Biometric ID and Crypto Exchanges

The use of biometric ID is critical to comply with anti-money laundering/countering financing of terrorism (AML/CFT) obligations in the booming virtual asset (VA) or crypto currency markets, e.g. Bitcoin. For the purposes of this article, the FATF terminology of VA will be used rather than crypto currency.

Blockchain

The blockchain technology allows creations such as Bitcoin and other crypto assets. The blockchain technology also can enhance compliance with AML/CFT related regulations and standards as transactions undertaken in the blockchain is recorded permanently in a public ledger. Anyone with the skill and appropriate software can verify, for example, VA's that are recorded in a public ledger such as Bitcoin.

Virtual Assets & Virtual Asset Service Providers

VASPs

The revised Financial Action Task Force (FATF) Recommendation 15 on VAs and Virtual Asset Service Providers (VASPs) have led many countries to amend, or introduce new or amended legislations to include VASPs within their AML/CFT regulatory ambit.

The FATF has been undertaking two 12-month reviews of the global implementation of Recommendation 15. Based on the latest review of the 128 jurisdictions that had responded to the FATF survey, 58 jurisdictions have established necessary AML/CFT legislations, with 52 permitting VASPs through licensing or registration, and six prohibiting VASPs. Another 26 jurisdictions are in the process of introducing legislations with all permitting VASPs. For the 12 jurisdictions that have decided but yet to introduce legislations, there is an even split with those permitting and those prohibiting. Finally, 32 have not decided. In Europe, EU allowed the existence of crypto assets but the Anti-Money Laundering Directive (AMLD) requires robust anti-money laundering measures in place to counter relevant money laundering risks.

It appears that globally most countries are allowing VASPs which include crypto exchanges, although some countries such as Algeria, Bangladesh, Bolivia, China, Ecuador, Egypt, Lebanon and Nepal have prohibited their operations. In Europe, Macedonia also prohibited VASPs. Others have VASPs operating but there is no regulatory framework.

Based on the FATF 12-monthly reviews, there are 2,374 VASPs licensed or registered globally. This number will grow significantly once more jurisdictions introduce the required legislations. In the Asian region, Singapore and Japan have the largest number of registered or licensed VASPs respectively. Globally, Canada and Australia have the largest numbers of registered or licensed VASPs respectively.

FATF – R. 15 & R. 16

FATF Guidance on VASPs

The updated Guidance of FATF for a Risk-Based Approach for VAs and VASPs issued in October 2021 forms part of the FATF's ongoing monitoring of VAs and VASPs, in line with FATF's updated Recommendation 15 (New Technologies) and Recommendation 16 (Wire Transfer). The updated Guidance, originally published in 2019, reflects the input from the public consultation in March –April 2021, and explains how the FATF Recommendations should apply to VAs and VASPs. It also provides relevant examples; identifies obstacles to applying mitigating measures; and offers potential solutions.

The Guidance also makes it clear that for FATF's purposes, central bank digital currencies are not VAs as they are digital representation of fiat currencies.

In particular, the Guidance focuses on the following six key areas:

- clarification of the definitions of VA and VASP;
- updated guidance on the licensing and registration of VASPs;
- guidance on how the FATF Standards apply to stablecoins;
- additional guidance for the public and private sectors on the implementation of the "travel rule";
- additional guidance on the risks and the tools available to countries to address the ML/TF risks for peer-to-peer transactions; and
- principles of information-sharing and co-operation amongst VASP Supervisors.

In general, VASPs and financial institutions have the same AML/CFT obligations. They must undertake Customer Due Diligence (CDD), keep records and prepare suspicious transaction reports (STRs), amongst other obligations. The major difference for a VASP implementing CDD is that all interactions are non-face-to-face as many VASPs do not have physical branches or agents i.e. all transactions are conducted online. Even if they do, they serve back office functions and not physical interactions with customers.

The FATF Guidance on VASPs reiterates that the CDD obligations for financial institutions and designated non-financial businesses and professions (DNFBPs) are also applicable to VASPs. The main difference is the threshold for CDD on an occasional transaction is USD/EUR 1 000, and not USD/EUR 15 000 for financial institutions and DNFBPs.

The Guidance notes that nearly all VAs include one or more features or characteristics that indicate activities in this space are inherently of higher risk, based on the very nature of virtual asset products, services, transactions, or delivery mechanisms. It involves pseudonymous or anonymous transactions, non-face-to-face business relationships or transactions, and/or payment[s] received from unknown or un-associated third parties.

The Guidance states some enhanced due diligence measures that may mitigate the potentially higher risks. They are as follows:

a) corroborating the identity information received from the customer, such as a national identity number, with information in third-party databases or other reliable sources;

b) potentially tracing the customer's IP address;
c) the use of analysis products, such as blockchain analytics; and
d) searching the Internet for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with national privacy legislation.

The FATF remains vigilant and will closely monitor the virtual assets and VASPs sector for any material changes that necessitate further revision on clarification of the FATF standards. This includes areas such as stablecoins, peer-to-peer transactions, non-fungible tokens (NFTs) and decentralized finance (DeFi).

Biometric ID and customers of crypto exchanges

Given the virtual nature of crypto exchanges, the use of biometric ID in the non-face to face onboarding world of VAs is essential for both compliance and business purposes.

Most crypto exchanges allow a person to apply as a new customer to onboard remotely by using a selfie biometrics via a smart phone. Normally the new customer will take a self-portrait photograph (selfie) and a photo of the ID document. The smart phone application will then match the selfie photo and ID document photo, and undertake a liveness check to thwart false presentation.

A sound system should also ensure that the ID document is genuine by either undertaking ID document verification or direct biometric verification to the original source i.e. government authority. If there is no check, then the customer may present a fake ID document which will match perfectly with the person's biometrics and liveness test.

Many countries, however, do not have a centralized national, biometric ID system, or if they do, for various reasons, businesses that are required to comply with AML/CFT cannot have access for customer verification purposes. In some cases, access can be available at a cost,

but the cost may be prohibitive. Some countries do not permit biometric verification because of fraud and data protection/privacy concerns.

The use of biometric verification by crypto exchanges is essential to prevent fraud, ransom payments, money laundering, terrorism and proliferation financing and other criminal acts. Biometric verification will also minimize the risk of using crypto exchanges based offshore in order to move funds out of a country. Such fund movement may be in violation of foreign exchange controls and/or domestic prohibitions in dealing in VAs and VASPs.

In today's digital world and particularly the crypto world, people buy and sell VAs online irrespective of their geographic locations or the physical locations of the crypto exchanges.

For the above reasons, it is important to have biometric verification for all new customers, or their representatives or beneficial owners, and even for ongoing surveillance for the existing customers of VASPs. This requires access by crypto exchanges to government held data to verify the authenticity of the scanned ID documents using a mobile app or other means. Without this, selfie biometric may not meet the AML/CFT requirements of some countries, such as those in the European Union. The adoption of biometric ID verification is also the best practice in line with the FATF's Guidance on Digital ID issued in February 2020.

Last but not least, reliable policies and procedures will help prepare VASPs to safeguard the assets in custody and to provide assurance to regulators, through embracing automation technology for ongoing monitoring, secure custody solutions as well as seamless connectivity and capability of cybersecurity, particularly by application of biometric ID verification and authentication technology, together with strong governance and robust risk management frameworks across customers, vendors and internal staff.

January 2022

Alliance for Financial Stability with Information Technology