FINANCIAL CONDUCT AUTHORITY

25 The North Colonnade
Canary Wharf
London
E14 5HS

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

11 June 2018

Dear CEO

CRYPTOASSETS AND FINANCIAL CRIME

As evidence emerges of the scope for cryptoassets[1] to be used for criminal purposes, I am writing regarding good practice for how banks handle the financial crime risks posed by these products.

There are many non-criminal motives for using cryptoassets. These include using them as high-risk speculative investments or as a means of funding innovative technological development. However, this class of product can also be abused because it offers potential anonymity and the ability to move money between countries. You should take reasonable and proportionate measures to lessen the risk of your firm facilitating financial crimes which are enabled by cryptoassets.

Clients offering services related to cryptoassets

Where you offer banking services to current or prospective clients who derive significant business activities or revenues from crypto-related activities, it may be necessary to enhance your scrutiny of these clients and their activities. Services may include:

- where your firm offers services to cryptoasset exchanges which effect conversions between fiat currency and cryptoassets and/or between different cryptoassets
- trading activities where your clients' or counterparties' source of wealth arises or is derived from cryptoassets
- where your firm wishes to arrange, advise on, or take part in an 'initial coin offering' (ICO)[2]

[1] Cryptoassets/cryptocurrencies, such as Bitcoin or Ether, are any publicly available electronic medium of exchange that features a distributed ledger and a decentralised system for exchanging value.

[2] An initial coin offering (ICO) is a means of raising finance online using digital currency and distributed ledger technology. An ICO is an event where digital tokens are offered and distributed to the public in exchange for investors' capital.

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 which pose a high risk of financial crime
- ensuring that existing financial crime frameworks adequately reflect the crypto-related activities which 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 in the client 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 which are involved in ICOs, considering the issuance's investor-base, organisers, the functionality of tokens (including intended use) and the jurisdiction

Following a risk-based approach does not mean banks should approach all clients operating in these activities in the same way. Instead, we expect banks to recognise that the risk associated with different business relationships in a single broad category can vary, and to manage those risks appropriately.

Customers using cryptoassets

Some of your customers or clients may be holding or trading cryptoassets, and selling them may be the source of a customer's wealth or funds. In a retail context, this may be discovered by, for example, enquiring about the source of a deposit, or because the customer has previously made large transactions with cryptoasset exchanges. Existing requirements for checking the source of wealth and funds are risk-sensitive; firms are given the flexibility to adapt their actions to the perceived risks. 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. One way cryptoassets differ from other sources of wealth is that the evidence trail behind transactions may be weaker. This does not justify applying a different evidential test on the source of wealth and we expect firms to exercise particular care in these cases.

Where a firm identifies that a customer or client is using a state-sponsored cryptoasset which is designed to evade international financial sanctions, we would see this as a high-risk indicator.

Retail customers contributing large sums to ICOs may be at a heightened risk of falling victim to investment fraud. In 2012 the Financial Services Authority (FSA) reviewed how banks then handled the risk of investment fraud[3], including the risk of retail customers becoming victims of this crime. Please see that review's findings for a discussion of good and poor practice which is also relevant to ICOs.

Should you have any questions about this letter, please contact our Contact Centre.

Yours sincerely

Jonathan Davidson

Executive Director of Supervision

Retail & Authorisations

Megan Butler

Executive Director of Supervision

Investment, Wholesale & Specialists

[3] http://www.fsa.gov.uk/static/pubs/other/banks-defences-against-investment-fraud.pdf