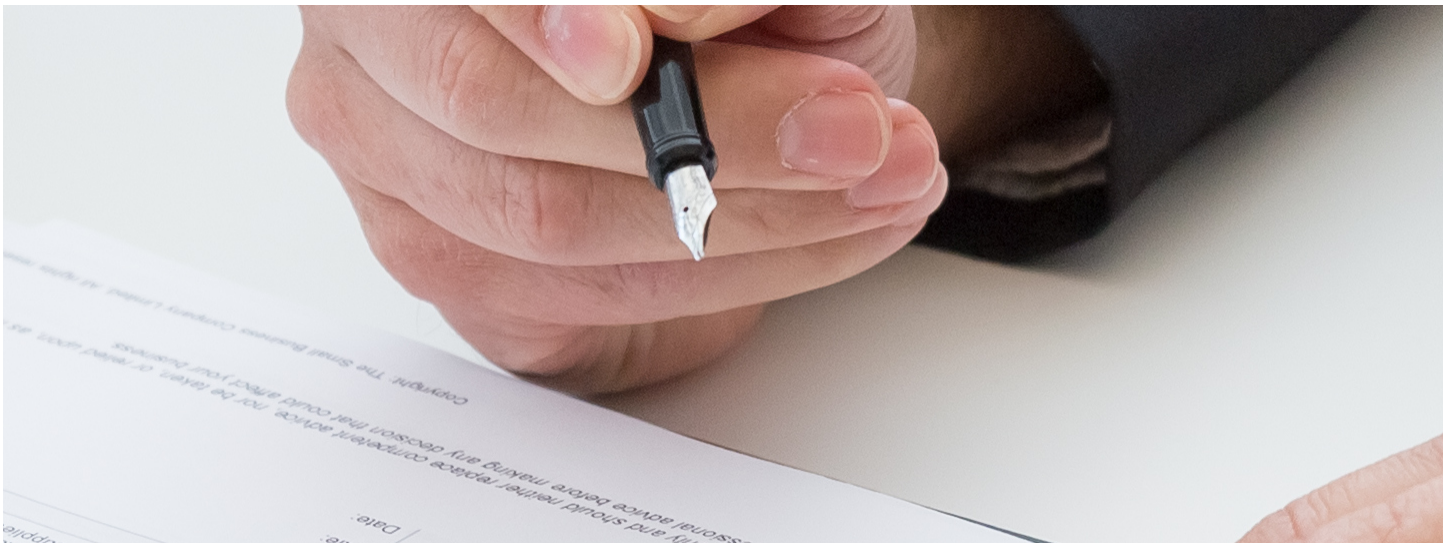
THE ANCHOR



SPOTLIGHT ON BENEFICIAL OWNERSHIP

The effective and accurate identification and verification of beneficial owners remains a key priority for the Cayman Islands in 2023. By obtaining and maintaining adequate, relevant and up to date information, financial institutions ("FIs") and trust and company service providers ("TCSPs") have greater visibility of the controllers and beneficial owners of the businesses they are serving, and a better understanding of their business relationships.

This year, a consultation is underway for the Beneficial Ownership Transparency Bill, 2023 (the "Bill"), which primarily seeks to enhance the transparency framework for legal persons and has been drafted to provide clarity to all users of the beneficial ownership legislation, to ensure greater efficiency of the framework, and to allow the overall effectiveness of the framework to be more easily improved. As part of the exercise in developing the Bill, a holistic review has been undertaken to ensure the legislative provisions are operational in practice, functional and clear of any ambiguities. The consultation closes on 25 April 2023.

The FATF also recently published revision to Recommendation 25 (Transparency and Beneficial Ownership of Legal Arrangements) following the newly published changes to Recommendation 24 (Transparency and Beneficial Ownership of Legal Persons). Amendments to

WHAT'S INSIDE

the Trust Act are underway to align the jurisdiction's trust framework to FATF's newly updated requirements.

Alert: Human Trafficking and Modern Slavery

On January 13, 2023, the Financial Crimes Enforcement Network (FinCEN) issued an alert to assist financial institutions in the detection of financial activity related to human smuggling along its South West border. These red flag indicators may also be relevant to Cayman regulated financial institutions to help detect and prevent similar crimes such as human trafficking, and other types of modern slavery.

'Human trafficking' refers to the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion for the purpose of exploitation. It is one of the most significant generators of criminal funds in the world, with proceeds estimated to be USD 150.2 billion in 2018. The magnitude of this crime has resulted in the FinCEN classifying human smuggling and human trafficking as one of the eight Anti-Money Laundering and Counter Financing of Terrorism National priorities.

'Modern slavery' is an umbrella term that includes forced labour, debt bondage, chattel slavery and other slavery-like practices, human trafficking and forced marriage. It refers to situations of exploitation that a person cannot refuse or leave because of threats, violence, coercion, deception, and/or abuse of power. Contemporary forms of forced labour, include migrant workers, who have been trafficked for economic exploitation across different economic sectors for the purposes of, for example, domestic servitude, the construction industry, food and garment industry, agricultural sector or forced prostitution. Human smuggling generates billions annually, funds of which are laundered into the financial system or used to make cash purchases of land, luxury items, vehicles and businesses. Contraband networks also engage in bulk cash smuggling, moving the currency across international borders which are then deposited at financial institutions in smaller increments under reporting thresholds. Smugglers frequently use legal businesses such as retail, wholesale and car dealership companies to undertake trade-based money laundering, often recruiting straw men and third parties, mainly relatives, to run these businesses.

The FinCEN alert provides financial institutions with trends, typologies, and red flag indicators to aid them to better identify and report suspicious transactions potentially related to human smuggling activity. These include:

- Transactions involving multiple wire transfers, cash deposits, or P2P payments from multiple originators from different geographic locations either across the US or Mexico and Central America, to one beneficiary located on or around the southwest border, with no apparent business purpose.
- Deposits made by multiple individuals in multiple locations into a single account, not affiliated with the account holder's area of residence or work, with no apparent business purpose.
- Currency deposits into US accounts without explanation, followed by rapid wire transfers to countries with high migrant flows (e.g., Mexico, Central America), in a manner that is inconsistent with expected customer activity.
- Frequent exchange of small-denomination for larger-denomination bills by a customer who is not in a cash-intensive industry.
- Multiple customers sending wire transfers to the same beneficiary (who is not a relative and may be located in the sender's home country), inconsistent with the customer's usual business activity and reported occupation.
- A customer making significantly greater deposits- including cash deposits- than those of peers in similar professions or lines of business.
- A customer making cash deposits that are inconsistent with the customer's line of business.
- Extensive use of cash to purchase assets, such as real estate, and to conduct transactions.

Financial institutions in the Cayman Islands should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.

Ransomware: Further Red Flag Indicators

FATF has also recently updated its red flag indicators for banks, virtual asset service providers (VASPs) and other financial and payment institutions to help spot potential illicit ransomware payments.

Obvious

- Client self-reporting of a ransomware attack or payment.
- Open-source information suggests ransomware attacks have been made on clients.
- Payment description contains words such as "ransom" or names of ransomware groups.
- Outgoing wire transfers to cybersecurity consulting or incident response firms that specialise in ransomware remediation.
- Unusual incoming wire transfers from insurance companies that specialise in ransomware remediation.
- VASPs identifying ransomware victim payment.
- VASPs identifying ransomware payment receipt/ransomware criminal account.
- Customer states to the VASP that they are purchasing virtual assets (VA) due to ransomware payment.
- Blockchain analysis on wallet addresses reveals ties to ransomware.
- Sending of VAs to wallets linked to ransomware.

Less obvious

- Request to buy VAs by an incident response firm or insurance company on behalf of a third party.
- User with no history of virtual asset transactions sending funds outside of standard business practice.
- A customer increases limit on an account and sends to a third party.
- A customer seems anxious or impatient with the amount of time taken for a payment.
- Inconsistent identification details or an attempt to create an account with a false identity.
- Multiple accounts linked to same contact details; addresses shared under different names.
- Following an initial large virtual asset transfer, a customer has little or no digital currency activity.
- Immediate withdrawal after converting funds to virtual assets.
- Customer appears to use a VPN and/or encrypted network.
- Purchases of or transfers involving anonymity-enhancing cryptocurrencies such as Monero.
- High volume of transactions from same bank account to multiple accounts at a VASP.
- Payments made to VASPs in high-risk jurisdictions.
- Transferring virtual assets to mixing service.
- Verification information is a photograph of data on a computer screen or has a file name containing "WhatsApp image" or similar.
- Customer's syntax does not match the customer's demographic.
- Customer information shows customer holds an email account known for high privacy such as proton mail or Tutanota.

The occurrence of a single financial red flag indicator is not automatically determinative of illicit or suspicious activity, however it should prompt further monitoring and examination, as appropriate.