

Minimizing Cryptocurrency Transaction Risk for Issuing Banks

As cryptocurrency gains wider adoption, Issuing Banks may face significant counter-party transaction risks from customers interacting with high-risk crypto exchanges. To minimize that risk, and the associated costs of potential threats and scams, Issuing Banks need to have cryptocurrency intelligence that offers deep-insights into their customer's cryptocurrency activities including tracking for anti-money laundering (AML) and KYC risks. By monitoring these transactions, Issuers can ensure that funds transferred to Acquiring Banks are not tainted.

CipherTrace Armada provides the following intelligence for Issuers:



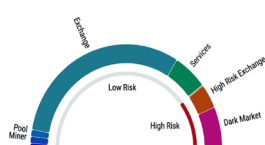
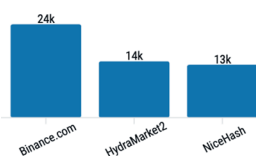
Privacy Coin	Yes
Fiat	Yes
Direct Onramp	Yes
Indirect Onramp	Yes
Offramp	Yes

Banks

Bank

Account

Routing



- **KYC Procedure Risk:** CipherTrace grades a VASP on their KYC practices, based on real-world interactions— not just what a VASP says they do for KYC.
- **Domicile Risk:** CipherTrace independently researches the legal domicile of each VASP and provides detailed information on these domiciles that can be used for risk assessment based on their registered location.
- **Asset Profile Risk:** CipherTrace identifies if VASPs support privacy coins like Monero or ZCash, which can make it easier to hide money laundering activities. Additionally, if there is support of Fiat and onramp/offramp capabilities.
- **Banking and Counterparty Relationships:** CipherTrace profiles a VASPs relationships with Financial Institutions.
- **B2B Risk:** Based on CipherTrace's attribution— the ability to tie crypto addresses and interactions to real-world entities— CipherTrace profiles the top 10 entities that a VASPs clients are sending and receiving funds to and from.
- **Transactional Risk:** CipherTrace profiles a VASPs attributed interactions with risky entities such as criminally controlled and sanctioned entities, ransomware and malware-associated addresses, gambling entities and more. CipherTrace also reveals the percentage of attributed interactions with often-opaque private wallets and high-risk exchanges.

Business challenges for Issuers:

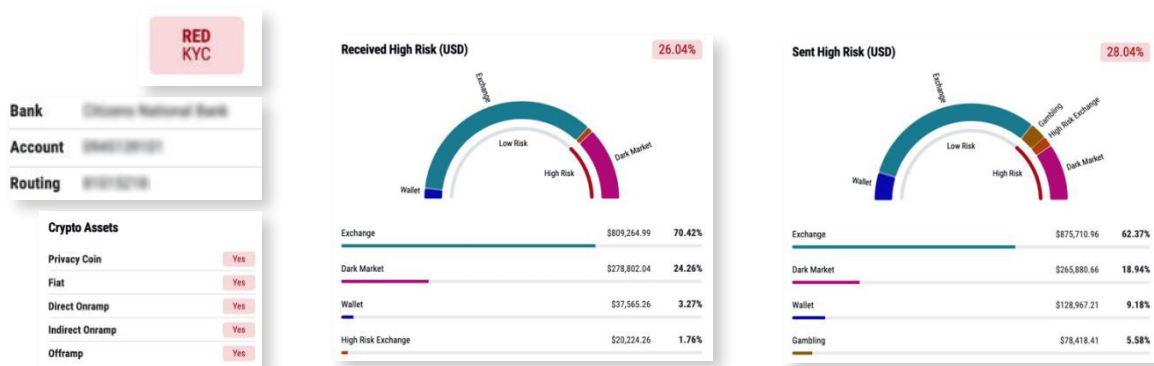
- Need to have monitoring controls in place to ensure that an Issuer's specific policies around the use or non-use of cryptocurrency are enforced.
- Mitigating against fraud & investment scams, often linked to funds being moved into cryptocurrency. (RTP/ACH deposits)
- Lack of visibility and trust with 3rd parties in the cryptocurrency space.
- Reduce rising operational costs due to lack of visibility into cryptocurrency transactions.
- Positioning their organization for economic growth in new markets, while putting in place safeguards to avoid criminal activity.

Results achievable with CipherTrace Armada:

- Easily flag high-risk fiat to cryptocurrency payments.
- Identify unregistered Money Service Business (MSBs) using client bank accounts.
- Reveal the risk associated with Virtual Asset Service Providers (VASPs) by their legal entity name.
- Prevent criminal exploitation of virtual currency products and platforms. CipherTrace datasets can be easily integrated into traditional AML and Fraud platforms.
- Adequately detect and identify risk exposures in the fast paced, constantly changing, cryptocurrency ecosystem.

Comprehensive blockchain analytics (from both on- and off-chain data) for identifying cryptocurrency counter parties and their associated risks

- CipherTrace Armada provides scorecards for each VASP so Issuers can easily view on- and off-chain risks.
- CipherTrace Armada Virtual Asset Feed can be ingested in traditional AML and Fraud platforms like NICE Actimize, BAE, Featurespace, Oracle, SAS, and Quantexa.
- CipherTrace Armada offers a dedicated graphical dashboard that empowers users to analyze historical data and trends to inform future decision-making by delivering actionable insights.
- With CipherTrace Armada, users can look at risk profiles for Virtual Asset Service Providers (VASPs) by their Credit Card Descriptors and Bank Accounts. Detailed risk analysis for each crypto entity is provided in a single dashboard view.



A high-risk entity's scorecard in CipherTrace Armada. The potentially hidden risks are immediately revealed.

About CipherTrace | CipherTrace develops cryptocurrency anti-money laundering (AML)/counter-terrorist financing (CTF), blockchain forensics, crypto threat intel and regulatory solutions. Leading exchanges, banks, auditors, regulators and digital asset businesses use CipherTrace to comply with regulatory requirements, investigate financial crimes, and foster trust in the crypto economy. For more information, visit: www.ciphertrace.com