CAYMAN ISLANDS

MONEY LAUNDERING, TERRORISM AND PROLIFERATION FINANCING

TRENDS & TYPOLOGIES

Anti-Money Laundering Steering Group

UPDATED JUNE 2022

Table of Contents

Glossary of Terms 3

1. Introduction 5

1.1 Risk and Context 5

1.2 Legislative Framework 7

2. Methodology 9

2.1 Data sources 9

3. Money Laundering Typologies: FIs, DNFBPs, VASPs 10

3.1 Fraud 10

3.2 Corruption 27

3.3 Tax Evasion 32

3.4 Drug Trafficking 34

3.5 Gambling 38

3.6 Misuse of Corporate Structures 42

4. Terrorism Financing 45

5. Proliferation Financing 54

6. Emerging Money Laundering Trends 64

6.1 Virtual Currencies 64

6.2 Gold Storage 65

6.3 Human trafficking 66

7. References 67

Glossary of Terms

Abbreviation	Meaning
AML/CFT/CFP	Anti-Money laundering/Countering the financing of terrorism/Countering the financing of proliferation
"Authority"	The Cayman Islands Monetary Authority
CDD	Customer due diligence
CFATF	Caribbean Financial Action Task Force
CIBFI	Cayman Islands Bureau of Financial Investigations
CIMA	Cayman Islands Monetary Authority
CSP	Corporate Service Providers
Competent Authorities	As defined in Part 1:2 (1)(a) of the Proceeds of Crime Law (2018 Revision).
DCI	Department of Commerce and Investment
DNFBPs	Designated Non-Financial Business and Professions
DPM&S	Dealers in Precious Metals and Stones
DPRK	Democratic Republic of Korea
Drug Trafficking Law	The Drug Trafficking Offenses Law
EDD	Enhanced Due Diligence
EFT	Electronic Funds Transfer
FATF	The Financial Action Task Force
FCIU	Financial Crime Investigation Unit
FIs	Financial Institutions
FIU	Financial Intelligence Unit
FINTRAC	The Financial Transactions and Reports Analysis Centre of Canada
FRA	Financial Reporting Authority
FSP	Financial Service Provider
GR	General Registry
IC	International Conglomerate
ICO	Initial Coin Offering

GLOSSARY OF TERMS

KYC	Know your customer
MLAT	Mutual Legal Assistance Treaty
MLCO	Money Laundering Compliance Officer
MLRO	Money Laundering Reporting Officer
ML/TF/PF	Money laundering/Terrorism financing/Proliferation Financing
MSB	Money Services Business
NRA	National Risk Assessment
NPO	Non-profit Organization
PEP	Politically exposed person
PF	Proliferation Financing
POCA	Proceeds of Crime Act
RCIPS	Royal Cayman Islands Police Service
REA	Real Estate Agent
SAR/STR	Suspicious activity report/Suspicious transaction report
TFS	Targeted Financial Sanctions
UNSCR	United Nations Security Council Resolution
VA	Virtual Assets
VASP	Virtual Assets Service Providers
VPN	Virtual Private Network
WMD	Weapons of Mass Destruction

1. Introduction

The Cayman Islands legislative and regulatory framework to counter money laundering, the financing of terrorism and the financing of proliferation is led by the relevant *competent authorities* responsible for monitoring compliance and developing the AML/CFT framework.

This document is an update to the Money Laundering (ML), Terrorism Financing (TF) and Proliferation Financing (PF) Typologies and Trends, published in September 2019. It aims to provide practical guidance on the ML, TF, and PF risks identified in the 2021 National Risk Assessment (2021 NRA), and other data sources noted in the Methodology (p.9), and to raise awareness of the methods and techniques relevant to the Cayman Islands.

The methods used by money launderers, terrorists and proliferation financers identified through the following typologies and cases should be regarded as critical sources of information for the purposes of developing policies and procedures, coordinating efficient monitoring, conducting risk assessments, and providing effective training to employees.

This document heavily focuses on information obtained from the AML/CFT/CFP competent authorities. The intention of this document is to provide competent authorities, financial institutions and designated non-financial businesses or professions with the red flags and warnings associated with the various types of ML/TF/PF to improve prevention and detection, to assist relevant persons with the identification of customers who may be engaged in criminal activities, and to further improve the quality of suspicious activity reports (SARs).

Data and information provided has been collated and trends have been identified and presented as practical guidance for Cayman Islands financial institutions (FIs) and designated non-financial businesses or professions (DNFBPs).

1.1 Risk and Context

As one of the leading financial jurisdictions in the world, the financial services sector is a major contributor to the Cayman Islands' economy. As such, the financial industry is

heavily dominated by domestic and international banking, investment funds, capital markets, insurance, trust and fiduciary services.[1]

As with any jurisdiction that is heavily focused on financial services both domestically and internationally, there are inherent risks and threats involved, including money laundering and terrorism financing.

Notwithstanding this, the Cayman Islands has had a long-standing commitment to fighting financial crime and has, over time, enacted legislation combatting ML, TF and PF. In terms of the Cayman Islands as both an international financial centre and the structure of its finance services sector, the information presented in this document aims to increase the understanding on the nature and scope of ML, TF and PF trends.

To further adhere to international standards, this document will provide valuable information on the warnings, indicators and red flags associated with the risks of ML, TF, and PF within the Cayman Islands.

[1] Jude Scott – Cayman Islands: Overview of The Cayman Financial Services Industry (2018)

1.2 Legislative Framework

Money Laundering

Adhering to international standards, the Cayman Islands has adopted legislation and other measures necessary to criminalise money laundering.

Under the Proceeds of Crime Act (2020 Revision)[2]:

- **Section 133.** (1) A person commits an offence if that person -

(a) conceals criminal property;

(b) disguises criminal property;

(c) converts criminal property;

(d) transfers criminal property; or

(e) removes criminal property from the Islands.

- **Section 134.** (1) A person commits an offence if that person enters into or becomes concerned in an arrangement which that person knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

(2) A person does not commit an offence under subsection (1) if -

(a) he makes a disclosure to the Financial Reporting Authority or a nominated officer;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;

(c) he is a professional legal adviser and does not disclose information or other matter which came to him in privileged circumstances; or

(d) the act that person does is done in carrying out a function that person has relating to the enforcement of any provision of this Law or of any other enactment relating to a criminal conduct or benefit from a criminal conduct.

[2] Proceeds of Crime Act (2020), p. 99

(3) But subsection (2) (c) does not apply to information or other matter which is communicated or given with the intention of furthering a criminal purpose.

- **Section 135.** (1) A person commits an offence if he -

(a) acquires criminal property;

(b) uses criminal property; or

(c) has possession of criminal property.

Terrorism Financing

The Cayman Islands has adopted legislation to criminalise terrorism financing. Under the Terrorism Act (2018 Revision): "terrorist financing" means the financing of acts of terrorism, of terrorists and terrorist organisations and includes offences contrary to sections 19, 20, 21 and 22.

Proliferation Financing

The Cayman Islands has also adopted legislation to criminalise proliferation financing. Under the Proliferation Financing (Prohibition) Act (2017 Revision) ('PFPA'), proliferation is defined as '*the development or production, or the facilitation of the development of production, of nuclear, radiological, biological, chemical weapons or systems for their delivery*.' Section 23A makes it an offence for anyone to: *provide funds and economic resources to fund unauthorised proliferation activities; or to enter into or become concerned in an arrangement which that person knows, or suspects facilitates, by whatever means, the acquisition, retention, use or control of funds and economic resources to fund unauthorised proliferation activities.*

2. Methodology

2.1 Data sources

The following sources of information have been used to prepare this document:

- Domestic and non-domestic sanitised SARs, typologies and cases presented by the CIBFI, RCIPS, CIMA, FRA, DCI, and GR.

- Data provided by the National Risk Assessments of 2015 and 2021; and updated sectoral risk assessments completed in 2020.

3. Money Laundering Typologies: FIs, DNFBPs and VASPs

The typologies and warning indicators outlined below are intended mainly to:

- inform *FIs, DNFBPs* and *VASPs* about the various methods and techniques criminals may use to launder the proceeds of their illicit activity;

- assist competent authorities in developing training for the prevention and detection of money laundering, terrorist financing and proliferation financing.

3.1 Fraud

Domestically generated proceeds from fraud/theft amounted to $4.7 million, according to the 2021 NRA. This compares with foreign generated proceeds from fraud, which amounted to $394.1 million during the same period, with a total or 879 SARs, and 17 related standalone ML cases. With the widespread use of computers and communication devices, cyber related fraud has emerged as a significant foreign threat, particularly to the business community in the Cayman Islands. Cyber fraud through virtual assets (VAs) and virtual assets service providers (VASPs) is also an emerging area in the fight against ML/TF/PF.

Typology 1 - Fraud through a general insurer

The "Authority" identified concerns relating to related party transactions, poor corporate governance and the board's inability to value certain assets on its balance sheet.

The Authority noted that the audited financial statements of the licensed insurance company "Company A" carried a qualified opinion, as Company A was unable to provide documentation to support movements in its financial statements.

Company A had engaged in multiple related-party transactions which appeared to have no legitimate business purpose. Money flowed in a circular fashion: incoming cash flows from individuals and outgoing cash flows to entities. The individuals who extended loans to Company A were the same ultimate beneficial owners of the entities

that received loans. Company A had a seemingly healthy balance sheet nevertheless, it obtained loans (promissory notes) from several related individuals. There were at least eight incoming promissory notes and seven were past maturity date without being settled.

It appeared that the proceeds received from Company A by these borrowers were utilized to purchase real estate properties in "Country A". The Authority's inspection team questioned the purpose of involving Company A, i.e, why Company A which was a Cayman-based entity at that time, provided funds for the acquisition of real estate properties by other entities from Country A, whose ultimate beneficial owners are citizens of that Country.

The Authority also identified issues regarding conflicts of interest and lack of due care in protecting the interest of Company A by the Board of Directors, in addition to the poor regulatory compliance framework of Company A.

The Authority filed a SAR with the FRA. Subsequent to the inspection, Company A has terminated its license.

Red flags/Indicators:

- purchase of valuable assets, i.e., real estate
- trade-related ML and TF
- co-mingling (business investment)
- use of non-domestic banks
- use of nominees, trusts, family members or third parties
- loans with no obvious economic purpose or need
- misuse of insurance policies
- related party transactions which appear to have no legitimate business purpose

Typology 2 - Securities fraud through mutual fund

A Cayman law firm and a Cayman Mutual Fund Administrator provided legal services and administrative services respectively to a regulated Cayman mutual fund, "the

Fund". Their ongoing monitoring discovered adverse information referring to entities that appear to be related to the Fund and on "Mr. X", a director of the Fund.
The adverse information included:

- An enforcement action by a securities regulator in "Country A" against a number of defendants, including Mr. X and affiliated companies domiciled in Country A, for their involvement in a fraudulent and unregistered securities offering. One of the entities was in the business of selling promissory notes and using those funds to purchase accounts receivable invoices at a discount, a practice referred to as factoring, from affiliated companies in "Country X".
- A petition by the financial regulator in "Country B" for the Court to appoint independent administrative managers to a fund domiciled in Country B that had the same investment manager as the Cayman Fund. Both funds appeared to have the same investment mandate, which included to invest in factoring companies in Country X.

The FRA's research revealed that companies connected to Mr. X in "Country C" were in administration, with independent administrative managers appointed. These entities appeared to have the same investment mandate, i.e., investing in factoring companies. It was alleged that the monies raised from investors had ended up in companies owned by Mr. X in Country X, and had been used to fund Mr. X's interests, including funding his other companies.

The FRA made disclosures to the Financial Crime Investigation Unit of the Royal Cayman Islands Police Service ("RCIPS"), the Cayman Islands Monetary Authority ("CIMA") and the FIUs in Countries A, B and C.

Red flags/Indicators:

- investment primarily into affiliated entities
- adverse information about the client detected from ongoing monitoring
- similar structures in multiple jurisdictions

Typology 3 - Proceeds of fraud through jewelry theft

A US$2 million ($1,700,000 KYD) diamond sold to a Cayman jewelry dealer proved to be the breakthrough in an international police investigation into the theft of millions of dollars' worth of gems from a Gentlemen's Club, in "Country A". In June 2009 a USA diamond merchant, "the merchant," lost a bag of gems worth US$10 million ($8,300,000 KYD) in Country A. The merchant, who was at a jewelry show in Country A, was carrying rings in a small zip-up jewelry bag in the front of his pants. He attended a private club for about an hour, after leaving he realized the black pouch was missing. He went back to the club where the manager gave him back the pouch, which had been found by "Mr. Y", an employee at the club. The merchant rewarded the manager US$3,200 ($2,700 KYD) for returning the bag.

Later on closer inspection of the pouch, the merchant realized that two diamond rings were missing. One had a rare 3.01 karat purplish-pink diamond and two yellowish diamonds on the side, with a retail value of US$2 million ($1,700,000 KYD). The other had a 10.05 karat princess-cut diamond, with two 1.6 karat baguettes diamonds and multiple diamonds on the shank, which was worth US$960,000 ($768,000 KYD). He returned to the club and offered a US$10,000 ($8,000 KYD) reward for the return of the rings. When the rings were not returned, he notified the police. Further investigation revealed that Mr. Y and his fiancé sold the diamond to "Mr. Z", the owner of a prominent Jewelry Store in "Country B".

Mr. Z indicated that Mr. Y and his fiancé who were on vacation from Country A came to his store in Country B with the diamond, stating that they wanted to trade it for other jewelry. Mr. Z stated that Mr. Y came to the store dressed sophisticated and gave the impression that they have a lot of money.

He identified himself as "Mr. G" and stated that the diamond was an inheritance and he wished to trade it. Mr. G and his fiancé spent several hours at the store negotiating the deal. Mr. Z examined the jewel and knew it was expensive but estimated the value of US$130,000 ($108,000 KYD). He offered to purchase the diamond from Mr. G for US$7,000 ($5,600 KYD) cash and the remainder in other precious stones totaling of US$130,000 ($108,000 KYD). He then sent the jewelry to be appraised and certified by the Gemological Institute of America, the industry's foremost authority on diamond grading. The appraisal valued the jewel at US$500,000 ($417,000 KYD) but Mr. Z

believed it was valued more and requested a second appraisal which returned a value of US$1 million ($800,000 KYD). The appraiser also recognized the jewelry as being stolen.

The police in Country A was notified and an international investigation was launched. Mr. Z. identified Mr. G as the person who sold him the jewel. The police revealed that Mr. G's real identity is Mr. Y. It was later revealed that Mr. Y had sold the two loose diamonds they had received from Mr. Z in a second city in Country A for US$18,000 ($15,000 KYD).

Mr. Y reveals that they visited Country B after asking a family friend, "Mr. D", who worked in the jewelry business, in Country B, how to sell diamonds they hoped would fetch US$1.5 million ($1,300,000 KYD). Mr. D previously helped them to sell the 10.05 karat diamond for US$55,000 ($46,000 KYD) to a third City in County A. Mr. D then briefed Mr. Y on what to do when he visits Country B. Mr. D. was paid US$5,000 ($4,200 KYD) for his involvement.

US$14,000 ($12,000 KYD) in cash from a safe deposit box owned by Mr. Y was also seized. The 10.05 karat princess cut diamond has not been recovered.
Mr. D confessed to his role in the matter and was sentenced to 3 years' probation. Mr. Y and his fiancé each faced three charges, including felony possession of stolen property and conspiracy to possess stolen property.

Red flags/Indicators:

- the customer eagerness to sell the jewel
- the manner in which the jewel was transported
- customer willingness to accept below market value
- customer had little regard for the price, value, and colour of the jewelry he received
- customer offered jewelry for sale outside of his country of residence in an usual trading manner
- diamond was not accompanied by a valid Kimberly Process Certificate
- unusual method of payment

Typology 4 - Fraudulent use of trusts to buy real estate

Two trusts were established in "Country A" by a law firm as primary shareholder of a Holding Company. The Cayman Islands trustee was directed to accept two payment orders in favour of a bank in order to buy real estate in the name of the Holding Company in Country A.

The law firm controlled all communications regarding the trusts and the trustees had no idea who the beneficiaries were. The trustees made contact with a local Real Estate agent who assisted in the holding company purchasing two properties for US$450,000 ($360,000 KYD) and US$650,000 ($520,000 KYD).

Investigation revealed that individuals "Y" and "Z" were the beneficiaries of the trusts. Y and Z were Senior Managers of two fund management companies, established in "Country B" and were the subject of a fraud investigation regarding serious misappropriation of the funds in excess of US$1million ($800,000 KYD).
The funds in the trusts originated from criminal activity of the companies. The trust had been used to conceal the identity of the beneficial owners.

Red flags/Indicators:

- use of trusts to buy real estate
- the trusts were used to conceal the identity of the true owners
- the use of an intermediary without good reason
- the attempts to disguise the real owner or parties to the transaction
- the involvement of structures in multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason
- the client being known to be under investigation for crimes

Typology 5 - Corporate services fraud through foreign voluntary liquidator

"CSP A" is contacted by "Mr. B" living in "Country Y", to set up a Cayman Islands exempted limited liability company, "Company A". Mr. B states on the application form that the purpose of the company is to act as a "holding company".

Over time, Company A acquires and holds various assets and liabilities including documented (but fictitious) loans from "Mr. A". CSP A receives share transfer instructions received from Mr. B, approved by the directors of Company A, for the transfer of all issued shares to "Mr. M" who resides in "Country B" (a non-cooperative country).

Within a week, CSP A also receives from Company A, written resolutions of the new sole shareholder, Mr. M, commencing the winding up of Company A and appointing a foreign individual as Voluntary Liquidator (VL). All assets are realised by the VL and debts extinguished. "Loans" from Mr. A are repaid.

After the CSP files the relevant Companies Winding Up Rules ("CWR") forms and final returns with the Registrar of Companies, Company A is dissolved, the net proceeds of the liquidation having been paid by VL to Mr. M's order.

Red flags/Indicators:

- failure to establish source of wealth and source of funds of Company A and business activities
- failure to establish the legitimacy, purpose and evidence of Loan from Party A
- no explanation of need to transfer shares immediately prior to dissolution.
- failure to establish legitimate business reason to transfer and basis for dissolution
- no CDD or EDD on Party A, and Party M (jurisdiction risk high).
- no information on the VL provided to CSP

Typology 6 - Laundering the proceeds of fraud through deception

The defendant was a 50-year-old woman, "Ms. A", who took advantage of a wealthy elderly and vulnerable man, "Mr. B". Ms. A stole in excess of $2 million dollars over an 18-month period from the victim. She manipulated Mr. B into giving her large amounts of his wealth and unfettered access to his wealth. With that access she spent large sums on jewellery and transferred $1.4 million to her account in Canada.

Her criminality was detected due to the diligence of the victim's Wealth Manager at his Bank. However, once she realised that a formal complaint to the police was imminent, she transferred approximately USD $900,000 to Canada. She further attempted to transfer an additional USD $200,000 to Canada, but the bank refused to complete the transaction.

Red flags/Indicators:

- transfers of large sums of money from joint account to a sole account
- large transfers of money out of the jurisdiction in a short period of time
- no viable explanation as to the transfers
- large purchase within short time-period

Typology 7 – Cyber Fraud - Business Email/Contract[3]

The FRA received a SAR from a Class A Bank,"Bank 1", regarding a fraudulent wire transfer made by their customer, "Mr. Z", to an account maintained by "Company R" (domiciled in "Jurisdiction 8") at a bank in "Jurisdiction 9".

Bank 1 received email instructions from Mr. Z to send a wire transfer payment for approximately €25K. Mr. Z visited Bank 1 to sign the wire transfer documents as well as to produce identification for verification purposes, following which the wire transfer was executed. A few days later Mr. Z informed Bank 1 that his email had been hacked and the beneficiary information was changed; Mr. Z stated he was not aware that the

[3] FRA 2020 Typologies Project

beneficiary information was changed when he visited Bank 1. Mr. Z requested a re-call of the wire and the funds were returned approximately a month later.

The FRA's review revealed another recent SAR from another Class A Bank, "Bank 2". advising that Mr. Z ordered a wire transfer to "Company S" (domiciled in the Cayman Islands) at a bank in "Jurisdiction 10" for approximately US$1 million. Bank 2 conducted a verification phone call with Mr. Z to confirm the wire instructions and executed the wire transfer. A few days later Mr. Z contacted Bank 2 to report that his email was hacked, that the hackers intercepted his communication with Company S and provided fraudulent wire instructions which resulted in Mr. Z's funds being sent to an account in Jurisdiction 10. Bank 2 confirmed that approximately US$240K had been successfully recalled.

Disclosures were made to the RCIPS, CIMA and the FIUs in Jurisdictions 8, 9 and 10 for intelligence purposes.

Red flags/Indicators:

- the receiving Bank and recipient were in two different jurisdictions
- the name of the intended recipient company did not match public information
- transactions in multiple jurisdictions

Typology 8 – Cyber Fraud – Business Email/Contact[4]

The FRA received a SAR from a Real Estate Agent (the REA) regarding a series of suspicious communications from "Mr. B" and his attorney, which ultimately appeared to be an attempt to defraud the REA.

Mr. B expressed an interest in investing in real estate in the Cayman Islands and was seeking someone to assist in the purchase and development of property to be acquired. Mr. B subsequently provided the acreage of the property being sought and that he needed a partner to manage the development. He also provided the name of a Law firm and contact number for his attorney, "Law1", in order for the REA to provide information for a MOU to be prepared.

[4] FRA 2020 Typologies Project

The REA's attempts to contact Law1 by phone were unsuccessful; the REA then sent an email to the Law1, who responded with a series of one line text messages late at night. The REA requested to be emailed instead.

The business communications were conducted through Law1, who was appointed as power of attorney for Mr. B for the intended transactions. Law1 sought various information from the REA for the MOU, including full name, nationality, religion, gender, D.O.B, company address, driver's license or passport. The REA provided responses including sending a copy of his driver's license. Law1 indicated that a bank account would be set up in the REA's name in order for land to be purchased and to fund the development. Law1 also indicated that he would provide details of who to contact at the bank. The REA assumed that the account could only be possibly set up if he had in fact contacted the bank.

The REA provided listings for real estate in line with what was understood to be Mr. B requirements, along with the pros and cons of each, and invited him to review and advise if any listings were of interest. Law1 responded with their choices in a short time frame, without asking any questions about price, viability, profit and loss for the properties chosen, which caused the REA to suspect that purchase of the properties was not their prime purpose.

The REA requested Know Your Customer (KYC) details and highlighted the requirements under the AMLRs; these KYC details were not provided despite Law1 indicating that they were ready to move forward with property purchase.

The REA subsequently received via WhatsApp bank account details, a customer service email address and telephone numbers. The REA did not contact the bank and blocked the two phone numbers previously used for communication. The REA also contacted his local FI to have a caution notice put on his bank accounts, although he was assured that there can be no activity without him or his joint account holder knowing about it.

All queries including open-source data searches were negative for Mr. B and Law1. It appears that the communication may have been an attempt to garner information from the REA with the intent to defraud him and by extension the real estate company he works for.

A disclosure was made to RCIPS for intelligence purposes.

Red flags/Indicators:

- unsolicited business enquiry coupled with unusual business practices to conduct transactions
- informal and inappropriate communication practices
- lack of questions regarding cost and profitability of proposed development
- reluctance to provide necessary KYC details for verification purposes

Typology 9 – Cyber Fraud - Advanced Fee Scam[5]

The FRA received a SAR from "Bank 2" concerning one of its customers who was purportedly defrauded of US$2K.

The suspected advanced-fee fraud involved the stated funds being wired by the customer to an account in "Jurisdiction 4", in the name of "Subject A". The customer made the payment in order to receive a package containing several hundred thousands of dollars and other valuables. According to the information submitted, the package's alleged point of origin was "Jurisdiction 5". It was also noted that the package was shipped by "Subject B" via a dispatcher, "Company A".

Despite the funds being sent by the customer, copies of email exchanges showed that "Individual C" (a friend of the customer), was the sole person who communicated with the purported fraudsters. At various stages, Individual C sought updates regarding the package including details of its arrival and also requested feedback from Subject B as to how payment could be made for its release given that Company A had stated that the package was allegedly restrained and awaiting custom clearance in "Jurisdiction 6" which included "diplomatic handover charges".

Based on the events noted, it was ultimately determined that Individual C was potentially the true intended receiver of the fraudulent package and that the customer had wired the funds to assist Individual C with funding its shipment.

[5] FRA 2020 Typologies Project

Disclosures were made the RCIPS and the FIU in "Jurisdiction 4" for intelligence purposes.

Red flags/Indicators:

- client sent funds to unknown person as payment for substantial cash and valuables promised in return
- the fraudulent scheme included various cross border components and multiple jurisdictions
- alleged fraudster(s) used the excuse of package being restrained in Jurisdiction 6 as a delay tactic to mislead client

Case Study 1 – Cyber Fraud - Wire transaction through email hack

The owner of a small business reported that due to an email hack, a sum of US$16,149 ($12,900 KYD) was sent to a recipient in Michigan, when it was supposed to be sent to the vendor in Canada.

The victim's business used a Cayman email account to conduct their daily business. In 2018, the owner engaged in an email conversation regarding the purchasing of some expensive specialized Ultraviolet (UV) lighting from a technology company with office locations based in USA, and Canada. This company was used on a regular basis by the victim's company when they required various office equipment. The victim was conversing with the administrative assistant (AA) of the UV company who used an email address incorporating his name in the company's email. During this conversation, the victim received an email regarding specifications of payment for the equipment. This was not unusual and common practice for the victim to deal with them.

A few days later the victim then received an email from what appeared to be the AA from the UV company. The email followed the same conversation that had previously taken place; however, the email address was slightly different. This was unnoticed by the victim. The email contained wiring instructions attached for the payment of the equipment. Following the instructions, the victim then wired US$16,149 ($12,900 KYD)

to a recipient in Michigan. The Bank created a SAR regarding the unusual transaction as the vendor was not known and had not been previously used by the business, and the amount was unusually high.

Email headers were obtained from all communication which took place to determine the IP address locations used to communicate with. The recipient IP address being in Michigan. Security checks were scanned on the vendor's website/email servers for vulnerabilities, and it was found that the victim was using an outdated and vulnerable version of WordPress, known for exposure/vulnerability. This suggests how the emails were compromised.

Notes:

Intelligence was shared with the USA regarding the amount taken and as such were awaiting any feedback.

In order to obtain further information regarding the suspect as his IP is non-domestic would require an MLAT. This would not be considered by the US authorities due to the amount taken (less than US$20,000), therefore unable to identify any suspect, although the suspect was potentially aware of this threshold.

Issues to consider:

- require email headers in order to conduct cyber fraud investigations. A forward of the email removes the header from the original, so a copy of the original email is required
- fake domains
- potential false job advertisements (solicitation of money mules)

Red flags/Indicators:

- money muling, use of VPN (Virtual Private Networks),
- proxy servers (ways to hide behind alternate IP addresses)
- criminal knowledge and response to law enforcement/regulations
- use of internet i.e.: encryption, payment systems, online banking
- identity fraud – use of false identification

- use of non-domestic bank accounts
- wire transfers
- fake domains

Additonal notes:

The victim was advised:

- to keep the software etc up to date at all times.
- use antiviral software and conduct scans regularly
- use platforms requiring several levels of authentication when sending money.
- look for tell tail signs of criminal activity, for example:
- slightly different email addresses to originator,
- hover over email address being used to confirm it is the same,
- be wary of any strange, or unusual behaviour the computer has displayed which can be a sign the computer / software has been hacked into. Scan for viruses if this is the case.
- consider having own domain and email server for the business, as they will have full control over their own server. This will need to be kept up to date to minimise any vulnerabilities in the software being used.

Typology 10 - Proceeds of insider trading

A Cayman bank maintained an account with "Company A", domiciled in "Country A". "Mr. Z" was the director and ultimate beneficial of Company A, and was a national of, and resided in "Country B". The Bank's research revealed that Mr. Z was a Co-Founder of "Entity S" and was previously an executive office, and also served as a previous director.

The suspicious activity occurred over 4 business days and consisted of 85 trades in the stock of Entity S in the account maintained by Company A, involving the purchase of almost 400K shares at a cost of almost US$7 million.

The stock traded on an exchange in "Country C". Nine days after the last trade was executed, Entity S announced that its board of directors had received a non-binding "going-private" proposal. This proposal meant acquiring all of the outstanding

ordinary shares of Entity S not already owned by the Buyer Group at a 15.5% premium above the previous day's closing price.

The pattern of activity is indicative of insider trading. The FRA made disclosures to the RCIPS, CIMA and the FIUs in Countries A, B and C.

Red flags/Indicators:

- client trading in a security that he had material connections to, and was a previous 'Insider' of
- concentrated trading activity over a short period of time
- major announcement following the concentrated trading activity
- multiple jurisdictions involved

Case Study 2 - VA Fraud - Crypto Pyramid Scheme

The FRA received SARs from various financial service providers (FSPs) regarding Cayman exempt entities that belong to a collective investment scheme. "Mr. P", the ultimate beneficial owner and controlling person of the investment scheme had been charged in "Jurisdiction 5" with operating a Ponzi scheme that misrepresented itself as a cryptocurrency investment scheme. The FSPs provided information about the group structure and identified bank accounts owned by the exempt entities.

The FRA issued section 4(2)(c) Directives to local FIs and DNFBPs in furtherance of its analysis. A review of the banking transactions and the AML/KYC records revealed that several suspicious transactions, including excessive incoming funds that resulted in the schemes being over-subscribed. These funds would then be transferred out to other entities instead of being returned to the subscribers. There were also unusual purchases of several luxury items that did not appear consistent with the purpose of the investment scheme, including the purchase of a Cayman Islands registered yacht.

In early 2019, additional SARs were received concerning other previously unknown entities and bank accounts related to known associates of Mr. P. Based on a review of the banking, corporate and AML/KYC records obtained from local

banks and DNFBPs, the FRA concluded that these persons were also complicit in the alleged fraud and that these entities were also used to launder criminal proceeds.

A series of disclosures were made by the FRA to the overseas FIU in Jurisdiction 5. The information was also disclosed to the FCIU and CIMA for intelligence purposes. Sometime after the disclosures were made the FRA became aware that a criminal conviction was secured in Jurisdiction 5 against a subject included in the disclosures.

Red flags/Indicators:

- records revealed suspicious transactions, including excessive incoming funds that resulted in the schemes being over-subscribed.
- funds would then be transferred out to other entities instead of being returned to the subscribers
- unusual purchases of several luxury items that did not appear consistent with purpose of investment scheme

Case Study 3 – VA Fraud - Unauthorised Payment Through a Virtual Asset Account

A local FI (securities firm) filed an STR regarding unauthorised payments between the VA accounts of their broker and a foreign national. The securities firm reported the activity after it determined that the foreign national intended to make transfers totalling US$ 4.8 million (two separate transactions that occurred six minutes apart on the same day) and filed an application to the broker for a trading account the next business day. The wallet was not hosted in Cayman Islands. The STR reporting led to a successful information exchange with foreign FIUs and the successful return of most of the funds to the victim, as the online platform in a foreign jurisdiction had been able to freeze the suspect's account before the offence had been completed.

Red flags/Indicators:

- two separate transactions that occurred six minutes apart on the same day) totalling an unusually high amount
- filed an application to the broker for a trading account the next business day
- wallet was not hosted in Cayman Islands

3.2 Corruption

Domestic Corruption

The 2021 National Risk Assessment suggested that the suspicion of corruption accounts for between 7% to 11% of the total SARs received by the FRA each year; 16% of the corruption SARs received during the reporting period concerned domestic corruption.

During the same period, the total value of domestic corruption as a predicate offense is currently $1.3 million with 37 cases[6]. Domestic corruption poses a money laundering threat in the Cayman Islands. However, the volume of proceeds generated from domestic corruption is relatively minor compared to the threat resulting from foreign generated proceeds of corruption. The domestic corruption cases all related to public procurement fraud or unexplained wealth. SARs about domestic corruption predominantly involved individuals.

Typology 1 - Laundering the proceeds of theft by defrauding non-profit organization

In 2018, "Mr X" was accused of embezzling funds amounting to over $300,000 KYD ($360,165 US) from his employers over a five-year period by using his position of trust within the organisation to conceal his criminality. Mr X was employed as the general manager of a prestigious members-only club that operated as a non-profit company limited by guarantee. Mr X was answerable only to the board of directors and worked with considerable autonomy. He was entrusted to conduct the day-to-day management of the club premises and employees and was a signatory on the club bank accounts. In his position of financial trust, he was responsible for the timely payment of staff wages and all other club expenditure.

Mr X was personable and well thought of by staff and popular with club members. The club bank accounts required two signatures on cheques, and such was the trust placed in him that he was regularly provided with numerous blank cheques that had been signed by a second account signatory. This lack of scrutiny over the club's finances enabled Mr X to systematically steal over $300,000 KYD ($360,165 US) of club funds over a five-year period by simply making the blank cheques payable to himself and cashing

[6] Cayman Islands National Risk Assessment 2021

them at the bank. Mr X was well known by bank staff and was never questioned as to the level or frequency of his cheque encashment.

Mr X used the funds to finance his day to day living expenses, travel and the purchase of a vehicle. Club records were falsified by Mr X to show the cash being used for miscellaneous club expenditure and bogus invoices.

Notes:

The case resulted in a restraint order that was placed on Mr X's assets to prevent the risk of dissipation; prosecution was pending.

Lessons learned:

This was a relatively unsophisticated and straight forward fraud that relied on the unquestioned acceptance of Mr X's integrity in his management of the club and his high level of trust by the company. At the heart of the matter is the internal governance of the company by its board of directors. The lack of corporate governance and scrutiny – even for a small non-profit organisation – exposed it to abuse and provided a perfect platform from which Mr X exploited the company finances.

A contributing factor in the success of the criminal enterprise was the lack of scrutiny of the relevant financial institution. Retail banks need to have a heightened level of sensitivity to cash transactions in account usage involving cash withdrawals and cheque encashment and be ready to challenge account holders when patterns of such activity are regularised.

Red flags/Indicators:

- association with corruption
- purchase of valuable assets i.e.: vehicles
- poor governance

Foreign Corruption

The 2021 NRA suggests that 84% of SARs from 2016-2019 involved allegations of foreign corruption. The cases reported by Cayman Islands' FIs and DNFBPs involved procurement fraud, private sector corruption and unexplained wealth/income scenarios. This suggests a diverse use of the Cayman Islands financial system for different corruption schemes.

Typology 2 - Laundering the proceeds of local and international corruption

Mr. "A" was the chairman of the board of a Cayman Islands Government authority. Mr. "B" was a PEP and executive with a local Cayman bank. Mr. "C" was the owner of an overseas company, "Company C". Mr. C submitted a bid proposal, in the name of Company C for a government contract to supply services, which was overseen and approved by Mr. A.

Mr. A and Mr. B secretly established their own company in Cayman, "Company A", utilising a similar name to that of Company C, intending that they should be thought to be one and the same entity. Mr. C was in full knowledge and agreement with the deception.

Mr. A oversaw the award of the contract without disclosing his conflict of interest. All funds derived from the contract were routed through bank accounts of Company A which had been opened and operated by Mr. B.

The proceeds of the corruptly obtained contract were dispersed between Mr. A, Mr. B and Mr. C with the majority being transferred to accounts held overseas. In all cases the transfers were arranged through several different 'layers' in order to disguise the purpose and origins of the payments.

Red flags/Indicators:

- PEP involvement with overseas company
- two different companies with similar names and with links to PEP
- transfers made through different layers

Corruption with PEP involvement

Typology 3 - Laundering funds for bribery purposes

A Cayman bank maintained a relationship with two companies incorporated in "Country C". "Mr. X" was the ultimate beneficial owner, and "Mrs. Z" was a director of these companies. The clients' source of funds was declared as dividends received as a shareholder of a retail business in "Country B".

Ongoing monitoring revealed that Mr. X and his brother, "Mr. Y", were under criminal investigation in "Country A" regarding their alleged involvement in bribery payments made by an international conglomerate (IC). Messrs. X and Y are the sons of the former President of Country B.

Further research by the FRA revealed that subsequent to the SAR filing, Mr. X was charged with money laundering in Country B, and Mrs. Z was accused of setting up transactions for millions of dollars in bribes to pass from the IC to Messrs. X and Y.

Details of the banking transaction were obtained and included in disclosures to RCIPS and to FIUs in Countries A and B.

Red flags/Indicators:

- dealing with PEPs
- adverse information about the client detected from ongoing monitoring
- use of legitimate business to give an appearance of reputable source of funds
- multiple jurisdictions involved ins schemes

Typology 4 - Laundering the proceeds of corruption through financial institution

"Mr. D" was a Director of a FI. Mr. D was appointed joint Voluntary Liquidators for two connected funds registered in the Cayman Islands. The U.S. Securities and Exchange Commission had initially won a settlement of approximately US$21.4 million against the former investment manager. As Voluntary Liquidator of the funds, the defendant held a fiduciary role and was able to make decisions in the administration

of the funds' assets including authorisation of payments to third parties including creditors and investors.

Mr. D proceeded to steal US$500,000 from the funds for which he was the liquidator. He managed to conceal his criminality in the following way:

- Incorporated a company in the British Virgin Islands (BVI) in the name similar to one of the genuine creditors;
- Opened a bank account in the Cayman Islands with a similar name to the company he had registered in the BVI;
- Set up an email in the company's name and sent an email to the bogus company from his work email address;
- Gave instructions to his administrator to pay the fictitious company large sums of money over a period of 10 months; and
- Created a fictitious advisory agreement between his bogus company and the trust.

In January 2016 the United States courts made a decision to reverse the settlement of US$21.4 million and ordered the U.S. Securities and Exchange Commission to return the US$21.4 million to the creditors and investors of the various funds. On learning of this decision, "Accounting Firm A" contacted the investors to offer their assistance in securing, collecting and distributing the US$21.5 million that was to be returned.

It was in the course of the review of these funds that a number of discrepancies were discovered; this ultimately led to the discovery of the defendant's criminality. Immediately upon the commencement of the investigation an application for a restraint order was made and granted. The defendant has since repaid the sums stolen. A full compensation order was made with interest.

Red flags/Indicators:

- opening a bank account in a slightly different name than the company name
- Cayman Islands resident registering a company in the BVI and within a short space of time receiving large sums of money into the Cayman Islands bank account

- limited detail as to the company source of income
- following the two main deposits into the Cayman Islands bank account it was limited activity thereafter

3.3 Tax Evasion

The possibility of foreign nationals evading taxes in their home jurisdictions and using the Cayman Islands' financial system to launder the proceeds remains one of the most prevalent potential ML threats to the jurisdiction according to the 2021 NRA. The value of foreign related tax evasion during 2016 to 2020 was US$177.0 million, with 366 SARs, and 12 related stand-alone ML cases.[7] However, this threat is significantly reduced due to the number of multilateral and bilateral arrangements relating to the exchange of tax information operating within the Cayman Islands.

Notwithstanding the current existence of these avenues for information exchange, the Cayman Islands has been working to strengthen its AML/CFT framework by incorporating the widest array of cooperation mechanisms regarding all overseas tax crimes through explicit provisions in law.[8]

Typology 1 - Tax evasion through a bank

A Cayman bank reported that "Mr. A" visited a "Bank" to complete a large cash withdrawal and close his account. There were a number of outstanding due diligence and KYC documentation for Mr. A and his wife. The Bank advised Mr. A that it required the outstanding information prior to the withdrawal request and ultimate closure of the account.

Mr. A advised the Bank that he would not be providing the requested information, as he would incur unnecessary questions from his tax authority in "Country A" and was not willing to answer any questions. Mr. A also mentioned that he was purchasing land and the seller wanted cash, not a cheque or bank draft. Mr. A left the Bank without the completion of the transaction. The account was restricted, and a caution was placed on the account, advising no transaction activity until the customer met all of the Bank's due diligence and KYC requirements.

[7] Cayman Islands National Risk Assessment 2021
[8] NRA Summary (2015)

The Bank was suspicious that the customer was unwilling to provide requested due diligence and KYC information in the event that that they were reportable under the relevant tax reporting regime; however, a check against their reportable clients revealed that the customers were already reported.

The FRA made disclosures to RCIPS, the Department of International Tax Cooperation and the FIU in Country A.

Red flags/Indicators:

- client reluctance to provide standard due diligence information
- comment by client avoiding tax scrutiny in his home jurisdiction
- large cash withdrawal to close account

Typology 2 – Tax Evasion through Mutual Fund Administration[9]

The FRA received SARs from a Mutual Fund Administrator and a "Cayman Fund" regarding "Mr. J" and "Company G" in relation to charges of conspiracy, witness tampering, obstruction of justice and multiple tax violations in a barratry scheme. The SARs identify that funds were being held by Company G in the Cayman Fund.

Mr. J is an attorney practicing through his firm Company G, both based in "Jurisdiction 6". Mr. J is also the trustee of the investor and potentially a beneficiary.

An announcement was made by the relevant Attorney's Office in Jurisdiction 6 that an indictment had been unsealed alleging that Mr. J along, with other co-conspirators, defrauded Jurisdiction 6 through tax evasion in a barratry scheme. Mr. J evaded taxes through filing false documentation. Mr. J was further charged with witness tampering and obstruction of justice due to ordering co-conspirators to destroy documentation and to not cooperate with the investigation.

Analysis by the reporting entities showed that there is no evidence directly linking the invested monies of Company G with the criminal activities; however, given the scale of the criminal enterprise and illicit gains of millions of dollars there were reasonable grounds to suspect that the invested funds could be tainted.

[9] FRA 2020 Typologies Project

The FRA issued a section 4(2)(c) directive to obtain additional information to amplify its analysis, including a schedule of subscriptions and redemption and bank account details of where monies were received from or paid to.

Disclosures were made to the RCIPS, CIMA and the FIU in Jurisdiction 6 for intelligence purposes.

Red flags/Indicators:

- adverse information about the beneficial owner

3.4 Drug Trafficking

The 2021 NRA notes that the Cayman Islands is not a producer or exporter of illegal drugs and is also not a facilitator of international drug trafficking. Findings also show that drugs imported into the Cayman Islands are primarily for domestic consumption. During 2017 to 2020, the total value of domestic drug related criminality amounted to $13,884,000 with 735 cases. Furthermore, the years 2018 to 2020 saw law enforcement seize cash totaling $786,298.00 in relation to drug related activities.[10]

However, the Cayman Islands is a major financial centre within the Western Hemisphere, and the inherent risk that drug traffickers will seek to utilise the Cayman Islands' financial system to launder the proceeds of crime is recognised and presents an on-going threat. Due to the geographic proximity to drug producing countries and being a diverse and accessible international financing centre, the Cayman Islands may be an attractive conduit for large, organised drug cartels.

Typology 1 - Laundering the proceeds of drug trafficking

"Mr. A" was released two years ago from prison having served a sentence for the possession and supply of drugs. On their release Mr. A opened both a personal and business bank KYD account with the business being a tattoo and piercing studio. The various supporting documents showed Mr. A to be a partner in the business with an

[10] Cayman Islands National Risk Assessment 2021

expected income into the business of $5,000 KYD ($6,000 US) per month. A lease for the business premises was also supplied in the name of the business partner "Mr. B".

The business immediately started to see cash credits into the business account and these cash credits continued to increase and greatly exceed the projected business income.

The account was being debited by cash withdrawals and what appeared to be a general personal spend pattern with no evidence purchasing of stock for the business, rental payment for the business property, utility bills and any salary payments. After a number of months, the business account showed a monthly debit of $4,000 KYD ($4,800 US) titled 'Salary' to Mr. A. No salary was ever shown to Mr. B. The account continued to show no purchase of stock or materials. The personal account of Mr. A started to show the monthly credit titled 'Salary' from the business account held.

On the same date cash credit of a varying amount between $3,000-$5,000 KYD ($3,600-$6,000 US) was also shown being credited to the personal account of Mr. A. The personal account showed no spend to support the business but again showed personal spend as well as significant cash withdrawals on an irregular basis and of varying amounts. A wire transfer from the account was also shown on an irregular basis and of a varying amount to an account held overseas and titled land purchase. Examination of the personal account showed a notification to the bank of overseas travel to Colombia on a regular basis and the usage of the debit card overseas. This notification also correlated with a large cash withdrawal requested in USD from the account a day or two before travel.

Red flags/Indicators:

- the account shows income greatly exceeding the projected
- throughout the course of business there is no spend that can be attributed to the business such as the purchase of stock or materials or the payment of expected bills
- the business account has the profile of being used as a personal account
- although a salary is now shown to AB there is also a cash deposit of varying amounts into the personal account on the same date
- Mr. A notifies the bank of regular overseas travel to Colombia and the possible usage of the DEBIT card abroad but also makes large cash withdrawal in USD just prior to departing

- purchase of valuable assets

Typology 2 - Drug Trafficking[11]

A Money Services Business (MSB) submitted a SAR in relation to the remittance activity of "Mr. A", as a result of his high volume of remittances sent to numerous unrelated individuals residing in "Jurisdiction 1". The MSB also flagged that it appeared that Mr. A was attempting to 'structure' his remittances. The MSB provided remittance statements for a two-year period.

The FRA issued a section 4(2)(c) directive to obtain additional information to amplify its analysis. The additional information revealed that Mr. A had remitted over CI$50K to numerous individuals residing in "Jurisdiction 3" over a three-year period.

Further analysis by the FRA identified that Mr. A had been arrested and charged for drug offences in the Cayman Islands. In addition, he had travelled numerous times to Jurisdiction 3 over the years.

A disclosure was made to the RCIPS for intelligence purposes.

Red flags/Indicators:

- high volume of transfers between client and multiple individuals / unrelated third parties
- client appears to be structuring amounts to avoid additional KYC by the MSB

Case 1 - Proceeds of drug trafficking through a Category B bank

A SAR was filed by the Authorised Agent in relation to a client of a Bank.

A bank, "Company A", domiciled in a country which is considered to be high risk for drug crime, violence and corruption. It obtained a licence to operate as an offshore branch in the Cayman Islands. Its main business activities included the provision of US dollar term deposits to nationals of its home country. Due to restrictions on US dollar accounts in its home country, off-shore products were in high demand by nationals. The accounts of the offshore branch were opened and managed by Company A

[11] FRA 2020 Typologies Project

through branches in its home country, as the offshore branch had no physical office or employees.

Company A maintained the account assets and conducted transactions through its US dollar nostro accounts at a related bank. Company A used the nostro accounts at a related bank to supply the needed dollars, process US dollar wire transfers, cash US dollar travelers cheques and perform similar US dollar services. Separate nostro accounts were not opened for the offshore branch despite its high risk nature.

US dollar accounts were used by drug cartels to place cash into the financial system. Shipments of US dollars were brought into the country, and then deposited directly into US dollar accounts through branches in Company A's home country. Law enforcement and regulatory authorities were concerned that Company A's bulk cash shipment was at a volume that could only be reached if illegal drug proceeds were included, as it far exceeded that of larger banks within the same jurisdiction and far greater than what the bank's market share suggested.

An internal audit report noted that there was no functioning compliance department, limited transaction monitoring, a backlog of alerts identifying supsicious activity that had not been reviewed, and no KYC focus on high risk clients, with specific mention of inadequate KYC information on the offshore accounts.

Company A maintained limited information on the account holders of the offshore branch, due to the threats from drug cartels and weak internal controls. There was a history of corrupt account executives within Company A, who established fictitious accounts for drug traffickers. Employees routinely accepted and processed large quantities of illicit proceeds under circumstances that showed obvious signs of money laundering.

For example, employees accepted cash deposits of hundreds of thousands, sometimes millions, of US dollars from individuals with no identifiable source of income, delivered in multiple boxes specially designed to fit the precise dimensions of the teller windows.

Some employees regularly fabricated documents indicating that they had performed required customer due diligence when they had not out of fear of violence against themselves or their families. Even when money laundering accounts were identified and accounts were ordered to be closed, employees often refused to report the activity to authorities and allowed those accounts to remain open and active for years.

The Authority has revoked the licence of the branch operating in the Cayman Islands.

The case resulted in the revocation of the offshore license; a fine in excess of US$1billion levied by an overseas regulator, and deferred prosecution.

Red flags/Indicators:

- association with corruption
- currency exchanges/cash conversion
- cash couriers/currency smuggling
- underground banking/alternative remittance services
- trade-related money laundering and terrorist financing
- use of non-domestic bank accounts
- managed by branches in home country
- bulk cash shipments
- poor governance
- no functioning compliance department

3.5 Gambling

While not designated by the FATF as a "predicate offence" for money laundering, gambling is illegal in the Cayman Islands and seems to generate a significant volume of illicit proceeds. Intelligence and law enforcement information suggests that proceeds generated from illegal gambling are in the millions annually and are integrated into the local economy through legitimate businesses. However, while the activity is organized domestically, there is no indication of any links to well organised transnational criminal groups.[12]

Typology 1 - Laundering the proceeds of gambling

Law enforcement-led operations at a small retail store for women's clothing and small electronics resulted in the recovery of drugs, receipt books/tickets indicative of lottery and a large amount of cash in various denominations. Several persons were arrested

[12] Cayman Islands National Risk Assessment 2021

including one of the business partners. The investigation revealed that the business has two partners and had been in operation for over a year. "Partner A" obtained the TBL and "Partner B" the Lease for the business. Partner A was responsible for the daily operations and Partner B of all other aspects of the business.

The business had a very small amount of inventory of clothing & small electronics and employed three or more persons in various roles. This includes: sales clerk, banker and cash collection clerk from persons who sell lottery on behalf of the business. Financial investigation reveals that the business had not established any relationship with any FI or MSB. All business transactions conducted used cash. Funds seized were detained in Court with a view for Forfeiture.

Notes:

Examination of the case reveals how small business entities are being used as front for illegal gambling activities which represents great risk for the ML activities. It generates enormous revenue streams for providers and their participants and presents a number of challenges for Law enforcement and regulators.

Issues to consider:

- scope of illegal gambling/types of gambling/locations used to facilitate criminal activities and ownership of this business establishment
- law enforcement cases - use of intelligence to identify how illegal gambling is used for ML or is associated with predicate offences
- impact on community
- social harms associated with illegal gambling
- movement of persons involved/foreign nationals
- potential ML/TF Risk: (predicate offences/fraud, drug trafficking, human trafficking, loan sharking, prostitution)
- currency smuggling/cross border/movement of funds (pose particular ML risk)

Red flags/Indicators:

- competitive in its growth/vulnerable to criminal exploitation
- operates almost 24 hours per day

- high volumes of large cash transactions taking place very quickly
- collusion with professional persons to include: law enforcement officers, bankers
- funds obtained are then distributed as winnings to various footmen
- the winnings are remitted or used for other legitimate business purposes
- the business owner has limited involvement in the illegal gambling activities
- cash couriers
- gambling activities i.e.: use of casinos, internet gambling
- co-mingling (business investment)
- use of nominees, trusts, family members or third parties
- use of non-domestic bank accounts
- use of internet i.e.: encryption, payment systems, online banking
- criminal knowledge of and response to law enforcement/regulations
- new payment technologies i.e.: mobile phone payment and remittance system
- cash intensive – all business transactions were in cash
- use of third parties/undertake transactions

Case Study 1 – Money Laundering and Illegal Gambling

In 2019, during operational activity involving the execution of a number of search warrants, large quantities of unexplained cash were located at a number of addresses. Cash in excess of US$100,000 was seized as it is suspected that it represents recoverable property, namely it is derived from the proceeds of unlawful conduct or was to be used by a person in unlawful conduct.

This operation involved the arrest of several individuals, and a number of them have been charged with illegal gambling and possession of criminal property.

Considerable analysis of financial material has been undertaken. It is anticipated that the organisers of the criminal enterprise will be indicted with alleged criminal conspiracy and money laundering lifestyle offences.

The underlying predicate criminality appears to be illegal gambling. In developing the investigation, requests were made of the FRA to identify accounts, assets and other intelligence or information which it held. This information has been of great value for the parallel financial investigation.

Red flags/Indicators:

- large quantities of physical cash
- several individuals involved including in the ownership of business
- multiple addresses

Issues to consider:

- scope of illegal gambling/types of gambling/locations used to facilitate criminal activities and ownership of this business establishment
- predicate offense for money laundering

3.6 Misuse of Corporate Structures

According to the 2021 NRA, as of September 2021 the corporate sector in the Cayman Islands is relatively large with around 140,000 companies and partnerships. Further, most of these entities do not carry-on domestic business. In relation to SAR filings to the FRA between 2019 and 2020, 1,380 of those SARs related to various types of companies and partnerships formed in the Cayman Islands: 340 of those SARs related to alleged fraud, 315 to general suspicious activity and 284 to tax evasion[13].

Typology 1 – Using TCSPs to launder the proceeds of crime [14]

A Cayman bank and two TCSPs provided services to a recognised international conglomerate (IC), who had been a client for number of years. Their ongoing monitoring revealed publicly available information that the IC had engaged in corrupt practices. Investigations in multiple jurisdictions involved allegations of using offshore companies to pay bribes in order to obtain contracts, accusations of fraud and overpricing contracts.

The reports disclosed information about Cayman Islands entities ultimately owned and controlled by the IC, as well as the ownership structure and the private banking activities of such entities.

The profile of the entities identified in the reports raised the possibility that they could have been indirectly involved in the allegations against the IC. Information about exempt Cayman Islands entities ultimately owned and controlled by IC, their ownership structure and the information about bank accounts of such entities were disclosed to the RCIPS and to overseas FIUs in jurisdictions with relevant investigations for intelligence purposes.

Red flags/Indicators:

- adverse publicly available information

[13] Cayman Islands National Risk Assessment 2021
[14] Cayman Islands National Risk Assessment 2021

- multiple offshore accounts registered in different jurisdictions to obscure identity of beneficial owners
- profiles of the Cayman entities raised suspicious

Typology 2 - Laundering funds through Limited Partnership

A Cayman Islands CSP acted as the registered office for a number of Cayman Islands entities where the applicant for business is a sovereign investment fund. One of those entities is a Limited Partnership that involves numerous other investors with multiple or complex layers of ownership. Recent publicly available information about the ultimate beneficial owner of an investor in the Limited Partnership raised suspicions that the Cayman Islands entities may be holding criminal property.

Publicly available information suggested that the ultimate beneficial owner was being investigated in his home country and in other jurisdictions for an international conspiracy to launder funds misappropriated from a sovereign investment fund. Further research by the FRA identified that the Limited Partnership and the investor had been identified as the owner of assets subject to a civil forfeiture complaint in an overseas jurisdiction. The civil forfeiture complaint sought the recovery of more than $1 billion in assets associated with an international conspiracy to launder funds misappropriated another sovereign investment fund.

The ownership information disclosed in the SAR, together with the activities described in the civil forfeiture complaint, suggests that the funds invested into the Limited Partnership are proceeds of the alleged diversion of funds and appears to be criminal property.

This information was disclosed to the RCIPS and to FIUs in several jurisdictions that had applicable investigations.

Red flags/Indicators:

- adverse information about the client detected from ongoing monitoring
- use of legitimate business to give an appearance of a reputable business
- multiple or complex layers of ownership

Typology 3 – Misuse of Foreign Trust to purchase property in the Cayman Islands[15]

Two trusts were established in "Country A" by a law firm as primary shareholder of a Holding Company. The Cayman Islands trustee was directed to accept two payment orders in favour of a bank in order to buy real estate in the name of the Holding Company in Country A. The law firm controlled all communications regarding the trusts and the trustees did not ascertain the identity of the beneficiaries. The trustees made contact with a local Real Estate agent who assisted in the holding company purchasing two properties for US$450,000 and US$650,000.

The investigation revealed that individuals "Y" and "Z" were the beneficiaries of the trusts. Y and Z were Senior Managers of two fund management companies, established in "Country B" and were the subject of a fraud investigation regarding serious misappropriation of the funds in excess of US$1 million. The funds in the trusts originated from criminal activity of the companies. The trust had been used to conceal the identity of the beneficial owners.

Red flags/Indicators:

- trustee was directed to accept two payment orders in favour of a bank in order to buy real estate
- The law firm controlled all communications regarding the trusts
- the trustees did not ascertain the identity of the beneficiaries

[15] Cayman Islands National Risk Assessment 2021

4. Terrorism Financing

The 2021 NRA notes that the Cayman Islands is historically a low-risk jurisdiction regarding terrorism given the Islands' demographics and geography. With regards to terrorism financing, there is a limited body of evidence relating to terrorism financing typologies that affect the Cayman Islands.

The Terrorism Act was amended to provide for an offence to possess or acquire terrorist property with intent or knowledge that it will be used for financing terrorism, terrorists or terrorist organisations as well as that "terrorist property" is property that is used in the financing of acts of terrorism, terrorists and terrorist organisations.[16]

Terrorist financing activity is unique in comparison to drugs and fraud cases, as money used to fund terrorist operations is sometimes derived through legitimate means; as such, concealing the source of funds is not required. However, in some terrorist financing cases, a crime may be committed, and the proceeds may be sent by electronic funds transfer (EFT) directly or indirectly to a foreign terrorist organization. Terrorist financiers may also attempt to send an EFT (electronic fund transfer) to individuals in unexpected locations, or through several countries, to further complicate the money trail.

Terrorists and terrorist groups use a wide variety of methods to move funds through organisations, including the financial sector, the physical movement of cash by couriers, and the movement of goods through the trade system.[17]

TF Typology 1 - Illicit petroleum dealings with Islamic State

"Ms. X" is the daughter of a government minister in "Country A". The government of Country A imposed sanctions against neighbouring "Country B", prohibiting the trade of petroleum and its byproducts into or out of Country A. One exception to the relevant law, however, allowed Country A's government to grant a specific company, "Company A", the rights to trade in petroleum. Country B was a major producer of crude oil, and the government was waging war against the Islamic State.

[16] NRA Summary (2015), p.18
[17] FATF: Terrorist Financing - Feb 2008

Media reports indicated that Islamic State was dealing in petroleum production and sale from Country B. When Islamic State petroleum became available, Company A set up schemes to transfer the petroleum by tanker trucks to Country A and its international ports.

News outlets began investigating the Islamic State's illicit petroleum dealings, and leaked data revealed that Ms. X had ties to Company A, the front company, and the Islamic State. Company A was established by another company, "Company B". It was later revealed that Company B was established as a front company in "Country C". Company B then later transferred its operations to the Cayman Islands.

The MLRO of the Cayman Islands Company Manager reviewed the files of Company B and realized that Ms. X was the beneficial owner; and took the decision to file a SAR with the FRA. Cayman Authorities immediately revoked Company B's license and began an investigation.

Red flags/Indicators:

- links to country known for terrorist group activities
- links to a PEP
- links to countries near other high-risk countries
- links to countries with sanctions

TF Typology 2 – Terrorist Financing[18]

The FRA received a SAR from Bank 1 following a review it conducted on transactions made by a Nonprofit Organization, "NPO 1", domiciled in "Jurisdiction 1", based on adverse media reports alleging that NPO 1 had provided hundreds of thousands of dollars to a former Nonprofit Organization, "NPO 2", also domiciled in Jurisdiction 1, now designated as a terrorist organization by the Government of Jurisdiction 1.

"Bank 1" identified numerous transactions totaling over USD$3 million that were processed through a multicurrency account held by a company domiciled in "Jurisdiction 2" that provides online transaction and payment processing solutions; approximately

[18] FRA 2020 Typologies Project

USD$250K was paid by NPO1 to NPO 2 over a 10-year period through this account. The payments were made prior to NPO2 being designated as a terrorist organisation.

Disclosures were made to the RCIPS, CIMA and to the FIUs in Jurisdictions 1 and 2 for intelligence purposes.

Red flags/Indicators:

- the ultimate source of funds and purpose of the wire transfers passing through the multicurrency account were unknown
- the frequency and rate of the activity observed is high and unusual
- conducting transactions/business with an entity subsequently designated as a terrorist organization

TF Case 1 - Suspected terrorist financing – Canada[19]

MSB service highlighted: MSB EFT services used by suspected terrorist financiers to send funds to a country of concern for terrorism.

Canadian Law enforcement provided information on two individuals who were suspected of being involved in a variety of criminal activities such as weapons trafficking and various fraud schemes, including credit card and real estate fraud. It was also suspected that a portion of these criminal proceeds was for the benefit of a terrorist organization based overseas.

The two individuals owned a business which law enforcement suspected of being used as a vehicle for the proceeds of fraudulent activity. A financial institution advised FINTRAC of cheque deposits by a third individual to the business' account. The financial institution also reported that the cheques were issued by two companies suspected of being associated to the aforementioned credit card fraud scheme.

Based on STRs provided by MSBs, FINTRAC determined that the newly identified individual provided the same address as three other people. The STRs also revealed that wire transfers were ordered by all of these individuals for the benefit of individuals in the country where the terrorist organization is based.

[19] Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MSBs) – July 2010

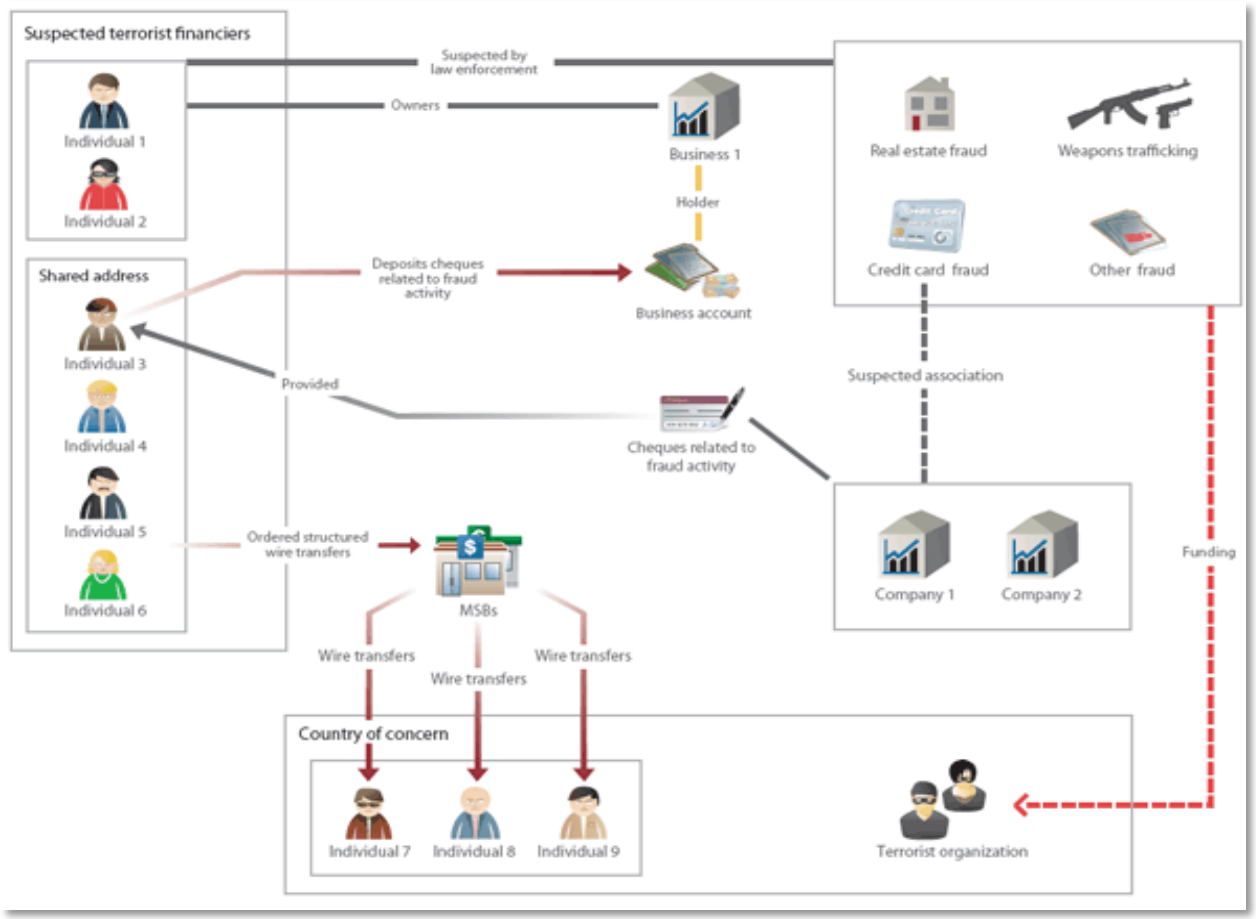
The wires were conducted in concentrated bursts over a two-year period, with each burst consisting of a series of wires which were generally structured below mandatory reporting thresholds and conducted within days of each other. FINTRAC also received STRs from another MSB describing the same pattern of activity and suggesting that some of these individuals were providing multiple dates of birth and address information, and similar sounding name variations.

This case highlights how individuals who were suspected of providing funds to a listed terrorist organisation used an MSB to transfer funds, a portion of which was believed to be derived from fraud schemes. Given that the wire transfers in this case were below the mandatory reporting threshold, this case also underscores the importance of STRs filed by the MSBs.

Red flags/Indicators:

- multiple senders shared common address information
- multiple senders sent funds to the same beneficiary in a country of specific concern for terrorism
- senders conducted structured transactions within days of each other
- at least one individual involved in this case used multiple dates of birth (DOB), IDs, and addresses to MSBs

Sanitized case example: Suspected terrorist financing



Sample of cases received from Egmont FIUs[20]:

TF Case 2 - Credit card fraud supports terrorist network - Egmont

One operation discovered that a single individual fraudulently obtained at least twenty-one Visa and Master Cards using two different versions of his name. Seven of those cards came from the same banking group. Debts attributed to those cards totalled just over USD$85,000. Also involved in this scheme were other manipulations of credit cards, including the skimming of funds from innocent cardholders. This method

[20] Egmont/FATF Collection of Sanitised Cases Related to Terrorist Financing

entails copying the details from the magnetic strip of legitimate cards onto duplicate cards, which are used to make purchases or cash withdrawals until the real cardholder discovers the fraud. The production of fraudulent credit cards has been assisted by the availability of programmes through the Internet.

Methods:

- copying the details from the magnetic strip of legitimate cards onto duplicate cards
- different versions of name
- availability of programmes through the Internet.
- manipulations of credit cards
- use of false and stolen identities to open and operate bank accounts

Red flags/Indicators:

- using different versions of names
- seven of cards came from the same banking group.
- the transaction inconsistent with the customer's profile

TF Case 3 - High account turnover indicates fraud allegedly used to finance terrorist organization - Egmont

An investigation in "Country B" arose as a consequence of a STR. A FI reported that an individual who allegedly earned a salary of just over USD$17,000 per annum had a turnover in his account of nearly USD$356,000. Investigators subsequently learned that this individual did not exist and that the account had been fraudulently obtained. Further investigation revealed that the account was linked to a foreign charity and was used to facilitate funds collection for a terrorist organisation through a fraud scheme.

In Country B, the government provides matching funds to charities in an amount equivalent to 42 percent of donations received. Donations to this charity were being paid into to the account under investigation, and the government matching funds were being claimed by the charity. The original donations were then returned to the donors so that effectively no donation had been given to the charity. The charity retained the matching funds. This fraud resulted in over USD$1.14 million being fraudulently obtained. This case is currently under investigation.

Red flags/Indicators:

- use of false and stolen identities to open and operate bank accounts
- unusually high amount in account inconsistent with previous salary
- use of foreign charity
- transferring funds into third-party accounts
- funds transferred to and from a charity fund

TF Case 4 - Purchase of cheques and wire transfers by alleged terrorists - Egmont

STRs outlined unusual activity involving three grocery markets, two of which shared a common location. The activity was conducted by individuals of the same origin using a single address, which corresponded to one of the business locations. Two individuals employed by a grocery store and a third whose occupation was unknown each deposited funds just under applicable reporting thresholds and immediately drew cheques payable to a fourth individual.

The cheques cleared through two different banks in a foreign country. All three bank customers supplied the same address. In addition, two individuals associated with a second grocery store located at the common address above each purchased bank cheques just under the applicable reporting threshold at the same bank branch, at the same time but from different tellers. One of the cheques was purchased on behalf of the second grocery store, the other on behalf of third party.

The cheques were payable to two different individuals, one of whom shared the same last name as one of the purchasers. In related activity, a third business used the common address discussed above when opening a business account which immediately received a USD$20,000 wire transfer from a wholesale grocery located in another region of the country. Filings of cash transaction reports indicated that a total of about USD$72,000 was withdrawn in cash from other accounts associated with this business.

Red flags/Indicators:

- using third parties to undertake wire transfers
- multiple senders shared common address information
- unusually large transfer of money from an individual to a business and vice versa
- immediately drew cheques payable to a fourth individual
- withdrawal of a large amount of funds in cash
- use of companies to move funds under the guise of legitimate transactions
- elaborate movement of funds through different accounts
- associations with multiple accounts under multiple names
- depositing multiple large amounts of cash and receiving multiple cheques drawn on that account
- bank account opened for front companies.
- when compared to similar types of business bank accounts, transactional activity was not in keeping with that type of business.
- large amounts of money withdrawn in cash from other accounts associated with this business
- multiple transactions of a similar nature on the same day in different locations
- a third business used the common address discussed above when opening a business account
- cheque purchased on behalf of third party

- all three bank customers supplied the same address
- deposits and bank cheques just under reporting threshold

TF Case 5 - TF Transactions using wire transfers to support terrorist activity - Egmont

A pattern of cash deposits below the reporting threshold caused a bank to file a STR. Deposits were made to the account of a bureau de change on a daily basis totalling over USD$341,000 during an approximately two and one-half month period. During the same period, the business sent ten wire transfers totalling USD$2.7 million to a bank in another country.

When questioned, the business owner reportedly indicated he was in the business of buying and selling foreign currencies in various foreign locations, and his business never generated in excess of USD$10,000 per day. Records for a three-year period reflected cash deposits totalling over USD 137,000 and withdrawals totalling nearly USD$30,000.

The business owner and other individuals conducting transactions through the accounts were nationals of countries associated with terrorist activity. Another bank made a suspicious transaction report on the same individual indicating an USD$80,000 cash deposit, which was deemed unusual for his profession. He also cashed two negotiable instruments at the same FI for USD$68,000 and USD$16,387.

Red flags/Indicators:

- unusual pattern of cash deposits below reporting threshold
- unusual wire transfers
- nationals of high-risk countries for terrorist activity
- cashing two negotiable instruments at high amounts

5. Proliferation Financing

The Proliferation Financing (Prohibition) Act 2017 specifically requires the FRA to publish lists of persons who the FATF or such other international organisation has advised may be involved in unauthorised proliferation activities and also allow for the creation of regulations which may provide penalties for breaches.

The Cayman Islands is not a weapon manufacturing jurisdiction, an international trade centre nor a market for proliferation goods. However, the 2021 NRA notes that the jurisdiction offers a range of products and services which makes it attractive for non-residents to establish businesses in the jurisdiction without having a physical presence in the Cayman Islands. Whilst there may be no direct PF links to Cayman Islands entities, the exposure to the international financial market poses risks of PF related sanctions being evaded through the Cayman Islands. In addition, as noted in recent typologies, designated persons and entities continue to explore new ways to evade targeted financial sanctions ('TFS").

The following is an extract from a report on the "Study of Typologies of Financing of WMD Proliferation" by Jonathan Brewer. The report was prepared by Project Alpha at the Centre for Science and Security Studies (CSSS) at King's College, London.[21]

The UN Security Council has put in place a framework of measures to prevent proliferation financing (**PF**) with the implementation of resolution 1540 (2004) on non-proliferation, 2231 (2015) on Iran and 1718 (2006) and seven successor sanctions resolutions on DPRK. These resolutions include requirements on UN member states to implement controls on financial transactions, and on financing of goods and services related to the proliferation of nuclear, chemical and biological weapons and their means of delivery (WMD) together with related goods and materials.

The Financial Action Task Force (FATF) has also introduced standards for implementing targeted financial sanctions imposed under the UN Security Council resolutions on Iran and DPRK. However, identifying and tracking PF is difficult because most transactions occur within normal business transaction pathways. Most states, as well as banks, other financial institutions and designated non-financial businesses and persons are unclear about what constitutes PF and how to recognize it. This is potentially serious because

[21] https://projectalpha.eu/wp-content/uploads/sites/21/2018/05/FoP-13-October-2017-Final.pdf

identification of proliferation-related financial transactions may enable the use of financial tools to combat WMD proliferation. Financial information may be used to initiate an investigation, prosecute an offender or disrupt networks by seizing funds, for example.

A comprehensive report on the threat of PF and options to counter the threat was published by the Financial Action Task Force (FATF) in 2008. The report concluded that it was not possible to identify any single financial pattern uniquely associated with proliferation financing, but it listed twenty indicators of possible proliferation financing (Annex 1).[22]

Indicators of Possible Financing of Proliferation

(A) Trade-related transactions potentially highly indicative of PF

1) Involvement of individuals or entities in foreign country of proliferation concern

PF Typology 1 - Trade in oil and coal with the DPRK

"Mr. X", was a businessman from "Country A", living in a port city known for illicit trading with the Democratic People's Republic of Korea (DPRK). His company, "Company A" was engaged in the importation of oil from the Middle East and exportation of coal to countries in the region. The latest United Nations Security Council Resolution (UNSCR) 2345(2017) Sanctions Committee (DPRK) Panel of Experts Report highlighted the illicit trade in these two commodities between that port city and the DPRK in violation of UNSCR 1874 (and related UNSCR 2397).

Mr. X had an account in the name of Company A in "Bank A", located in the same port city. In addition to himself, another signatory to the account is the son of a DPRK diplomat living in Country A.

"Mr. X" established an exempt company "Company K" in the Cayman Islands as Company A's holding company, to transact business in US dollars for the benefit of Bank A. On reviewing the on-boarding documentation, the MLRO at the "Company Manager K" in the Cayman Islands took note of the location and lines of business for Company A, as well as the authorised signatures for Company A at Bank A. She suspected

[22] Annex 1 of FATF's 2008 Report

that Company K was being used as a front by Mr. X, and that funds were being deposited in into Company A's account in Country A that were the proceeds of this illicit trade, in violation of UNSCR 2397.

Upon verification that a signatory to the account was the son of a DPRK diplomat in Country A who was on the EU sanctions list, and with no funds in the Cayman Islands, the MLRO submitted a TF/PF Asset Freeze Report Form (Annex 2 to the Industry Guidance on "Targeted Financial Sanctions with respect to Terrorism, Terrorism Financing, Proliferation, Proliferation Financing within the Cayman Islands, 2017").

Red Flags/Indicators:

- Mr. X's bank was headquartered in DPRK
- links to country determined to be high risk for proliferation financing.
- beneficial owners located in port city and country near DPRK border
- large sums credited into accounts from 'interesting' countries
- many transactions just under threshold limit
- "Mr. X" lived in a port city known with illicit trade with the DPRK
- "Mr. X" is involved in trade involving commodities that the UN Panel of Experts report highlighted as being actively traded by the DPRK in violation of PF sanctions
- beneficial owners of "Company A" include the son of a DPRK diplomat on the EU sanctions list

PF Case 1 - A designated Democratic People's Republic of North Korea (DPRK) bank maintains financial operations through DHID front companies (2009-2015)

The following is based on the contents of US court documents[23].

Korea Kwangson Banking Corporation (KKBC) was listed by OFAC on 11 Aug 2009 for providing financial services in support of DPRK's WMD and ballistic missile programs.

[23] United States District Court District of New Jersey Criminal Complaint Case 16-06602 filed 3 August 2016, United States of America v Dandong Hongxiang Industrial Development Co Ltd, and others, and related Verified Complaint for forfeiture in rem dated 26 Sep 2016.

Dandong Hongxiang Industrial Development Co Ltd (DHID) is a trading company based in Dandong, China, on the border with DPRK. DHID management personnel created a series of front companies, and opened corresponding bank accounts, in China and overseas, to facilitate transactions funded by and/or guaranteed by KKBC.

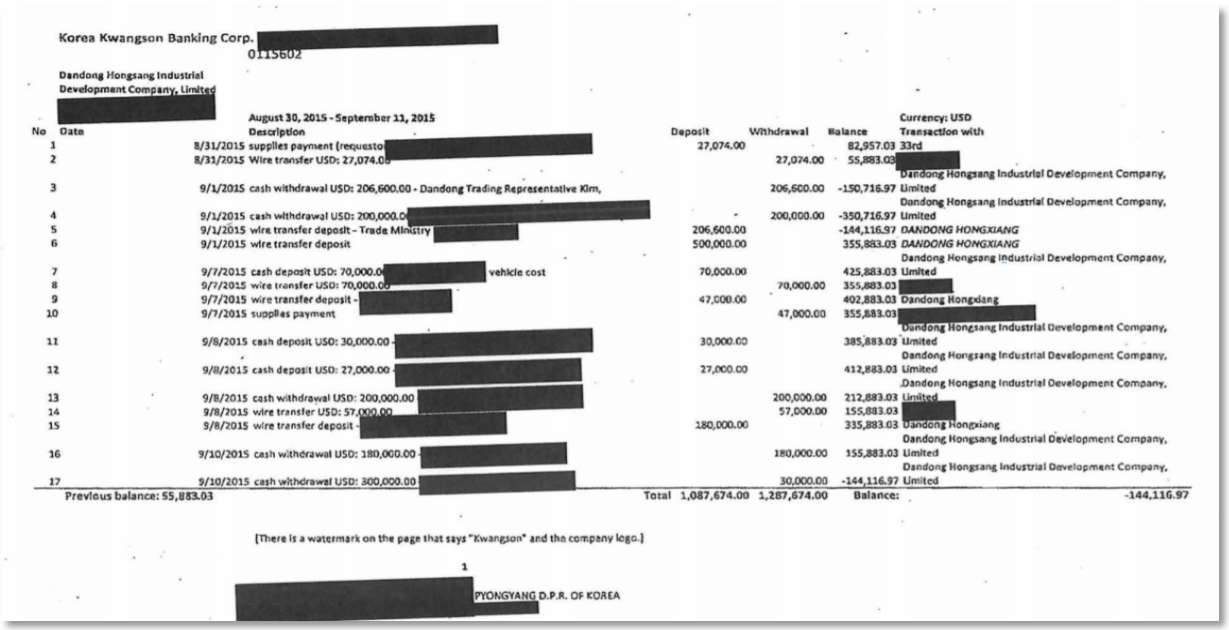
According to its owner, DHID, a China-based trading company, accounted for over 20% of China's trade with DPRK in 2010. At times, DHID and its front companies managed the full logistical chain of commodity contracts; at other times they facilitated US-dollar transactions between DPRK-based entities and suppliers in other countries.

According to US court documents, a US-dollar account held by DHID at a KKBC branch in Pyongyang was used by KKBC to fund DHID for commodity purchases made by DHID's front companies overseas. A bank statement (figure 1) shows deposits from a variety of sources (including cash) that frequently correspond to withdrawals (including cash) of equivalent or similar funds around the same time.

According to US court documents, these bank statements show that a "ledger" accounting system was in operation between KKBC and DHID although the documents do not specify how this system operated in practice. Some of the credits and debits to DHID's bank account in Pyongyang may have corresponded to records of equivalent debits and credits at different DHID front companies overseas.

Withdrawals in cash may also have been physically transferred overseas and credited to DHID front companies. In some of the cases recorded in the documents, the KKBC Dandong Representative Office was responsible for managing DHID's proxy role with KKBC. Such mechanisms would have enabled KKBC to settle outstanding balances with DHID without transmitting funds in USD through the US financial system (where they would have been blocked).

Figure 1. Bank statement for the DHID account held at a branch of KKBC in Pyongyang



Korea Kwangson Banking Corp. [redacted]
0115602

Dandong Hongsang Industrial Development Company, Limited [redacted]

August 30, 2015 - September 11, 2015 — Currency: USD

No	Date	Description	Deposit	Withdrawal	Balance	Transaction with
1	8/31/2015	supplies payment (requesto [redacted]	27,074.00		82,957.03	33rd
2	8/31/2015	Wire transfer USD: 27,074.00		27,074.00	55,883.03	[redacted]
3	9/1/2015	cash withdrawal USD: 206,600.00 - Dandong Trading Representative Kim,		206,600.00	-150,716.97	Dandong Hongsang Industrial Development Company, Limited
4	9/1/2015	cash withdrawal USD: 200,000.0[redacted]		200,000.00	-350,716.97	Dandong Hongsang Industrial Development Company, Limited
5	9/1/2015	wire transfer deposit - Trade Ministry [redacted]	206,600.00		-144,116.97	DANDONG HONGXIANG
6	9/1/2015	wire transfer deposit	500,000.00		355,883.03	DANDONG HONGXIANG
7	9/7/2015	cash deposit USD: 70,000.0[redacted] vehicle cost	70,000.00		425,883.03	Dandong Hongsang Industrial Development Company, Limited
8	9/7/2015	wire transfer USD: 70,000.0[redacted]		70,000.00	355,883.03	[redacted]
9	9/7/2015	wire transfer deposit - [redacted]	47,000.00		402,883.03	Dandong Hongxiang
10	9/7/2015	supplies payment		47,000.00	355,883.03	[redacted]
11	9/8/2015	cash deposit USD: 30,000.00 [redacted]	30,000.00		385,883.03	Dandong Hongsang Industrial Development Company, Limited
12	9/8/2015	cash deposit USD: 27,000.00 [redacted]	27,000.00		412,883.03	Dandong Hongsang Industrial Development Company, Limited
13	9/8/2015	cash withdrawal USD: 200,000.00 [redacted]		200,000.00	212,883.03	Dandong Hongsang Industrial Development Company, Limited
14	9/8/2015	wire transfer USD: 57,000.00		57,000.00	155,883.03	[redacted]
15	9/8/2015	wire transfer deposit - [redacted]	180,000.00		335,883.03	Dandong Hongxiang
16	9/10/2015	cash withdrawal USD: 180,000.00 [redacted]		180,000.00	155,883.03	Dandong Hongsang Industrial Development Company, Limited
17	9/10/2015	cash withdrawal USD: 300,000.00 [redacted]		30,000.00	-144,116.97	Dandong Hongsang Industrial Development Company, Limited
Previous balance: 55,883.03		Total	1,087,674.00	1,287,674.00	Balance:	-144,116.97

[There is a watermark on the page that says "Kwangson" and the company logo.]

1

[redacted] PYONGYANG D.P.R. OF KOREA

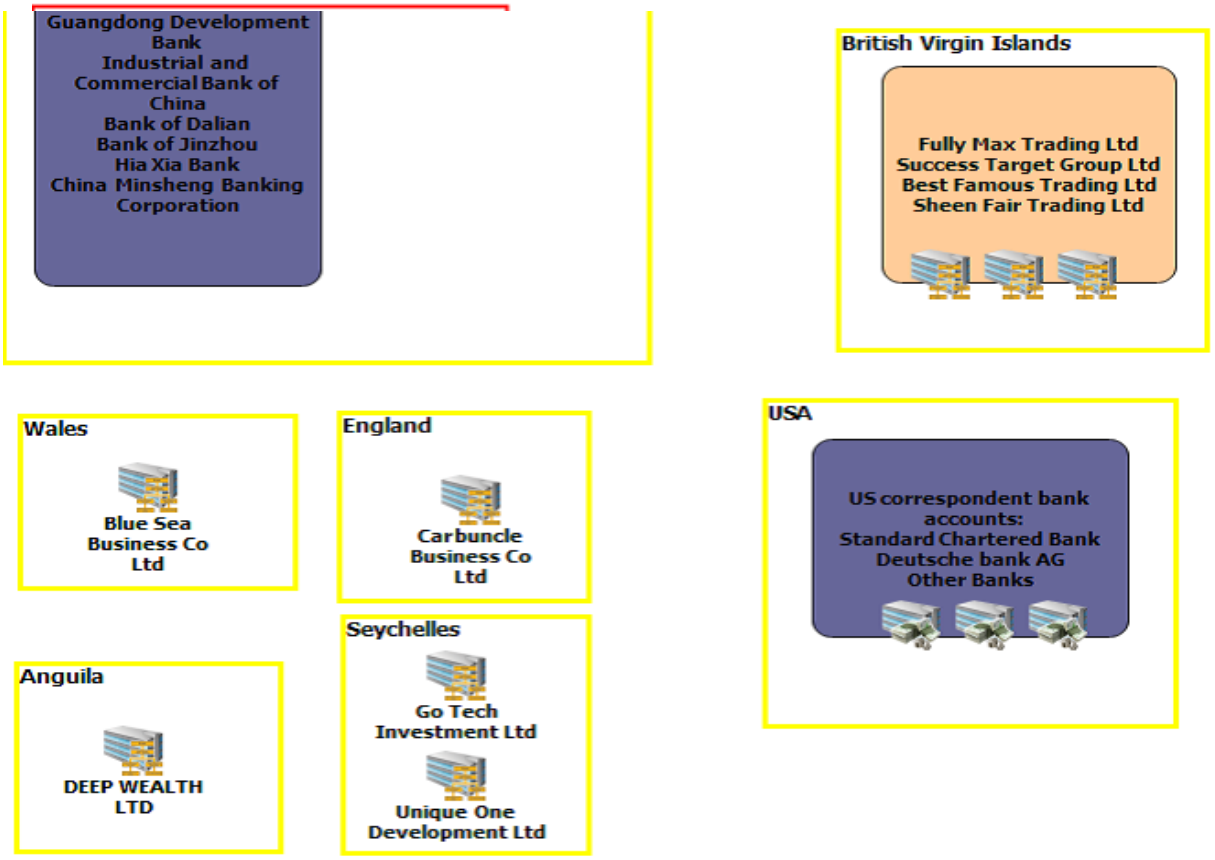
illustrating a number of contemporaneous matching deposits and withdrawals. Note that because the identities of payers and payees have been redacted it is not possible to determine whether all entries reflect activity by DHID and its front companies on behalf of KKBC, or whether some reflect other transactions by DHID within DPRK (Image taken from United States District Court District of New Jersey Criminal Complaint Case 16-06602 filed 3 August 2016).

As a further indication that DHID was conducting US dollar transactions on KKBC's behalf, court documents note that DHID's US interbank remittance transactions through Standard Chartered Bank in the US "increased from $1.3 million for the approximately three-year period prior to KKBC's designation to $110 million from 2009 to 2015, after KKBC was designated."

US court documents identify many front companies created or purchased by DHID and its executives for the purposes of transmitting and/or receiving money through the US on behalf of KKBC, and the banks involved (figure 2).[24]

[24] Separate case brought by US authorities alleges that Minzheng International Trading Limited, a company based in Hong Kong, acts as a front company for the Foreign Trade Bank of DPRK, sanctioned under UN and US legislation and owner of KKBC, similarly to the way in which DHID is described as acting for KKBC (Verified Complaint for Forfeiture *In Rem,* United States District Court for the District of Columbia case 1:17-cv-01166-KBJ, filed 14 June 2017).

Figure 2. The network of DHID and its front companies supporting KKBC, and the banks used by them in China[25]



Key Points

- The US-dollar bank account of DHID at a KKBC branch in Pyongyang was used by KKBC to fund DHID for commodity purchases by DHID front companies overseas. This enabled KKBC to finance activities overseas indirectly, despite its designation;
- Multiple banks in China were involved in transactions subsequently carried out by DHID and its front companies;
- DHID made use of multiple front companies overseas, including in Anguilla, Seychelles, England, Wales, British Virgin Islands and Hong Kong;

[25] Based on information referenced in United States District Court District of New Jersey Criminal Complaint

- A "ledger" system was used to record transactions carried out by DHID and related companies.
- There was a failure to freeze without delay.

PF Case 2 - DHID front company facilitates financing of urea trade by designated bank (2013)[26]

The following is based on US court documents.

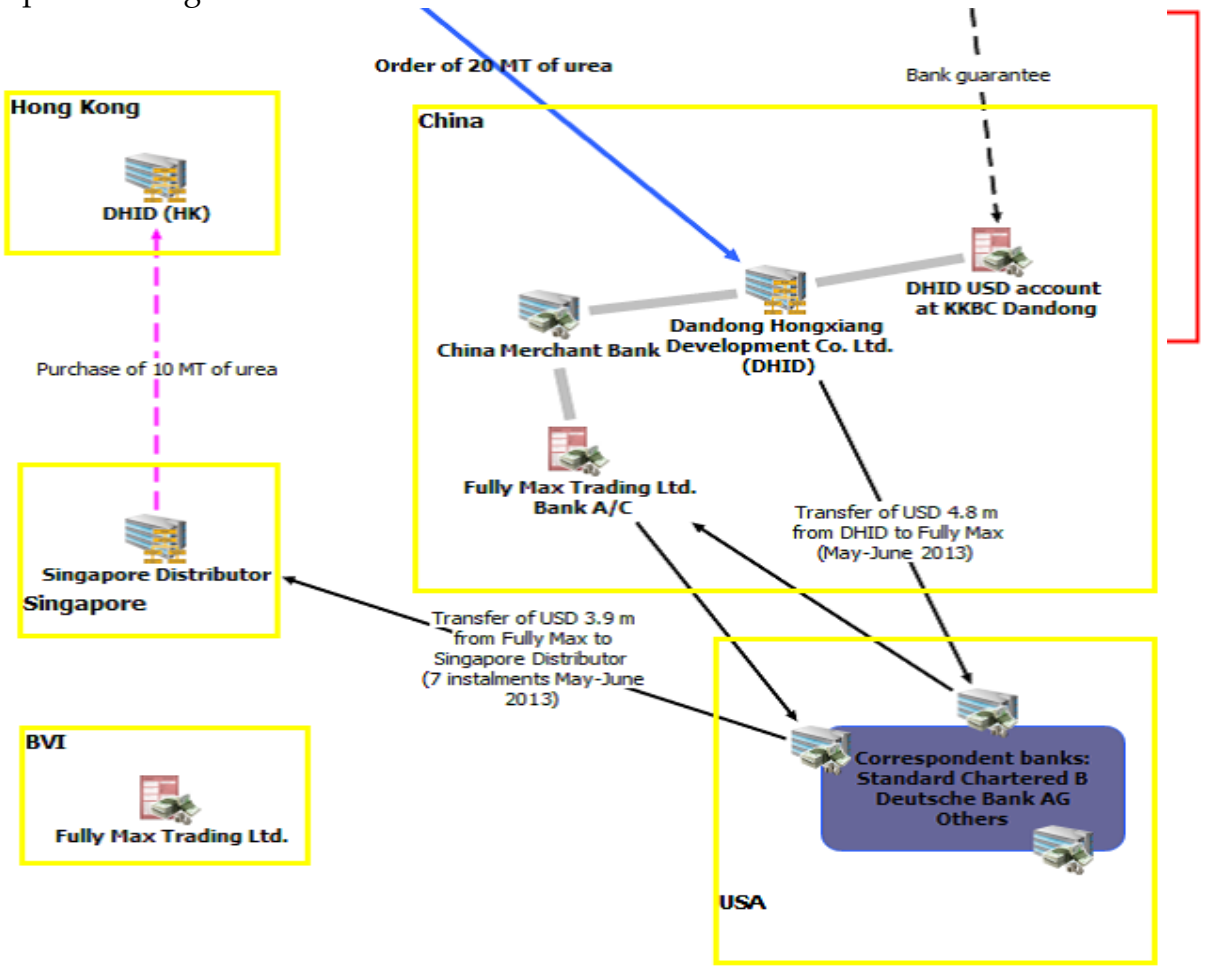
The documents describe a number of cases of the use of the front companies to circumvent KKBC's listing by OFAC. The following is the most recent, involving purchase of urea fertilizer in 2013 (Figure 3). Although this does not involve WMD goods and materials, the methods of circumvention of financial sanctions by KKBC and DHID could readily be adapted to such procurement.

In March 2013 DHID agreed to sell 20,000 metric tons of urea fertilizer to a DPRK company, subject to a guarantee from KKBC that payment had been made by the company before the cargo was to be loaded. Hongxiang Industrial Development (H.K.) Limited, a DHID front company in Hong Kong, subsequently arranged the purchase of 10,000 metric tons of urea from a Singapore Distributor.

Bank records show that Fully Max Trading Ltd, a BVI-based DHID front company, paid the Singapore supplier almost USD 3.9 million, in a series of seven installments between May and June 2013. All the payments transited the US financial system. Bank records also show that between May and June 2013, Fully Max Trading Ltd received a deposit of about USD 4.8 million into its account at China Merchants Bank from a DHID account.[27] These funds transited the U.S. financial system through a US correspondent banking account at Standard Chartered Bank. DHID made a profit of about 23% on the deal (DHID made similar profits on other deals described in the court records).

[26] https://www.govinfo.gov/content/pkg/USCOURTS-njd-3_12-cv-05882/pdf/USCOURTS-njd-3_12-cv-05882-2.pdf
[27] Based on details contained in US court documents the DHID account was almost certainly also held at China Merchants Bank.

Figure 3. DHID and its network of front companies enable KKBC to finance the urea trade despite its designation.



Key Points

- The network of DHID and front companies involved extended to China, Hong Kong and the British Virgin Islands;
- Payments made by the DHID network were based on a bank guarantee from KKBC;
- It is likely that the KKBC Dandong Representative Office was responsible for transferring funds to enable DHID to pay the Singapore supplier.

2) Activity that does not match customers' or counterparties business profiles or end-user information does not match end-user's business profile

(B) Trade-related transactions potentially moderately indicative of PF

1) Pattern of transactions of a customer or counterparty, declared to be a commercial business, suggest they are acting as a money-remittance business

PF Case 3 - Sanctions circumvention by a company acting as remittance agent (probably 2012-2013)

A company in Iran, "Company A", entered into an agreement with a company in a State in the Middle East, "Company B", under which Company B agreed to accept or process payments on behalf of company A.[28] Company B had a bank account at a non-Iranian FI.

Company A informed its customers to direct their payments to Company B and informed beneficiaries to expect payments from Company B's bank (see figure 8).

It is not known how Company B and Company A in Iran settled their financial liabilities.

PF Case 4 - Foreign flagged ship owned or controlled by a BVI entity[29]

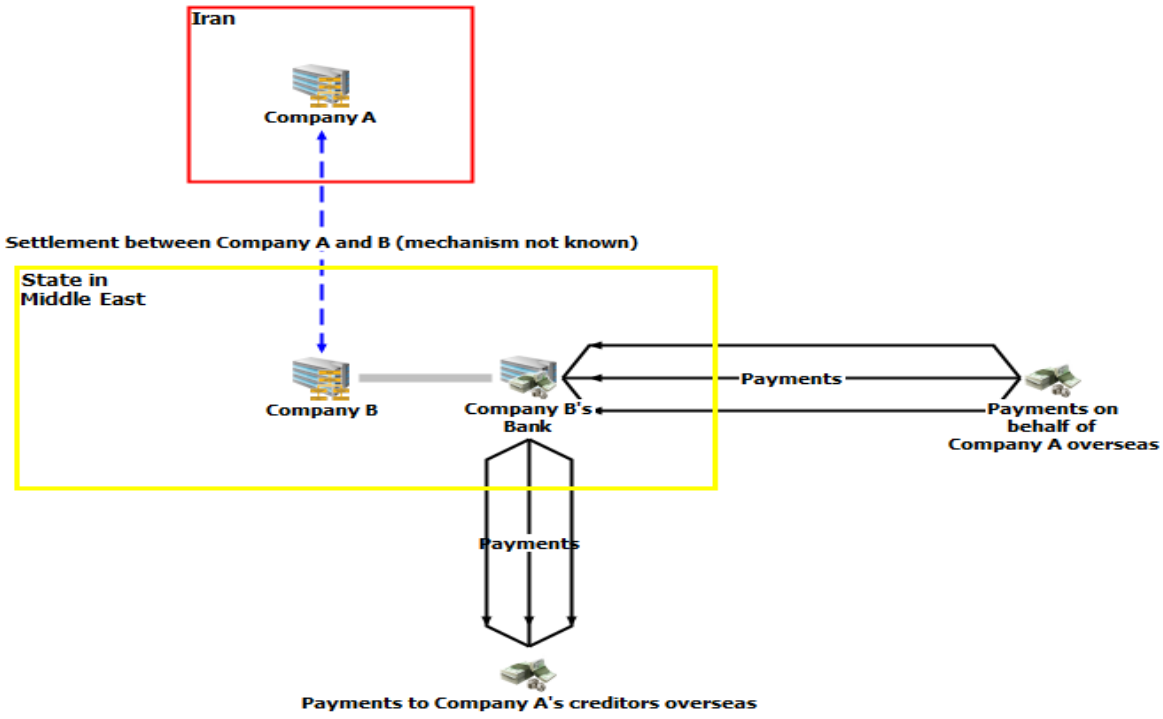
According to the UN Panel of Experts' Report, companies including the British Virgin Islands-registered company, Faith Trade Group Limited, owned a vessel from May 2018 reported by the Panel to have delivered refined petroleum to the DPRK. The case forcefully illustrates how Caribbean legal entities may own ships associated with sanctioned countries and may be misused for sanctions evasion purposes. In terms of the considerations for the Cayman Islands, there is the threat of Cayman Islands entities owning foreign flagged ships linked or associated with sanctioned countries for evasion purposes.

Red flags/Indicators:

- multiple companies and layers of ownership to obscure identity of ultimate owners

[28] Annex V of UN Panel on Iran Final Report 2014 (S/2014/394).
[29] Cayman Islands National Risk Assessment 2021

Figure 8 - Sanctions circumvention by company acting as remittance agent



Key Points

- Monitoring by the bank presumably revealed that Company B's financial transactions were inconsistent with its expected financial profile.

6. Emerging Money Laundering Trends

As a premier financial centre heavily dependent on globalisation, we constantly have to examine emerging global trends as the world continues to evolve and modernise. Continued modernisation brings with it new money laundering, terrorist financing and proliferation financing risks and threats associated with newly created technologies, as well as emerging ideologies.

6.1 Virtual Currencies

According to the 2021 NRA, fraud and ransomware attacks using virtual assets is an emerging risk for the Cayman Islands. In 2019 Cayman raised US$1.4 billion from 119 Initial Coin Offerings (ICOs). Based on the amount raised from ICOs, the Cayman Islands is the 6th largest jurisdiction in the world. Although the year 2020 saw a significant decrease in ICOs around the world and in the Cayman Islands, other fraudulent schemes (including ransomware attacks) are increasingly using virtual assets to move illicit funds globally.

The Cayman Islands Monetary Authority published a public advisory report in 2018 on the potential risks of investments in Initial Coin Offerings (ICOs) and all forms of virtual currency[30]. Some startup companies are using initial coin offerings, also called ICOs or token sales, to raise capital. In an ICO, a company creates a new virtual coin or token that is offered for sale to the public.

CIMA presents a number of risks associated with ICOs and virtual currencies, such as:

- potential for incomplete information on the investment;
- a high degree of technical expertise needed to understand the investment;
- exaggerated expected returns;
- rapidly changing prices;
- potential for not being able to resell the virtual currency;
- potential for losing the investment to hackers;
- no regulatory protection for the investor;
- funds raised could be used to finance terrorism; and
- fraud

[30] See CIMA Public Advisory: Virtual Currencies – April 2018

Moreover, CIMA stated that the public should be aware of the following **red flags** to help identify potentially fraudulent ICOs:

- claims of endorsements by CIMA
- there is limited information about the investment, the project and the development team,
- including insufficient or vague technical information relating to the coin
- the promoters are pushing for you to make a quick decision
- well-known persons are investors or associated with the project
- there is an aggressive marketing campaign around the ICO, with promises of large or quick returns the project developers are anonymous

On 22 November 2019, CIMA issued a public advisory on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) to increase public awareness about the potential risk of fraud. Investors were encouraged to conduct thorough research on the potential risks of VAs. In 2020, CIBFI actioned four international requests for assistance, resulting in the restraint of virtual assets on behalf of three separate jurisdictions, with a combined estimated value of US$14 million.

The FATF published a 2018 report advising on the regulation of virtual assets. FATF has adopted various changes to the FATF recommendations and glossary. These changes clarify how the recommendations apply to financial activities, which include virtual assets. This involves adding to the glossary of definitions, "virtual assets" and "virtual asset service providers". These include exchanges, certain types of wallet providers, and providers of financial services for Initial Coin Offerings (ICOs).[31] The FATF also published Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers in October 2021.

6.2 Gold Storage

Analysis from the 2021 NRA revealed that the Cayman Islands has emerged as major centre in the Western Hemisphere for the storage of gold and other precious metals, in addition to the US and Canada. This is due to the safety, political and economic stability of the jurisdiction, making it attractive for this line of business. Furthermore, other attractive policies include there being no import duties levied on commodities and also no sales

[31] See FATF Publication: Regulation of Virtual Assets – October 2018

taxes associated with storage fees. It should be emphasized that safe custody services fall under the definition of relevant financial business in paragraph 13 of Schedule 6 of the POCA.[32]

Data from the 2021 NRA showed that non-monetary gold imported into the Cayman Islands peaked at $26.6 million in 2015 and declined to a low of $5.5 million in 2017. Nonetheless, the past two years have seen significant increases to $62.3 million in 2019 and $74.0 million in 2020. Competent authorities urge that continued vigilance is required with respect to money laundering risks through gold coming from South America. Illegal mining and gold smuggling from South America have been linked to drug trafficking, organised crime, and sanctions evasion.

6.3 Human trafficking

In recent years, human trafficking and smuggling of migrants have become a major concern. By definition, human trafficking is the movement of people for the purpose of exploitation: sexual exploitation, forced labour, or enslavement. The COVID-19 pandemic has indeed intensified the drivers and root causes of human trafficking: poverty, war, climate change, demand for cheap labour, and the opportunity for high profits. FIs and DNFBPs headquartered in the UK have put out statements in accordance with the UK's Modern Slavery Act 2015. This covers the branches and subsidiaries domiciled in the Cayman Islands. The Cayman Islands "Trafficking in Persons (Prevention and Suppression) Act (2015 Revision) is modelled after the UK's Modern Slavery Act.

There have not been significant numbers of refugees and economic migrants being smuggled into the Cayman Islands and also no sufficient information to form conclusions on this activity. However, analysis in the 2021 NRA shows that there are signs that organised human trafficking rings within the region are manipulating work permit systems to bring in victims of human trafficking and modern slavery. It is therefore necessary to identify any vulnerabilities within our work permit system to mitigate against the risks of human trafficking and smuggling within the Cayman Islands.

In conclusion, the Cayman Islands must proactively understand these emerging risks and red flags and take appropriate measures to mitigate them.

[32] Cayman Islands National Risk Assessment 2021

7. References

CIG (2021) *Results of the 2021 Cayman Islands National Risk Assessment Relating to Money Laundering, Terrorism Financing and Proliferation Financing,* Cayman Islands Government, Cayman Islands,

- CIG, (2020), *Proceeds of Crime Act 2020 Revision*, Cayman Islands Government,
- CIG, (2018), *Terrorism Act 2018 Revision*, Cayman Islands Government
- CIG (2015), *Results of the 2015 Cayman Islands National Risk Assessment Relating to Money Laundering, Terrorism Financing and Proliferation Financing*, Cayman Islands Government, Cayman Islands, http://www.gov.ky/portal/pls/portal/docs/1/12408457.PDF

CIMA, (2018), *Public Advisory: Virtual Currencies*, Cayman Islands Government, Cayman Islands. April. 2018. https://www.cima.ky/upimages/noticedoc/1524507769PublicAdvisory-VirtualCurrencies_1524507769.pdf

GJ, (2015), *Money Laundering Typologies and Trends,* Government of Jersey, January 2015, https://www.gov.je/Government/Pages/StatesReports.aspx?ReportID=1131

FATF, (2021), *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers* – FATF. Paris, October 2021, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

- FATF, (2018), *Regulation of Virtual Assets*, FATF, Paris, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html
- FATF, (2015), *Emerging Terrorist Financing Risks*, FATF, Paris www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html
- FATF, (2008). *Financial Action Task Force Annual Report*., FATF-GAFI. http://www.fatf-gafi.org/media/fatf/documents/reports/2008%202009%20ENG.pdf

REFERENCES

FINTRAC, (2010), *Typologies and Trends Reports: Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MSBs)*; June 2010. https://www.justice.gov.il/Units/HalbantHon/docs/cana.pdf

FRA, (2020), Typologies Project, Financial Reporting Authority, Cayman Islands Government

Scott, Jude. (2018), *Cayman Islands: Industry Overview of the Financial Services Sector,* Cayman Finance, Cayman Islands, May 2018. http://www.mondaq.com/cayman-islands/x/704006/Industry+Overview+Of+The+Financial+Services+Sector

Egmont Group, (2002), *Egmont/FATF Collection of Sanitised Cases Related to Terrorist Financing., http://www.ctif-cfi.be/website/images/EN/typo_egmont/20casesgb.pdf*

Brewer, Jonathan. (2017)., *Study of Typologies Financing of WMD Proliferation,* Final Report., October 13. 2017., Project Alpha., King's College of London, https://projectalpha.eu/wp-content/uploads/sites/21/2018/05/FoP-13-October-2017-Final.pdf

United States District Court for the District of Columbia (2017), Verified Complaint for Forfeiture in REM. against Minzheng International Trading Limited. 2017. http://online.wsj.com/media/Mingzheng.pdf

- United States District Court District of New Jersey (2016), Criminal Complaint Case 16-06602 filed 3 August 2016, United States of America v Dandong Hongxiang Industrial Development Co Ltd. https://www.govinfo.gov/content/pkg/USCOURTS-njd-3_12-cv-05882/pdf/USCOURTS-njd-3_12-cv-05882-2.pdf

United Nations Security Council (2014). *Annex V of UN Panel on Iran Final Report 2014*, (S/2014/394)., http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2014_394.pdf