Stop cybercriminals from exploiting your platform while strengthening compliance

Navigate the current regulatory climate and threat outlook around crypto-cybercrime

The convergence of heightened regulatory oversight with increased cybercrime activity creates operations obstacles and pressures

Cryptocurrencies are **moving into the mainstream financial system and garnering more regulatory oversight** amid expanding expectations for increased Anti-Money Laundering (AML)/ Combating the Financing of Terrorism (CFT)compliance

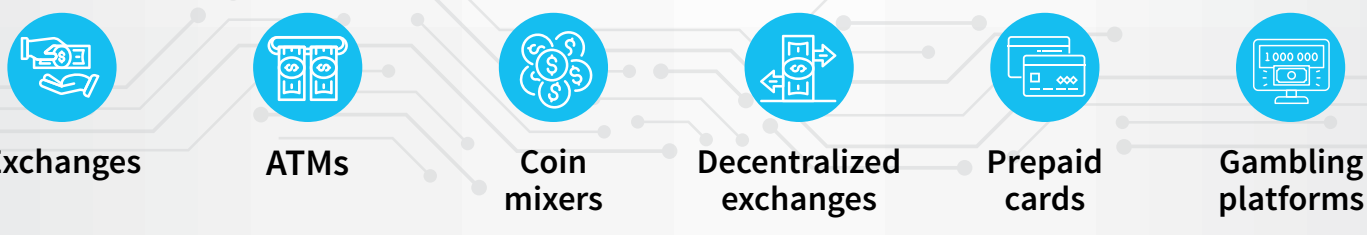
Cryptocurrencies are also the **expanding medium for the proceeds of cybercrime** which opens crypto- exchanges up to significant exposure to money laundering and financial crime risks

Virtual Asset Service Providers (VASPs) have to balance a strong compliance offense with a solid defense against criminal activities

To strengthen business sustainability, **VASPs must demonstrate a commitment to compliance that instills confidence** in trusted customers and partners from traditional Financial Institutions

Cybercrime schemes designed to leverage technology and the pseudo-anonymous nature of cryptocurrencies are everywhere

Technology also opens many avenues for cybercriminals to launder cryptocurrencies and evade detection



Regulatory agencies are taking notice of escalating crypto-cybercrime and expectations have expanded

New oversight of cryptocurrencies and VASPs from:

- Financial Action Task Force (FATF) Interpretative Note on **Recommendation 15**
- FATF Interpretive Note on **R16, Update to the Travel Rule**
- **Singapore Payment Services Act 2019**
- AUSTRAC: Digital Currency Exchange's need to **comply with AML/CFT Act 2006**
- Europe's **5th AML Directive**

Expanded regulatory expectations around:

- Complete and documented **due diligence**
- Performing thorough and ongoing **Know Your Customer, Customer Due Diligence** and **AML/CFT Screening**
- Increased **transaction monitoring**
- Understanding and **mapping relationships between originators and beneficiaries** in virtual asset transfers

Defend against crypto-cybercrime by taking advantage of digital identity intelligence

Digital identity intelligence and transactional behavior insights support a more dynamic, risk-responsive approach to due diligence that helps block the entire identity, not just the digital wallet.

Digital identity intelligence delivers a more unified view into:

Data: Devices, email, phone, address, payment amount and beneficiary

Location: IP address, GPS, activity patterns, proximity and distance anomalies

Link Analytics: Age of data attribute, history as a combined entity and activity velocity

Threat Analytics: Location masking, previous risk association and behavioural biometrics

Stay ahead of constantly escalating crypto-cybercrime threats and expanding regulatory expectations. Find out how our solutions can help you effectively protect against crypto-cybercrime and prioritize business growth.

For more information on our Financial Crime Compliance solutions visit:

https://risk.lexisnexis.com/KYC-EN

Get a Free Demo

LexisNexis® RISK SOLUTIONS