Link to Article on website

Financial crime and cryptocurrencies

Whilst the challenges of cryptocurrencies may on the face of it appear to be new, the truth is that navigating the risks associated with them is familiar territory for experienced AML professionals.

WHEN I WAS DOING SOME RESEARCH for this article, I was struck by how many negative comments there are, for example, that cryptocurrencies are used by terrorists, by drug dealers, money launderers and other criminals. Well, yes this is quite possibly true. But, please remember that so is the mainstream banking system. Every debit card, every payment system known to man is used by terrorists, drug dealers and money launderers. Viewed in this way digital currencies are no better and no worse, than any other financial tool.

What sort of crimes are being committed using cryptocurrencies?

Tax evasion, money laundering, fraud, illegal arms trades, financial sanctions breaches, corruption, contraband transactions, human trafficking, terrorist financing and the theft of cryptocurrency itself. Cryptocurrencies are commonly used in the dark web markets, by criminal groups, by sanctioned countries, and by terrorist groups.

In addition, since ICOs became fashionable, there has also been a number of crimes around ICOs, most of all fraud and illegitimate ways of offering of securities and securities selling.

New AML risks?

Whilst cryptocurrencies are a new challenge for compliance teams to grapple with, the risks are no different to the types associated with Hawala and various other money services businesses, and products that store value such as on prepaid credit cards which are all high risks areas for both money laundering and terrorist finance. AML procedures and risk assessments will need to change regularly and keep up with the technological advances in this area. Failure to do so will give criminal gangs an easy way to beat their AML systems and controls.

Cryptocurrencies have no boundaries?

Digital currencies are not hindered or limited by political or geographic boundaries, allowing criminal gangs to relocate wealth across the globe quickly, hassle free, discretely and out of sight of the Regulators. Because of its peer-to-peer nature there is no distinction between domestic and international payments. This makes life much easier for cross border channelling of illicit funds.

Size of the risk

The size of this risk is growing each year. Rob Wainwright Executive Director of Europol recently told the BBC's Panorama that regulators and industry leaders need to work together to tackle the problem. Wainwright said that Europol, estimates that about 3%-4% of the GBP100 billion in illicit

proceeds in Europe are laundered through cryptocurrencies.

Why do enforcement agencies get so animated about cryptocurrencies?

What most upsets the law enforcement community is the word 'untraceable', but cryptocurrency activity is not actually untraceable. However, there are so-called "privacy coins," which provide personal anonymity and allow criminals to carry out covert transactions.

Blockchain activity is public ledger, so by definition the transactions are public and traceable. The only problem is that the authorities have no idea who the parties are in the transaction. The question is how much money is law enforcement, going to be able to spend on this, and how soon before they can catch up.

It is reported that some persons/entities have actually mapped some of the most popular cryptocurrency blockchains and identified a number of users based on public information on some transactions and behaviour. The owner of the public key can be identified in some cases in this way. However, there have also been reports that you can change your public key. Tracing crypto is made simpler when the recipient slips up and sends the sender his address through a traceable means (e.g. email). It is then possible to trace the address through the explorer, and find out how many similar sends there were to a particular recipient.

The FBI are spending a significant proportion of its financial crime-related budget investigating digital currency.

However, there are so-called "privacy coins," which provide personal anonymity and allow criminals to carry out covert transactions.

A sense of regulatory diversity

Regulation in itself is never sufficient to deter crime. Criminals just find new ways to circumvent those regulations. If a criminal chooses to invest and take advantage of advances in technology then law enforcement must also invest to keep up.

On January 18, 2018 Reuters reported - "Financial crime fighters at the U.S. Treasury are 'aggressively' pursuing virtual currency platforms that lack strong internal safeguards against money laundering...

"With more criminals using the emerging asset class to store and transmit their ill-gotten gains, Treasury's Financial Crimes Enforcement Network (FinCEN) will pursue malfeasant virtual currency platforms even if they are located overseas, Sigal Mandelker, the U.S. Treasury Department's undersecretary for terrorism and financial crimes, told the Senate Banking Committee."

Addressing this matter, a European Central Bank governing council member has been quoted as saying that the same rules ought to apply as in any other financial transaction, namely that everyone involved should reveal their identity. He was also reported as expressing frustration that the ECB had stopped printing 500-euro notes in order to fight money laundering, while at the same time anonymous transactions in cryptocurrencies such as bitcoin were proliferating.

Even though every country in the world now has anti-money laundering regulations, it was only one year ago that America brought in provisions requiring people to understand who the beneficial owners of companies are. Any expectation of global consensus on cryptocurrency regulation is still a long way off.

As cryptocurrency transactions are generally anonymous, which makes them vulnerable to being misused for unlawful activities. If a cryptocurrency intermediary is found to have used cryptocurrencies illegally, its operations could be shut down by law enforcement agencies. There is also a risk of loss should the cryptocurrency intermediary be hacked, as it may not have sufficiently robust security features.

The Monetary Authority of Singapore (MAS), the only regulator I am aware of which has spoken in favour of blockchain technology. They see valuable real-world applications, but it is important to note that they are differentiating the technology from the digital manifestations such as bitcoin. But regarding the cryptocurrencies themselves, the MAS has been careful to advise the public to act with extreme caution and to understand the significant risks they take on if they choose to invest in cryptocurrencies.

On August 1, 2017 the Monetary Authority of Singapore (MAS), said in a statement that ICOs are "vulnerable to money laundering and terrorist financing risks due to the anonymous nature of the transactions, and the ease with which large sums of monies may be raise in a short period of time."

In addition, MAS has proposed AML/CFT regulation for providers of services in cryptocurrencies in their Consultation Paper on Proposed Payment Services Bill, namely cryptocurrency exchanges.

Mark Carney, governor of Bank of England, recently said he thinks more regulations should be applied to exchanges in an effort to reduce the use of cryptocurrencies in financial crimes: "In my view, holding crypto-asset exchanges to the same rigorous standards as those that trade securities would address a major underlap in the regulatory approach," Carney said. It should also be noted that according to Andrew Bailey, head of the UK's Financial Conduct Authority (FCA), buying bitcoin is tantamount to gambling, in that it has a similar level of risk, and that it is not a currency.

It should also be noted... buying bitcoin is tantamount to gambling, in that it has a similar level of risk, and that it is not a currency.

The risk of misuse draws the attention of law enforcers and the Americans say that they are now developing software which will help them analyse transactions in order to identify those they want to invest more effort and time in.

But, as it appears right now, this market is not capable of being directly regulated. Why? Because nobody knows where it is. Whilst there is a record of what has happened, there is no record of exactly where it happened and who was involved.

Cryptocurrency market players

Many cryptocurrency market players have already introduced AML/CFT measures; for example, it is market standard with ICOs and with cryptocurrency exchanges. In some cases, the effectiveness may still be questionable, but the market players have become aware of their regulatory risk and are clearly moving to meet the general standards applicable to financial institutions. In fact, with ICOs standards are often applied more rigorously as all contributors, even when they pay an equivalent of SGD10, must provide documentation and are screened.

Jurisdictional competitive advantage

Exchanges can move jurisdictions as well, if rules or compliance become too onerous and other jurisdictions offer a simpler and less costly interface with the customer base.

Social media caution

Twitter and Google have recently banned all adverts for cryptocurrencies, including bitcoin and initial coin offerings (ICOs).

Cryptocurrencies and taxation

The US authorities are taking a different approach, treating cryptocurrencies such as bitcoin as a commodity. It is a mechanism for trying to hold people accountable and, not surprisingly as with most things in America to do with law enforcement, it is also a taxation issue and therefore has a revenue-generating aspect.

The IRS [The Internal Revenue Service in the US] has started to issue summons to coin exchanges to identify transactions.

Tax amnesty for cryptocurrency profits?

With millions of people now investing in cryptocurrencies, and with a high percentage of those investing having seen their investments grow significantly, it is of no surprise that tax authorities around the globe will want to get their taxable portion of those gains. At present, only a small proportion of tax returns are recording gains made from investment in cryptocurrencies. It is just a matter of time before the tax authorities start taking collection enforcement action. It may well be that given the number of people now engaged in this sort of cryptocurrency there may be incentives introduced such as a crypto currency amnesty to encourage rectification of historic tax returns.

… the market players have become aware of their regulatory risk and are clearly moving to meet general standard applicable to financial institutions.

The future

Perhaps the biggest problem right now is that the majority of people, do not understand the risks they are addressing. In addition, the security of cryptocurrencies themselves may get undermined as a consequence of greatly enhanced capabilities of quantum computers that may through their enormous processing power be able to hack a cryptocurrency key. There is already a race on to develop cryptography that could withstand such quantum computer attacks.

There must be a global regulatory standard that is applied consistently. The approach must address the risks cryptocurrencies represent. And law enforcement must be targeted and enabled to allow for effective action against wrongdoers. That will require significant new training of staff and significant new funding. There needs to be increased collaboration between international law enforcement and regulatory agencies to maximise disruption of these new means of money laundering for criminals. One thing is for certain, criminals will continue to try and find new ways to keep ahead of law enforcement, and will find the funds through illegitimate means to accomplish that end. ■