CRYPTOASSETS: ECONOMIC CRIME THREATS AND RISKS

PLENITUDE

INTRODUCTION

Whilst cryptoassets and their supporting infrastructure (such as cryptoasset exchanges) are becoming rapidly more popular and multi-purposed (e.g. Paypal opening up to cryptocurrencies), perceptions remain widespread that they are the preferred medium for criminals seeking to launder their illicit funds. The recently published UK National Risk Assessment of Money Laundering and Terrorist Financing 2020[i] made the following observations relating to the vulnerability of cryptoassets to abuse:

- They are pseudo-anonymous in nature – users are not able to be easily or immediately identified on the distributed ledger (blockchain) that records the provenance of a cryptoasset due to the use of pseudonyms and keys rather than real world identities. This means that users can employ a degree of obfuscation to hide their identity;
- They are easily accessible and have global reach – cryptoassets enable criminals to quickly move funds across national borders at scale, without requirement for a face-to-face business relationship;
- Uneven regulatory requirements leads to regulatory arbitrage – some jurisdictions do not require firms facilitating the exchange of cryptoassets to perform adequate due diligence checks on customers and their transactions.

Our collective understanding of the ML/TF risks presented by cryptoassets has developed considerably in recent years through the sharing of case studies, indicators and red flags identified by law enforcement and the private sector, facilitating the sharing and understanding of information through initiatives such as the public-private-partnership (PPP), Joint Money Laundering Intelligence Taskforce (JMLIT).

> "What baseline controls do we have in place to identify customers? Do we have institutional or peer-to-peer virtual currency customers? How does our financial institution interact with emerging payment systems? Do we have the tools we need to identify and report potentially suspicious activity occurring through our financial institution?"

KENNETH A. BLANCO

DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK (SEPT 2020)

CRYPTOASSET ML/TF THREAT ENVIRONMENT

Multiple risks have been identified across the breadth of cryptocurrencies, the infrastructure that supports their use (e.g. exchanges and digital wallet providers) and their underlying distributed ledger technology. The Financial Action Taskforce (FATF) and Department of Justice (DOJ) have highlighted the continuing money laundering / terrorist finance risks associated with cryptoassets. With a $4bn US money laundering investigation[ii] and increasing evidence indicating more widespread criminal use, the scale of wider economic crime risks from cryptoassets has expanded as use of cryptoassets has become more mainstream. In other recent cases, cryptoassets have been used to launder proceeds earned from selling fraudulent COVID-19 medicine. This paper builds on our first briefing paper and focuses on the risks presented by crystalised economic crime threats that fall under the scope of current (and future) regulated activity.

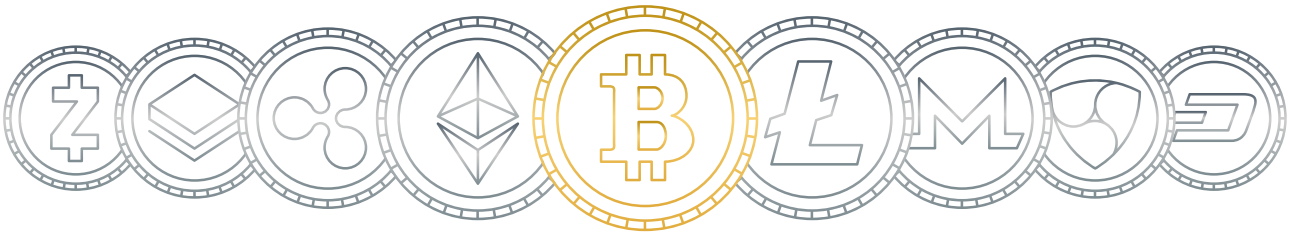
It is inevitable that individuals conducting transactions via primarily centralised crypto-exchanges present a risk of money laundering as they account for 99% of all cryptocurrency exchange trading activity. KYC Controls within exchanges' is judged to be historically weak considering they provide users with the ability to buy, sell and exchange cryptoassets quickly and anonymously. However, as regulatory expectations broaden, further activity is captured in scope and scrutiny leads to more enforcement activity and AML frameworks develop innovative approaches to financial crime, mitigation can be effective.

A new generation of crypto-currencies (also known as privacy coins), such as Monero and ZCash, have emerged to challenge the previously dominant Bitcoin. These new currencies have enhanced levels of security and anonymity which makes them extremely difficult to trace.

The FATF requires that service providers, such as exchanges, be able to manage and mitigate the risks associated with engaging in activities with these types of cryptoassets. Even with progress being made in tracing illicit money flows, exchanges and other FIs whom consider themselves to be at low risk of exposure to cryptoassets will require enhanced controls to demonstrate to regulators that they can mitigate the threat posed by privacy coins.

Until recently, evidence to indicate that terrorist groups and individuals were using cryptoassets to raise, move or store funds in the UK and elsewhere was limited. Recent reporting[iii] has demonstrated that some organisations appear to be diversifying away from traditional methods of terrorist financing such as cash couriers, MSBs and bank transfers despite their simplicity. Having already witnessed efforts by threat actors to evade sanctions (both at state level and by cyber criminals), any empirical increase in terrorist organisations using cryptoassets might necessitate an enhanced supervisory regime at multilateral and domestic levels. As with fiat currencies, the reputational risk of facilitating terrorist financing and/or sanctions evasion would be highly significant to any market participant.

The COVID-19 pandemic has seen an influx of cryptocurrency investment scams, where scammers are impersonating crypto traders or crypto exchanges promising investors high returns in exchange for buying cryptocurrency such as Bitcoin. Bitcoin is seemingly the cryptocurrency of choice for cybercriminals because of its dominance on the crypto market. It is the cryptocurrency most people are familiar with and therefore can lead to such schemes appearing more genuine to investors.



REGULATORY AND TECHNOLOGICAL DRIVERS

Due to the expanded scope of the UK's Money Laundering Regulations (MLRs), a number of the higher risk activities identified by the FATF's guidance on cryptoassets such as the exploitation of crypto automated teller machines (CATMS) and informal peer-to-peer transactions have been partially mitigated by regulation but still pose a high risk to intermediaries exposed to their use. It remains likely that limited KYC controls, the prevalence of bitcoin, and the anonymity these services offer mark them out as presenting high risk exposure to other entities.

As technology develops to improve cryptoasset transparency and Governments globally move towards harmonised regulation, it is likely that more secure and private blockchain models will continue to evolve. In addition, there is also the risk of regulatory arbitrage through crypto-to-crypto exchanges in weaker or non-regulated jurisdictions (the same risk applies to criminal use). Some industry observers have concluded that FIs might be missing up to 90% of crypto trading volume while looking for illicit activity[iv]. A continued investment by crypto-actors and other obliged entities in the monitoring and evaluation of cryptoasset risk and threats may be necessary to reduce firms risk exposure.

A positive development for the cryptoasset sector has seen new technology increasingly being adopted to prevent the misuse of cryptoassets for ML/TF purposes in order to screen out bad actors. The increase in AML and trade surveillance measures employed by cryptoasset exchanges and wallet providers bodes well for the industry and demonstrates that there are a variety of technological solutions to improve regulatory compliance with transaction monitoring and user verification. Such 'off the shelf solutions' can complement KYC verification and AML programmes designed to mitigate ML/TF risk and protect users at both ends of the transaction as well as companies who may have hidden exposure to cryptoassets.

Despite well-known historic failings, some cryptoasset firms registered in the UK and elsewhere are known to have adequate financial crime systems and controls and due diligence processes. Prior to the MLRs being extended to cryptoasset firms, some firms had already implemented more robust onboarding and due diligence checks, transaction monitoring systems, and customer analytics to more effectively mitigate financial crime risks. Some firms also made use of crypto-forensic services to detect criminal abuse. However, the quality of firms' control frameworks has so far proven varied. Regulators will expect firms to maintain innovative monitoring controls and CDD solutions as well as meet other requirements under the MLRs such as conducting risk assessments and reporting suspicious activity.

New business models are emerging all the time in the cryptoasset marketplace; this creates new economic crime threats and regulatory risks and means that the regulatory framework needs to remain flexible in order to adapt to an ever-changing threat landscape. For example, current rules around physical entities such as exchanges and wallet providers may become redundant if, in future, the entity moving funds through the blockchain is not a physical entity that can be regulated, such as an artificial intelligence programme that effectively runs itself. The approach regulators take to the opacity of such business models will need to be cognisant of this fast-moving technological landscape.

Regulation of the cryptoasset sector remains nascent. FCA regulation currently captures those cryptoasset service providers who have a physical footprint within the UK and is premised on firms complying with the same requirements as banks and other financial institutions including the requirements for an MLRO governance function, registration by the FCA and regular reporting into the c-suite. In the UK, the regulatory framework is primarily focused on AML and TF, but in a fast-moving sector with innovative technology solutions, regulatory overlap between the alignment of technology and the scope of money laundering legislation is likely to mean further regulatory developments around definitions, international standards and a wider conduct regime.[v]

CONCLUDING THOUGHTS

Firms applying a risk-based approach need to be proactive in seeking out information about money-laundering trends, threats and typologies from external sources in order to update existing policies and procedures and enhance existing AML controls. Key considerations include:

- Establishing a horizon scanning capability and maintaining a comprehensive Obligation Register in order to keep on top of evolving regulations, leveraging proven tools such as Plenitude RegSight;[vi]
- Employing established strategic intelligence techniques in order to identify relevant typologies and update the existing AML risk assessment methodology;
- Developing an enhanced set of risk indicators or red flags based on the typologies identified and incorporate these into guidance, staff training and awareness initiatives;
- Perform analysis to identify any current controls (manual or automated) in place to mitigate money laundering risks and determine whether existing or new transaction monitoring scenarios could be used to monitor activity associated with the red flags;
- Compliance teams should maintain a close link with the business teams to understand any new products or services that will be offered in order to assess the risks and mitigate them with updated scenarios;
- Enhancing the existing controls testing and monitoring framework in order to identify and proactively address any gaps and weaknesses in the AML control framework.

Finally, at the centre of an intelligence-led ML/TF mitigation model is the public-private partnership ("PPP") – a collaboration between financial institutions, law enforcement and the regulatory community. Not only are PPPs an important first step in the ability to deliver operational benefits and efficiency gains (such as the real time ability to share and enrich intelligence), but they can also provide a framework to build positive relationships and dialogue between stakeholders. The establishment of a joint 'picture of threat' utilising evidence-based intelligence from the private sector is vital. Clearly there are outstanding issues across the public and private sector in the efficient sharing of intelligence. The private sector requires legal clarity and assurance that sensitive data sets and intelligence can be shared without fear of being punished for doing the right thing.

PLENITUDE CAPABILITY

Plenitude is actively supporting our clients address the risks associated with cryptoassets. This includes:

- Accelerating the assessment of risks associated with cryptoassets or cryptocurrency services based on detailed research including national/ supranational risk assessments;
- Producing strategic analysis on emerging and crystalised threats presented by the misuse of cryptoassets;
- Assessing clients existing AML control frameworks to ensure they comply with AML requirements and guidance;
- Developing a risk-based approach, including risk differentiation of clients based on usage of cryptoassets;
- Improving financial crime risk rating methodologies to appropriately identify and rate exposure to the risks associated with cryptoassets;
- Improving Customer Due Diligence procedures, transaction monitoring and KYC controls;
- Assisting integration with leading third-party cryptocurrency-specific AML solutions;
- Provision and delivery of bespoke cryptoasset risk training.

CONTACTS

Joby Carpenter
Senior Manager
E-mail: joby.carpenter@plenitudeconsulting.com

Alan Paterson
Managing Director
E-mail: alan.paterson@plenitudeconsulting.com

Ⓣ **+44 (0)203 102 9526**
Ⓔ **enquiries@plenitudeconsulting.com**
Ⓦ **www.plenitudeconsulting.com**

INFORM · PREPARE · TRANSFORM

Plenitude Consulting Limited, 30th Floor,
40 Bank Street, Canary Wharf, London E14 5NR