making balancing financial crime prevention with friction more challenging than ever.

All this is occurring at a time when digital transactions and interactions across markets have been accelerating at dizzying speed. **Global retail e-commerce sales of $2.84 trillion in 2018 are expected to reach $4.88 trillion in 2021.**[2] In 2020, 53% of surveyed customers prefer to open a new bank account using a mobile app, website or other channel not involving face-to-face interactions.[3] As the digital revolution continues to experience explosive adoption, criminals are taking advantage of the anonymity of digital channels, hiding behind faceless transactions to avoid detection and presenting as an alternate physical identity that they know will pass traditional compliance name screening checks. This is particularly true in the case of sanctions. Sanctioned entities know better than to submit their true identities for watchlist name screening, and if blunt tools such as IP blocking are in place, they are also wise enough to obsfucate their true location with a VPN or proxy in order to bypass them.

Regulators are becoming wise to these emerging evasion techniques and threat vectors, as evidenced by a recent slew of OFAC enforcements and FinCEN and FATF guidance related to digital identity and location intelligence that indicate an emerging recognition that traditional sanctions controls of the past are not sufficient for fighting financial crime in the digital era.

As criminals swarm the customer ecosystem, compliance challenges abound

Financial institutions (FIs) and other businesses are struggling to balance the benefits of accelerated digital transformation with increased financial crime risk and regulatory scrutiny. Some of the key issues facing compliance teams include:

- Bad actors leveraging technologies such as VPNs and proxies that hide their true locations
- Alert volumes continuing to grow each year—it takes four hours (on average) to clear a sanctions alert[3]
- Overwhelmed analysts—half a week of productivity is lost per year due to job dissatisfaction[4]

As a result, some businesses and FIs may unintentionally find themselves in default of the spirit of regulations and incur exorbitant fines, reputational damage and significant disruption to business operations. Many businesses have not pivoted their approaches to mitigating financial crime perpetuated behind false or borrowed identities in digital channels to include thorough risk assessment of the digital identity that may rest behind the provided physical identities. All this is occurring while watchdog scrutiny continues to grow, and the consequences of non-compliance can be dire.

OFAC has recently enacted a number of enforcements related to failure to block transactions originating from sanctioned countries when the penalized organization had IP address or location intelligence that could have been used to assess the originating location of the transaction.

A February 2020 OFAC penalty >$7.8M USD involving a telecom.[5]

A U.S. technology company was penalized for failing to block transactions in digital wallets based on IP address.[6]

In April 2021, a software company was fined for selling solutions that their customers made available in a sanctioned country.

As financial crime continues to rapidly evolve, adaptability is key. Detection of digital evasion requires digital solutions. Companies must quickly determine in near real-time whether a buyer in a faceless transaction presents a true sanctions risk—without driving up false positives, increasing manual workloads or creating undue friction for loyal customers. Unfortunately, traditional methods of mitigating these risks—which largely involve manual look-back processes heavily reliant only on physical identity—only add friction to the customer experience. Financial crime compliance best practices and tools simply haven't kept pace with the evolving risk of digital change—until now.

Evolving digital financial crime requires a game-changing digital solution

With rapidly-accelerating changes in financial crime evasion techniques and consumer behavior, the status quo approach to sanctions compliance is no longer sufficient for our new digital normal. It's time to harness the unique, real-time digital trail consumers leave behind as they traverse the digital world to beat financial criminals at their own game.

Introducing LexisNexis® Financial Crime Digital Intelligence—a game-changing solution for digital financial crime compliance that leverages the power of LexisNexis® ThreatMetrix® shared global digital identity and location intelligence, so we can outsmart financial crime together. Financial Crime Digital Intelligence enables organizations to better identify true sanctions risk in near-real time, using custom-designed policies and automated workflows that match their risk appetite. Financial Crime Digital Intelligence makes it possible to:

Better identify true location-based sanctions risk in the digital channel, using the crowd-sourced digital identity and location intelligence of the LexisNexis ThreatMetrix digital identity network to detect entities that have previously been associated with transactions originating from a sanctioned location.

Recognize returning entities who may be attempting to evade IP blocking controls by obfuscating their true location with technologies such as proxy or VPN.

Combine digital identity and location intelligence with traditional financial crime data to create automated workflows that reduce false positives and drive efficiencies.

Speed investigations and meet emerging regulatory requirements related to digital identity and location using dynamic identity visualization tools.

Working with the LexisNexis® Risk Solutions team, you can create customized policies and automated workflows that match your risk tolerance to better identify true sanctions risk and create efficiencies in your current process. While this solution is not a replacement for your standard screening process, it provides another strong barrier to thwart criminals, reducing your organization's exposure to both compliance risk and reputational damage.

The bottom line:

Decreased sanctions risk without adding friction to the customer experience

By harnessing the power of crowd-sourced digital identity and location intelligence, seamless customer experiences can coexist with effective sanctions controls. Organizations not currently managing sanctions risk in an automated, near real-time manner using this intelligence must act quickly to improve customer experience and avoid the escalating potential for financial and reputational fallout. LexisNexis® Risk Solutions helps companies keep pace with rapid changes to decrease the likelihood of transactions with undetected sanctioned entities while elevating the digital customer experience.

For more information, call 800.658.5638 or visit risk.lexisnexis.com/FCDI

LexisNexis® RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

[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] LexisNexis Risk Solutions 2019 True Cost of AML Compliance Study – U.S. and Canada edition

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

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