May 2024 AML/CFT NEWSLETTER

THE ANCHOR

AND WE'RE OFF! REMOVAL FROM THE FATF AND EU 'GREY LISTS'

Effective 7 February, the Cayman Islands was removed from the EU's list of jurisdictions with deficiencies in their AML/CFT (anti-money laundering and countering the financing of terrorism) regimes. This followed the successful removal from the Financial Action Task Force ("FATF") 'grey list' in October 2023.

The EU's Delegated Regulation sets out the European Commission's assessment that the Cayman Islands has strengthened the effectiveness of its AML/CFT regime and addressed technical deficiencies to meet the FATF's action plans.

Notwithstanding this, the Authority continues its work to promote and safeguard the integrity of the Cayman Islands financial services industry through sustainable, data-led, risk-based AML/CFT supervision. CIMA will also continue its work to track deficiencies, requirements and remediation to assess industry compliance with onsite findings, and ensure prompt and consistent escalation to enforcement where required. The Authority will maintain high levels of AML/CFT supervisory oversight to drive compliance by regulated entities and has already commenced its preparation for the 5th round mutual evaluation by the FATF.

WHAT'S INSIDE

NEW TARGETED FINANCIAL SANCTIONS UPDATES

Targeted financial sanctions continue to be a major focus for regulated entities in 2024. The Russian (Sanctions) (Overseas Territories) (Amendment) Order 2024 came into force on 14 March 2024. The UK Government has also recently issued important updates, including:

Russia Guidance

While there are different types of sanctions related to Russia, this guidance expands specifically on financial and investment restrictions and additional reporting obligations for designated persons and relevant firms. In addition to asset freezes, which are common among other sanctions regimes, these restrictions include additional unique measures that restrict access to capital markets, loans and credit arrangements, clearing services, dealing in reserves for certain Russian state-owned financial institutions, investments in Russia and investments in nongovernment controlled Ukrainian territory. There are also restrictions on the provision of trust services. They also detail restrictions on investments in relation to the Republic of Crimea and the city of Sevastopol.

A Red Alert for Exporting High-Risk Goods with Red Flag Indicators

A red alert has been issued on Russian efforts to circumvent sanctions to purchase restricted goods and services, through intermediary countries. Red Flag indicators include (but are not limited to):

- Transactions related to payments for goods on the Common High Priority list, from a company incorporated after 24 February 2022 and based in known diversionary destinations.
- A customer who lacks or refuses to provide details on banks, shippers, or third parties, including about end users, intended end-use, or company ownership.
- Transactions involving smaller value payments, all from the same end user's foreign bank account, to multiple, similar suppliers of Common High Priority list items.
- A customer that significantly overpays for a Common High Priority list item, compared to known market prices.
- Purchases under a letter of credit that are consigned to the issuing bank, not to the actual end user. In addition, supporting documents, such as a commercial invoice, do not list the actual end-user.
- Transactions involving entities with little to no web presence, such as a website or domain based email account.
- Transactions involving customers with phone numbers with country codes that do not match the destination country.
- The item or service (commodity, software, service or technology) does not fit the purchaser's line of business.
- The customer's name or its address is similar to one of the parties on the OFSI consolidated list.
- Transactions involve a purported civil end-user, but research indicates customers with counterparties with connections with the military, such as an address that is a military facility or is co-located with military facilities in a country of concern.
- Transactions involving companies that are physically co-located, or have shared ownership, with an entity on the OFSI consolidated list.
- Transactions that use open accounts/open lines of credit when the payment services are conducted in conjunction with known diversionary destinations.
- Transactions involving a last-minute change in payment routing that was previously scheduled from a country of concern, but now routed through a different country or company.
- Transactions involving payments being made from entities located at known transhipment points or involve atypical shipping routes to reach a destination.

No single red flag is necessarily indicative of illicit or suspicious activity. All the surrounding facts and circumstances should be considered before determining whether a specific transaction or customer is suspicious or associated with potential sanctions evasion.

NEW 'TRAVEL RULE' GUIDANCE

The Authority has recently amended its Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (the "GNs") to include amendments to Part IX – Section 1 – VASP, to reflect Part XA of the Anti-Money Laundering Regulations (the 'Travel Rule').

VASPs are encouraged to have robust policies and procedures in place to ensure a consistent and adequate approach to obtaining, exchanging and storing the appropriate information. These may include (but are not limited to) procedures for the ongoing monitoring of incoming transactions without full Travel Rule information, a description of the risk indicators that would prompt cancellation of an outgoing or incoming transaction, timelines for restricting funds without complete Travel Rule information, policies to keep records secure, and procedures for the sanction screening of counter parties. For further information see: Guidance Notes from CIMA for Anti-Money Laundering.

SPOTLIGHT: ML/TF RISKS POSED BY INFORMAL FUNDS TRANSFER NETWORKS (HAWALA, HUNDI, FEI CHI'IEN AND CHITTI)

Informal funds transfer networks ("IFTN") such as Hawala, Hundi, Fei ch'ien, and Chitti offer an alternative to traditional wire transfers and can be used by criminals to launder money or finance terrorism. They are honour systems predominately used among people of the same family, village, clan, ethnic group and regional affiliation to remit or transfer funds without any physical money moving from one place to another. These networks originated many years ago to carry out trade transactions yet continue to be a popular method of transferring funds across geographical borders outside of the traditional formal banking system.

How Does it Work?

Fundamental to the IFTN are the brokers/dealers who usually run the service through legitimate businesses. The broker/dealers accept money from persons to remit or transmit funds to another person (recipient) in a different jurisdiction, through another IFTN broker/dealer in that jurisdiction.

The sending broker/dealer, provides the intended recipient's name and a password. The sender also shares the same password with the intended recipient.

The sending broker/dealer then contacts another broker/dealer in their network located in the jurisdiction of the recipient, shares the password, and instructs of the amount to be paid to the recipient. The funds are paid, usually minus a small commission once the recipient informs the receiving broker/dealer of the password. The broker/dealer in the sender's jurisdiction now owes the receiving broker/dealer who has paid the recipient. There is no actual transfer of funds between broker/dealers and no promissory instruments are exchanged, the two broker/dealers simply settle the accounts as a trade transaction.

Why is it So Popular?

The Hawala, Hundi, Fei ch'ien, and Chitti IFTN have many advantages: they are typically more efficient than wire transfers sent through the traditional banking system, with lower fees and a quicker processing time for the remittance of funds. IFTN broker/dealers can also offer more attractive currency exchange rates than those offered by banking institutions. Importantly, they can provide services to the financially excluded, and those in rural areas or of a lower socioeconomic position, who are unable to access the formal banking platform. IFTN are particularly useful for immigrants or persons without bank accounts who wish to transfer their money to their families overseas. IFTN have also been legitimately utilised by nongovernmental organisations and aid donors in conflict-afflicted jurisdictions with restrictions around formal remittance services.

IFTN and Money Laundering/Terrorist Financing

Unfortunately, IFTN may also be attractive to money launderers and the financing of terrorism. The anonymity of the transactions, the lack of customer identification and verification, the inability to trace the source of funds and the lack of an audit trail for law enforcement purposes make IFTN vulnerable to criminals and terrorists seeking to transfer illicit funds across international borders.

While Hawala, Hundi, Fei ch'ien, and Chitti IFTN may not play a major role in the Cayman Islands domestic economy (no IFTN have been identified in the Cayman Islands, and none are registered at CIMA as a money value transfer service), financial service providers should nevertheless be aware of their existence and develop procedures for identifying transactions that may be linked to such systems and take appropriate risk mitigating measures.

Informal Money Transfer Network Red Flags for Financial Service Providers

The types of businesses that participate in the informal money transfer networks (as opposed to the people who make use of the networks) are often those that routinely engage in foreign trade (travel agents, import-export agents, foreign exchange bureaus, and used car dealers who ship older vehicles overseas.)

In examining bank account information of these and other businesses, there are several red flag indicators that suggest a higher likelihood that the account holder is part of an informal money transfer network:

- Customer has travelled unexplained distances to locations to conduct transactions with no apparent business or lawful purpose.
- Transfers to sole traders or companies engaged in a very different kind of business to the customer with no clear reason for the payment.
- Frequent international wire transfers from bank accounts which appear inconsistent with stated business.
- Frequent wire transfers to foreign countries but customer does not seem to have any connection to the destination countries.
- Business accounts used to receive or disburse large sums of money but show virtually no normal business related activities, such as the payment of payrolls, invoices, etc.
- Frequent deposits of third party cheques and money orders into business or personal accounts.
- Daily transfers of large sums that are not commensurate with the business of the customer.
- Repeated small deposits from a variety of local individuals in round numbers and fewer large transfers to parties in a known hawala centre, such as London or Dubai.
- Frequent deposits by multiple individuals into a single bank account, followed by international wire transfers and/or international withdrawals through automated teller machines (ATMs).