

CASE STUDY



LexisNexis® Risk Solutions Helps a Digital Currency Exchange Reduce Fraud by Preventing Fraudulent New Account Creations and Account Compromises

LexisNexis Risk Solutions helps detect and block use of stolen identity credentials in real time

AT A GLANCE

COMPANY

Crypto Currency Exchange

REQUIREMENTS

- To detect fraudulent new account creations.
- To identify and reduce account compromises.
- To reduce fraud losses.

SOLUTION

Working closely with LexisNexis Risk Solutions Professional Services team to define policies and models, interpret the data, and establish operational efficiencies. The exchange leveraged intelligence from the LexisNexis® Digital Identity Network® to accurately detect fraudulent activity in real time, including the use of stolen identity credentials and account compromises.

BOTTOM LINE

- Accurately identified fraudulent activity using stolen identity credentials.
- Reduction in fraudulent activity on the platform at account registration through to account compromises.
- Reduced customer friction, speeding up payments and transactions for trusted users.

Overview

This digital currency exchange allows users to buy and sell a variety of different cryptocurrencies and has a strong global footprint with over 10 million customers and over \$50 billion exchanged in digital currency. The platform services both merchants and consumers who want to transact with digital currencies such as Bitcoin, Ethereum, Litecoin and Bitcoin Cash.

The LexisNexis® Risk Solutions Professional Services team collectively has over 150 years of fraud and security experience, guiding and supporting customers to achieve fraud rates that are one-third of the industry average. Their leadership in state-of-the-art identity initiatives with Internet Top 500 customers helps facilitate more business online and saves hundreds of millions of dollars each year by securing accounts and payments against the most sophisticated threats.

Using intelligence from the LexisNexis® Digital Identity Network®, the exchange could better differentiate between good customers and criminals, the moment they landed on the site. In addition, it could:

- More accurately verify the identity of new customers wanting to open an account, to better prevent the infiltration of fraudsters attempting to launder money or finance global cybercrime.
- Accurately detect anomalies in payments transactions that might indicate a fraudulent account takeover.
- Identify instances of device and identity spoofing in real time.

Business Problem

Although cryptocurrencies have revolutionized the face of payments, investments and banking, they operate in a landscape of heightened risk, bringing together several features that cybercriminals value most. Cryptocurrencies present a huge opportunity for fraudsters to launder money and finance global cybercrime, providing anonymity, security and operating outside the jurisdictions of countries, governments and banks.

This marketplace was experiencing a number of fraudulent new account creations, which could potentially be mule accounts that could be used to launder money, as well as fraudulent payments, as cybercriminals attempted to hack in to good user accounts and then transfer cryptocurrency balances out. Furthermore, reports last month indicate a surge in transactions from OFAC listed countries as fraudsters attempt to benefit from the upward trajectory of cryptocurrency.

The Power of Global Shared Intelligence to Detect High-Risk Events in Real Time

The best way to tackle complex, global cybercrime is using the power of a global shared network. The LexisNexis® Digital Identity Network® collects and processes global shared intelligence from millions of daily consumer interactions including logins, payments, and new account applications. Using this information, LexisNexis® Risk Solutions creates a unique digital identity for each user by analyzing the myriad connections between devices, locations, and anonymized personal information. Behavior that deviates from this trusted digital identity can be accurately identified in real time, alerting the exchange to potential fraud. Suspicious behavior can be detected and flagged for review, step-up authentication or rejection before a transaction is processed, creating a frictionless experience for trusted users.

By partnering with LexisNexis Risk Solutions we have reduced fraudulent activity on the platform at account registration through to account compromises.

Key Features of the LexisNexis Risk Solutions/Currency Exchange Partnership

- **LexID® Digital** helps businesses go beyond simple device identification by connecting the dots between the myriad pieces of information a user creates as they transact online and looking at the relationships between these pieces of information at a global level and across channels/touchpoints. LexID Digital comprises a unique digital identifier, a confidence score and a visualization graph for each connecting user, which together act as a benchmark for the trustworthiness of current and future transactions.
- **Smart ID** identifies returning users that wipe cookies, use private browsing, and change other parameters to bypass traditional device fingerprinting tools. Smart ID improves returning user detection and reduces false positives. Derived from the analysis of many browsers, plug-in, and TCP/IP connection attributes, Smart ID generates a confidence score that detects multiple fraudulent account registrations from the same device.

CASE STUDY

- **Deep connection analysis technologies** provide the exchange a clearer view of suspicious events. Fraudsters often attempt to hide behind location and identity cloaking services such as hidden proxies, VPNs and the TOR browser. With Proxy piercing technology, LexisNexis® Risk Solutions examines TCP/IP packet header information to expose both the Proxy IP address and True IP address. These techniques help the exchange gain detailed network level signals for more accurate decision making.
- **LexisNexis® Risk Solutions Professional Services** team works closely with customers to understand business goals, evaluate security infrastructure and then rapidly implement LexisNexis Risk Solutions digital identity solutions, providing ongoing services including risk systems consulting and design.

Attempts to compromise digital wallets are increasing every day. With LexisNexis Risk Solutions we can accurately identify anomalies in payments transactions that indicates an account at risk of a takeover.



For more information,
call 866.528.0780 or visit risk.lexisnexis.com/FIM-EN

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 Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com, and www.relx.com

About ThreatMetrix

ThreatMetrix®, A LexisNexis® Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion tokenized digital identities, LexID® Digital delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time. ThreatMetrix is recognized as the sole Leader in the 2017 Forrester Wave™ for risk-based authentication.

LexisNexis, LexID, and the Knowledge Burst logo are registered trademarks of RELX. ThreatMetrix and Digital Identity Network are registered trademarks of ThreatMetrix, Inc. Copyright © 2019 LexisNexis Risk Solutions. NXR14086-00-0919-EN-US