How to Tap the Power of Virtual Assets Without Putting Your Business at Risk

Identity-based analytics is the key to security.

Throughout this paper we use the terms "virtual assets" and "virtual currency", but other acceptable terminology includes: digital currency, cryptocurrency, virtual money and digital money.

Virtual assets were primarily developed in response to a market desire to establish a new system, free from brokers or bankers, due to a distrust of traditional financial markets. Despite fluctuations in price, virtual currency value has risen immensely since its inception in the early 2000s. However, such exponential growth has also come with its share of risk.

The virtual currency market is a tempting target for cybercriminals trying to infiltrate virtual asset exchanges and compromise digital wallets. They've been quick to recognize vast potential in the unregulated, largely unsecure world of cryptocurrency.

Unlike traditional, government-issued currency, virtual currency doesn't have the layer of protection provided by financial institutions or agencies such as the Federal Deposit Insurance Corporation or the Financial Stability Bureau of the People's Bank of China. Victims of virtual asset crimes have limited recourse for recovering stolen digital currency.

Security threats

Cybercriminals typically use stolen identity credentials to deceive businesses and gain access to virtual currency. The identities may have been harvested from a data breach or phished via a scam. These credentials then allow the fraudster to:

- Take control of an account belonging to a legitimate customer, either using an automated bot attack to test credentials or via direct takeover
- Create a fraudulent new account application

Each of these methods can be defeated by:

- Digital and identity verification and risk-based authentication
- Differentiating between trusted and high-risk behavior in real time and on a per user basis
- Real-time anomaly detection

LexisNexis®
RISK SOLUTIONS

Since virtual currencies have minimal regulation and are not governed by a central authority, they've become an attractive vehicle for laundering money and financing criminal activity around the globe.

With new currency comes new challenges

Virtual assets have revolutionized the face of payments, investments and banking. However, the convenience they offer comes with the price of heightened risk. The anonymity associated with virtual assets makes them the currency of choice for cybercriminals. They use them to launder money and finance global cybercrime, taking advantage of the ability to operate outside the jurisdictions of countries, governments and banks.

Millions of new investors have entered the realm of virtual assets but many are unaware of the security risks, making them easy prey for cybercriminals. Hacks, malware, phishing attacks and virtual currency Ponzi schemes are common. Security is critical to supporting the ongoing development of the global digital economy.

When cybercriminals leverage stolen identities, organizations can have difficulty distinguishing between legitimate customers and fraudsters. Recent data breaches and the growth of crimeware tools have exacerbated the problem. Fraudsters are able to tap into the latest technologies to dupe digital wallet providers into setting up bogus accounts or processing fraudulent payments.

In the coming years, bots, malware and phishing schemes designed to steal virtual assets are likely to become as prevalent as email and phone-based scams. To accurately detect and mitigate the risk of fraud, while maintaining the frictionless experience that customers have come to expect, organizations will need to invest in the right tools and technology.

Identity intelligence: The key to security

The next generation fraud, identity and authentication solution will utilize multiple layers of defense to give organizations a single view of their transacting users across every online touchpoint. This will help identify and verify trusted users and authenticate them with minimal friction, while detecting high-risk behavior in near real time. This solution should be underpinned by global, digital identity intelligence, harnessed from billions of online events, growing more powerful with every new piece of information.

A digital identity-based solution can empower virtual currency exchanges and digital wallet providers to:

Stop fraudulent new account registrations

Prevent fraudsters from opening accounts with spoofed and stolen information. Fraudulent accounts are used to purchase virtual assets within a digital wallet.

Protect against takeover and unauthorized access of existing accounts

Defend existing accounts against phishing attacks, bad devices, malicious personas, shared passwords and keyword loggers often used by fraudsters.

Analyze subsequent access requests in real time

Minimize friction for legitimate users while identifying suspicious patterns, compromised devices, unusual locations (including attempts from known botnets or hidden proxies/VPNs) and suspicious configurations.

Identify the presence of malware on a legitimate user's device

Detect anomalies and threats on a device.

Minimize fraud-related losses

Prevent fraudulent transactions before they happen.

Recognize legitimate customers

Accurately authenticate trusted users.

Thwart payment fraud

Detect stolen credit cards in near real time by combining device attributes, malware detection and sophisticated analytics with the user's identity and transaction details.

Protecting your virtual assets

The use of virtual assets simplifies and accelerates the transfer of funds between two parties. It eliminates the need for a trusted third party such as a bank or credit card company, allowing users to circumvent hefty processing fees.

At the same time, the semi-anonymous nature of virtual assets and the ability to conduct transactions outside the jurisdictions of banks, countries and governments makes them appealing for a host of nefarious activities.

Organizations that want to safely tap into the power of digital currencies will need to invest in the right tools to protect their business and customers. Working with a data and analytics partner, one that has the latest identity-based technology to tackle security issues in the fast-evolving virtual assets market, is the best way to reduce risk.

LexisNexis®
RISK SOLUTIONS

For more information,
visit risk.lexisnexis.com/virtualassets

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