LexisNexis®
RISK SOLUTIONS

WHITE PAPER

AML Issues for Virtual Assets in Asia Pacific: A Regulatory View

Even as virtual assets are emerging from the shadows, with some banks taking their first steps towards engaging with digital assets, there remain significant regulatory and operational challenges tied to the implementation of existing know your customer (KYC), anti-money laundering (AML) and counter terrorist financing (CTF) regimes in the nascent asset class.

Some of the risks associated with virtual assets have to do with a limited understanding of the technology, but it is mainly due to the anonymity surrounding the sources and uses of virtual funds.

The use of peer-to-peer or network authentication for virtual asset transactions was meant to bypass institutional intermediaries, who serve as key gatekeepers in global KYC/AML regulation. It is therefore natural that the onboarding of counterparties to virtual asset transactions is difficult to integrate into financial institutions' existing KYC/AML processes around customer identification and monitoring.

There are also several issues around the very nature of the underlying technology for virtual assets – distributed ledger technology (DLT) – which prevent changes of any kind. This means that any errors or fraudulent activity are permanently locked into the ledger.

No geographic limitations for transacting in virtual assets exist either, making it difficult to pinpoint which jurisdiction or regulatory regime applies to a particular transaction.

Still, some regulators are taking steps towards creating a regulatory regime around virtual asset transactions, mandating KYC/AML processes for entities involved in these businesses and, importantly, imposing these requirements on virtual currency exchanges (VCEs).

The regulatory landscape

Recently, there has been some movement towards the approach espoused by the Financial Action Task Force (FATF) – that virtual asset platforms offering payment services should be subject to the same regulations as traditional payment service providers.

In a note on global AML regulation, Barbara Stettner, a US-based partner at Allen & Overy, detailed the following differences in national virtual asset regulations in relation to virtual assets in a note on global AML regulation:

(i) whether special licensing requirements exist for VCEs;

(ii) the extent to which AML rules also cover administrators and wallet services;

(iii) the extent to which initial coin offerings (ICOs) are covered by securities laws or equivalent regulations with AML regulatory implications; and

(iv) the extent to which crypto-to-crypto exchange is treated differently from crypto--to-fiat exchange.

In Asia Pacific, regulatory practices around virtual assets are especially divergent. While China and India ban virtual asset transactions and ICOs outright, Japan, Hong Kong, Singapore, Malaysia, Thailand and Australia have taken a more welcoming approach to virtual assets and have developed or are in the process of developing licensing and regulatory regimes for VCEs.

Regulating virtual currency exchanges

Japan's Financial Services Agency (FSA) began giving out "Virtual Currency Exchange Operator" licenses in September 2017 after the government amended its Payment Services Act to provide a definition of such exchanges in May 2016. In 2018, Japan also amended its existing rules to tighten the regulation of VCEs by including them under the Financial Instruments and Exchange Act instead of the Payment Services Act, following the USD530 million theft at Tokyo-based exchange Coincheck in January 2018.

The country has favored a self-regulatory approach to the industry, however, encouraging the development of risk management best practices by virtual asset firms themselves. In October, the FSA gave the Japan Virtual Currency Exchange Association (JVCEA), whose members include all sixteen licensed virtual currency exchanges in the country, the authority to regulate the industry.

Meanwhile, Singapore and Hong Kong are actively changing the way ultimate beneficial ownership (UBO) information is collected and accessed. Singapore requires all locally incorporated firms to keep a register of all owners that control more than the FATF-recommended 25% of the entity. Hong Kong's Financial Services and Treasury Bureau (FSTB) is in the process of reforming its Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, introduced on 1 March 2018, to include VCEs.

Hong Kong's Securities and Futures Commission (SFC) has also recently proposed placing VCEs in its regulatory sandbox on a voluntary basis, where their compliance with a set of terms and conditions will be one of the key factors in determining how to regulate these businesses. Among the requirements are AML/CFT systems that include KYC obligations, enhanced customer due diligence, ongoing monitoring and tracking of virtual assets through transaction chains to identify their source and destination.

The Monetary Authority of Singapore (MAS) is likewise in the process of reviewing its regulatory framework for recognized market operators (RMOs) to introduce a three-tier system for approving exchanges, partly in recognition of the emergence of VCEs. Smaller exchanges under the new regime will face reduced capital requirements but will still be required to comply with KYC and AML/CTF obligations.

The MAS has also recently finalized its Payment Services Bill to include virtual currencies and virtual currency intermediaries under a single regulatory framework alongside all other payment services. According to the MAS, the regulatory focus in relation to virtual currency intermediaries will be on AML/CFT risks, but this scope may change in due course as the sector develops further.

Malaysia also adopted new AML/CFT policy guidelines that require VCEs to have KYC processes, which include the collection of identity documentation. According to the government's latest budget announcement on 2 November, a new regulatory framework for approving and monitoring VCEs and ICOs is expected to come into effect by the end of the first quarter of 2019.

China, on the other hand, shut down all domestic platforms dealing in virtual assets in 2017 and Vietnam deemed all virtual assets and related transactions illegal after a USD658 million fraud took place in April 2018.

In November, the US Treasury's Office of Foreign Assets Control (OFAC) said in a press release, that it was targeting digital currency exchanges that "enabled Iranian cyber actors to profit from extorting digital ransom payments." The agency's actions follow attacks from ransomware known as 'SamSam', which hackers used to exploit vulnerable networks, typically targeting government agencies, hospitals, universities and corporations, by holding them hostage in exchange for ransom in bitcoin.

Meanwhile, the European Union in December 2017 agreed on its fifth Anti-Money Laundering Directive (5AMLD) and published the new rules in June 2018. The rules, among other things, require all EU-based exchanges, including VCEs, to run KYC/AML checks on all clients and transactions. Member states will have until January 2020 to incorporate these rules into national legislation.

Regulating investors in virtual assets

Investors in the virtual asset space are typically regulated through VCEs, but the uncertainty around the classification of digital assets means there is less consistency in the treatment of these investments across different jurisdictions.

Hong Kong's SFC recently brought asset managers that invest more than 10% of their AUM in virtual assets under its remit and is restricting these funds only to professional and institutional investors. Hong Kong does not apply any capital gains tax on investments in virtual assets or ICOs, and does allow the general public

to participate, even as it warns retail investors to beware of fraudulent players. However, the new sandbox approach proposes to restrict any participating VCEs to offering services only to professional investors.

In May 2018, Thailand said that its Securities and Exchange Commission (SEC) has the "duty and authority" to oversee and regulate all virtual asset transactions, including verifying the identity of clients. It also imposed a 15% withholding tax on gains from digital tokens and virtual asset trade. While ICOs may be offered to institutional investors in unlimited quantities, Thailand's regulatory framework caps retail investment at THB 300,000 (USD 9,000) per person per ICO project.

In its November release cited above, the OFAC said that it would include bitcoin wallet addresses of individuals on its Specially Designated Nationals (SDN) list, in addition to other information like physical addresses, post office boxes, email addresses and aliases. The SDN list includes individuals, groups and entities like terrorists and narcotics traffickers that do not fall under a specific jurisdiction. OFAC has added two Iranian nationals and their bitcoin addresses to the list as part of its new wave of tightening AML screening by blacklisting wallets.

Risks of dealing in virtual assets

The opaque nature of transactions involving virtual assets makes KYC/AML checks and enhanced due diligence even more important for crypto and non-crypto financial institutions alike, as there are significant regulatory and reputational risks associated with breaches of KYC/AML norms.

For fiat-to-crypto transactions, banks and VCEs require robust compliance programs to mitigate the associated legal, financial, reputational and regulatory challenges. Best practices in KYC/AML are widespread in the financial industry but they need to be adapted to virtual asset businesses.

Strong onboarding and monitoring processes as well as enhanced due diligence for high-risk clients are important aspects of mitigating virtual asset risks. VCEs must know and verify their customers' identities, check them against sanctions lists and monitor them on an ongoing basis.

For VCEs, eKYC processes become even more important in end-to-end risk management as, unlike banks, they don't meet their clients face-to-face and are unable to verify identity documents directly. As such, banks can continue to use their existing KYC approaches, whereas VCEs must rely on better technology to automate, validate, qualify and improve onboarding and monitoring processes.

Crypto-to-crypto transactions currently do not touch the mainstream financial system directly, effectively reducing the money laundering and terrorism financing risks to the system as a whole. However, the reputational or legal risk to the VCE itself remains, especially when multiple virtual asset pairs are involved

KYC/AML processes at virtual assets exchanges

Given a lack of consistent regulation for virtual assets, many banks, in a bid to de-risk, are denying banking services to VCEs, which are considered high risk across the board. This may be because many VCEs have a reputation for failing to run basic checks on their clients. A recent survey of 25 VCEs based in Europe and the US by analytics house P.A.ID Strategies showed that just 32% perform full identity checks on their users.

According to press reports, a number of financial institutions like JP Morgan Chase, Bank of America and Citigroup have banned correspondent banking clients from dealing with transactions related to virtual currency in order to avoid breaching KYC/AML regulations.

Douglas Wolfson, Director, Financial Crime Compliance, at LexisNexis Risk Solutions, says that banks in Asia Pacific continue to be reluctant to deal with third-party virtual asset platforms and exchanges. Banks, he says, are not only concerned about the conflicting regulatory environments in different jurisdictions but also about the quality of virtual asset platforms' KYC/AML processes.

"Banks are very keen on meeting regulatory expectations and tend to be concerned if there is no regulator in a certain space. If banks are going to deal with virtual asset platforms, they are going to want to deal with a regulated entity. So, banks avoid these platforms as there is no regulatory guidance about how to deal with virtual currency exchanges, and the exchanges themselves often have no rules to follow and are not necessarily expected to do KYC/AML checks," he says.

What's particularly interesting about the issue of money laundering is that, while the (virtual asset) industry is rapidly tightening up its own codes and conduct, the established financial industry still seems stuck on a plateau of underlying illegality,

despite its vastly superior position and resources. The recent Morgan Stanley $10 million AML compliance penalty assessed by FINRA being a case in point.

Indeed, virtual currency exchanges are increasingly observing Know Your Customer (KYC) and AML regulations, while new trade bodies are being established with the aim of erecting self-regulatory guidelines for the crypto industry to follow.[1]

Most transactions in this space are between the US dollar and virtual assets, and therefore implicitly fall under the remit of US authorities, specifically, the Department of Justice (DOJ).

“The US looms large over virtual asset transactions. So banks, even though they may be Asian, are concerned about the business they’re doing in US dollars. Because these transactions are potentially monitored by the DOJ, they don’t want to risk running afoul of US sanctions,” Wolfson says.

Banks’ compliance teams will often not accept the due diligence conducted by VCEs, the standards for which are not specifically set by regulators, although, Wolfson adds, the type of virtual asset also matters. For example, banks steer completely clear of privacy coins which guarantee absolute anonymity to both sides of a transaction.

Most banks consider VCEs to be high risk off the bat and require enhanced due diligence. Additionally, they need to investigate and understand the regulatory environment in every jurisdiction in which the exchanges operate.

“Banks should consider an internal, global regulatory portal or centralized database that will allow bankers in one region to understand the regulatory issues of dealing in crypto in another,” Wolfson adds.

“Banks should consider an internal, global regulatory portal or centralized database that will allow bankers in one region to understand the regulatory issues of dealing in crypto in another,” Wolfson adds.

Regulation – a cost that provides value

Despite the costs of implementing KYC/AML processes, VCEs should welcome regulation mandating such checks. According to Wolfson, most regulation in the virtual asset space has a positive value to companies operating in the sector. For example, he says the recent April 2018 regulation by the Australian Transaction

Reports and Analysis Centre (AUSTRAC) requiring VCEs to register with the agency and comply with AML/CTF and reporting requirements is an important step in legitimizing the industry.

“AUSTRAC is a very well-respected regulator that understands KYC/AML/CTF risks, so this adds an air of legitimacy to a market that has historically struggled to gain it in the mainstream. Having a regulator in a market like Australia provides credibility with a value that’s greater than the cost of implementing what it takes to meet the regulation,” he says.

Despite being a relatively new requirement, regulation in Australia and beyond is fulfilling its intended purpose, Wolfson says; that is, to side-line individuals looking to use virtual assets for criminal purposes, while encouraging people who have no nefarious intention to enter the space.

“Virtual asset platforms that are looking to build legitimate businesses and/or list publicly already have KYC/AML platforms in place and understand what is required of them from a regulatory perspective,” said Wolfson.

Most VCEs have a relatively clear idea of the regulatory scrutiny they face and are extremely careful to do everything they can to avoid money laundering and terrorism financing risk. However, given banks’ efforts to de-risk by avoiding business relationships with entities without a clear regulatory standing, all technology firms, whether dealing with virtual assets or not, tend to get lumped into the same ‘high-risk’ category.

In 2017, many banks in Hong Kong and Singapore closed most accounts associated with fintech or virtual currency businesses for this reason. Furthermore, not having a dedicated regulator makes it difficult to show that a VCE is explicitly regulated.

According to Wolfson, increasing regulation would have a positive impact by reducing the gap between traditional finance and the virtual asset sector, whereby regulatory certainty can mitigate many of the frictions between virtual asset platforms and banks. Wolfson says that within an environment with clarity on the rules, banks can make a pure risk/reward judgment when engaging with virtual assets, instead of fearing the prospect of running afoul of regulations.

“Banks will be able to assess the cost of doing due diligence with the potential benefits of the business relationship with every client they deal with. They will look at the amount of revenue they can generate from the client versus the costs of managing and monitoring that client on an ongoing basis. So the virtual asset sector would fall in line with other industries that they’re taking those risk/return decisions for every day,” he says.

Standardizing the KYC process for VCEs and assets could also open the door for trading virtual currency derivatives like exchange-traded funds or futures. Industry

and regulators will be watching for this in jurisdictions like Australia and Japan, where regulators have begun regulating the virtual asset space.

“If the risk of money laundering and terrorist financing doesn’t increase there, then other countries may potentially follow suit,” says Wolfson.

As with any new line of business, banks and VCEs should approach their respective clients with an understanding of potentially elevated risks. Both types of institutions must perform a complete risk assessment to ensure AML compliance. Confirming the true identity of a customer, both for serviced clients and transaction counterparties, is a necessary aspect of sanctions compliance as well as for anti-fraud and transaction monitoring. Risk-based watchlist screening, as well as enhanced due diligence, may also be appropriate in some instances. And similar to traditional financial relationships, VCEs will need to establish an understanding of the purpose and intended nature of the transaction or business relationship.

Conclusion

In the years without any regulation and following the downfall of the former online black market known as Silk Road, the virtual asset sector was more or less delegitimized at it became associated with criminal activity.

The relationship between the traditional financial industry and the virtual asset space will improve only when the latter is subject to robust regulatory regimes. For banks to deal with them, VCEs in Asia Pacific will need a dedicated regulator accountable for ensuring safety in the space, as is the case with all the other entities banks deal with. A minimum level of regulation, therefore, is necessary to push VCEs towards more stringent KYC/AML checks, in order to close the virtual asset space off as an avenue for possible money laundering and terrorism financing.

Robust KYC/AML practices at VCEs benefit not just individual institutions but the industry as a whole. The infrastructure built around the traditional financial system, which requires due diligence on prospective customers and ongoing monitoring,can be a useful starting point for virtual currency firms. Adding a layer of technology and innovation to traditional checks can help reduce onboarding time and costs, while providing credibility to the virtual asset sector and paving the way for greater participation from retail and institutional investors.

Works Cited

Stettner, Barbara. "Anti-Money Laundering Regulation of Virtual assets." 2018. *Allen & Overy, LLP*. <http://www.allenovery.com/publications/en-gb/Documents/AML18_AllenOvery.pdf>.

Liu, David. "Virtual assets in APAC: Opportunity, Challenge and Risk." *Enterprise Innovation* June 2018.

Lai, Karry. "New Rules Could Enhance Credibility of Japan's Virtual Market." *International Finance Law Review* August 2018.

Christensen, Claus. "Europe's AMLD5 and its Impact on AML Regulations in Asia." 15 October 2018. *Regulation Asia.* 15 October 2018.

Chandler, Simon. "Crypto Is Tightening Up Its Anti-Money Laundering Game, While Banks Are Still Being Fined for Non-Compliance" Cointelegraph January 2019.

[1] https://cointelegraph.com/news/crypto-is-tightening-up-its-anti-money-laundering-game-while-banks-are-still-being-fined-for-non-compliance

For More Information visit risk.lexisnexis.com/KYC-EN

LexisNexis® RISK SOLUTIONS

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 Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com, and www.relx.com.