ANTI-MONEY LAUNDERING: THE BASICS

Installment 7: Virtual Assets

"Virtual Assets" refers to a broad new class of assets powered by Distributed Ledger Technology (DLT). DLT allows for data to be stored at multiple locations ("decentralized") on a shared network allowing participants to track the ownership and transfer of virtual assets, like Bitcoin. Virtual assets present unique features, advantages and disadvantages vis-à-vis traditional assets and payments. Professional accountants must familiarize themselves with the ways in which these unique features can be used by money launderers and terrorist financiers to acquire, move, and store value, often outside the regulated financial system and conceal the origin or destination of funds.

How can criminals misuse virtual assets?

Virtual assets may be involved in any of the stages of money laundering including:

- Predicate crime: for example, raising funds through illegal activity by selling illegal goods or services in return for virtual assets.
- Placement: converting ill-gotten virtual assets into fiat currencies within a traditional financial system.
- Hiding: Crypto-based transactions can generally be followed with blockchain analytics, however there may not be any link between a transaction and any given individual when conducted outside of the regulatory perimeter. Criminals can also use anonymizing services like mixers and tumblers to break the links between crypto transactions.
- Layering: Converting fiat assets into virtual assets, exchanging virtual assets, conversion between virtual assets and converting virtual assets into fiat currencies.
- Integration: similar to laundering of dirty fiat money, an online company that accepts crypto payments can be formed to legitimize income and clean dirty crypto.

Definitions

Virtual Asset (VA): A virtual asset is a digital representation of value that can be transferred or used for payment. It does not include digital fiat currencies.

Cryptocurrency: A decentralised virtual asset that is protected by cryptography that can be used as a means of exchange, transferred, stored and traded electronically. The most popular of the thousands of cryptocurrencies are Bitcoin and Ether.

NFT (Non-Fungible Token): A completely unique virtual asset. While there are many Bitcoins, there is only one of each NFT. These often represent a specific piece of digital artwork or some other digital or real property.

Virtual Asset Service Provider (VASP): A business that provides any of the following services:

- Transferring or exchanging between virtual assets and fiat currencies, or between different virtual assets;
- Safekeeping/administration of virtual assets;
- Providing financial services related to virtual asset issuance.

Virtual currency wallet: A means for holding, storing, and transferring virtual assets.

CASE STUDY

Colonial Pipeline Ransomeware Attack

Virtual assets have quickly become a favorite form of ransom payment for cyber "ransomware" attacks, which are increasingly being seen by professional accountants, particularly auditors, and their clients.

The Colonial Pipeline attack in the United States is an indicative example of the ransomware attacks suffered by companies on a regular basis. In May 2021, the Colonial Pipeline Company suffered a major ransomware cyberattack that resulted in a five-day operational shutdown. The attackers demanded 75 Bitcoin in ransom, equivalent to USD 4.4 million, which Colonial Pipeline paid. While authorities were able to recover much of the ransom, further research revealed that the attackers had received over USD 90 million in Bitcoin from 47 different sources in the prior year.

Eventually, those illegal proceeds would need to be integrated into the legitimate financial system, potentially presenting an opportunity for professional accountants to identify and report. At the same time, ransomware attacks highlight the importance of effective cybersecurity controls.

Recent Additions to the FATF Standards

The terms "Virtual Asset" and "Virtual Asset Service Provider" are new additions to the FATF Glossary, having been added in 2018. At the same time, VASPs were brought into the FATF regulatory framework. For an in-depth look at VAs and VASPs from an AML/CFT perspective, see the FATF's Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

ADDITIONAL ASSISTANCE

For general guidance, see the FATF's *Guidance for a Risk-Based Approach for the Accountancy Profession*. For detailed local information, including applicable regulatory requirements, contact your Professional Accountancy Organization.

⚠ Key Red Flags

The red flags for "traditional" money laundering apply. In addition:

- Bulk of a client's source of wealth is derived from investments in VAs, without any paper trail.
- A client's source of wealth is disproportionately drawn from VAs originating from VASPs that lack AML/CFT controls.
- Client utilises a VA exchange in a high-risk jurisdiction lacking AML/CFT controls.
- A client frequently changes their identification information, including email addresses, IP addresses.

Recent crypto money laundering schemes have leveraged the following:

- Unregulated cryptocurrency exchanges (non-AML / KYC compliant).
- Gambling and gaming sites.
- Use of 'mixing services' or tumblers (e.g., Anonymix).
- Crypto ATMs with weak risk management.
- Prepaid crypto debit cards.

Significant activity leveraging these products / services should prompt a second look and further examination by accountants.

When to Walk Away

- The services requested may be of a specialist nature outside of your area of competence.
- There are no trading or investment records detailing the origin of the funds.
- You have concerns about the reputation of the virtual asset, its issuer(s) and exchange(s).
- There is a lack of effective AML/CFT controls put in place by the issuer(s) and exchange(s).
- You have concerns about the veracity of the information provided by, or otherwise have concerns about, the client.

Filing a Suspicious Activity Report ("SAR")

If you become suspicious that there may be criminal activity or proceeds of crime involved in the asset transfer, then you may wish to report your suspicions to the local Financial Intelligence Unit. In some jurisdictions this is a legal obligation for professional accountants.

IFAC International Federation of Accountants®
529 Fifth Avenue, New York 10017
www.ifac.org | +1 (212) 286-9344 | @ifac | company/ifac

ICAEW
www.icaew.com
@icaew | company/icaew