THE ANCHOR

CAYMAN'S TOP SCORE FOR TECHNICAL COMPLIANCE

In 2021, the Cayman Islands was successfully re-rated as "Largely Compliant" with Financial Action Task Force's ("FATF") Recommendation 15 which relates to New Technologies.

Significant to this achievement was the introduction of the Virtual Asset Service Providers ("VASP") Act, 2020, completion of a risk assessment of the VASP sector and implementation of a system of registration for anti-money laundering ("AML") and countering the financing of terrorism ("CFT") supervision.

This means that the Cayman Islands is now compliant or largely compliant with all 40 of the FATF Recommendations. Only one other country has done the same, demonstrating that the Cayman Islands is a global leader on technical compliance.

CIMA remains committed to meeting its AML/CFT international obligations.

WHAT'S INSIDE

ENVIRONMENTAL CRIME: UNDERSTANDING THE RISKS

"

Environmental crimes have become "low risk, high reward" activities that provide a safe source of income for criminals, while causing devastating damage to the world's ecosystem.

Financial service providers ("FSPs") and trust and corporate service providers ("TCSPs") are important actors in tackling financial crime, including environmental crime. Developing a sufficient understanding of the money laundering ("ML") risks associated with environmental crime is essential to developing a strategy to tackle this type of criminality.

Environmental crime has no universal definition, but generally refers to criminal offences harming the environment. These include illegal extraction and trade of forestry and minerals, land clearance and waste trafficking. The clean-up costs for governments are significant, as well as posing serious threats to public health and safety.

According to the Financial Action Task Force ("FATF"), environmental crime generates around US$110 to $281 billion in criminal gains each year. However, there has been limited action by governments and the private sector to identify, investigate and prosecute laundering of proceeds from these crimes. Only a small number of countries have conducted ML risk assessments to consider their position in the global environmental crime supply chain. As a result, environmental crimes have become "low risk, high reward" activities that provide a safe source of income for criminals, while causing devastating damage to the world's ecosystem.

In 2020, FATF published a report focusing on money laundering from illegal logging, illegal mining and waste trafficking, due to the significant criminal gains involved, and their convergence with other serious offences. Forestry crime (including illegal logging and illegal land clearing) was identified as the most significant environmental crime by value of gains, producing an estimated US$51 to $152 billion annually. Illegal mining was calculated to generate an estimated US$12 to $48 billion a year in criminal proceeds, with gold and diamonds considered to be the most significant source materials. Illicit waste trafficking produced an estimated US$10 to $12 billion annually.

Unlike many other environmental crimes, criminals use the mining sector to both generate illicit proceeds through illegal mining, and to launder proceeds from other crimes using the cash-intensive nature of the industry. Precious metals and stones, in their raw (or unprocessed) form, also carry an inherent value. As a result, they act as a form of currency that allows for trade/payment for goods outside the formal financial sector.

Both illegal logging and mining place a heavy reliance on front companies located in offshore centers, third party transactions and complicit intermediaries to both conceal payments and launder gains. There is also a common trend for environmental crimes to comingle legal and illegal goods, or to over or under declare goods being shipped or to use false descriptions, creating challenges in distinguishing between trade-based money laundering, trade-based fraud, and ML from environmental crimes.

ENVIRONMENTAL CRIMES: UNDERSTANDING THE RISKS CONT'D

Recognising these risks, in July 2021, FATF published a report on "Money Laundering from Environmental Crime", which identified some of the following red flags for potential illegal mining, logging and waste trafficking:

- Transfers from country where the gold smelters are located to origin country, and almost immediate cash withdrawal of majority of the transfer.
- Deposits and wire transfers from several origins without economic or financial grounds, or from regions far from the legal person's main site of operations or the natural person's domicile.
- Frequent payments to suppliers or beneficiaries unrelated to the legal person's activity or business.
- Increase in companies' purchases and imports of goods and products for use in logging and mining, for example chainsaws, mercury or explosives.
- Large volume and value of cash transfers to cash-intensive businesses (such as petrol or gas stations) in areas known as a source of gold mining or illegal deforestation.
- Sudden and unexplained increases in economic activity (formal and informal) in rural or isolated zones. This may include not only value but volume and frequency of transactions involving banks, money service businesses and remitters, or unusually high volume of business turnover in cash transactions at businesses providing consumer goods and services in proximity to at-risk zones.
- Co-mingling of funds through related businesses and export/sale of undervalued products, using back-to-back invoicing suggesting ongoing illegal transfer pricing scheme.
- High deposits and withdrawals of cash recorded on bank accounts held by waste management sector companies.

- Company operating in the metals and waste disposal sector or without an adequate organisational structure or whose address did not report any economic activity and/or shares sold at lower than book value or high withdrawals of cash recorded on bank accounts held by waste management sector companies.
- Non-substantiated claims by companies that they are recycling operations, contrary to actual business activities.
- Sudden and unexplained investment in waste facilities from sources with unclear beneficial ownership information.

FSPs and TCSPs should take note of these red flags and consider how to incorporate them into their AML/CFT/CPF compliance frameworks.

"

By building a deeper understanding of the Cayman Islands' role within environmental crime supply chains, FSPs and TCSPs may help combat the harm posed by environmental crime.

RANSOMWARE ATTACKS USING VIRTUAL ASSETS

FSPs, TCSPs and public authorities are increasingly at risk from ransomware attacks. Ransomware is a type of malware that threatens to publish the victim's personal data, or perpetually block access to it, or shut down a system, unless a ransom is paid. Criminals are increasingly opting for ransomware payments using virtual assets due to the speed of transactions, global reach and anonymity provided.

As set out in FATF's September 2020 Report on Virtual Assets Red Flag Indicators, proceeds of ransomware attacks are often moved via unhosted or privacy wallets and/or other anonymity-enhancing tools and methods to VASPs, where they are exchanged for other virtual assets or fiat currency and can be used by illicit actors to pay for their criminal enterprises.

ACTIONS FOR FSPS AND VASPS

Criminal operations undertaking ransomware attacks are now subject to targeted financial sanctions and should be appropriately monitored and screened as part of any FSP's compliance framework. In addition to sanctions compliance, regulated entities should also strengthen their detection and alert systems to prevent and protect against ransomware attacks. This includes reporting attacks immediately to law enforcement, filing related suspicious activity reports ("SARs"), conducting regular ransomware awareness training with staff, and continually reviewing and updating new financial red flag indicators of ransomware.

These red flags occur when a:

- customer provides information that a payment is in response to a ransomware incident.
- transaction occurs between an organisation, especially an organization from a sector at high risk for targeting by ransomware, and company known to facilitate ransomware payments.
- company known to facilitate ransomware payments receives funds from a customer company and shortly after receipt of funds sends equivalent amounts to a convertible virtual currency ("CVC") exchange. Research indicates that many ransomware schemes involve CVC as it is the preferred payment method of ransomware perpetrators.
- customer shows limited knowledge of CVC during onboarding or via other interactions with the financial institution, yet inquires about or purchases CVC, which may indicate the customer is a victim of ransomware.
- company that has no or limited history of CVC transactions sends a large CVC transaction, particularly if outside a company's normal business practices.
- customer uses a CVC exchanger or foreign-located money services business in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities.
- customer initiates multiple rapid trades between multiple CVCs, especially AECs, with no apparent related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.