"'"At present, crypto-assets raise a host of issues around consumer and investor protection, market integrity, money laundering, terrorism financing, tax evasion, and the circumvention of capital controls and" international sanctions"

Mark Carney 'The Future of Money' March 2018

Crypto-assets and Financial Crime

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

Asad Choudhary
Partner
E-mail: asad.choudhary@plenitudeconsulting.com

Graeme Ford
Senior Manager
E-mail: graeme.ford@plenitudeconsulting.com

Alerts to UK financial institutions have recently been issued by the FCA over the financial crime risks associated with crypto-assets or crypto-currencies. Regulators in other jurisdictions are anticipated to apply a similar approach; hence the inclusion of specific requirements within the Fifth Anti Money Laundering Directive. EU regulators have also highlighted initial coin offerings (ICOs) and crypto-currencies as one of their priorities and the UK government has recently established a Crypto-assets Taskforce to explore the possibilities and risks arising from crypto-assets.

In response, financial institutions need to undertake a thorough risk assessment of their risk exposure. They may have to adjust their approach to financial crime risk management, even if they do not trade crypto-assets or crypto-currencies themselves.

Advocates of crypto-assets/currencies continue to praise them, while others are more measured in their commentary (see Mark Carney 'The Future of Money'). Given the early adoption phase of crypto-assets/currencies in the economy, it is increasingly evident that they bring increased financial crime risks and financial institutions must act promptly to avoid regulatory censure or potential enforcement action.

Crypto-Assets/Currencies Key Facts

- Crypto-currencies are exceptionally volatile with value driven by sentiment, utility, legal, governmental issues and market manipulation
- There are more than 1, 600 crypto-currencies
- Bitcoin is by far the largest crypto-currency with over $100 billion in market capitalisation
- Institutional investors have stayed on the sidelines (until recently)
- Crypto-currencies are not backed or regulated by a central bank or government
- A number of countries have outlawed crypto-currencies

What Financial Institutions Need to Do.

The FCA has stated that Banks should follow a risk-based approach in relation to crypto-assets and crypto-currencies. Plenitude advises financial institutions to take the following measures:

1. Review Existing Guidance and Regulation

Firstly, you should consult existing guidance and regulation along with SME input, in relation to crypto-assets and crypto-currencies. Advice and regulatory perspectives on the inherent risks of money laundering and terrorist financing associated with crypto-assets and crypto-currencies are readily available through national /supranational risk assessments.

Sanctions currently imposed by the authorities of key jurisdictions are another relevant source of information. Furthermore, some crypto-assets may be state-sponsored, for example Venezuela issued in February 2018 the "Petro", a crypto-currency considered by several analysts to be a means by which to evade international financial sanctions. It has also been rumored Russia will launch a "Crypto-Ruble" in 2019. However, it should be noted that state-sponsored crypto-assets are not only issued by sanctioned nations, for example Japan (J-Coin), Sweden (eKrona) are also similarly preparing their own ICOs.

Securities and Investments related regulation and guidance, although not specific to ICOs, are also relevant. The Financial Service Authority's review in 2012 of "Banks' defences against investment fraud" is an example. A further example is that of the US SEC where, under certain conditions, it may consider that ICOs constitute security offerings.

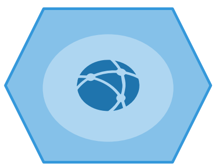
2. Identify Risk Exposure Through Crypto-assets

The second measure is to undertake an accelerated risk assessment of your risk exposure and where necessary, initiate remediation activity. A number of questions should be asked:

- Does your firm offer crypto-asset or crypto-currency related services?
- Do your clients or their counterparties offer services related to crypto-assets or crypto-currency?
- Do your clients or their counterparties accept crypto-assets and crypto-currencies in exchange for their products and services?
- Do your clients or their counterparties derive their wealth, either fully or partially, from trading in crypto-assets or crypto-currencies?

A cryptocurrency has no intrinsic value

A cryptocurrency doesn't physically exist; it only exists in a network



A crypto-currency is not controlled by a central authority and exists in a completely decentralised network

What Financial Institutions Need to Do.

Once your risk assessment is complete, you must identify the risk-based client segments. Depending on your financial institution's business, you may identify clear differences in the risks associated with clients operating with crypto-assets, depending on where they stand in the value chain; for example those that provide wallet services (storing crypto-currency for third parties) may have a different risk profile to those that provide exchange (crypto-currency to national currencies) or payment (cryptocurrency to crypto-currency) services; or different to those mining crypto-currency (validating transactions, updating the digital ledger and introducing new fresh currency). Other client segments may be rather defined by their source of wealth, you may find differences between the risk profile of clients that actively trade in crypto-currency, and those that invest in funds that maintain a position in crypto-assets (discretionary or non-discretionary), or those that hold shares in business operating with crypto-assets.

3. Define and Implement a Risk based Approach

Third, you should define a risk based approach, with differentiated risk management measures per client segment and proportionate to the associated risks. Measures will include enhanced scrutiny of your clients, counterparties or your clients' counterparties. This may mean performing enhanced due diligence on key individuals, including adverse intelligence, or assessing their investor base. It may include assessing the adequacy of your own arrangements in place to fight financial crime (e.g. financial crime risk assessment, policies, KYC/CDD, transaction screening and monitoring among other relevant controls).

4. Strengthen Policies, Procedures and Controls

The fourth measure is to update your anti-financial crime policies, procedures and controls, ensuring these clearly reflect crypto-asset and crypto-currency activities and your improved risk based approach.

Among the enhancements required, financial institutions will likely need to update their client risk rating methodologies. One example is that economic activity using crypto-assets and crypto-currencies is not often articulated in standard industry activity classifications (e.g. NACE, SIC) and you will need to improve your methodology to more clearly identify these.

As an improvement to your client due diligence procedures, depending on your risk exposure and client types, you may want to integrate with third party service providers that can trace the transaction history of your client in the crypto-currency's publicly available distributed transaction ledger.

Finally, a financial institution should also examine its transaction monitoring capabilities, and ensure not only crypto-assets are integrated into the transaction monitoring solution, but that the same standards are maintained (e.g. for sanctions screening or beneficiary information).

Plenitude Capability

Plenitude is actively supporting our banking clients address the risks associated with crypto-assets. This includes:

- Pro-actively incorporating the guidance received from the FCA and requirements of the Fifth Money Laundering Directive;
- Accelerating assessment of risks associated with crypto-assets or cryptocurrency services based on detailed research including national/supranational risk assessments;
- Developing a risk based approach, including risk differentiation of clients based on usage of crypto-assets;
- Improving financial crime risk rating methodologies to appropriately identify and rate exposure to the risks associated with crypto-assets;
- Improving due diligence procedures, transaction monitoring and;
- Assisting integration with leading third-party cryptocurrency-specific AML solutions;
- Provision and delivery of bespoke crypto-asset risk training.