A Risk-based Approach to Virtual Currencies

The evolving regulatory compliance environment

LexisNexis®
RISK SOLUTIONS

> "There is an urgent need for all countries to take coordinated action to prevent the use of virtual assets for crime and terrorism."
>
> – Financial Action Task Force (FATF)

As the adoption of virtual assets increases, so do the risks for service providers, jurisdictions and Member States. The risks—**mainly due to the anonymity surrounding the sources and uses of these funds**—have led to an emerging regulatory landscape to stem the use of virtual assets for financial crime.

Three to four percent of Europe's annual criminal takings —£3bn-4bn ($4.2bn-5.6bn)—are crypto-laundered.[1]

Head of Europol

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

LexisNexis® RISK SOLUTIONS

How are “virtual assets” defined?

As used by the Financial Action Task Force (FATF), the term refers to digital representations of value that can be digitally traded or transferred for payment or investment purposes. These digital representations of value can include those that function as a medium of exchange, a unit of account and/or a store of value.

The FATF emphasizes that these virtual assets are distinct from fiat currency (a.k.a. “real currency,” “real money” or “national currency”), which is the money of a country that is designated as its legal tender.

LexisNexis® RISK SOLUTIONS

The European Union's (EU) Crime Regulation is rapidly changing.

Regulators in Europe are swiftly implementing virtual asset guidelines. The Fourth Anti-Money Laundering Directive (4AMLD), which came into force on 26th June 2017, introduced the risk-based approach and removed automatic exemptions from due diligence.

In 2018, the FATF published 5AMLD, establishing that there is a **significant money laundering and combating terrorism financing risk associated with virtual assets.** New rules required all EU-based exchanges, including virtual currency exchanges (VCEs) to run KYC/AML checks on all clients and transactions. These rules were followed by 6AMLD, requiring Member States to criminalize money laundering arising from six specified predicate offenses.

Legislation related to virtual currencies and financial crime—defined and regulated by 5AMLD—requires Member States to incorporate these rules into national legislation by 10th January 2020.

LexisNexis®
RISK SOLUTIONS

In conjunction with these stricter regulations, FATF recommendations have also changed.

In the last few years, FATF has recommended that virtual asset platforms offering payment services should be subject to the same regulations as traditional payment service providers.

On 19th October 2018, the 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 Foreign Currency*. Additionally, the text of the new Interpretative Note was finalized and formally adopted as part of the FATF Standards in June 2019.

In the upcoming year, FATF will provide further information on how the new requirements should be applied to virtual assets.

Service providers, jurisdictions and countries are under expanded scrutiny to ensure compliance.

Existing terms such as cryptocurrency, digital assets and virtual currency are now consolidated into a new definition of virtual assets and related service providers. These terms refer to certain types of wallet providers and providers of financial services for Initial Coin Offerings (ICOs). Service providers are to be licensed or registered and subject to monitoring to ensure compliance.

The jurisdictions are charged with ensuring that virtual asset service providers are subject to AML/CFT regulations, including CDD, ongoing monitoring, record-keeping and reporting of suspicious transactions. Each jurisdiction must identify effective systems to conduct risk-based monitoring or supervision of virtual asset service providers. Some have already achieved this goal in accordance with the 2015 guideline.

At the same time, countries must apply a risk-based AML/CFT approach when assessing the risks associated with virtual assets in their jurisdictions and should also possess a good understanding of these risks.

LexisNexis® RISK SOLUTIONS

Still, blind spots and red flags exist relating to virtual assets.

A number of key players in cryptocurrency markets are not included in the scope of 5AMLD. As a result, blind spots still exist in the fight against money laundering, terrorist financing and tax evasion. It is important to note that blockchain technology, on which a large number of cryptocurrencies run, is not designed to launder money, facilitate terrorist financing or evade taxes.

In addition, the Egmont Group of Financial Intelligence Units (FIUs) has not yet released standards. As of now, it is the task of Member Countries' regulators to define and set examples of what would be a suspicion of money laundering, terrorist financing and sanctions violations as it relates to virtual assets.

As they wait for guidance, reporting entities are advised to apply a risk-based approach and determine suspicious behavior aligned with the types of risk that are seen in their business. The lack of such identification could lead to regulatory sanctions.

LexisNexis® RISK SOLUTIONS

How is the market getting ready?

Currently, many entities with financial crime compliance or virtual currencies/blockchain background are working together, but also with some regulatory representations. Together, they are setting up risk indicators of suspicion in the virtual currency (asset) space, such as dark markets, gambling sites, ransomware attacks and other criminal transactional links.

Additionally, new Internet technology solutions are appearing in the market, designed and tailored to address the financial crime compliance challenge.

The time has come to follow a risk-based approach to help curtail regulatory risks.

With rapid technology deployment, Fintech compliance professionals must keep up with the changes and be ready to assess and control all risks.

Virtual currency service providers will be regulated and will need to proactively carry out AML procedures. Other reporting entities must be willing to carry out the risk-based approach when working with virtual asset providers.

On the regulatory front, jurisdictions will have flexibility to decide what body will regulate virtual assets. The FATF will provide clarifications to jurisdictions in managing the money laundering and terrorist financing risks of virtual assets. Simultaneously it will create a sound AML/CFT regulatory environment in which companies will be free to innovate. It may well be that some Member States may decide to prohibit virtual assets entirely based on their own assessment of risk.

As regulation continues to unfold and evolve in the emerging virtual asset service provider space, we can reasonably expect further guidance in the future as the sector develops.

For more information, call +44 203 2392 601
or visit risk.lexisnexis.com/EMEA

LexisNexis®
RISK SOLUTIONS