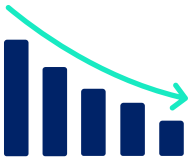
Cryptoassets
Regulation and Financial Crime

Joby Carpenter
Global SME – Cryptoassests and Illicit Finance
ACAMS

Overview



Crypto Winter

Since November 2021 cryptoassets have collectively collapsed losing almost $2 trillion in value with Bitcoin down approximately 70%. The collapse of algorithmic stablecoin TerraUSD led to contagion across the sector with firms such as Three Arrows Capital (a cryptoasset led hedge fund) and crypto lending platform Celsius being high-profile examples with tens of billions of dollars of losses.

Commentators have broadly welcomed the collapse of certain business models as helping to cleanse the market. However, individuals and institutions have been exposed to a sector accused of prioritizing short-term profit above integrity, a reluctance to accept regulation, zero compliance culture and, amongst some actors, a tendency to ignore criminal activity.

Financial Crime Compliance

Firms who wish to do the right thing will look to enhance their reputations for anti-money laundering (AML), fraud and market abuse controls in the minds of regulators, law enforcement and the media. Some firms are renowned for having high-quality financial crime frameworks with sophisticated technology and strong recruitment to attract anti-financial crime (AFC) professionals.

Largescale exchanges can demonstrate compliance with AML requirements whereas others outside of current AFC regulation including stablecoins, DeFi applications and non-fungible token providers have more limited capabilities. A risk-based approach with a full complement of AML controls remains nascent in some firms, highlighting AML/CTF deficiencies.

More TradFi firms see the advantages of proprietary blockchain technology, investment in Web3 and opportunities presented by tokenization through the blockchain. Other TradFi firms have maintained clear risk appetite statements outlining restrictions and prohibitions against crypto-based services. Firms will look to broaden their exposure in parallel with increased regulatory oversight.

Threats

Over the crypto winter multiple examples of criminal exploitation including money laundering, cybercrime, market abuse, fraud and sanctions evasion have been exposed. This has led to concerted activity by law enforcement and regulators to act against criminal activity including using supervisory powers intended for other activity.

Regulators have acted to curtail financial crime whilst seeking to balance calls for innovation and investment. ATM providers have been barred from registration, wire fraud laws used to prosecute market manipulation and safeguards put in place on retail promotions. Utilizing these tools is a stopgap whilst multilateral organizations devise policies for domestic regulators to implement.

Despite a series of liquidations, defaulted loans and liquidity traps, financial crime remains a priority. The war in Ukraine, the rapidly expanded sanctions regime and an unrelenting series of hacks continue to cause serious concerns amongst national authorities. The intersection between the blockchain and financial crime is at the nub of improved relations between different sectors.

Mitigating Actions

The cryptoasset sector can enhance its reputation by learning from its early mistakes. Sharing intelligence, attending public-private partnerships and outreach to regulators will help bridge the current divide. The sectors' messaging must also reflect progress in a comparable way to earlier disruptive sectors such as money service businesses.

Whilst overall criminality declines in proportion with legitimate uptake, volume of criminal abuse continues to climb. Advancements in cryptoasset forensics and often superior technology should be leveraged. Work to share typologies, report market manipulation and campaigns against high harm crimes offer an opportunity to instill a strong, lasting top-down compliance culture.

International

Jurisdictions with requisite infrastructure, investment flows and regulatory frameworks will be at the forefront of blockchain and Web3 development. Concurrently the same jurisdictions will be targeted by criminal and hostile state activity against the cryptoasset sector. These jurisdictions include USA, UK, France, UAE, Singapore, South Korea and Japan.