# CRYPTO CURRENCIES AND CRIMINAL CUSTOMERS:
# Taming the Crypto Wild West

## As someone who spends most of his life helping banks in the fight against financial crime, I always enjoy stories of hapless criminals caught in the act trying to get money into the system.

There was the man who arrived at a building society with a bag of £50 notes, and exclaimed "I'm definitely not a drug dealer!" when questioned by staff. Then there was the gentleman who visited his safe deposit box in the city twenty times a day, whisking in and out on his motorbike to dispense with his illicit wares.

These crooks were, to put it kindly, unsophisticated. Or to put it bluntly, they were idiots. For every Vito Corleone there will be a hundred Del Boys. The real challenge for law enforcement, regulators and compliance professionals will always be the smart crooks, particularly those using new technologies and tools to disguise their behaviour.

Depending on your opinion, virtual currencies represent either the vanguard of a utopian future, or the latest speculative bubble just waiting to burst. Despite uncertainty about the future of virtual currencies, criminals have been quick to seize new technology, and benefit from the perceived anonymity, speed of transactions and ease of access to international markets.

## So what do crooks get from virtual currency that they don't get from banks?

Let's take a worked example. I'm a politician in a country with a high degree of corruption and I've been plundering the public purse. I want to buy a property offshore as an investment to house my collection of Bentleys, Kalashnikovs and football clubs.

I might struggle with getting my money into a bank in the UK. This is because any bank worth their salt will be carrying out Enhanced Due Diligence checks to determine my source of wealth and funds. The same is true for any lawyers or estate agents that might be involved in the transaction. Failure to carry out the measures could mean fines, business restrictions and public censure. Whilst there is no guarantee the bankers, lawyers and agents will do the right thing – and a significant of the world's money laundering still goes through London - at least there is a framework in place to stop it from happening.

Currently, there are no such requirements for virtual currency traders. So I could place funds into an account in my country. I could then use the funds to purchase some Crypto Currency, let's call it DodgyCoin. I then go to a currency exchange and convert it to CrookCoin, and on to Baddiecoin and Villaincoin before converting back to Dodgycoin.

I then approach a virtual currency exchange service, converting my virtual coins into hard currency. The result? I have successfully obfuscated the original proceeds and disguised the original funds.

## The current state

The above may seem unnecessarily disparaging of the Virtual Currency world. Certainly, there are many exchanges that conduct AML checks to ensure that the above does not happen. But a recent study into Bitcoin Money Laundering, indicated that "*this is out of choice rather than obligation...there are some who choose not to, possibly to attract business from criminals*[1]".

Of course, we know that regulated institutions will often flout the rules where there is money to be made. So it is likely that unregulated institutions will not take AML and sanctions controls as seriously as they could do.

## Is the money launderers dream over?

This brings us to the Fifth Money Laundering Directive (5MLD). The EU has determined that anyone converting virtual currency into hard currency, will now be subject to the same rules and regulations as other financial institutions. This is due for implementation by member states by October 2019.

The UK Government has indicated that the new Directive "*may...be transposed in full, by the UK during the post-Brexit period*[2]". In addition, just this month the FCA has published a dear CEO letter, advising financial institutions on measures to apply where dealing with crypto-exchanges. It seems virtual currencies are on the regulatory radar, and it would be surprising if the 5MLD requirements were not adopted by the UK government in full.

So maybe the dream isn't over – but certainly governments and regulators are taking steps to tame the Crypto Wild West.

## I offer cryptocurrency to fiat exchange services, what should I be doing?

The new legislative framework for crypto exchanges will mean adhering to the established rules laid down in the Fourth Money Laundering Directive, which has been incorporated into UK law in the Money Laundering Relations 2017.

It's easy to reel off a list of Money Laundering Requirements, and simply state that Currency Traders now need to adhere to them. The basic measures involve:

i) Customer screening for PEPs and sanctions;

ii) Carrying out a financial crime risk assessment for each customer;

iii) Identifying individual and corporate customers and verifying that they are who they say they are;

iv) Carrying out regular reviews of due diligence to confirm it is up to date, and carrying out additional reviews where anything about the relationship has changed;

v) Carrying out enhanced checks for customers that pose a higher risk of Money Laundering or Terrorist financing, including more stringent checks on customer Source of Wealth and Source of Funds.

vi) Monitoring accounts for unusual activity;

vii) Reporting any suspicions of Money Laundering or Terrorist Financing to the NCA.

The problem with this, however, is that this framework was largely designed with financial institutions in mind. Virtual Currencies are by their very nature different, and a tailored, specific approach is required.

The key starting point therefore is the Business Wide Risk Assessment. This means understanding the inherent financial crime risks across your business, in order to inform the designing of controls to mitigate those risks. Virtual currency risks may be entirely different to those in a retail banking, commodities trading or wealth management context, and so the controls designed need to reflect this.

Currency Exchanges should ask themselves the following:

i) Are we converting coins for cash, for individuals or corporates? What is the proportion of individuals vs. corporates? Does the existence of corporates in our portfolio make it harder to understand who we are dealing with? Are the individuals PEPs? Are they based in high-risk locations, is there any negative information about them in the news?

ii) What virtual currencies do we convert? Is it just well-known coins like Bitcoin, or do we trade in more unique, start-up offerings. Is there evidence any of the currencies have been used for criminal purposes?

iii) Are any of the currencies based in jurisdictions with a high risk of money laundering or terrorist financing? Can we determine where the currency was established and how?

iv) What is the volume and value of the trades? How quickly can someone use us to convert virtual currency into cash? Does the speed of service make it difficult to monitor unusual or suspicious transactions?

v) Can we always see a clear audit trail to the individual's initial purchase of virtual currency?

vi) Can our customers' identities be clearly identified in the public blockchain? Do we have measures in place to confirm customer identity at the point of conversion to cash?

vii) What are our delivery channels?

The above framework should assist in developing an understanding of the core financial crime risks. It is then a case of developing the pre-existing MLREGS 2017 controls, in line with the identified inherent risks.

1 https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf?__hssc=222901956.3.1516201470218&__hstc=222901956.b7d6531ad164bec182c043c05b5510ba.1516201470217.1516201470217.1516201470217.1&__hsfp=3478668143&hsCtaTracking=66a034a3-865d-481a-8e56-f510419fde74%7C840a3208-7448-4fe6-ad03-a3731f462b7d

2 House of Commons Library Briefing Paper 20 April 2017 P19

This is no easy exercise, and much of the published guidance will relate to more mainstream financial products and contexts. A good example of this is Source of Funds. For a retail bank, this is easy. You simply identify the account money has come from, and how that money was initially generated.

With virtual currency, the initial payment from a bank account might have happened years ago. The customer might have traded hundreds of times in different virtual currencies, before deciding to make the exchange to real money. In higher risk cases, currency exchanges may wish to see verifiable records and a clear audit trail of all transactions to confirm the initial source of funds.

This is not easy to do, but if the crypto exchanges can't do it, they will be in the same position as the building society approached by the man with a bag of cash. If you can't tell where your client's money has come from, then you shouldn't be doing business with them.

There are no easy solutions, and new technologies mean new types of crime and new regulations. The application of existing regulation to new service providers will be a source of challenge for many years to come.

James Fanning
Director
T: +44 (0)20 3727 1846
james.fanning@fticonsulting.com

EXPERTS WITH IMPACT™

## About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.