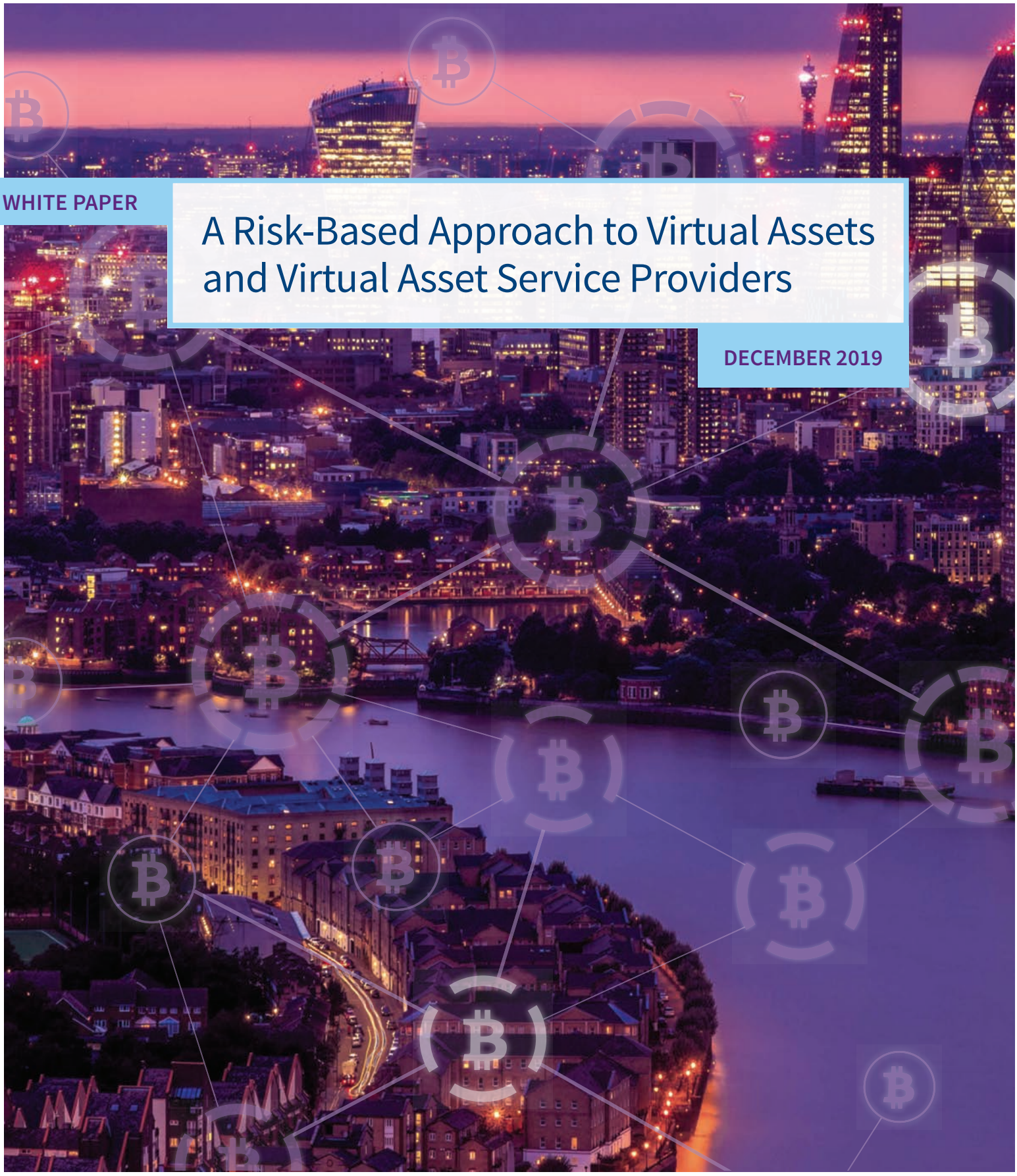
LexisNexis®
RISK SOLUTIONS



WHITE PAPER

A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

DECEMBER 2019

In 2018, the Financial Action Task Force (FATF) published changes to its recommendations and glossary relating to virtual assets and virtual asset service providers. These changes supplemented the 2015 FATF report, *Guidance for a Risk-Based Approach to Virtual Currencies*. **The FATF establishes that there is a significant money laundering and combating terrorism financing risk associated with virtual assets. Transactions are instant, non-face-to-face, cross jurisdictional and largely anonymous hence there was the need to bring them within scope of regulation.**

In June 2019, the FATF issued new guidance in the form of an interpretative note to its 40 recommendations to further clarify how the FATF requirements should apply in relation to virtual assets and virtual asset service providers. This guidance was issued to help both national authorities in understanding and developing regulatory and supervisory responses to virtual asset activities and virtual asset service providers, and the private sector seeking to engage in virtual asset activities in understanding their obligations in prevention of financial crime. The guidance will also help private sector organizations to apply FATF requirements to businesses within their sector.

The FATF guidance was in response to the increasing use of virtual assets for money laundering and terrorism financing and was also intended to be useful in an environment of fast changing digital technologies, services and products used in the financial sector. Some of the innovative FinTech products that are now alternatives to traditional financial products were prone to anonymity and therefore attractive to criminals and terrorists who wish to launder their dirty proceeds.

Short overview of the June 2019 FATF guidance

Amended FATF Recommendation 15 states that:

- Countries are required to…
  - Assess and mitigate risks associated with virtual asset service providers;
  - License or register virtual asset service providers;
  - Subject virtual asset service providers to supervision or monitoring by competent national authorities.
- Virtual asset service providers are subject to the same relevant FATF measures as other financial institutions.

Interpretive note to Recommendation 15 is intended to further clarify how the FATF requirements should apply in relation to virtual assets and virtual asset service providers, especially with regard to:

- The application of the risk-based approach (RBA) to virtual asset activities or operations and virtual asset service providers;
- Supervision or monitoring of virtual asset service providers for AML/CFT purposes;
- Licensing or registration;
- Preventive measures (customer due diligence (CDD), recordkeeping, Suspicious Transaction Reporting (STR));
- Sanctions and other enforcement measures;
- International co-operation.

Virtual assets

For many years, cryptocurrencies and blockchain technology remained a mystery to the compliance sector. With a lack of understanding in the way new technologies and new methods of payment are working, not to mention potential financial crime risks, it was only a question of time before virtual assets would be defined and regulated. Seen as peripheral, many organizations simply categorized cryptocurrencies as too risky and dangerous, and too difficult to assess or control risks related to it. In short, compliance professionals have been waiting for guidance on how to recognize red flags and suspicious transactions related to digital products and business models in the virtual assets area.

Apart from a lack of understanding or knowledge in this area, many were also concerned about the anonymity associated with virtual assets and virtual asset service providers. Cryptocurrencies, decentralized platforms, digital wallets and digital exchanges were largely developed in a culture of low transparency.

Regulators, law enforcement agencies and policy makers have long since recognized the financial crime risks in emerging digital financial products and services, and that the absence of AML controls and regulation has increased the risk of money laundering, terrorist financing and market abuse.

Money laundered globally = $800 million – $2 trillion[1]

Virtual assets and financial crime framework

Figures from respected bodies such as Europol and the United Nations Office on Drugs and Crime (UNODC) estimate that the amount of money laundered globally is between 2% and 5% of global GDP or $800 million – $2 trillion. Europe's police agency estimated that 3 – 4% of the EU's annual criminal takings, or £3bn – 4bn ($4.2bn – 5.6bn), are crypto-laundered.[1]

In July 2019, the European Parliament press release, *Commission Assesses Risks and Calls for Better Implementation of the Rules*, called to further strengthen the EU's AML framework.

It has been well known for a while that virtual currencies have been used in online criminal payments and particularly in large-scale cybercrime and on the Dark Web.

All major stakeholders involved in prevention of financial crime are reacting faster than ever, providing guidance and warning about dangerous trends they have noticed, especially in those connected to virtual assets. The FATF is not the only body taking action. Other organizations, such as the European Securities and Markets Authority (ESMA), have also actively participated in giving guidance related to virtual assets. In July 2019, the ESMA published a report on the status of licensing regimes of FinTech firms. Their survey confirmed "that NCAs do not typically distinguish between FinTech and traditional business models in their authorization and licensing activities since they authorize a financial activity and not a technology."[2]

The Egmont Group's Annual Report addressed that they had issued *Internal Guidance on Emerging Financial Technologies: A Typology of Virtual Currencies*. Also, they held many workshops covering topics such as virtual currency regulation and analysis.[3]

What we are now witnessing are first fines by the regulators. FinCEN, the U.S. Treasury Department's financial crimes unit, says the move represents its first enforcement action against a peer-to-peer cryptocurrency exchange.[4]

Guidance for a risk-based approach to virtual assets and virtual asset service providers

1. Definition

The FATF emphasizes that virtual assets are distinct from fiat currency (aka "real currency," "real money" or "national currency"), which is the money of a country that is designated as its legal tender. Existing terms such as *cryptocurrency, digital assets* and *virtual currency* were consolidated into the definition of virtual assets and related service providers such as exchanges, certain types of wallet providers and providers of financial services for Initial Coin Offerings (ICOs). The FATF uses the term "virtual asset" to refer to digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account and/or a store of value.

2. Regulation and RBA

Jurisdictions should ensure that virtual asset service providers are subject to AML/CFT regulations (CDD, ongoing monitoring, record keeping and reporting of suspicious transactions). Countries should apply the risk-based AML/CFT approach when assessing the risks associated with virtual assets in their jurisdictions and should also have a good understanding of such risks. Reporting entities are advised to apply the risk-based approach and determine suspicious behavior aligned with types of risks applicable in their business.

In particular, the guidance also clarifies that virtual asset service providers that engage in virtual asset transfers will need to obtain, hold and transmit customer information. The required information for each transfer includes the:

- Originator's name (i.e., the sending customer);
- Originator's account number where such an account is used to process the transaction (e.g., the virtual assets wallet);
- Originator's physical (geographical) address, national identity number or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth;
- Beneficiary's name; and
- Beneficiary account number where such an account is used to process the transaction (e.g., the virtual assets wallet).

When the risk assessment shows a higher risk, enhanced due diligence (EDD) is required.

Another guiding principle is that the risk-based approach is to be followed in national implementation of crypto regulation based on a local risk assessment of crypto entities. This will vary country to country and there should not be an automatic assumption that all virtual assets and all virtual asset service providers are high risk.

3. Licenses, registration and supervision

The note instructs governments to ensure that virtual assets (e.g. cryptocurrencies) and virtual asset service providers (e.g. digital wallet providers and exchanges) register with a national regulator and comply with "the full range" of measures against illicit finance, from vetting customers to reporting suspicious transactions. Virtual asset service providers must be licensed or registered and subject to monitoring in order to ensure compliance. One of the guiding principles is equivalence, i.e. that regulation apply equally and in the same way to virtual assets and virtual asset service providers as to any other Obliged Entities. Countries should take steps to identify natural or legal persons that operate unlicensed virtual asset entities and apply measures to prevent them. In addition, third party business introducers to virtual assets/virtual asset service providers must also be regulated entities.

Each jurisdiction should identify effective systems to conduct risk-based monitoring or supervision of virtual asset service providers. Some jurisdictions already regulate virtual assets activity in accordance with the 2015 guidance. Jurisdictions will have flexibility to decide what body will regulate virtual assets. Also, each country is advised to decide where the boundaries of virtual assets and virtual asset service providers lie in their country (e.g. the EU's current 5th Anti-Money Laundering Directive consultation is covering this aspect).

Some countries may decide to prohibit virtual assets based on their own assessment of risk.

4. Transactions: threshold

For "occasional transactions" the designated threshold above which virtual asset service providers are required to conduct CDD is USD/EUR 1,000. Countries may go further than what Recommendation 10 requires by requiring full CDD for all transactions involving virtual assets or performed by virtual asset service providers (as well as other obliged entities, such as banks that engage in virtual asset activities), including "occasional transactions" below the USD/EUR 1,000 threshold, in line with their national legal frameworks.

5. Beneficiary information

Countries must ensure that providers of virtual asset transfers provide the required originator and beneficiary information immediately and securely—identifying beneficial owners and legal persons behind a virtual asset or virtual asset service provider is crucial, especially the understanding of where they are in relation to where their business operates.

Governments should require cryptocurrency firms to collect "accurate originator information and required beneficiary information" on transactions and share those details with other firms involved in the payment chain. This is the so-called 'Travel Rule' and the obligation is identical to wire transfers of fiat currency.

6. Risk indicators and Suspicious Transaction Reports (STR)

The absence of face-to-face contact in virtual asset financial activities or operations may indicate higher ML/TF risks. Furthermore, virtual asset products or services that facilitate pseudonymous or anonymity-enhanced transactions also pose higher ML/TF risks, particularly if they inhibit a virtual asset service provider's ability to identify the beneficiary. With regard to transactions related to targeted sanctioned entities, countries should freeze all assets including virtual assets without delay.

Use of Suspicious Transaction Reports (STRs) is mandated in the same way as the rest of the regulated sector. Collation of STRs' statistics is also mandated. Statistics are to be available on request by permitted authorities, e.g. law enforcement agencies.

Member Countries' regulators are yet to define exactly what constitutes "suspicion" of money laundering, terrorist financing and sanctions violations in the context of virtual assets.

7. International cooperation

International cooperation between supervisors is identified as critical. Countries should have in place relevant channels for sharing information as appropriate to support the identification and sanctioning of unlicensed or unregistered virtual asset service providers.

Conclusion

With rapid technology development, FinTech compliance professionals must also keep up with the changes and be ready to assess and control all new risks. Virtual assets are changing the face of finance and their use is growing rapidly, similarly the virtual asset service provider sector is growing equally fast. The new regulatory obligations and rules will have an impact on both virtual assets and virtual asset service providers in equal measure.

To respond to all new risks, much more research is needed to understand typologies and much more needs to be known about them. It took time before the world had agreed that Blockchain is technology, on which a large number of cryptocurrencies could run, but this technology was not intended to facilitate money laundering, terrorist financing or even tax evasion.

The FATF's new guidance on crypto assets is very welcome and essential to the proper and effective regulation of this emerging sector of financial services. We can reasonably expect further guidance as the sector develops. Many private sector associations and various groups at national and international level are working on financial crime risk indicators in the virtual asset space (dark markets, gambling sites, computer and video games, ransomware attacks and other criminal transactional links).

However, we also need to recognize that many of the key players in cryptocurrency markets will remain outside of the scope of EU's 5th Anti-Money Laundering Directive, leaving blind spots in the fight against money laundering, terrorist financing and tax evasion. However, it is fair to expect further developments in the short term. We may count on the fact that the FATF will provide further clarification to jurisdictions in managing the ML and TF risks of virtual assets, while creating a sound AML/CFT regulatory environment in which companies are free to innovate.

It will be a case of 'watch this space very carefully' as regulation unfolds and evolves in the emerging virtual asset and virtual asset service provider space, and financial institutions which up until now have decided not to get involved in the crypto space may actually have no choice in the next few years.

[1] https://www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering

[2] https://www.esma.europa.eu/press-news/esma-news/esma-publishes-report-licencing-fintech-firms-across-europe

[3] https://egmontgroup.org/sites/default/files/filedepot/EGAR_2017-2018/EGAR-2018-Annual-Report-Digital.pdf

[4] https://cointelegraph.com/news/fincen-takes-first-enforcement-action-against-p2p-cryptocurrency-exchanger

For more information, call +44 203 2392 601 or visit
risk.lexisnexis.com/global/en/financial-services

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.