LUCY FREW'S FINTECH COLUMN: JULY 2018

Lucy Frew is a Partner in Walkers' Regulatory & Risk Advisory Practice Group. Lucy shares her views on topical FinTech issues with our subscribers.

In this edition of her column, Lucy considers the Financial Action Task Force's (FATF) review of the application of its Recommendations to cryptoassets and virtual currencies, and considers what actual guidance and regulation has been forthcoming to date from UK and EU regulators to tackle, in particular, the money laundering and terrorist financing risks insofar as they relate to cryptoassets and virtual currencies.

by *Lucy Frew*, Partner, Regulatory & Risk Advisory Practice Group, Walkers

RESOURCE INFORMATION

RESOURCE ID
w-015-9359

RESOURCE TYPE
Article

PUBLISHED DATE
24 July 2018

JURISDICTION
European Union, International, United Kingdom

ADDRESSING THE AML/CTF RISKS OF CRYPTOASSETS

FATF review: application of standards to AML/CTF

In my *previous column* I noted that regulatory developments are a major contributing factor in cryptocurrency price fluctuations. One forthcoming development with global impact will be the Financial Action Task Force's (FATF) review of the application of its *Recommendations* to cryptoassets and virtual currencies. We can expect the impact of this review to be far greater than changes in approach by any individual country or regulator as the FATF's Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard: although the Recommendations themselves are non-binding, they are implemented by countries worldwide.

In a *statement* released in March 2018, the G20 committed to implement the FATF's Recommendations as they apply to cryptoassets and looked forward to the FATF's review of those standards, which will be carried out under the US presidency of the G20.

At the FATF Private Sector Consultative Forum in April 2018, governments and private sector experts considered two key policy issues, namely digital identity and cryptoassets. According to the FATF Chair's *summary*, the discussion focused on the extent to which the current FATF standards and guidance adequately address the recent developments in cryptoassets.

In its July 2018 *update* to the G20, the FATF explains that it plans to consider detailed proposals to clarify the application of its standards to activities involving virtual currencies and cryptoassets in October 2018, following an intersessional meeting in September. The FATF will take this work forward under the US presidency from 1 July 2018 to 30 June 2019. According to the incoming President's *objectives paper*, the US Presidency will prioritise clarifying how the FATF standards apply to virtual currency providers and related businesses.

How has the FATF addressed cryptoassets to date?

In its 2015 *Guidance for a risk-based approach to virtual currencies* (2015 Guidance) the FATF sought to explain how specific FATF Recommendations should apply to virtual currency exchanges and any other type of entities that enable virtual currency activities to intersect with the regulated fiat currency financial system, as this was seen as higher risk.

It said that the specific FATF Recommendations applicable to such entities should include applying a risk-based approach, customer due diligence, record-keeping, registration or licensing requirements for exchanges, identification and mitigation of risks associated with new technologies, AML/CFT programme requirements and suspicious transaction reporting.

The FATF plans to review the 2015 Guidance as part of its wider review of its Recommendations.

So why is a review necessary?

The issue for the financial sector is that it is not always apparent how to apply the FATF Recommendations to cryptoassets in practice.

Real world customer due diligence is less useful when, as acknowledged by the FATF itself in its 2015 Guidance, cryptoassets may have no customer identification attached, nor any records of transactions that are necessarily associated with real world identity.

Moreover, as also noted by the FATF, decentralised systems have no central server or service provider when it comes to monitoring, identifying and reporting suspicious transaction patterns. Decentralised systems may also seem to exist in a digital universe entirely outside the reach of any particular country when it comes to supervision and enforcement.

Also, as the number of businesses accepting digital currency payments grows, the risk of criminals using the currencies to launder funds without needing to cash out into fiat currencies increases. The rationale for limiting the application of the FATF Recommendations only to exchanges that enable cryptocurrency activities to intersect with the fiat currency financial system may need to be revisited.

In light of the above, and as the FATF acknowledges in its July 2018 *update* to the G20, there is an immediate need to clarify how the FATF definitions and Recommendations concerning customer due diligence, money or value transfer services, wire transfers, supervision, and enforcement apply to virtual currency and cryptoasset providers and related businesses.

Industry approach

Many banks have shunned relationships with customers whose activities relate to cryptoassets, concerned by perceived links between cryptoassets and money laundering and terrorist financing and because of the difficulty of conducting AML checks on transactions.

A small, but ever increasing, minority of service providers are offering specialised cryptocurrency services. However, activities related to cryptoassets are unlikely to become part of the mainstream financial industry until there is workable guidance available on how to handle the money laundering and terrorist financing risks.

Approach of national regulators

Even national regulators may be reluctant to adopt AML/CFT measures in respect of cryptoassets out of concern that any FATF AML/CFT country assessors will not condone their approach. While nowadays national regulators are comfortable embracing FinTech, they have been less forthcoming in respect of cryptoassets.

To date, many national regulators have focused on warning the retail public of the risks associated with investment in cryptoassets or, at the other extreme, imposing bans. What has proved less straightforward for regulators is to produce specific tailored guidance for the financial industry on how to handle the risks in practice.

The FATF conducted a stocktake in June 2018 to identify the different regulatory approaches to virtual currencies and cryptoassets among G20 participants as well as in a number of other countries, noting that many countries are in the process of establishing law or regulations. The measures currently in effect in G20 participants are summarised by the FATF in its July 2018 *update* to the G20 as follows:

Regulatory action	Jurisdiction
Prohibition (on issue/use/dealing/ settling of virtual currencies/cryptoassets)	China, India, Indonesia
Regulation of intermediaries/exchanges and others (using new or existing AML/CFT regulation)	Australia, France, Germany, Italy, Japan, Switzerland, US
Suspicious transaction reporting only	Argentina, South Africa
Preparing laws or regulations	Brazil, Canada, EU, Mexico, Netherlands, Russia, Saudi Arabia, South Korea, Spain, Turkey, UK

The FATF rightly notes that the global regulatory environment for virtual currencies and cryptoassets is changing rapidly. Given their highly mobile nature, there is a risk of regulatory arbitrage or flight to unregulated safe havens.

FCA approach

Having said that, in a *"Dear CEO" letter* published just last month, the FCA has set out good practice for how banks should handle the financial crime risks posed by cryptoassets. The FCA says that firms should take "reasonable and proportionate measures" to "lessen the risk" of facilitating financial crimes that are enabled by cryptoassets. The FCA's tone is helpful, as it recognises that risk cannot be altogether eliminated, and gives reassurance that banks can, albeit cautiously, proceed with cryptocurrency related activities and customers.

The FCA suggests that it may be necessary for banks to enhance scrutiny of clients and their activities where a bank offers services to cryptocurrency exchange, engages in trading activity where a client's or counterparty's source of wealth is derived from cryptoassets, or arranges, advises on, or takes part in an initial coin offering (ICO). Appropriate steps or actions to consider may, subject to the circumstances and services being provided, include:

- Developing staff knowledge and expertise on cryptoassets to help them identify the clients or activities that pose a high risk of financial crime.
- Ensuring that existing financial crime prevention frameworks adequately reflect the crypto-related activities that the firm is involved in, and that they are capable of keeping pace with fast-moving developments.
- Engaging with clients to understand the nature of their businesses and the risks they pose.
- Carrying out due diligence on key individuals within the client's business including consideration of any adverse intelligence.
- In relation to clients offering forms of crypto-exchange services, assessing the adequacy of those clients' own due diligence arrangements.
- For clients that are involved in ICOs, considering the issuance's investor-base, the organisers, the functionality of tokens (including intended use) and the jurisdiction.

The FCA notes that some customers or clients may simply be holding or trading cryptoassets. Firms should assess the risks posed by a customer whose wealth or funds derive from the sale of cryptoassets, or other cryptoasset-related activities, using the same criteria that would be applied to other sources of wealth or funds (for example, in the case of retail clients, the criteria they would apply to a property transaction, inheritance, or sale of a valuable artwork or car).

The FCA addresses the key point that one way in which cryptoassets differ from other sources of wealth is that the evidence trail behind transactions may be weaker. The FCA is clear that this does not justify applying a

different evidential test on the source of wealth and it expects firms to exercise particular care in these cases. The FCA appears to be referring to the anonymity aspects of cryptocurrency and does not expand on what form of "particular care" it expects to be exercised in practice.

The "Dear CEO" letter refers specifically to banks, but is also instructive for other types of financial sector businesses.

EU approach: MLD V

It is worth also mentioning the *Fifth Money Laundering Directive* (*(EU) 2018/843*) (MLD5), which entered into force on 9 July 2018 and must be implemented by member states by 10 January 2020. MLD5 has extended the scope of the existing EU legislation to include providers engaged in exchange services between virtual currencies and fiat currencies, and custodian wallet providers (meaning entities that safeguard private cryptographic keys on behalf of customers to hold, store and transfer virtual currencies).

These exchanges and custodians will now be subject to the requirements of the MLD5, including to identify suspicious activity, in the same way as other financial institutions. This expansion in scope was seen as crucial to reduce the risk of terrorist groups being able to transfer money into the EU financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity via such exchanges or custodians.

The recitals to MLD5 do recognise that the inclusion of such exchanges and custodians will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers. This is a key shortcoming in the legislation, as it is perfectly possible to use an exchange or custodian in a jurisdiction in which no or inadequate AML/CFT measures apply or to simply transact OTC. Ultimately, unless regulators can be reassured, they may seek to force all trading into regulated exchanges in order to facilitate customer due diligence, suspicious reporting and regulatory supervision.

It is suggested that to combat the risks related to the anonymity issue, national financial intelligence units (FIUs) should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency. This may be easier said than done given that decentralised systems may be outside the reach of any particular country when it comes to supervision and enforcement.

Further considerations for the cryptoassets sector

It may be worth considering existing mobile payments regulation, which requires not only initial customer identification and verification, but also authentication of each individual transaction to link it to the customer using biometric data (for example, iris scanning, facial recognition using a "selfie" and fingerprint scanning). There may be potential for such biometric authentication as a necessary enabler of a given blockchain transaction. It is well worth watching for convincing technology solutions, as these may be the key to workable regulation. It is in the interests of the cryptoasset sector to engage with national and international regulators to find ways in which the benefits of cryptoassets can be preserved while also meeting the AML/CFT standards that the rest of the financial sector must comply with.