FOLLOW THE MONEY

FINANCIAL INTELLIGENCE UNIT
FIUTT
TRINIDAD AND TOBAGO

STRATEGIC ANALYSIS CASE COMPILATION

2015 - 2020

FINANCIAL INTELLIGENCE UNIT OF TRINIDAD AND TOBAGO

STRATEGIC ANALYSIS CASE COMPILATION

2015 - 2020

This is a Financial Intelligence Unit of Trinidad and Tobago (FIUTT) product for Reporting Entities, Law Enforcement Authorities, Supervisory Authorities, Competent Authorities and the general public of Suspicious Transaction/Activity Reports (STRs/SARs), in line with the FIUTT's commitment to share perspectives on the STRs/SARs regime. This is accordance with Section 17(b) of the FIUTT Act; and Regulation 26 (1) (d)(ii) of the FIUTTR.

COPYRIGHT

Website: www.fiutt.gov.tt

Published: May 2021

OVERVIEW

This publication is timely for the Financial Intelligence Unit of Trinidad and Tobago ("the FIUTT") in its 10th year of operations highlighting financial analysis for the period 2015 to 2020. Money Laundering (ML) and Financing of Terrorism (FT) are serious crimes that have significant corrosive effects at all levels of society. The cases in this publication will serve Reporting Entities, Competent Authorities and the general public to better understand how ML and FT works and what the role of FIUs is to prevent and combat these forms of crime.

The FIUTT's financial analysis present key teachings, best practices, and relevant case examples with red flags to help identify, deter, detect, and report ML/FT and other serious criminal conduct both at the national and international levels. The report reveals the diversity and importance of the threats facing Reporting Entities, Competent Authorities and the wider community.

This report presents a snapshot of how criminals are seeking to abuse Trinidad and Tobago's financial system. They describe suspected cases involving drug trafficking, fraud of varying types, human trafficking, sophisticated local and overseas tax evasion schemes, and financing of terrorism. These cases would be instrumental in helping to identify additional suspected criminal bank accounts, phone numbers and assets that may not have been previously known to law enforcement.

Notably, the FIUTT has flagged in this report virtual assets as an emerging new technology that can be misused by criminals and has provided some red flags to the Reporting Entities.

The case studies in this report also demonstrate the enormous financial intelligence value of the suspicious transaction/activity reports (STRs/SARs) the FIUTT receives from a wide range of reporting entities. The valuable contribution of Reporting Entities and the FIUTT's designated partner Competent Authorities in producing this document is acknowledged. Therefore, continued input is crucial in ensuring our reports remain useful and relevant to our collective efforts to protect Trinidad and Tobago against financial and other serious crimes.

The information in this publication should further assist with establishing risk mitigating measures for national strategies.

DISCLAIMER

TABLE OF CONTENTS

TABLE OF CONTENTS (cont'd)

2019

2020

Glossary

- END -

LIST OF ABBREVIATIONS

ABBREVIATION	MEANING
AML/CFT	Anti-Money Laundering/Counter Financing of Terrorism
ATA	Anti-Terrorism Act, Chapter 12:07
CDD	Customer Due Diligence
CU	Credit Union
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FIUTT	Financial Intelligence Unit of Trinidad and Tobago
FTFs	Foreign Terrorist Fighters
FT	Financing of Terrorism
ISIL	Islamic State of Iraq and the Levant
ISIS	Islamic State of Iraq and Syria
KYC	Know Your Customer
LB	Listed Business
LEA	Law Enforcement Authority
ML/FT	Money Laundering/Financing of Terrorism
ML	Money Laundering
MVTS	Money or Value Transfer Services
NPOs	Non-Profit Organisations
PEP	Politically Exposed Person
PMC	Private Members' Club
STR/SAR	Suspicious Transaction Report/Suspicious Activity Report
TTPS	Trinidad and Tobago Police Service
UN	United Nations
UNSCR	United Nations Security Council Resolution
VA	Virtual Asset
VASP	Virtual Asset Service Provider

AT A GLANCE - STRATEGIC ANALYSIS CASE COMPILATION 2015 - 2020

1. Advisory-Counterfeit Notes
2. Typology-Undue Influence or Duress
3. Typology-Trends in Insurance Sector
4. Strategic Analysis-Suspected Extortion & Money Laundering within the Prison system.

2015

5. Typology- Suspected Financing of Terrorism
6. Scam Alert – STOP
7. Typology- Suspected Insurance Fraud
8. Typology-Suspected Human Trafficking

2016

9. Typology-Real Property Fraud
10. Typology-Fraudulent Motor Vehicle Insurance Certificates/ Policies

2017

STRATEGIC ANALYSIS CASE COMPILATION 2015 - 2020 (CONT'D)

2018

11. Typology-Tax Evasion
12. Typology-A Self-Funded Jihadi
13. Typology-Suspected Jihadi Funded by Credit

2019

14. Typology-Suspected Foreign Nationals' Tax Evasion
15. Typology-The Suspected Abuse Of Non-Profit Organizations', Relative To The Financing Of Terrorism
16. Advisory-Rise in Email Compromise
17. Advisory-Foreign Nationals 'Suspected' Involvement In Organised Criminal Activity
18. Typology- Suspected Government Salaries Fraud

2020

19. Typology - Romance Scam/Fraud
20. Advisory - Pyramid Schemes
21. Advisory - Unauthorised Account Access
22. Advisory - Abuse Of The Duty Tax Concession On Vehicle Imports
23. Advisory-Virtual Assets Red Flags & Indicators
24. Covid-19 Scam Alert for the Public and Business Community
25. Strategic Analysis - Suspected Movement of Funds out of the Conflict Zone – A T&T Perspective
26. Typology - Financial Flows – A Human Trafficking Perspective

2015

In the year 2015, the FIUTT noted several trends and possible future behaviour based on STRs/SARs submission by the Reporting Entities including:

1. **The use of counterfeit notes;**
2. **Undue influence or duress (to the elderly);**
3. **The emergence of fraudulent motor vehicle insurance certificates, third party requests for insurance, as well as, authorized brokers** (persons purporting to be employed with a registered insurance company);
4. **The use of the Money Value Transfer Services (MVTS**) sector to transfer funds to incarcerated persons (through close associates) to facilitate the purchase of contraband within prison.

Advisory

1. Counterfeit Notes

Suspected Offence	Fraud; Forgery
Customer Type	Individual
Industry	FI's; CU's
Channel	Physical
Jurisdiction	Local

In 2015, the FIUTT noted that suspected counterfeit Trinidad and Tobago currency was being circulated by members and visitors of Private Members' Clubs (PMCs) in conducting their gaming transactions. The PMCs specifically identified the use of counterfeit bills - TTD 100 and TTD 20. Persons involved in the fraud appeared to be nationals of Trinidad and Tobago and may have been in possession of the counterfeit notes, knowingly or unknowingly. The fraud was prevalent in Central Trinidad; and/or; Chaguanas and environs. The persons involved in this activity declared their occupations to be, sales representatives, equipment operators, tradesman and home-maker.

Details of the Fraud **-** The method of operating by persons in possession of the counterfeit notes was to conduct two transactions at the cashiers. For example, they attempted to change a ticket from a slot machine and change the counterfeit notes.

Suspicious Indicators

- The texture of the note appeared to be firmer than a real note;
- Absence of watermark and/or, security thread;
- Absence of the various security features and symbols of a genuine note;
- Absence of the metallic feature on the TTD 20 and TTD 100 notes; and
- May be smaller than the genuine note in that denomination.

Typology

2.Undue Influence or Duress

Suspected Offence	Extortion
Customer Type	Individual
Industry	FI's; CU's
Channel	Physical; Electronic
Jurisdiction	Local

Mr. X, a member of a Credit Union (CU) persuades an elderly person (alleged victim) to apply for membership in the CU. Upon enrolment, Mr. X states that he would make deposits to the alleged victim accounts. The accounts included an Indemnity Plan, Life Insurance policy and other investment products. Mr. X was described as a relative and/or friend of the applicant and was placed as the beneficiary on the accounts. Upon the death of the elderly victim, Mr. X provides the CU with a copy of the death certificate and claims the death benefit.

Family members of the deceased appear unaware of their relative's membership in the CU. It would appear that Mr. X resided in close proximity to the elderly person and may have been well known to the alleged victim. Mr. X then accompanied several other applicants for membership, all of whom were elderly, infirm or otherwise vulnerable persons*, and who named him as beneficiary on their accounts. * *Vulnerable person: an individual who is at risk of abuse or harm due to life circumstances—e.g., frail and elderly, underage, homeless, mentally ill or differently abled.*

Suspicious Indicators

- Accompanies the vulnerable person to the Credit Union and enrolls them as a new member;
- Agrees to pay the indemnity or insurance premium payments on the vulnerable person's behalf;
- On the death of the vulnerable person, the perpetrator provides the Credit Union with a copy of the death certificate and collects the death benefit; and
- The relatives of the elderly and/or infirmed persons are unaware of his/her membership in a Credit Union; and
- The perpetrator being the named beneficiary for several elderly persons.

Typology

3. *Trends in the Insurance Sector - Fraud*

Suspected Offence	Fraud; Forgery
Customer Type	Individual; Group
Industry	Insurance
Channel	Physical
Jurisdiction	Local

The FIUTT noted an increase in the use of fraudulent documents to conduct business at Insurance Companies. This type of fraudulent activity was observed predominantly in the motor vehicle insurance sector.

MOTOR VEHICLE INSURANCE

1. FRAUDULENT CERTIFICATES OF INSURANCE

An increasing number of individuals have been using fraudulent certificates of insurance as well as other misleading documentation in order to make claims arising from accidents. These activities are especially noted in Insurance Companies that have changed their names but retained certificates of insurance, which were issued in the company's previous names. Several of these fraudulent activities have been observed where the policies are issued by sales agents operating out of branch offices, particularly agents who engage with '' Spotters**" working with brokers operating on behalf of an Insurance

Suspicious Indicators

- False certificate number/Policy number;
- Certificate number/Policy number is a legitimate number that is assigned to another insured person;
- The name on the certificate is not the name to whom the Insurance Company issued the certificate;
- Dates of commencement and expiration of the policy are altered;
- Forged signature of an authorised signatory to the Insurance Company, on the certificate;
- The signature cannot be identified to any authorised signatory for the Insurance Company;
- Use of a fraudulent stamp of the company;
- The formatting/font of the certificate may be different to that used by the Company; and
- Renewed certificates of Insurance, which are not authorised by the Insurance Company.

Company.

***A Spotter is described as someone who liaises with clients on behalf of an insurance agent. The Spotter collects and reviews the client's documents prior to entering into a business relationship with the agent.*

2. THIRD PARTY REQUEST FOR INSURANCE

Another activity noted is that of individuals requesting motor vehicle insurance (usually third party) on multiple vehicle(s), which are not registered in their name. These individuals appear to be making the applications on behalf of car dealers with whom the Insurance Companies do not wish to transact business.

3. UNAUTHORISED BROKERS

Unauthorised brokers or former employees hold out themselves as agents of Insurance Companies. The unauthorised brokers produce fabricated documents, (on which the company's stamp and other company insignias are inscribed) and issue the fabricated documents to unsuspecting customers. The "policies" issued by the unauthorised brokers are not reported to the Insurance Companies. In the instances brought to the attention of the FIUTT, the "insured" only finds out of the fraud when they file a claim at the Insurance Company.

Persons obtaining insurance should contact the headquarters of the Insurance Company to ensure that their motor vehicle insurance is registered.

Strategic Analysis

4. Suspected Extortion & Money Laundering within the Prison System

Suspected Offence	Organised Crime Group
Customer Type	Individual; Group
Industry	MVTS
Channel	Electronic
Jurisdiction	Local; Regional

Strategic Analysis conducted by the FIUTT revealed that Organised Crime Group's (OCGs) utilized legitimate financial systems to perpetrate contraband trafficking within state run prison institutions, which amounted to over TTD 10,000,000.00 in suspected criminal proceeds. This ongoing activity appears to have perpetuated the occurrence of Corruption and Misbehaviour in Public Office amongst Public Officers, as well as lead to offences such as Murder, Drug Trafficking and other related serious crimes as depicted in **Diagram 1** below.

Key Money Laundering (ML) Techniques

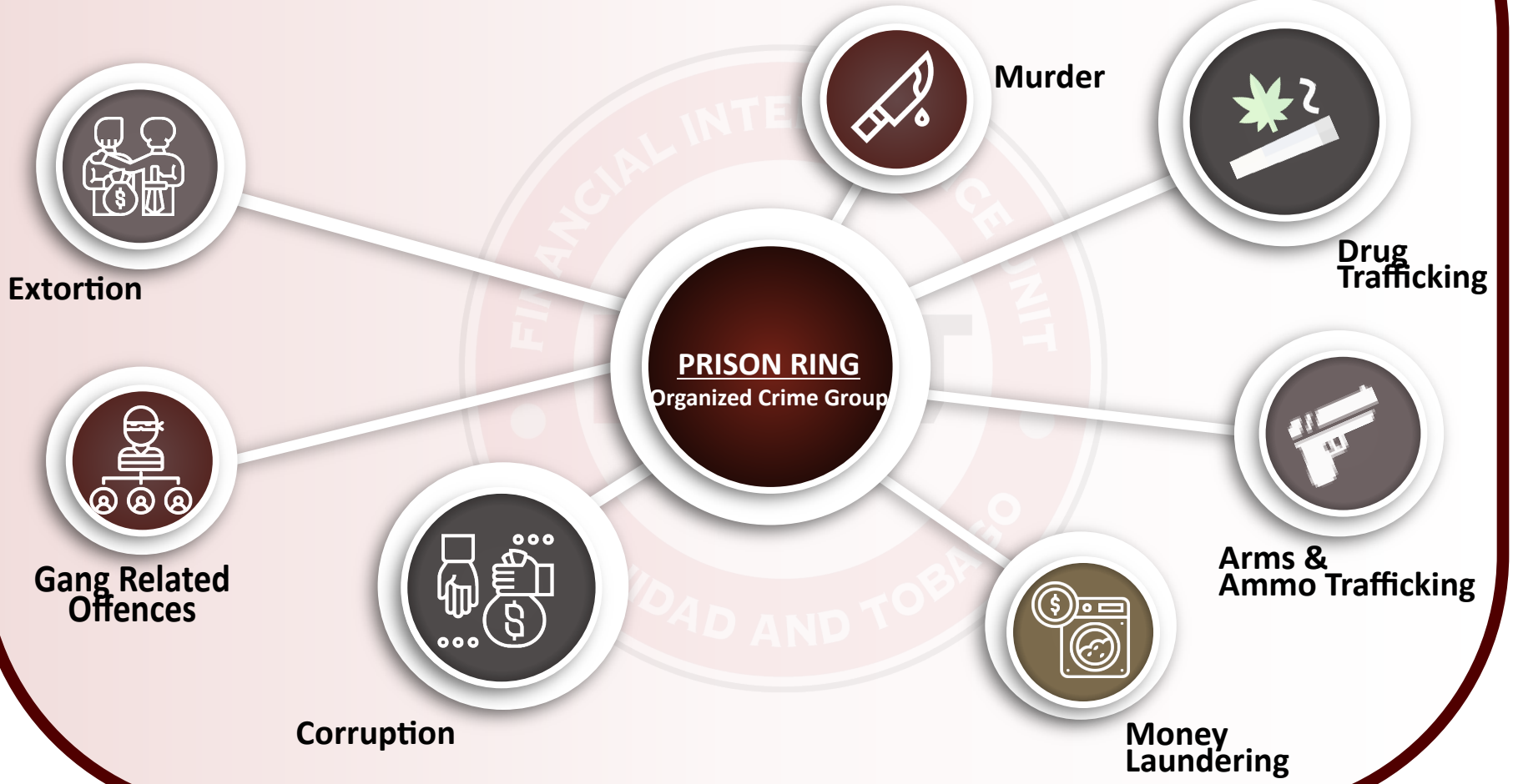
- Use of funds derived from the activity to support contraband trafficking within a state institution;
- Movement of cash to foreign jurisdictions (transfers through MVTS Sector);
- Movement of funds via multiple actors;
- Funds used to finance other serious criminal offences (Drug trafficking/corruption/murder); and
- Purchase of USD currency

Suspicious Indicators

- Intra-Island money transfers;
- Some individuals were criminally known to Law Enforcement Authorities (LEAs);
- Age groups were generally below 30 years;
- Low income occupations – Labourer, housewife etc.;
- Common geographic location for the majority of senders;
- Low valued rounded amounts – TTD 200, TTD 300, TTD 400; and
- Receivers generally unknown to senders.

DIAGRAM 1

OFFENCES OBSERVED DURING EXTORTION & MONEY LAUNDERING WITHIN PRISONS



2016

FIUTT noted several trends in the year 2016 based on STRs/SARs submission by the Reporting Entities including:

5. **Suspected Financing of Terrorism**
6. **Scam Alert – STOP**
7. **Suspected Insurance Fraud**
8. **Suspected Human Trafficking**

Typology

5. Suspected Financing of Terrorism

Suspected Offence	Terrorism; FT
Customer Type	Individual; Group
Industry	FI's; CU's; MVTS
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

AREAS OF FOCUS

The following areas were considered:

•THE RISKS OF FINANCING FOREIGN TERRORIST FIGHTERS

•TERRORISM OFFENCES IN TRINIDAD AND TOBAGO

• INTERNATIONAL DRIVERS - COUNTERING FINANCING OF TERRORISM

The analysis focused on the group listed on the United Nations **ISIL (Da'esh)** & Al-Qaida Sanctions List known as **AL-QAIDA IN IRAQ** also known as **ISLAMIC STATE IN IRAQ** and the **LEVANT (ISIL)** and sometimes anecdotally called the **ISLAMIC STATE IN IRAQ AND SYRIA (ISIS) OR DA'ESH.**

1. THE RISKS OF FINANCING FOREIGN TERRORIST FIGHTERS

1.1 Foreign Terrorist Fighters:

A report released by the United Nations Security Council's Counter-Terrorism Committee and its Executive Directorate (UNSCR-CTED), stressed that foreign terrorist fighters constitute *"a significant and evolving"* global threat. *"With some 30,000 foreign terrorist fighters coming from over 100 countries, terrorism is a global threat, which requires a global response."* - United Nations' S/2016/306.

Further, the United Nations Security Council Report, UN/2015/358, on the threats posed by Foreign Terrorist Fighter (FTFs), cites Trinidad and Tobago as one of three

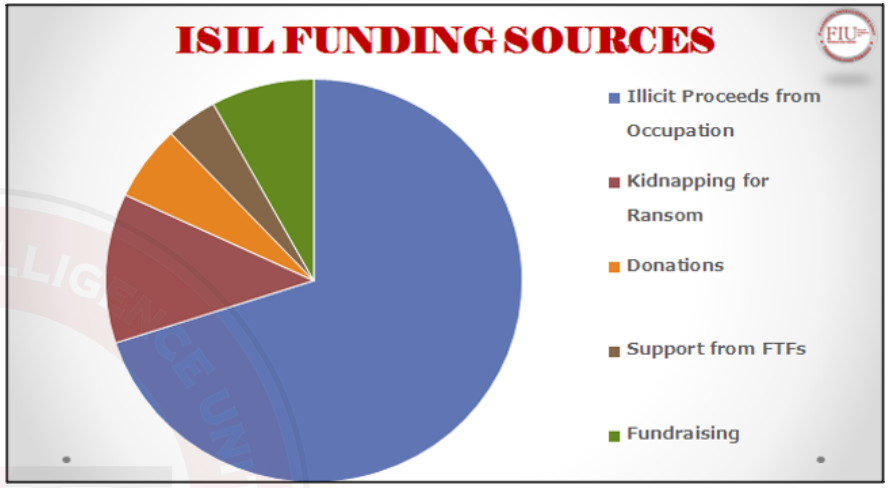
countries from which "…there are increasing flows of Foreign Terrorist Fighters…"

International studies on the phenomenon have revealed that a number of terrorist attacks in several countries have been perpetrated by returning FTFs, as well as by individuals whose attempts to travel to the conflict zones in Syria / Iraq were unsuccessful. For this reason, understanding the role of 'money/finance' can provide new intelligence since it is not unlikely that ISIL-inspired individuals seeking to reach the conflict zones to join terrorist groups would use similar methods and techniques to finance their travel.

1.2 ISIL/Da'esh Funding: ISIL/Da'esh's vast amount of revenue is from recurring sources generated internally. Unlike most Terrorist Organizations, ISIL/Da'esh's funding is generated within the vast territory in Iraq and Syria where it currently operates. Most of the group's revenue comes from occupation of the territory e.g. Oil, Bank Looting, Extortion, Taxes on goods, and from the local population.

Estimates are that oil yields USD 500 million per year; extortion and taxation– USD hundreds of millions and looting of bank vaults, e.g. Central Bank in Mosul bank vaults – USD 400 million. **Diagram 2** below depicts the breakdown of major sources of funding for ISIL/Da'esh.

DIAGRAM 2
MAJOR SOURCES OF FUNDING FOR ISIL/DA'ESH



The images in **Diagram 3** are from actual terrorist attacks in various countries, which resulted in hundreds of deaths and serious injuries perpetrated with the support of FTFs.

DIAGRAM 3

TERRORIST ATTACKS IN VARIOUS COUNTRIES

2. TERRORISM OFFENCES IN TRINIDAD AND TOBAGO

*2.1 What is a Terrorist Act? Part I of the Anti-Terrorism Act, Chapter 12:07 (ATA)***:*

An act committed in or outside of Trinidad and Tobago, which causes or is likely to cause -

- Loss of human life or serious bodily harm;
- Damage to property; or
- Prejudice to national security or disruption to public safety including disruption in the provision of emergency services or to any computer or electronic system or to the provision of services directly related to banking, communications, infrastructure, financial services, public utilities, transportation or other essential infrastructure.

These acts are committed with the objective of advancing a political, religious, or ideological cause and is intended to compel governments to do, or not do an act, or to intimidate the public.

***Since the completion of this typology, the ATA has been amended. The changes can be found at: https://agla.gov.tt/anti-terrorism-unit/legislation/atu-legislation/.

2.2 Terrorism Offences created under Part II of the ATA

- Participating in the commission of a terrorist act;
- Providing financial or other services;
- Collecting, using, providing or allowing the use of property or devices to commit a terrorist act;
- Supporting – provides expertise, false documents, assistance to enter or remain in a country;
- Providing instruction or training;
- Recruiting;
- Concealing or habouring a person who committed or is planning or is likely to commit terrorist acts;
- Dealing with terrorist property.

2.3 Financing of Terrorism Offences created under Part IIIA of the ATA:

The offence of financing of terrorism is to wilfully provide or collect funds, or attempt to do so by any means, directly or indirectly with the intention or knowledge that the funds are to be used:

- in order to carry out a terrorist act;
- by a terrorist; or;
- by a terrorist organization.

INTERNATIONAL DRIVERS - COUNTERING FINANCING OF TERRORISM

3. INTERNATIONAL DRIVERS - COUNTERING FINANCING OF TERRORISM

3.1 International Conventions

There are over nineteen international conventions and protocols against Terrorism and Terrorism Financing including the International Convention for the Suppression of the Financing of Terrorism Convention (1999) and the regional Inter-American Convention Against Terrorism (2002).

3.2 United Nations Security Council Resolutions

- ***UNSCR 1267/2253***

The Terrorist Sanctions List made by the United Nations Security Council under Resolutions 1267/1989 now includes the Islamic State in Iraq and the Levant (ISIL/ Da'esh) and this 1267 list has been renamed to the "ISIL (Da'esh) & Al-Qaida Sanctions List."

By resolution 2253 (2015), the Security Council imposes individual targeted sanctions (on assets freeze, travel ban and arms embargo) upon individuals and entities designated on the ISIL (Da'esh) & Al-Qaida Sanctions List.

States are required to "move vigorously and decisively" to cut the flows of funds and other financial assets and economic resources to individuals and entities on the "1267/2253" Sanctions List.

- ***UNSCR 2178***

UNSCR 2178 focuses on tackling the threat of FTFs in Iraq and Syria by requiring States to take action to 'prevent their radicalization, recruitment and travel'. States are

required to criminalise financing the travel of individuals who travel to a State, other than their State of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. The strategy should include measures to:

- Gather information on potential and known FTFs;
- Disrupt – stop proposed travel of FTFs;
- Prevent – strategies to counter extremism;
- Rehabilitate, prosecute or monitor FTFs;
- Propose recruiters or facilitators of FTFs for listing.

UNSCR 1373

Countries are expected to:

- Prohibit & criminalize the willful provision or collection of funds;
- Freeze without delay funds and other financial assets or economic resources of Terrorists and those who fund Terrorists.

3.3 Financial Action Task Force (FATF) Recommendations

- Recommendation 1 - Identify, assess, and understand while there is no single pathway to radicalization and becoming an FTF, the decision-making and action phases associated with FTFs follow the same basic pattern. For the purposes of its analysis, the FIUTT used the framework identified in Diagram 3 below in its examination of FTF profiles.
- Recommendation 5 - Criminalize terrorist financing, criminalize financing of terrorist acts even in the absence of a link to a specific terrorist act(s);
- Recommendation 6 – Implement a targeted financial sanctions regime to prevent & suppress terrorism and terrorist financing.

In October 2015, the FATF revised the Interpretive Note to Recommendation 5 to clarify that Recommendation 5 requires countries to criminalize financing the travel of individuals who travel to a State other than their State of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

SCAM Alert

6. STOP - Scams Initiated Online

Suspected Offence	Fraud
Customer Type	Individual; Group
Industry	FI's; CU's; MVTS
Channel	Electronic
Jurisdiction	Local; Foreign

In 2016, the Financial Intelligence Unit of Trinidad and Tobago alerted the public of a continuing trend in 'scams' initiated primarily through the Internet. Scam techniques change constantly but retain one common feature – victims are led to believe that they have a chance to obtain a large financial benefit in return for a small up-front payment.

Some scams observed involve FAKE lottery winnings, conferences, inherited wealth, business opportunities, internet romances, work permit assistance and job offers. Citizens of Trinidad and Tobago including senior citizens have fallen victims to these scams and have lost considerable sums.

Anyone who is aware of fraudulent scams should report it immediately to:

The Trinidad and Tobago Police Service, Fraud Squad
Telephone: 1(868) 625-2310; 1(868) 623-2644 and 1 (868)652-8594 or Email: **fraud@ttps.gov.tt.**

DIAGRAM 4
FIU SCAM ALERT

Typology

7. Suspected Insurance Fraud

Suspected Offence	Fraud; Forgery
Customer Type	Individual; Group
Industry	Insurance
Channel	Cheque
Jurisdiction	Local

Mr. X has an insurance policy issued for his motor vehicle, TDI 1234, from Insurance Company "A". Mr. X then proceeds to obtain additional insurance policies on the same vehicle from Insurance Company "B" and Insurance Company "C". These three insurance policies are all "fully-comprehensive" and all are insured for the same period.

Mr. X. subsequently produces a claim to Insurance Company "A" for his vehicle which was purportedly involved in a motor vehicular accident. Photographs are provided to show the extent of damage to the vehicle and are submitted along with a copy of the Police Report and an estimate for repairs from an auto-body shop. Insurance Company "A" deems the vehicle unrepairable and as such categorised as being "written-off" and proceeds to make a cheque payment to Mr. X.

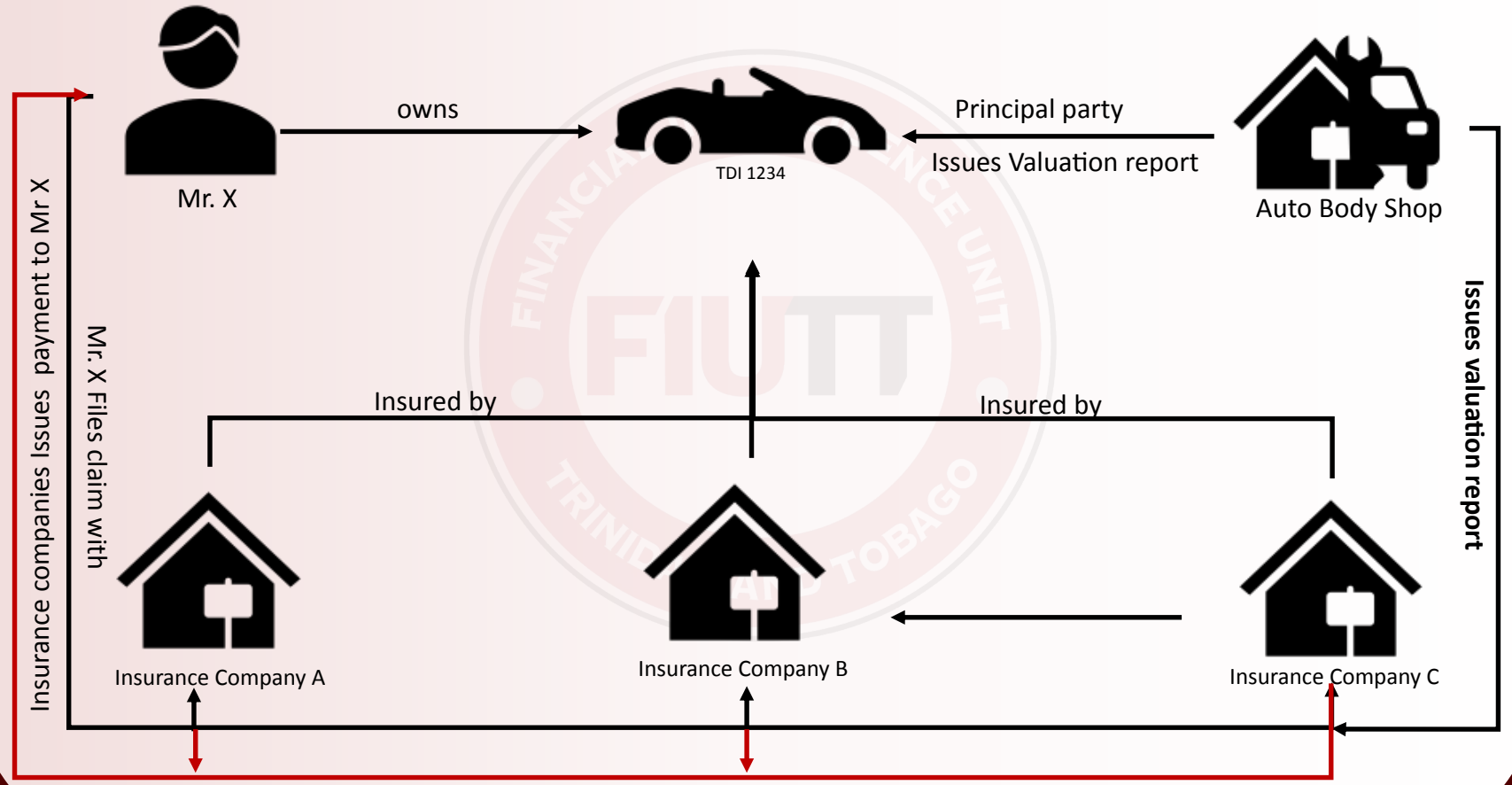
Mr. X then proceeds to file the identical claim to Insurance Company "B" and Company "C" with the same accompanying documents. Both Insurance Companies "B" and Company "C" also deem the vehicle unrepairable and "written-off" and both proceed to make payments to Mr. X via cheques. Further analysis reveal that Mr. X is in collusion with other parties including Auto-body Shop "Z" where the repair estimates were issued and the valuation provided by the auto-body shop was also deemed to be overestimated. **Diagram 5** illustrates the fraudulent technique.

Suspicious Indicators

- Insurance policies taken out from different insurance companies on the same vehicle;
- Claims submitted to the different insurance companies for damages to the vehicle arising from the same accident; and
- Cheques received from several companies.

DIAGRAM 5

SUSPECTED VEHICLE INSURANCE FRAUD



Typology

8. Suspected Human Trafficking

Suspected Offence	Human Trafficking
Customer Type	Individual; Group
Industry	FI's; CU's
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

Mr. X's employment record indicates that he is a low income earner and has a personal account at Bank A, which regularly maintains a very small minimum balance. He has multiple addresses and has started a business described as a 'guesthouse and bar'.

Mr. X approaches another financial institution, Bank B, with relevant supporting documents to establish a business relationship and open a business account. However, Bank B denies Mr. X's attempt to establish a business relationship due to enhanced customer due diligence measures implemented by Bank B, which took into account several risk factors including the nature of the business activities.

Within a two year period, Mr. X frequently deposited large amounts of cash in excess of 1.7 million dollars into his personal account at Bank A.

Suspicious Indicators

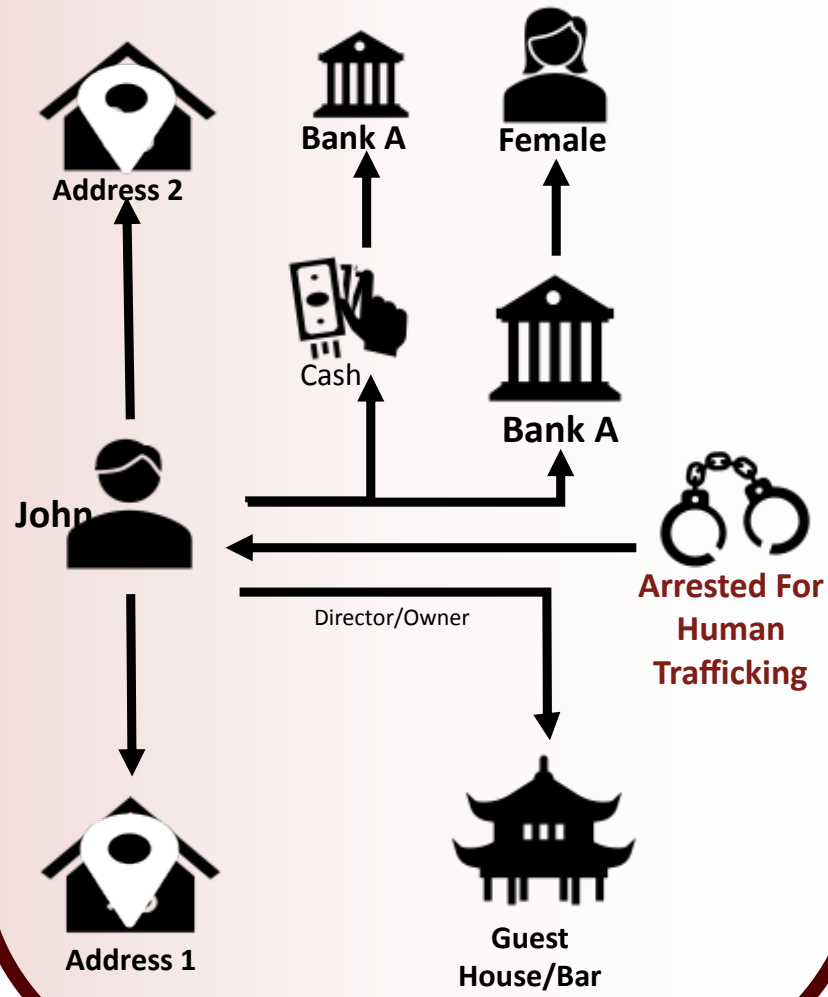
- Individuals with multiple addresses;
- Establishment of a cash-intensive business or several cash-intensive businesses;
- Financial institutions refusal to engage in a business relationship with individuals on completing its due diligence checks;
- Large, frequent cash deposits into personal accounts which normally maintained a minimum balance; and
- Frequent outgoing wire transfers to an unrelated individuals in another jurisdiction.

This amount represented an increase in cash deposits into that account of 485%. Mr. X is unable to give a reasonable explanation for the large volumes of cash deposited into his personal account and, as a result, Bank A flagged this activity and filed an STR/SAR with the FIUTT. The account balance has been reduced by frequent outgoing wire transfers to Ms. Y, an individual in an European jurisdiction and by expenditure on personal items.

Mr. X appears to be using his purported "business" as a cover for his suspected criminal activities. He also attempts to use it to integrate his criminal funds into the legitimate financial system. Mr. X was subsequently investigated, arrested and charged for human trafficking. This technique is illustrated in **Diagram 6.**

DIAGRAM 6

ILLUSTRATION OF HUMAN TRAFFICKING



2017

In the year 2017, the FIUTT noted several trends based on STRs/ SARs submission by the reporting entities including:

9. **Fraudulent Motor Vehicle Insurance Certificates/Policies**
10. **Real Property Fraud**

Typology

9. Real Property Fraud

Suspected Offence	Fraud; Forgery
Customer Type	Individual; Group
Industry	Insurance
Channel	Physical; Electronic
Jurisdiction	Local

Mr. X (Fraudster), purporting to be the owner of a parcel of land, enters into an agreement for sale of the land with Purchaser 1. As a result of this agreement for sale, Mr. X provides a copy of his deed of ownership to Purchaser 1. This deed reflects Mr. X as the owner of the said land, having purchased the land from Vendor 1. Purchaser 1 seeks the services of an Attorney-at-law who conducts title searches on the land. The title search revealed several discrepancies such as, the copy of the deed received from Mr. X, differed from the Deed held at the RGD, Land Registry and the property description of the deed received from Mr. X differed from the deed at the RGD, Land Registry. Other discrepancies noted included the signature of the Attorney-at-Law whose name and signature appears as the preparing Attorney on the copy of the Deed from Mr X appears unusual. Also, the deed to Mr. X from Vendor 1 showed an extensive time lapse between the dates of execution, payment of stamp duty and subsequent registration; and in-depth title searches suggest a series of fraudulent deeds prior to the deed to Mr. X.(**Diagram 7).**

Suspicious Indicators

Attorney's name and signature

- The signature of the attorney-at-law who purportedly prepared the deed appears unusual. The fraudulent deed contains the name of an attorney-at-law who purportedly prepared the deed and the name may be missing a letter, e.g. "John Smith" printed as "Jon Smith" (without the 'h').

Stamp Duty

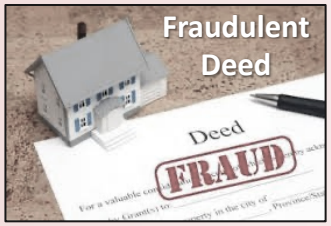
- The fraudulent deed was stamped "Adjudged not Chargeable with Any Stamp Duty" instead of an actual amount of stamp duty paid.
- Time lapse in relation to the date of the deed and date registered at the Registrar General Department
- Extensive time lapse between the execution, stamping and subsequent registration of the Fraudulent deed, e.g. a deed of conveyance for the sale dated December 04, 2012 but registered with RGD in July 2014.

Property description

- The description of the property varied from that shown in previous registered deeds.
- A series of deeds from the true owner to the purported owner
- The title search revealed conflicting deeds of conveyance from the previous owners to the person purporting to be the present owner of the land.

DIAGRAM 7

TYPOLOGY - REAL PROPERTY



Fraudulent deed registered at RGD

Attorney conducts searches & identifies anomalies in deed titles.

Shows several discrepancies

Fraudster

Subject X purported to be the property owner.

Purchaser/ Victim

Victim pays $75,000.00 downpayment.

Copy of fraudulent deed given to victim

Fraudulent deed given to attorney to conduct searches

1

Typology

10. Fraudulent Motor Vehicle Insurance Certificates/Policies

Suspected Offence	Fraud; Forgery
Customer Type	Individual; Group
Industry	Insurance
Channel	Physical; Cheque
Jurisdiction	Local

This analysis described the criminal activity of fraud in the insurance sector as it relates to fraudulent motor vehicle (MV) insurance certificates/policies purportedly issued by companies registered to carry on insurance business in Trinidad and Tobago (registered insurance company). Fraud is being committed in the MV Insurance sector as the following criminal actions have been observed:

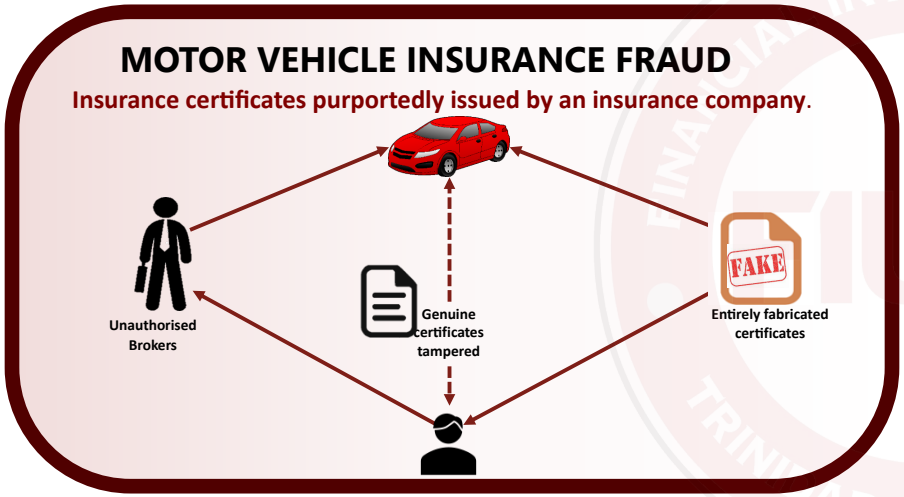
i. **Tampering with genuine motor vehicle insurance certificates or policies -** Pluto, in possession of an insurance policy for motor vehicle PDF XXX issued by Insurance Company C, is also stopped during routine road block by Law Enforcement Officers. Upon verification by Law Enforcement Officers with Insurance Company C, the policy number H3/DC/2017 is valid, however, the name of the insured and the motor vehicle registration number do not match with the company's records.

ii. **The creation of entirely fabricated motor vehicle insurance certificates or policies: -** Uranus, in

Suspicious Indicators

- The insurance company has no record of the Certificate number/Policy number/Vehicle Registration Number;
- The Certificate number/Policy number is a legitimate number but was assigned to another insured person;
- The name on the certificate is not the name of the person insured with the Insurance Company;
- Date of insurance coverage has been altered;
- The signature on the certificate/policy is not an authorised signatory for the Insurance Company; and
- The Certificate bears a Stamp with a name similar to the name of a registered Insurance Company. For example, the Insurance company is "Planet Mercury Insurance Company (Trinidad and Tobago) Limited," but the certificate stamp is "Planet Mercury Insurance Limited".

possession of an insurance policy for motor vehicle PDE XXX issued by Insurance Company B, is stopped during routine road block by Law Enforcement Officers. Upon verification by Law Enforcement Officers with Insurance Company B, the motor vehicle insurance certificate GY 00000 and policy G2/CC/2017 number for motor vehicle PDY XXX in the name of Uranus, does not exist.



iii. **The sale of motor vehicle insurance and issue of certificates and policies by unauthorised agents**. Venus produces an insurance policy for motor vehicle PDD XXX issued by Insurance Company A to prove a claim following a motor vehicle (MV) accident. Insurance Company A discovers that the motor vehicle certificate number FX 00000 bearing policy number F1/BC/2017 in the name of Venus for coverage for motor vehicle PDD XXX for the period August 2017 to August 2018 is invalid. Further checks reveal that the certificate number FX 00000 was legitimately issued to another client for a different motor vehicle. Venus informed Insurance Company A that he collected his motor vehicle insurance certificate from Mr. Zeus who claimed to be an insurance agent/broker.

Analysis has revealed that criminals hold out themselves as agents of a registered Insurance Company and fabricate documents, (on which the company's stamp and other company insignias are inscribed) and issue the fabricated documents to unsuspecting and willing customers. In the instances brought to the attention of the FIUTT, the "insured" only discovers the fraud when he/she files a claim at the Insurance Company.

2018

FIUTT noted several trends in the year 2018 based on STRs/SARs submission by the reporting entities including:

11. **Tax Evasion**
12. **Suspected Self-Funded Jihadi**
13. **Suspected Credit Funded Jihadi**

Typology

11. Tax Evasion

Suspected Offence	Tax Crimes
Customer Type	Individual; Group
Industry	FI's; MVTS; Insurance
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

This typology concerns cases where foreign nationals of Jurisdiction A, resident in Trinidad and Tobago (Jurisdiction T&T), created complex legal structures in a financial scheme to avoid payment of taxes in Jurisdiction A on income earned in Jurisdiction T&T. FIUTT's analysis of such cases revealed:

- existence of bank accounts held by nationals of Jurisdiction A in financial institutions in Jurisdiction T&T, which were unknown to Jurisdiction A;
- previous STRs/SARs on the subjects, associates and companies;
- transfers of large sums of money via wire remittance companies to associates in Jurisdiction A;
- frequent and large wire transfers out of Jurisdiction T&T by associates (both individuals and companies) of the foreign national;

Suspicious Indicators

- Financial transactions not in line with expected economic profile;
- Interconnection of seemingly independent businesses;
- Large and frequent movement of cash;
- Use of third party bank accounts e.g. Accounts of relatives,
- Use of gatekeeper to move cash through money remitters,
- Use of employees/third parties to conduct frequent and or large international wire transfers (structuring and smurfing);
- Multiple international wire transfers of large sums of cash; and
- Using 'front' companies to hide undeclared income.

- Use of the third party senders (individuals & companies) in Jurisdiction T&T, which indicated attempts to conceal and disguise the identity of the ultimate beneficiary;

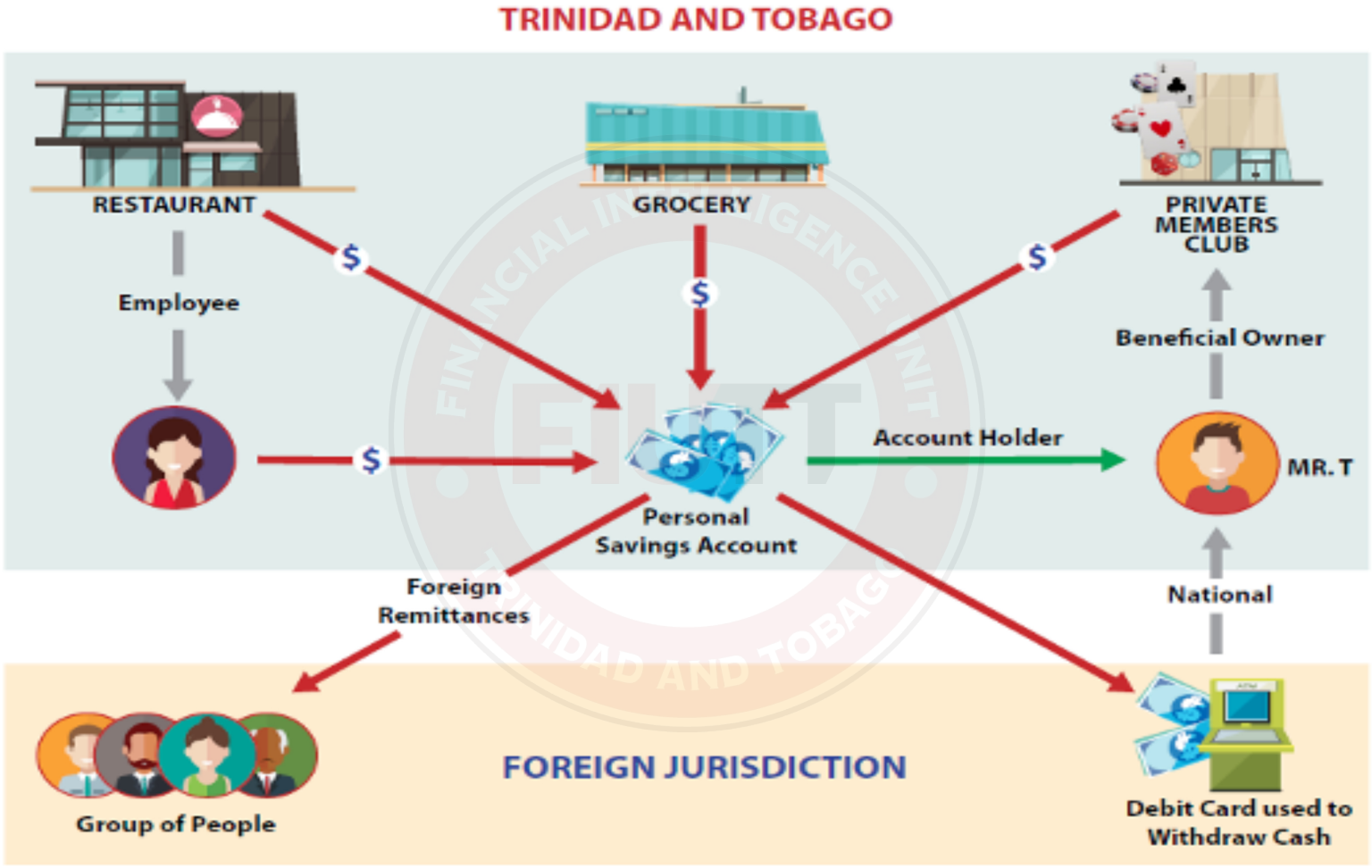
- large cash transactions such as account deposits, payment of insurance premiums and outgoing wire transfers were frequently conducted by employees of the foreign nationals in both jurisdictions; and

- movement of funds outside of Jurisdiction T&T by both individuals and companies.

In one such successful case, the subject, 'Blackjack' pleaded guilty and was sentenced to a 46-month prison term and three years of supervised release. As part of the plea agreement, 'Blackjack' was ordered to pay restitution of USD 1,286,657. 'Blackjack' has paid all of his restitution, which shows the success of this multi-jurisdiction tax investigation.

DIAGRAM 8

TYPOLOGY - TAX EVASION



Typology

12. Suspected Self-Funded Jihadi

Suspected Offence	Terrorism; FT
Customer Type	Individual; Group
Industry	FI's; CU's; MVTS
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

Subject T, a male business entrepreneur from Trinidad and Tobago in his late 20's first rose to notoriety in 2011 when he was implicated in an alleged plot to assassinate a high profile government Minister. Although Subject T was never charged for the plot, intelligence suggested that he fled to Syria in 2013 after taking part in a revenge killing. Several years later, Subject T was reported in media headlines again in 2016, when he was featured in a lengthy interview in the Islamic State of the Levant / Syria (ISIL/ISIS) Dabiq magazine in which he encouraged sympathizers to "attack the interests of the crusader coalition, including embassies, businesses and civilians."

FINANCIAL ACTIVITY:

Bank Accounts: - A review of the account activity of Subject T revealed financial accounts with little or no balances, which were generally inactive or dormant prior to late 2013. Activity was, however, observed in late 2013 and early 2014 when Subject T allegedly traveled to Syria via Turkey. Subsequent to Subject T's departure, several

Suspicious Indicators

- Currency exchanges/cash conversion days prior to the alleged departure to the conflict zone;
- Use of credit cards/debit cards to conduct cash advances in areas that lie in close proximity to conflicts zones;
- Use of numerous low value wire transfers;
- Multiple senders to a common receiver in high risk jurisdictions known for terrorist activities;
- Numerous transactions between unrelated parties;
- High levels of account activity followed by dormant or closed accounts
- Use of nominees, trusts, family members or third parties
- Use of the internet i.e. encryption, payment systems, online banking
- New payment technologies i.e. mobile phone payments and remittance systems
- Sudden sale of possessions (e.g. car, house, jewelry); and adverse media reports.

cash advances, approximately USD 1,500.00, were conducted in Turkey from a pre-paid card held in the name of Subject T.

An associate of Subject T also deposited approximately USD 4,500.00 into Subject T's account.

A relative of Subject T also conducted a stored value cash-out (over the counter transaction) withdrawal of USD 5,000.00 by order of Subject T. The purpose and destination of cash obtained by the said relative from Subject T's account remains unknown.

Pre-paid Card Purchases: - Subject T's pre-paid card was used to make purchases from Google Store for several gaming applications, which were strategy/tactical and weaponry based. Subject T also purchased Viber credit (telephone/message based application), to facilitate communication with possible associates or family members. Subject T's pre-paid card was also utilized in areas that lie in close proximity to conflict zones along the Turkey/Syrian border.

The travel footprints of Subject T, corroborated the existence of a known route utilized by suspected foreign terrorist fighters. Intelligence received by the FIUTT also indicated that Subject T sold all his valuables such as motor vehicle and television for cash in an attempt to raise funds to facilitate the travel to Syria.

Money Value Transfers: - During the years 2009 to 2011, Subject T sent several transactions, approximately under USD 1,000.00, to several individuals located in an African and Middle Eastern country. It was also observed that Subject T formed part of a network of individuals across Trinidad and Tobago who were sending wire transfers to countries located in Asia, Africa, the Middle East, the United Kingdom, the Caribbean, South America and North America. It is estimated that approximately USD 6,000.00 was conducted by Subject T and the network to persons for unknown purposes and with whom there was no determinable legitimate business association or family relationships.

Online Presence: - Subject T was also a central figure seen in videos and various media prints issued by or on behalf of ISIL/ISIS. Subject T was described as a sniper and an English Propagandist for ISIL/ISIS and was tasked with encouraging sympathisers to "attack the interests of the crusader coalition," including embassies, businesses and civilians in Trinidad and Tobago as well as several foreign jurisdictions.

Inference: - Subject T's close affiliation with an alleged facilitation network to transfer funds to persons within the high-risk Middle-Eastern jurisdictions and surrounding African territories with known affiliations to ISIL/ISIS in conjunction with Subject T's alleged participation in

terrorist activities in Syria and affiliation to other individuals suspected of traveling to join ISIL/ISIS point to the possibility of terrorism and the FT.

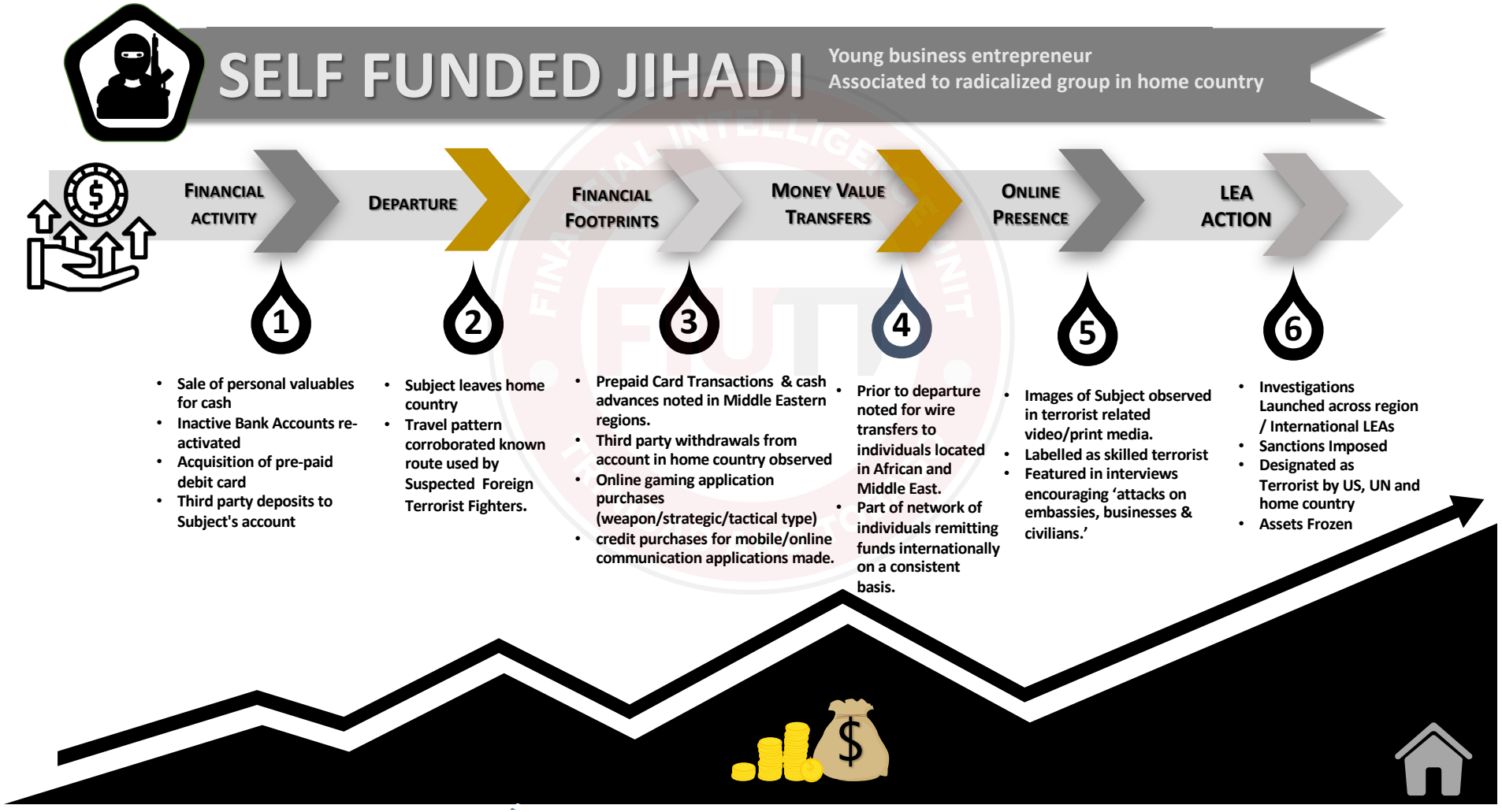
Case Result: - The U.S. Department of the Treasury listed Subject T on the Office of Foreign Assets Control, Specially Designated Nationals List in March 2017.

Subject T was listed an individual under the United Nations Security Council 1267 ISIL (Da'esh) & Al-Qaida Sanctions list in August 2017 for being associated with ISIL or Al-Qaida for "participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name if, or on behalf of, or in support of", "recruiting for", "otherwise supporting acts or activities of" and "other acts or activities indicating association with" Islamic State in Iraq and the Levant (ISIL).

The High Court of Trinidad and Tobago also declared Subject T as a listed Entity in Trinidad and Tobago and ordered that all his funds be frozen pursuant to the provisions of the Anti-Terrorism Act, Chap. 12:07 in 2017.

DIAGRAM 9

TYPOLOGY - SELF FUNDED JIHADI



Typology

13. Suspected Credit Funded Jihadi

Suspected Offence	Terrorism; FT
Customer Type	Individual; Group
Industry	FI's
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

Subject A, a male national of Trinidad and Tobago in his mid-thirties, was identified as being linked to a group of persons suspected of leaving Trinidad and Tobago to participate in suspected terrorist activities in support of the Islamic State of the Levant / Syria (ISIL/ISIS).

In 2014, it is believed that Subject A along with close members of his family journeyed to Syria and aligned themselves with the Islamic State terrorist group. Subject A, a skilled worker, was affiliated with a masjid suspected of embracing a radicalised ideology.

Print and news media published articles about individuals suspected of travelling to the conflict zone, which resulted in financial institutions conducting proactive monitoring. Subsequently, Suspicious Transaction/Activity Reports (STRs/SARs) were submitted to the Financial Intelligence Unit of Trinidad and Tobago (FIUTT).

Suspicious Indicators

- Application of small loans and withdrawing the funds in CASH shortly before departure;
- Currency exchanges/cash conversion days prior to the alleged departure to the conflict zone;
- Use of credit cards debit cards to make travel related purchases (airline and accommodation) along a suspected transit route utilized by suspected foreign terrorist fighters and their family members;
- Evidence of 'broken travel';
- Cash withdrawals at ATMs in recognized 'hotspots' in border areas close to conflict zones;
- Sudden depletion/closure of accounts via cash withdrawals;
- Use of nominees, trusts, family members or third parties;
- Use of the internet i.e. encryption, payment systems, online banking; and adverse media reports.

FINANCIAL ACTIVITY:

Acquisition of Credit Facilities: - Analysis conducted by the FIUTT revealed that several months prior to Subject A's alleged departure to Syria, he obtained two (2) loans from a financial institution for USD 30,000.00 and a credit card with a limit of USD 15,000.00. Subject A withdrew USD 15,000.00 in cash a week before his alleged departure.

Financial Footprint: Subject A utilised credit to purchase several airline tickets to European, South American and Central American destinations. Credit card usage was also observed for living expenses (hotel accommodation and food) along this route as well as an attempted cash withdrawal in Turkey.

Online Presence: Various online articles and videos portrayed images of Subject A receiving training in the use of high powered rifles and appearing in images in the ISIL/ISIS magazine 'DABIQ'.

Inference: Transactions conducted by Subject A indicated that he may have travelled to known terrorist jurisdictions and may have been financed by associates. The transactions highlighted also revealed that jurisdictions in Central America, South America, Caribbean countries and Europe are suspected transit routes for persons attempting or intending to travel to Syria to engage in terrorist or terrorist related activities.

Case Result: - A report was forwarded to the relevant Law Enforcement Authorities for investigation as well as a recommendation being sent to the Office of the Attorney General to have Subject A designated as a terrorist and his assets frozen.

Information pertaining to the activities and travel patterns of Subject A was spontaneously disclosed/requested to/ from FIU's in the Caribbean, Central America and Middle Eastern jurisdictions in which financial activities, online purchases and travel were observed.

Analysis conducted by the FIUTT also produced two Strategic Analysis Reports in:

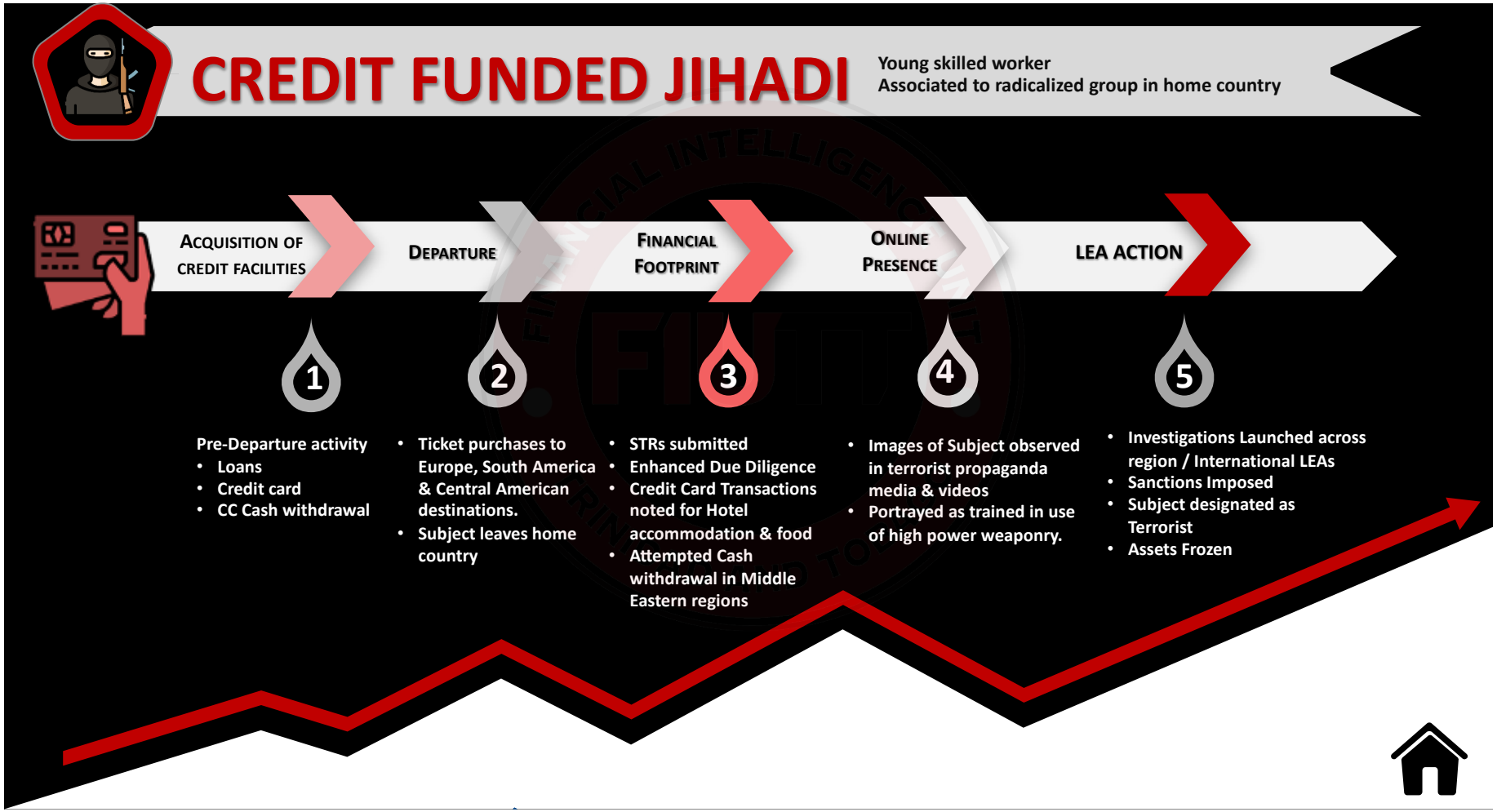
(1) 2015 - "Suspected Foreign Terrorist Fighters - Travel Routes and Indicators" and,

(2) 2017 - "Suspected Foreign Terrorist Fighters and their Facilitation Networks."

These reports were shared with Foreign FIUs and Law Enforcement Authorities. Redacted versions were also shared with Financial Institutions and other Supervised Entities, the Regulatory Authority and members of the public.

DIAGRAM 10

SUSPECTED CREDIT FUNDED JIHADI



2019

In the year 2019, the FIUTT noted several trends based on STRs/ SARs submission by the reporting entities including:

14. **Suspected Tax Evasion**
15. **The Suspected Abuse Of Non-Profit Organizations relative to the Financing Of Terrorism**
16. **Rise in Email Compromise**
17. **Foreign Nationals 'Suspected' Involvement In Organised Criminal Activity**
18. **Suspected Government Fraud**

Typology

14. Suspected Tax Evasion by Foreign Nationals

Suspected Offence	Tax Crimes
Customer Type	Individual; Group
Industry	FI's
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

This typology concerns cases where foreign nationals, domiciled in Trinidad and Tobago exploit the financial system to evade payment of the requisite taxes in Trinidad and Tobago. Income earned in Trinidad and Tobago is remitted to the homeland of the foreign nationals under the façade of the repatriation of funds to their diaspora. FIUTT's analysis of such cases revealed the following:

- Existence of cash-intensive companies incorporated within Trinidad and Tobago where the foreign Nationals are the principal parties and/or beneficial owners;
- Existence of bank accounts held by nationals of foreign jurisdictions in financial institutions within Trinidad and Tobago;
- Cash in TTD and USD currencies which represent business proceeds being deposited into the personal accounts of the foreign nationals;
- Frequent and large wire transfers out of Trinidad and

Suspicious Indicators

- Use of pre-dominantly cash intensive businesses;
- Multiple accounts being opened by foreign nationals;
- Co-mingling of funds;
- Frequent, large wire transfers to the home jurisdiction of the account holder for various personal expenses;
- Use of third-party individuals to deposit funds and transfer the same to accounts held or controlled by the foreign nationals;
- Reluctance or burst of aggression when asked to provide supporting documentation;
- Accounts appear to be used as a temporary repository; and
- Accounts are opened and closed in quick succession at various financial institutions; and
- Credit/debit cards being utilized in the foreigners home jurisdiction by a third party despite the foreigner being domiciled in Trinidad and Tobago.

Tobago to the homeland of foreign nationals with stated purposes such as: “gift for family”, “medical”, “to help build house” and “living expenses”.

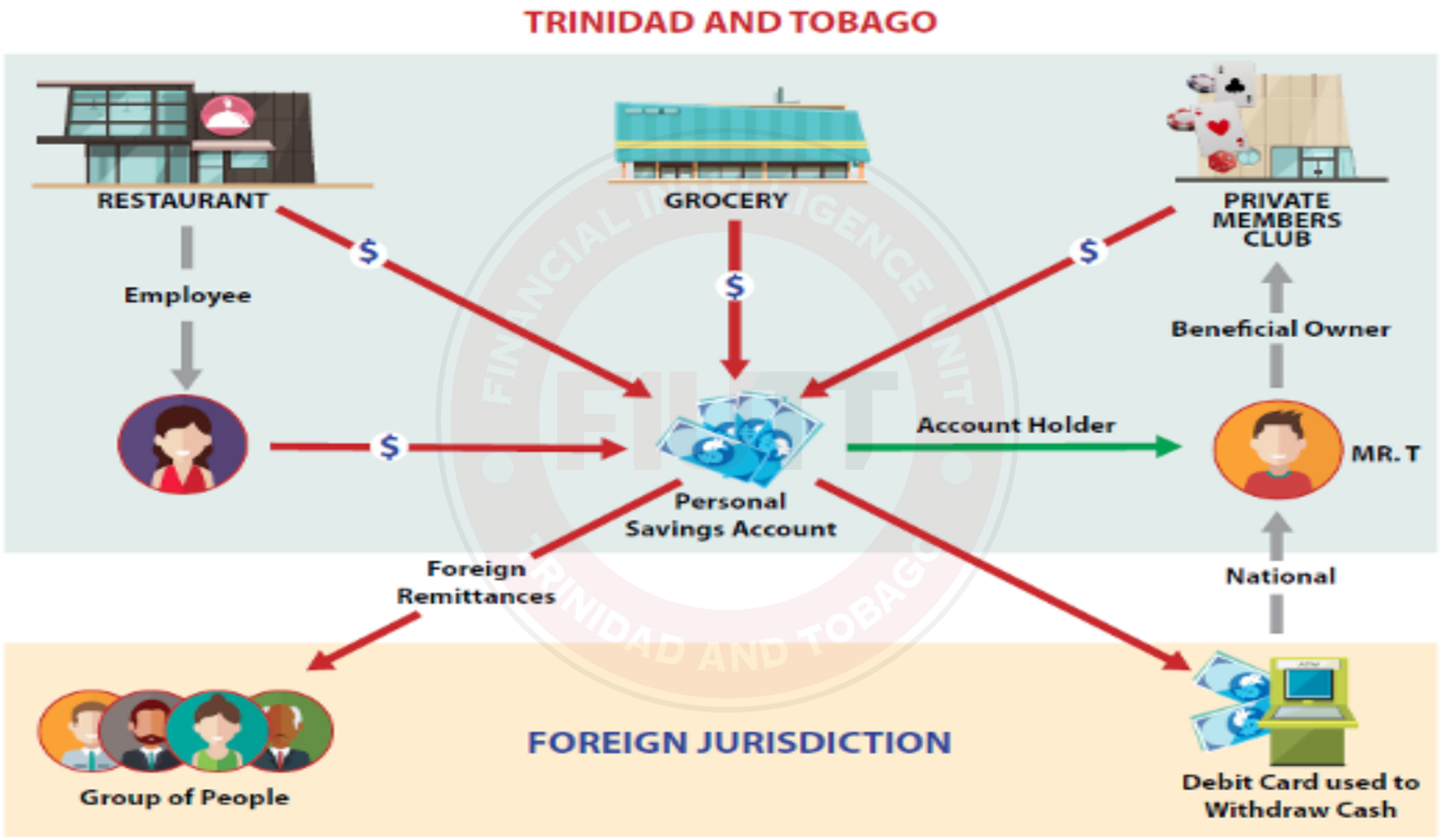
- Use of third party to remit funds to the homeland of foreign nationals. In a number of cases, employees of cash-intensive companies were used to open accounts and remit funds to foreign jurisdiction through their personal accounts;

- Unwillingness by the foreign nationals to provide information regarding the transactions and updated Know Your Customer (KYC) information when requested by the financial institutions;

- Excessive volume and frequency of ATM cash withdrawals being conducted in foreign jurisdictions while the card holder appear to be in Trinidad and Tobago; and short timeframe between the date the account was opened and the date it was closed.

DIAGRAM 11

SUSPECTED FOREIGN NATIONALS TAX EVASION



Typology

15. The Suspected Abuse of Non-Profit Organizations relative to the Financing of Terrorism

Suspected Offence	Financing of Terrorism
Customer Type	Individual; Group
Industry	FI's
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

A faith-based charitable organisation ("the NPO") was established to fund the renovation of local places of worship of the same faith as the NPO. Accounts were opened at Bank A to facilitate collection of donations from local persons of the same faith. The NPO subsequently conducts fund-raising activities in order to assist victims of natural disasters in foreign jurisdictions. Cash deposits to the NPO's account at Bank A increased exponentially. The NPO partnered with foreign agencies to provide relief to persons affected by natural disasters. Funds were subsequently remitted from the NPO's account to foreign agencies.

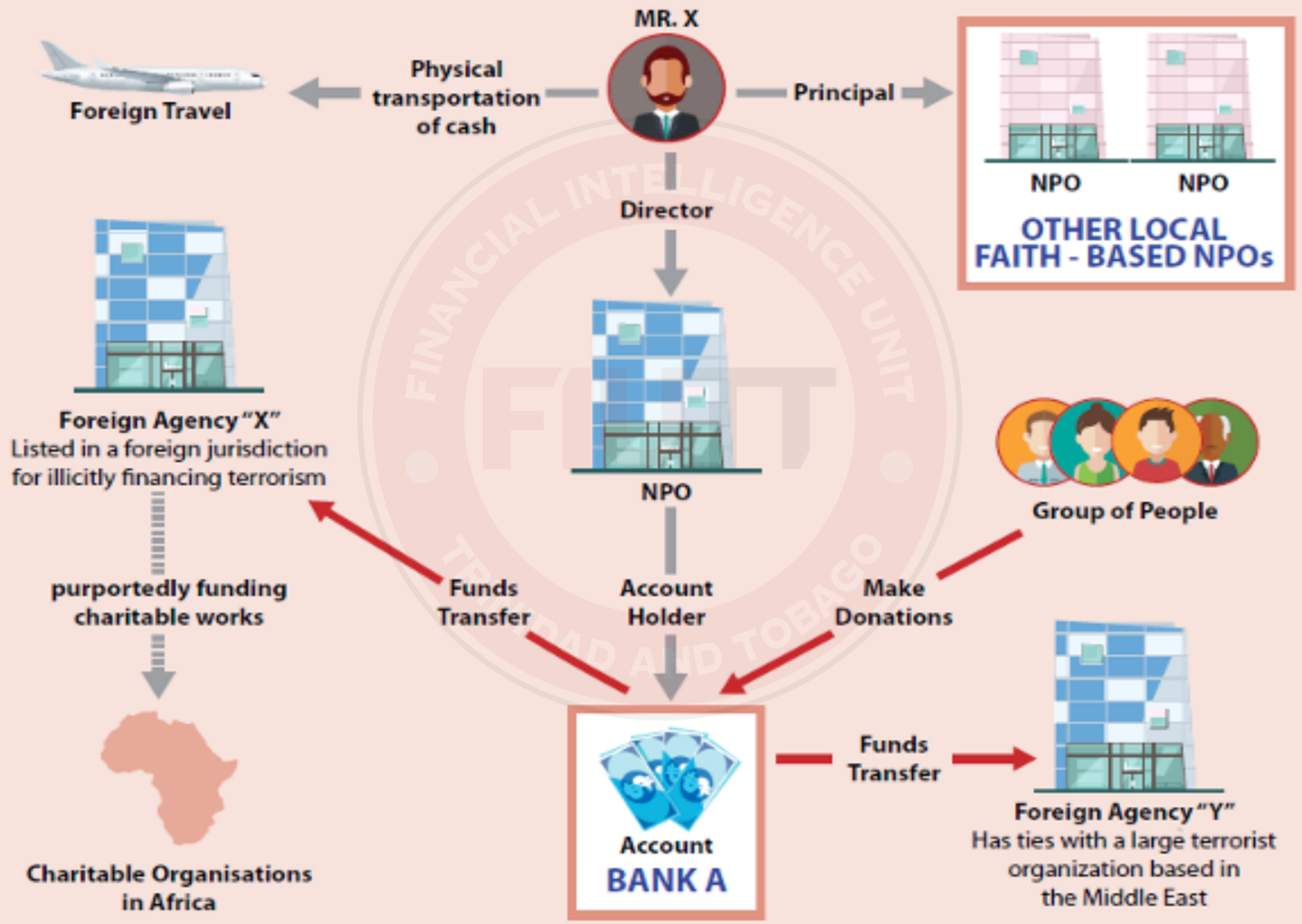
Ensuing fund transfers were declined by Bank A as a result of due diligence conducted which revealed that the foreign agencies were linked to suspected global terrorist organisations. It was later revealed that the director of the NPO was also linked to several other NPOs within Trinidad and Tobago and later identified as travelling internationally from Trinidad and Tobago with large amounts of cash on his person. The ultimate destination and/or beneficiary of these funds could not be verified.

Suspicious Indicators

- Significant cash deposits within a short period of time where the true source and legitimacy of the source(s) cannot be determined;
- The NPO's accounts are used to conduct suspicious or large, complex or unusual transactions;
- One of the foreign agencies being from a country listed as a high risk jurisdiction by the FATF;
- Large wire transfers to foreign agencies whom are suspected of being involved in the financing of terrorism; and
- Official of the NPO travelling to foreign jurisdictions with large amounts of foreign currency on his person circumventing the tracing of funds via the financial system.

DIAGRAM 12

SUSPECTED NPO ABUSE FOR FINANCING OF TERRORISM



Advisory

16. Rise in Email Compromise

Suspected Offence	Fraud
Customer Type	Individual; Group
Industry	Fis, CUs, Insurance
Channel	Electronic
Jurisdiction	Local; Foreign

The Financial Intelligence Unit of Trinidad and Tobago ("the FIUTT") is publishing this Advisory in accordance with Section 17(1) (b) of the Financial Intelligence Unit of Trinidad and Tobago Act.

PURPOSE OF THIS ADVISORY

This Advisory is intended to provide Financial Institutions (FI's) (in particular commercial banks), Listed Businesses (LB) and members of the public to exercise caution when handling email payment instructions for business transactions and large value personal foreign currency transactions, in order to reduce monetary loss and emotional harm.

GENERAL INFORMATION

The FIUTT has noticed an increase in cases of individuals and businesses falling victim to social engineering tactics such as email phishing.*** For the period December 2017 to December 2018, several businesses and individuals lost funds in excess of TT$2.5 Million in foreign currency

Suspicious Indicators

- Scrutinise documents thoroughly for any errors, missing information and alterations;
- Read emails carefully as fraudulent email messages often contain misspellings or poor grammar;
- Any new email instructions to transfer funds to a different beneficiary with a different address and banking account information from what was previously known, requires FIs and MVTS providers to conduct enhanced due diligence for suspicious payment instructions; and
- Conduct Customer Due Diligence or if in doubt, Enhanced Due Diligence, contact the sender of the email by telephone to verify the information before sending any money to the 'named' beneficiary.

transactions to cybercriminals through social engineering tactics.

Social Engineering techniques are used to manipulate financial institutions and members of the general public to unknowingly install malware onto their computers, workstations or wireless devices. This is an effort to compromise and steal personal sensitive information such as emails and other online account login credentials.

Once social engineering attackers get access to the account, they can then monitor emails, intercepting those that contain an invoice or a payment instruction to a Financial Institution (FI) or Money or Value Transfer Services (MVTS) provider.

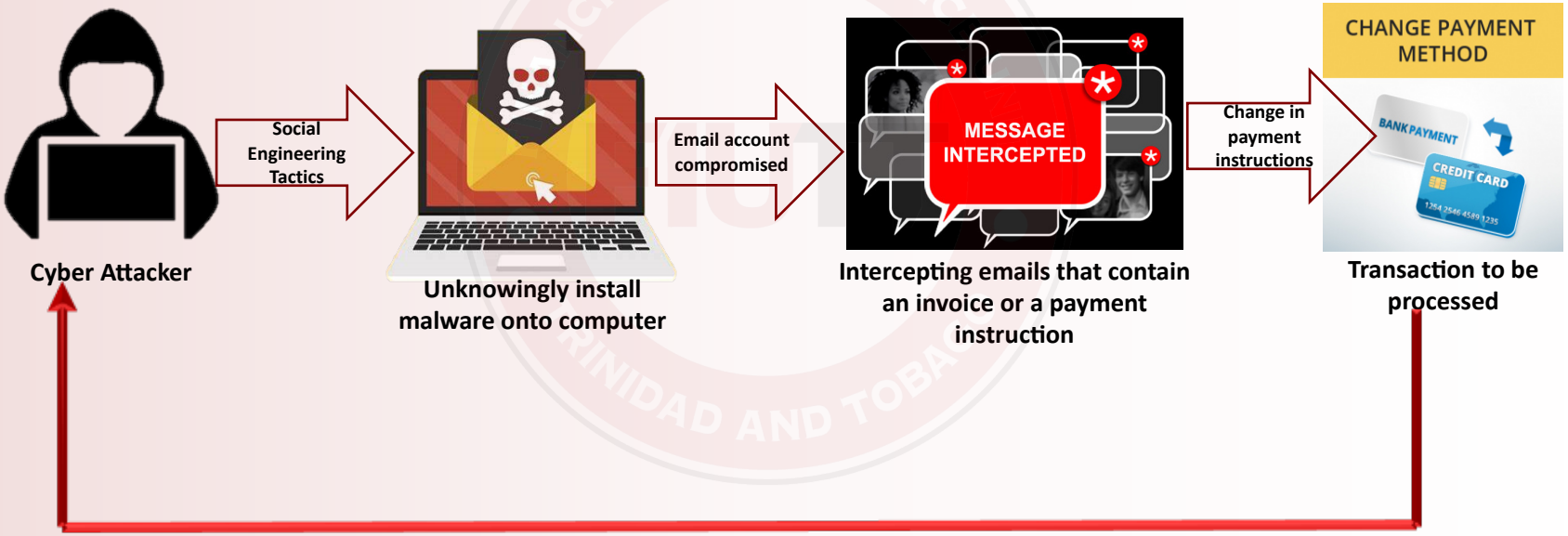
Social engineering attackers can now change the payment instructions on a specific invoice or planned transaction. This allows the transaction to be processed with the funds going to a bank account of a cybercriminal group instead of the intended and rightful beneficiary.

***Phishing remains one of the main social engineering techniques used on the Internet to steal ID-related nformation for fraudulent use. Variations include "SMiShing" (mobile phone text messages to seek the disclosure of information) and "spoofing" (a person or programme is masquerading as somebody or something else to gain trust and make them enter their details into a counterfeit website). http://www.coe.int/moneyval

DIAGRAM 13

TYPOLOGY - RISE IN EMAIL COMPROMISE

HOW IT WORKS



Transaction to be processed with the funds going to a bank account of a cybercriminal person/group instead of the intended and rightful beneficiary.

Advisory

17. Foreign Nationals 'Suspected' Involvement In Organised Criminal Activity

Suspected Offence	Organised Crime Group
Customer Type	Individual; Group
Industry	FI's, MVTS
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

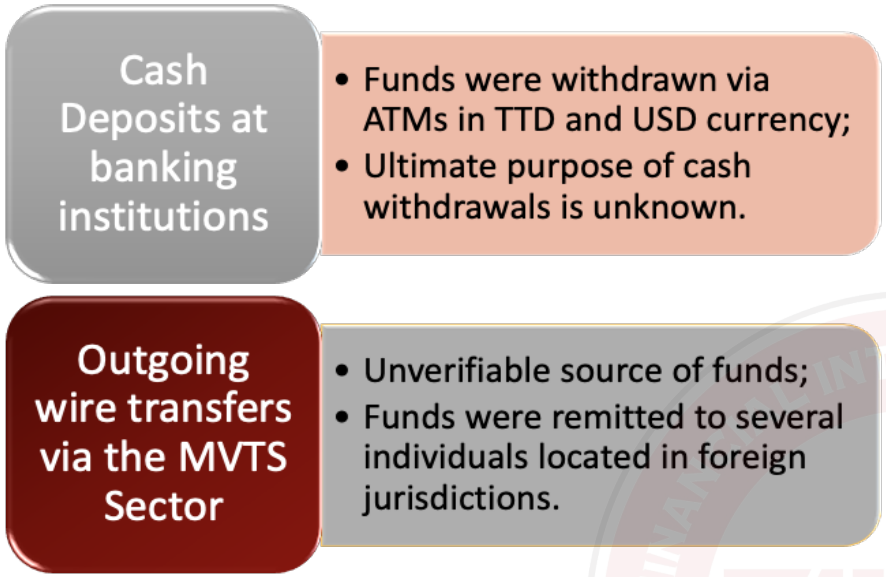
The FIUTT has noticed a sharp increase in the number of foreign nationals suspected involvement in suspected organised criminal activity in Trinidad and Tobago. Criminal activity referred to in this case, incorporates illicit trafficking in narcotics, illicit arms trafficking, trafficking in human beings and ML.

During the period January 2016 to September 2018, Foreign Nationals, were identified as being involved in suspicious financial activities; of which the total suspicious dollar value of these transactions amounted to approximately TTD 6 million. The suspicious activity is categorised and highlighted in the following diagram.

Suspicious Indicators

Patterns of financial transactions and account activity indicators

- Outgoing international wire transfers to persons where there exists no identifiable business link nor any discernible family link;
- Customers making regular international funds transfers of significant values to jurisdictions with a high-risk for the narcotic trade;
- Multiple customers conducting international funds transfers to the same overseas beneficiary and/or to persons located in the same geographic region;
- Customers working together to break up one transaction into two or more transactions.
- Frequent cash-in and cash-out activity on accounts;
- Unverifiable source of funds for high-value cash deposits and
- Excessive USD ATM withdrawals.



The source of the cash deposited into accounts held at banking institutions and funds wire transferred could not be verified and there exists the high possibility that these funds may have originated from organised criminal activity. Similarly, the purpose of the cash withdrawals and outgoing wire transfers could not be substantiated. In addition, the immigration status of some of the Foreign Nationals could not be verified.

Typology

18. Suspected Government Salaries Fraud

Suspected Offence	Fraud
Customer Type	Individual; Group
Industry	FI's; MVTS
Channel	Physical; Electronic; Cheque
Jurisdiction	Local

The case involves an organised criminal network comprising government employees at government agencies, X1, Y2 and Z3 agency. The criminal network also included persons who were subsequently identified as relatives and close associates of the government employees, as well as, shell structures, which were established by persons within the criminal network. The main subject was a payroll officer at government agency X1.

The typology is characterised by falsification/manipulation of the government agency's payroll (at X1) and the movement of funds from the accounts of X1 government agency to several accounts in the names of the government employees, shell structures and to the accounts controlled by the payroll officer employed at X1 government agency. The movement of funds from X1's account to the beneficiary accounts were disguised as 'salary payments'.

Suspicious Indicators

- Fictitious or 'ghost' employees in receipt of a salary;
- One individual receiving numerous salary payments in several bank accounts;
- Several individuals utilising the same bank account number to receive salary;
- Accounts used as a temporary repository for funds;
- Accounts with a high volume of activity and low balances;
- Deposits into accounts are followed by near and/or immediate withdrawals;
- Amount of funds channelled through the accounts does match the occupation;
- Collusion of staff members to circumvent or override payroll systems; and
- Manipulation or altering of cheque signatures to make payments.

Through the manipulation of payroll information by the payroll officer at X1, unauthorised 'salary payments' were moved from X1 payroll account to: 1) multiple personal accounts, 2) to multiple (personal) loan accounts, and 3) several accounts of 'shell' structures. The affiliates of the criminal network were also listed as 'controllers' of the shell structures. The criminal network beneficiary accounts were held at multiple financial institutions (FIs). The movement of the misappropriated funds were deposited as automated clearing house (ACH) salary credits.

The criminal activity identified in this case were conspiracy to defraud, falsification of accounts and unauthorised payment of salaries. Analysis showed that:

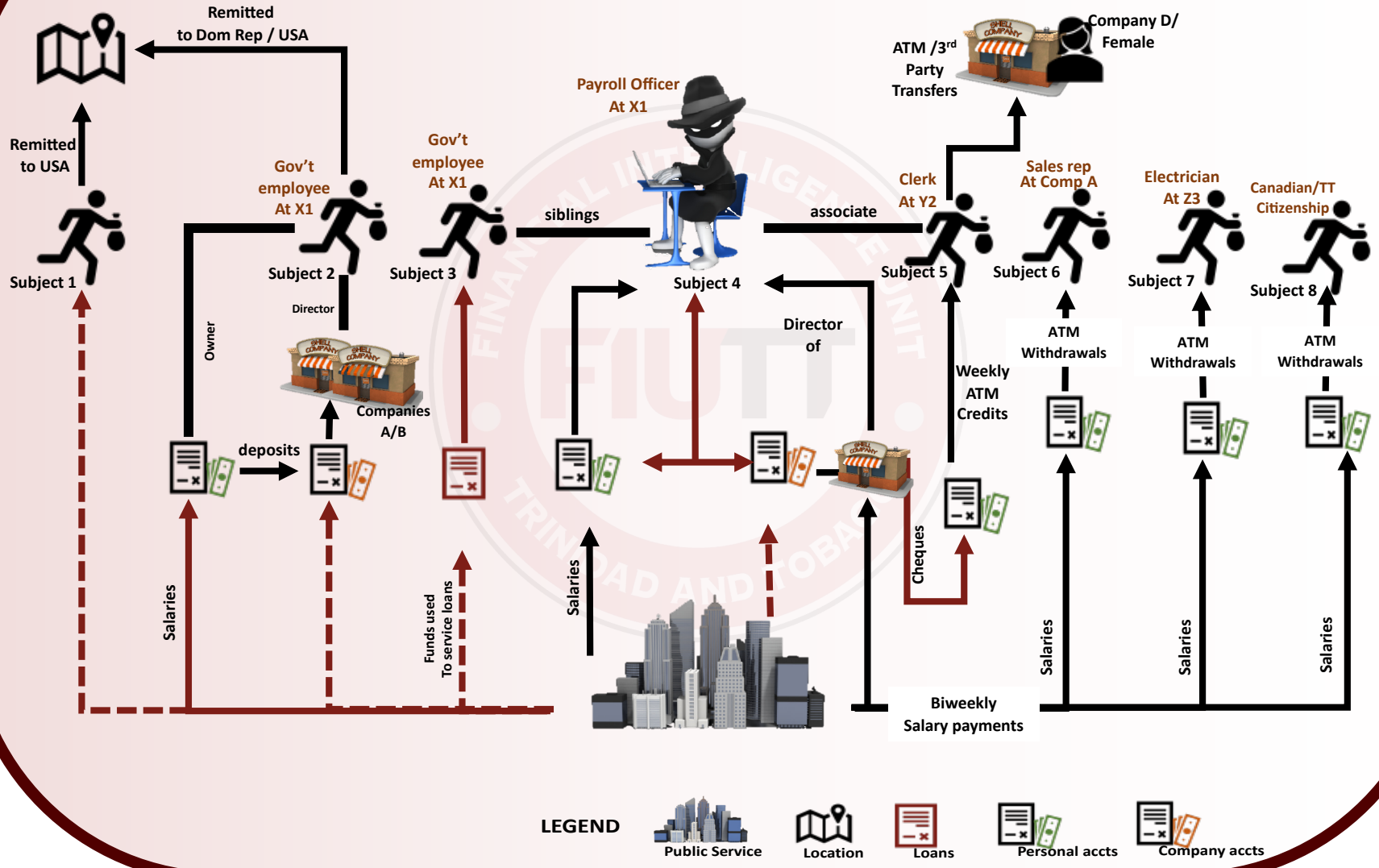
- Unauthorised persons/persons not employed at government agency, X1, were in receipt of fortnightly or weekly salaries from X1;
- At least two years prior to the movement of the unauthorised funds, persons linked to the criminal network registered multiple **shelf or ***front companies and established personal accounts at multiple FIs to facilitate/coordinate the scheme;
- The balances on the payroll officer's accounts, were minimal compared to the amount of funds which passed through the account;
- Loan balances on accounts held by the persons within the criminal network were paid-off long before the expected dates;
- One Subject in the criminal network is suspected to have laundered over TTD 3 million from his account, illicitly obtained from X1; and
- Two Subjects in the criminal network were flagged for remittance of funds to countries high risks for human trafficking.

**Shelf company – incorporated company with inactive shareholders, directors, and secretary and is left dormant for a longer period even if a customer relationship has already been established (Concealment of Beneficial Ownership, FATF, 2018).

***Front company – fully functioning company with the characteristics of a legitimate business, serving to disguise and obscure illicit financial activity (Concealment of Beneficial Ownership, FATF, 2018).

DIAGRAM 14

GOVERNMENT SALARY FRAUD TYPOLOGY



2020

FIUTT noted several trends in the year 2018 based on STRs/SARs submission by the reporting entities including:

19. **Romance Scam/Fraud**
20. **Pyramid Schemes**
21. **Unauthorised Account Access**
22. **Abuse Of The Duty Tax Concession On Vehicle Imports**
23. **Virtual Assets Red Flags & Indicators**
24. **Covid-19 Alert for the Public and Business Community**
25. **Suspected Movement of Funds out of Conflict Zones – A T&T Perspective**
26. **Financial Flows – A Human Trafficking Perspective**

Typology

19. Romance Fraud/Scam

Suspected Offence	Fraud
Customer Type	Individual; Group
Industry	FI's; MVTS
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

Romance scam/fraud is considered a social engineering tactic as it entails the 'engineering' of a friendship or relationship for fraudulent, financial gain. Romance scam/fraud involves a perpetrator articulating fabricated romantic intentions towards susceptible victims, mostly females, in an attempt to gain their trust and manipulate them to access their cash, bank accounts or even credit cards.

The FIUTT has observed an increase in this type of online scam/fraud during the COVID-19 pandemic. As persons are required to stay-at-home during the lock-down, and there is increase in the use of social media, perpetrators are taking advantage of this event, to identify potential victims.

Typology

Mr. X, using a fake social media account (with fake pictures) on Facebook and Instagram purports to be, or is, a foreigner, as he provides an international number as his contact number. He establishes an online 'relationship' with Ms. Y, a divorced middle-aged female (or any other female). Mr. X gains the trust of Ms. Y, promises to send her gift items, and even sends images of clothes. He then informs her that the items will be sent via a courier service and delivered directly to her.

Another individual, Mr. Z, contacts Ms. Y and notifies her that he is calling from an alleged courier service, for example, 'HPL International Courier Delivery Service' and request that Ms. Y make a deposit to a Mr. or Ms. Doe personal bank account in order to clear the 'gift items' from Mr. X. Ms. Y visits the financial institution and deposit monies into Mr. or Ms. Doe's personal bank account for the sum of TTD 5,000.00 (for example). Mr. Z then contacts Ms. Y and informs her that she needs to deposit/transfer TTD 3,000.00 into the same 'named' bank account to clear the gift items. The reason for the additional cost of TTD 3,000.00 is because the gift allegedly contains US cash or some other additional product and as such, there are higher Customs duties.

Based on a review conducted by the financial institution, the monies deposited by Ms. Y were withdrawn in cash via In-branch or ATM on the same day. The ATM withdrawals were from machines located along the East-West Corridor.

The review by the financial institution also revealed that Ms. Y was not the only person making third- party deposits into the account of Mr. or Ms. Doe. There were multiple credits of varying amounts into Mr. or Ms. Doe' account by order of various individuals, mainly women, through several branches of the financial institution. These deposits were also either withdrawn the same day or soon after.

The typology presented in this report describes a version of romance scam/fraud with the following sequence of possible steps ***(See Diagram 15).***

Suspicious Indicators

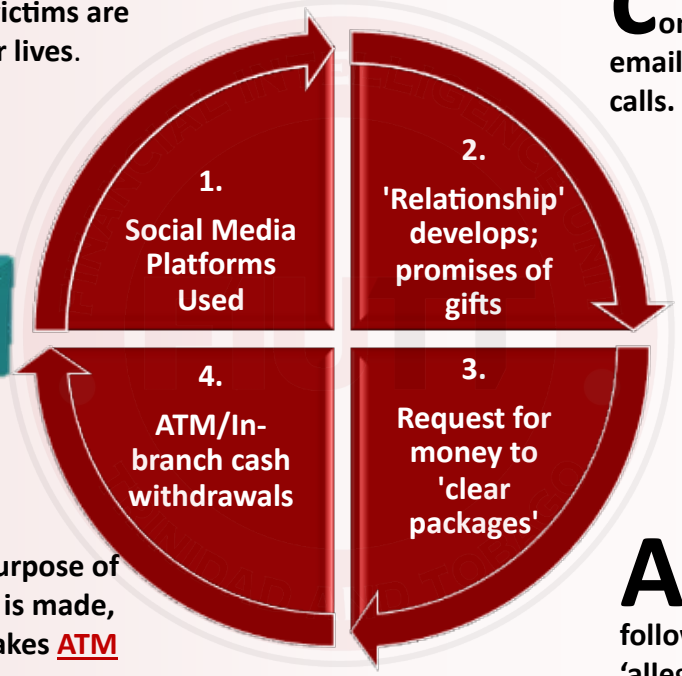
- **The Customer informing the CSR that the deposit to the third-party account is to clear a package;**
- **The Customer/Victim making payment for alleged package not to the courier company but to a third-party personal bank account;**
- **The customer never had any face-to-face interaction with the person they are transacting business with. The two parties usually communicates via text, email or voice calls;**
- **The customer can be considered at a more vulnerable stage in life, that is divorced, retired, widowed or single, and in most cases, women;**
- **The Customer may be apprehensive to answer questions relating to the transaction. Usually the customer provides minimal or inconsistent information, atypical of the customers' history;**
- **The Customer makes large funds transfer/payment atypical to their transaction history;**
- **ATM or In-branch cash withdrawals by the recipient subsequent to the deposit of the sender; and**
- **The Customer seeks to acquire a 'refund' of the third-party deposit.**

DIAGRAM 15

ROMANCE SCAM

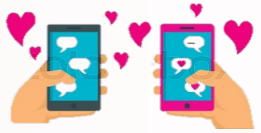
Social Media Platforms utilised; victims are usually at a vulnerable stage in their lives.

The perpetrator can continue to 'engineer' the relationship or target a new victim



Minimal information about the purpose of the transaction. Once the 'payment' is made, the perpetrator or co-conspirator makes ATM or in-branch cash withdrawals.

Communication is usually done through email, Facebook, Instagram, text or phone calls. There is NO physical meeting.



Requests for money can be made multiple times

Abnormal transaction completed by victim following requests by the perpetrator or an 'alleged Courier Service' to make deposits into named individual accounts for the purpose of 'clearing a package'. .

Advisory

20. Pyramid Schemes

Suspected Offence	Fraud
Customer Type	Group
Industry	FIs; CU's
Channel	Physical
Jurisdiction	Local; Foreign

Pyramid schemes are currently being heavily marketed to nationals through online chat groups, via virtual meeting platforms and by direct face-to-face contact. Pyramid schemes may take many forms and are often falsely presented as new investments including different types of securities, foreign currency trades and even traditional "sou-sou" arrangements.

How can you recognize a Pyramid Scheme?

They require persons to join groups and make an initial contribution of money with the promise of a significant pay-out or "return" on their contribution at a later date. They rely on the recruitment of new members in order to ensure high pay-outs – this is very different from "sou-sou "arrangements for example, which do not require recruitment of new members and are not profit-making ventures.

Early contributors to the scheme are paid from the money contributed by newer members.

Suspicious Indicators

- Promises of high returns with little or no risk;
- Success is based on recruiting new members;
- Numerous success stories of people who would have benefitted;
- Secretive and/or complex strategies based on assured mathematical models;
- Initial members receive hefty pay-outs from members in lower 'levels' who in turn experience difficulty in receiving payments; and
- Promises of overly consistent return and long-term financial freedom.

Existing members are encouraged to recruit new persons so that they can move to a different "level" or "circle" which promises higher returns on their contribution. The overall intention is to get to the "highest level" or to the top of the pyramid which will produce the highest pay-outs, while the newest members, those at the bottom of the pyramid, receive the lowest returns on their contributions. When fewer or no new members join the scheme, it collapses and disappears along with the payment platform and the money that was 'invested.'

Schemes outside of regulated financial facilities, such as pyramid schemes, promising exorbitant cash pay-outs pose a serious risk to those participating including loss of their hard- earned money. In addition, recipients of these funds may not be able to determine its true origins, which may be from illicit sources. You should therefore avoid pyramid schemes.

Typology

Ms. A, the Subject, is an administrative professional employed with a Government Ministry in Country A1. Ms. A established a personal savings account with XYZ Bank in mid-2011. The Subject's main "known source" of income is salary of USD 2,061.00 per month.

The Subject's account showed multiple third-party deposits at various branches of XYZ Bank. Several of the deposits were made in the 'standard' amount of USD 515.00, with accompanying descriptions of "gift". Further, the funds were withdrawn in cash or via online banking transfer/payments either on the same day or on average, 2-days after the deposits.

Over a one (1) month period, twenty-nine (29) deposits were made to the Subject's account. These payments were made by six (6) different third-party depositors (not the same as in para. 2). Of the six depositors, one (1) individual made a total of sixteen (16) deposits of amounts ranging from USD 48.00 to USD 515.00. The total amount deposited into the account by the six (6) depositors was USD 10,203.00. Conversely, withdrawals from this account amounted to USD 62,900.00. These withdrawals were conducted either via ATM withdrawals (19 transactions ranging between USD 44.00 to USD 441.00) or via internet transfers (8 transactions ranging between USD 37.00 to USD 737.00). The payees of the internet transfers were seven (7) identified individuals.

The Subject indicated that the credits represented "gifts from friends" and the withdrawals were for the "purchase of gifts" for her friends. The Subject did not provide any documents to support the claim, nor did she offer any further explanation since she deemed the activities personal. Additionally, the Subject advised XYZ Bank that she is not currently involved in any business activity at this

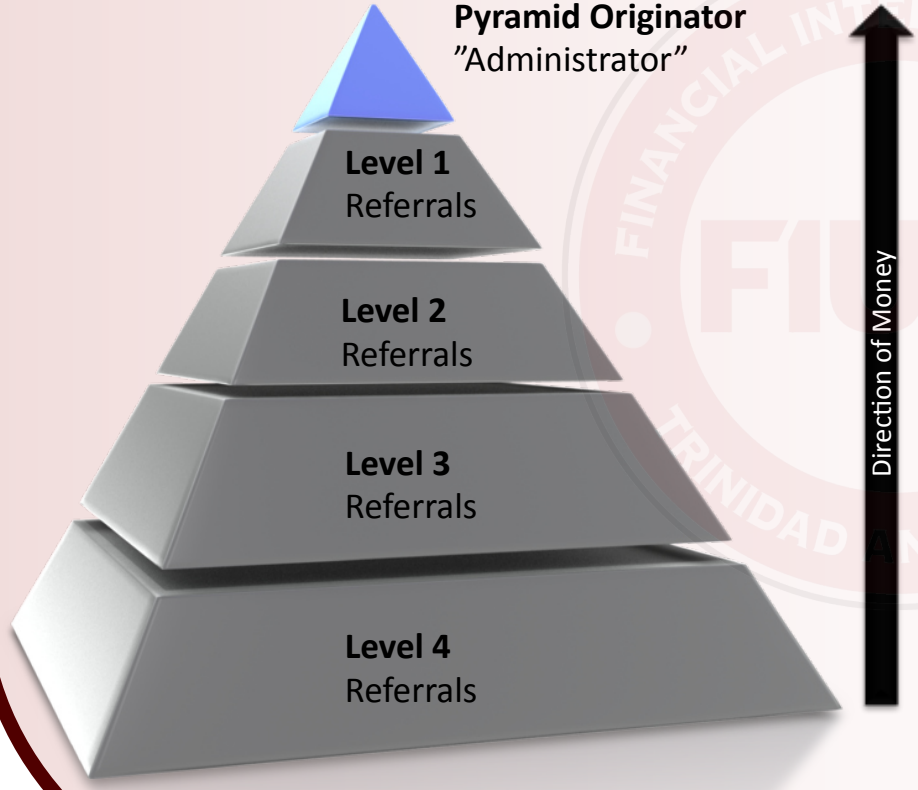
time.

The above case is a suspected pyramid scheme based on the following:

- Sudden increase in third-party deposits over a period in time.
- Similar pattern of amounts deposited by third-party depositors.
- Explanation given by the account holder that the suspicious deposits were “gifts” from friends.
- The deposited amounts were withdrawn via ATM and/or via internet transfers to other persons, in amounts similar to that deposited.
- The movement of fund out of the account was done either on the same day or on average 2-days after the deposits.

DIAGRAM 16

PYRAMID SCHEMES



HOW IT WORKS

- Require persons to make an initial contribution with the promise of significant pay-outs or 'returns.'
- Relies on continuous recruitment of new members in order to ensure high pay-outs.
- Early contributors to the scheme are paid from money by newer members. Existing members are encouraged to recruit new persons to move to a different 'level''.
- Those at the bottom of the pyramid receive the lowest return and when fewer or NO new members join, it collapses and disappears along with the payment platform.

(Joint Public Advisory - TTSEC, CBTT, FIUTT
On "Pyramid Schemes" Marketed In Trinidad And Tobago, 2020)

Advisory

21. Unauthorised Account Access

Suspected Offence	Fraud
Customer Type	Individual
Industry	FI's
Channel	Electronic
Jurisdiction	Local

The FIUTT noticed cases with individuals (perpetrators), likely to be utilizing social engineering tactics, receiving funds via a domestic transfer from one financial institution to another. The victim, of the unauthorised third party transfer, who holds a bank account with one financial institution, does NOT know the recipient of the third party transfer who holds an account with another financial institution, nor; did the victim authorise banking access. It would appear that the perpetrator gained banking access to complete the third party transfer.

Noteworthy, the perpetrator typically transfers a small dollar value (TTD 20.00) to test the system followed by a larger dollar value transfer (in excess of TTD 1,000.00). Subsequently, the recipient of the unauthorised third party transfer then transfers money among related bank accounts, consistent with layering of funds.

Suspicious Indicators

- The victim did not authorise banking access to anyone;
- The victim who holds a bank account with one financial institution, does NOT know the recipient of the third party transfer who holds an account with another financial institution;
- A small dollar value transfer is initially made (to test the system) followed by a larger dollar value transfer; and
- The recipient of the unauthorised third party transfer transfers money among related bank accounts.

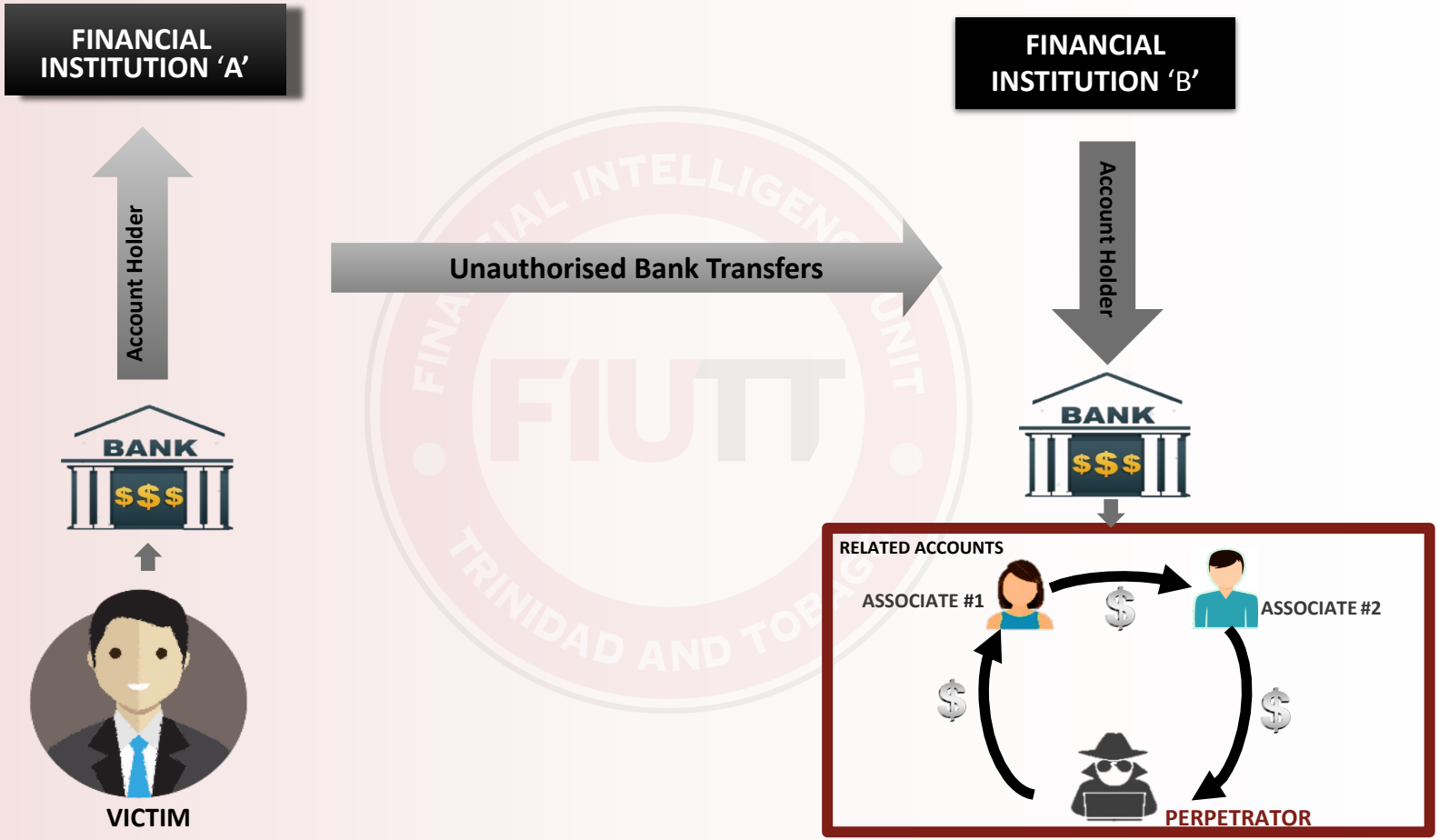
HOW THE FRAUD WORKS

Social Engineering techniques are used to manipulate either the financial institutions or members of the general public to unknowingly install malware onto their computers, workstations or wireless devices. This is an effort to compromise and steal personal sensitive information such as emails and other online account login credentials.

Once this data is acquired, unauthorised account transfers are made from the victims' accounts at one financial institution to the perpetrator account at another financial institution. A small dollar value transfer is made, followed by a larger dollar value transfer to an account NOT known to the victim. From the unauthorised third party transfers, there are usually several 'related accounts', to which monies are transferred. These 'related accounts' then send monies to each other, consistent with layering of funds.

DIAGRAM 17

UNAUTHORISED ACCOUNT ACCESS



Advisory

22. Abuse of Duty Tax Concession on

Suspected Offence	Tax Crimes
Customer Type	Individual; Companies
Industry	FI's; Insurance
Channel	Physical; Electronic; Cheque
Jurisdiction	Local; Foreign

The FIUTT observed a significant increase in reports involving individuals and/or businesses, who are suspected of having capitalised upon tax reliefs only available to first-time returning nationals to Trinidad and Tobago. In exchange for financial benefit or personal gain, nationals visiting Trinidad and Tobago for brief periods or otherwise, are encouraged or coerced to purport themselves as returning nationals in order to access the concession. In so doing, the 'alleged' returning nationals are able to import high-end vehicles at significantly lower prices without paying the 'fair' customs duties, Value-Added-Tax (VAT) and motor vehicle taxes. Many times these vehicles are imported on behalf of individuals residing locally for either personal gain and/or financial benefit.

Suspicious Indicators

- Cheque or cash payments made on behalf of the importer by a company and/or other individual;
- Specific businesses or individuals frequently making payments on behalf of persons claiming to be returning nationals;
- Business addresses utilised as the residence of the applicant for wire transfers or other related payments;
- Involvement of a range of third party individuals to carry out related transaction;
- Questionable reasons provided for the remittance of funds to foreign jurisdiction for the evident purchase of a vehicle;
- Vehicle appears to be brand new and not a used vehicle previously;
- Early sale or transfer of vehicles within the mandated two (2) year period stipulated for returning nationals;
- The name of the individual listed on the certified copy is not the name being requested for the relevant insurance certificates;
- Inclusion of additional authorised drivers on the insurance certificate;
- Temporary or short term insurance certificates requested; and
- Early cancellation or transfer of insurance certificates.

DIAGRAM 18

DUTY TAX CONCESSION ABUSE FLOW OF ACTIVITY

THIRD PARTY/ ULTIMATE BENEFICIARY
Sends funds for vehicular purchase & possible travel/ expenses.

FOREIGN RESIDENT
purporting to be a returning national submits application to Customs & Excise Division for duty concession.

VEHICLE IMPORTED
Vehicle in question either:

- Remains unregister for a period
- Registered in name of returning national (sold without transfer) and/or insured to or left with ultimate beneficiary/Beneficiary name added to insurance policy of returning national
- Insured for short period under name of returning national and then re-insured under new owner's name.

CUSTOMS & EXCISE DIVISION
C&E grants importation and tax concessions to returning applicant.

Advisory

23.Virtual Assets Red Flags & Indicators

Suspected Offence	Fraud
Customer Type	Individual; Group
Industry	FI's; CU,
Channel	Electronic; Cheque
Jurisdiction	Local; Foreign

Virtual Assets (VAs) refers to any digital representations of value that can be digitally traded, transferred, or used for payment and investment purposes. e.g. (cryptocurrencies such as bitcoins, litecoins and xrp). This new phenomena has the potential to spur financial innovation and efficiency as well as their distinct features also creates new opportunities for money launderers, terrorist financiers and other criminals to launder their proceeds or finance their illicit activities.

The ability to transact across borders rapidly, not only allows criminals to acquire, move, and store assets digitally outside the regulated financial system, but also to obscure the origin or destination of the funds and make it harder for Reporting Entities to identify suspicious activity in a timely manner.

The FIUTT noted an increase in Suspicious Transaction/ Activity Reports (STRs/SARs) where the use of, or the purchasing of VA's, were observed. VA's, particularly Convertible (or open) Virtual Currency (CVC), are increasingly used as alternatives to traditional payment and money transmission systems. Virtual Asset Service Providers (VASPs) are neither regulated, nor supervised in Trinidad and Tobago, at this time. Transactions involving VA's have limited transparency and creates a high degree of anonymity. As such, VA's provide a powerful tool for criminals and terrorist financiers to conduct criminal activity, including ML and FT.

The indicators included in this Report are specific to the inherent characteristics and vulnerabilities associated with VAs. They are neither exhaustive nor applicable in every situation. See also, FATF's Report on Virtual Assets Red Flag Indicators of ML and FT (September 2020).

CAUTION AND RED FLAG INDICATORS

▶ INDICATORS RELATED TO TRANSACTIONS

Although the use of VAs are not currently widely used by the public, the use of VAs is becoming increasingly common for criminal activity. The indicators below demonstrate red flags associated with VAs transactions, which are the same gauges, utilised in detecting potential illicit activity related to conventional financial transactions:

- Structuring VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under reporting thresholds, similar to structuring cash transactions;
- A customer receives multiple frequent high value cash deposits or wire transfers from multiple jurisdictions (with no relation to where the customer lives or conducts business) and almost immediately uses such funds to acquire virtual currency;
- Transferring VA's immediately to multiple VASPs: there is no relation to where the customer lives or conducts business, and there is non-existent or weak Anti-Money Laundering/ Counter Financing of Terrorism (AML/CFT) regulation;
- A customer receives a series of deposits from various sources, which in aggregate; amount to the same or near equal to funds transfers to a virtual currency exchange platform within a short timeframe; and
- Converting the VA's to multiple types of VA's, incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification).

▶INDICATORS RELATED TO TRANSACTION PATTERNS

The indicators illustrated in this section attempts to highlight how the misuse of VAs for ML/TF purposes can be identified through atypical or uncommon patterns of transactions conducted by a customer:

- customer is conducting transactions of large volumes/ amounts at a high frequency that appears to be inconsistent with their profile;
- A customer receives frequent deposits from virtual currency addresses followed by withdrawals within a short timeframe;
- Transactions involving the use of multiple VA's, or multiple accounts with no logical business explanation; and
- making frequent transfers at a particular time (e.g. a day, a week, a month), to the same virtual asset account by more than one person, from the same IP address, or, concerning large amounts.

▶INDICATORS RELATED TO ANONYMITY

- The various technological features identified in this section increases anonymity making it increasingly difficult to detect any criminal activity. This aspect makes VA's exceedingly attractive to criminals looking to disguise or store their funds:

- Transactions by a customer involving more than one type of VA, despite additional transaction fees, specifically those VA's that provide higher anonymity, such as [anonymity-enhanced cryptocurrency (AEC) or privacy coins];

- A customer purporting to be an Investment Advisor and operates as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customer handles large amounts of VA transfers on its customer's behalf. In addition, there may be concerns that higher fees are charged to customers than transmission services offered by other exchanges. Further, the use of bank accounts to facilitate P2P transactions;

- Receiving funds from or sending funds to VASPs whose Customer Due Diligence (CDD) or KYC processes are weak or non-existent; and

- Use of VAs whose design is not adequately documented, or linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.

▶INDICATORS ABOUT SENDERS OR RECIPIENTS

The indicators in this section are relevant to the profile and unusual behaviour of either the sender or the recipient of the illicit transactions relative to VAs:

- A customer presents contradictory details about the transaction or has few details about its purpose;

- Incomplete or insufficient KYC information - a customer does not provide information upon request; fails to provide supporting documentation or provides misleading or inaccurate information regarding source of funds and the destination of funds;

- A customer provides inaccurate or misleading information about third parties (sender/recipient) and the purpose of the transaction;

- A customer is known via publicly available information to law enforcement due to previous criminal association;

- A customer's contact information is connected to a VA exchange platform/forum whereby he/she advertise exchange or investment services;

- Sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be mules recruited by professional money launderers, or scam victims turned mules, who are deceived into transferring illicit proceeds without knowledge of their origins;

- Customer purchases large amounts of VA's not substantiated by available wealth or consistent with his or her historical profile, which may indicate ML, a money mule, or a scam victim;

- A customer's financial profile consists mainly of virtual currencies and online exchange platforms (e.g. Bitstamp.net; Skrill.com; dagcoin.org and Cex.io);

- A customer admits or makes statements about involvement in buying and selling virtual currencies, trading/investing on

online platforms that are not registered with the relevant authorities in Trinidad and Tobago;

- A customer's account appears to be a "pass-through" account and is not being used for its intended purpose; and
- A customer conducting VA transactions with charitable organisations/Non-Profits Organisations (NPO's) that is inconsistent with their profile.

▶INDICATORS RELATIVE TO SOURCE OF FUNDS OR WEALTH

The misuse of VA's are often linked to criminal activity. Below are some common red flags related to the source of funds or wealth associated to such criminal activity:

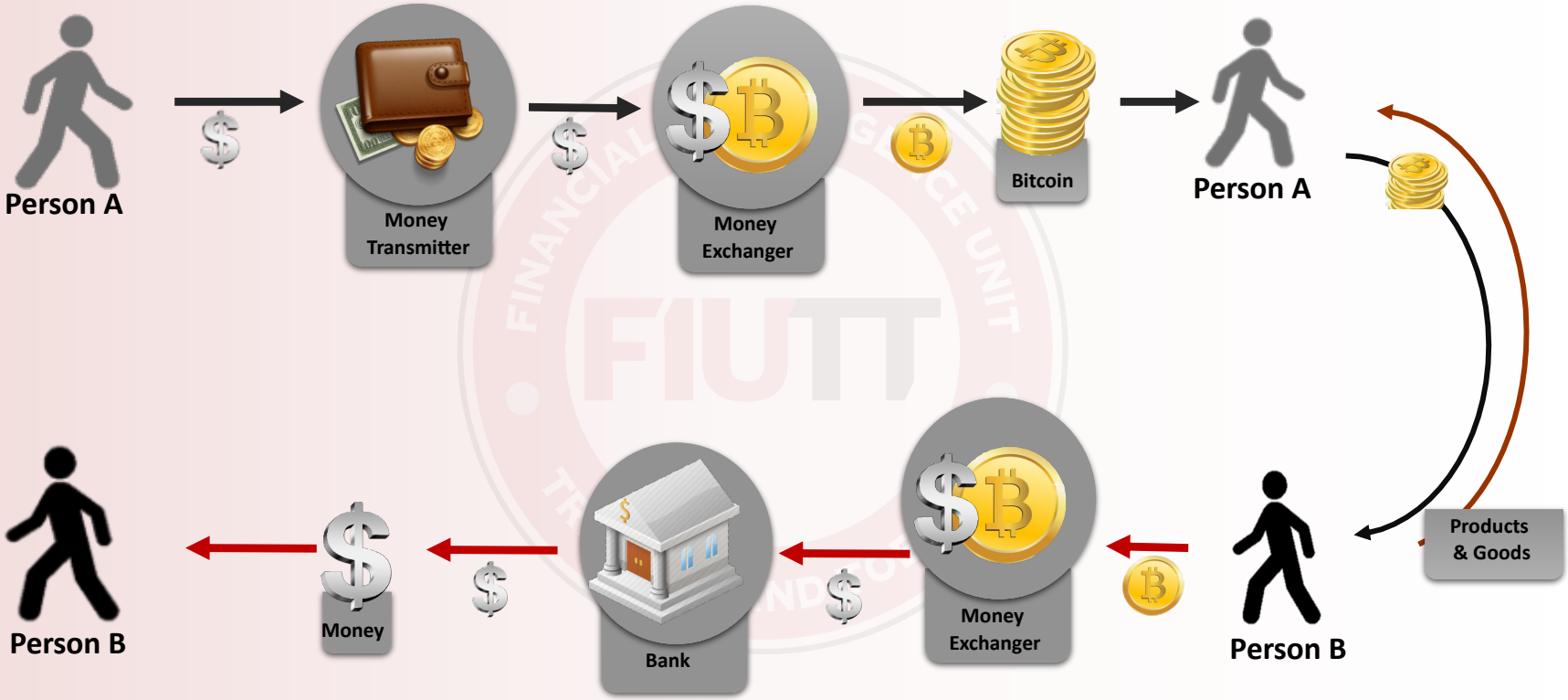
- Transactions with VA addresses or bank cards that are connected to known fraud, extortion, sanctioned addresses, dark net marketplaces or other illicit websites;
- The use of one or multiple credit and/or debit cards that are linked to a VA wallet, to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards;
- Deposits into an account or a VA address are significantly higher than average with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds;
- A customer's funds sourced directly from third-party mixing services or wallet tumblers; and
- A customer's source of wealth is derived from investment in VA, ICOs, or fraudulent ICOs.

▶INDICATORS RELATED TO GEOGRAPHICAL RISKS

- The indicators in this section highlight how criminals, when moving their illicit funds, have taken advantage of the varying stages of implementation by jurisdictions on the revised FATF Standards on VAs and VASPs:
- Funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located;
- Customer utilises a VA exchange or foreign located MVTS in a high-risk jurisdiction, lacking or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures; and
- Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls.

DIAGRAM 20

PROCESS OF VIRTUAL ASSET EXCHANGE



Alert

Suspected Offence	Fraud
Customer Type	Individual
Industry	-
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

24. COVID 19 Alert for the Public & Business Community

DIAGRAM 21

DIAGRAM 22

ALERT FOR THE BUSINESS COMMMUNITY

The FIU of Trinidad and Tobago advises that as the world struggles with the COVID-19 pandemic, and business communities worldwide face huge losses due to lock-downs; criminals remain a relevant threat as they can prey on local businesses in much the same manner as seen internationally.

SUPPLY SCAMS

- Funds transferred as payment for stocks of protective equipment/supplies, but no product is received.
- Substandard and/or counterfeit health and sanitary products purchased through businesses/NPOs who did not previously deal in these products and may have sourced them from unscrupulous online distributors.

CYBER ATTACKS

- Email scams targeting key employees to gain credentials for access to company funds (hacking emails to authorize fund transfers)
- Online Identity theft capturing information on company issued credit cards
- Exploiting (through blackmail) key individuals with work from home access to corporate data.

Suspicious Indicators

- Impersonation of officials particularly those involved in the provision of social welfare assistance;
- Individuals requesting a fee to 'speed up' or guarantee access to government social support services;
- Fundraising scams;
- Creation or exploitation of non-traditional/ informal financial services e.g. sou-sou;
- Personal and business email compromise, SMS phishing attacks, phone calls;
- Ransomware attacks;
- Counterfeit products (medical supplies, pharmaceuticals, personal protective equipment); and
- Human trafficking and exploitation of workers, children and immigrants.

Strategic Analysis

25. Suspected Movement of Funds out of Conflict Zones – A T&T Perspective.

Suspected Offence	FT
Customer Type	Individual; Group
Industry	MVTS
Channel	Electronic
Jurisdiction	Local; Foreign

Analysis conducted by the FIUTT revealed that a large group of related and seemingly unrelated individuals located within Trinidad and Tobago utilized the MVTS Sector to receive suspicious inbound transactions from individuals located in known high-risk terrorists related jurisdictions. During the period January 2014 to December 2018 individuals located in ten (10) jurisdictions with varying terrorism and terrorist financing risks sent suspicious inbound transactions totalling approximately TTD 800,000.00 to individuals located within various parts of Trinidad and Tobago.

Sender Analysis - Of the total number of individuals who remitted funds to Trinidad and Tobago, 61% conducted one-off transactions and 23% conducted two transactions. The use or employ of third-party individuals to conduct predominantly one-off transactions has been identified by the FIUTT as a common trend for various individuals to remit funds to various high-risk terrorist jurisdictions or countries that lie in close proximity to the conflict zone. It is possible that third party individuals may wittingly or

Suspicious Indicators

- The transfer of funds from countries that are situated in close proximity to known high risk terrorists jurisdiction;
- Individuals may wittingly or unwittingly be a medium that facilitates the movement of funds used in financing terrorism;
- Use of one-off transactions from seemingly unrelated parties located in known high risk terrorists jurisdiction;
- The transactions failed to identified any legitimate business;
- Transactions appear to lack economic and financial purpose;
- The true purpose/origin of the funds cannot be determined as having been derived from legitimate sources or to be used for legitimate reasons; and
- Individuals utilize the same address or reside in close proximity to each other.

unwittingly be employed or act as a medium used by various terrorist organisations and/or their affiliates to facilitate the movement of suspected funds used in financing terrorism.

Receiver Analysis - In contrast, of the total number of individuals who received funds in Trinidad and Tobago, 54% received one-off transactions. Third party transactions therefore emphasizes a terrorist organisation's ability to distance themselves from suspected financial transactions and evade regulatory mechanisms. It may also indicate their ability to gain support whether it be forcibly or not.

The transactions identified 'no legitimate business links' between the senders and receivers. One-off transactions indicate a lack of economic and financial purpose as it appears uncharacteristic that the individuals would receive funds from seemingly unrelated parties located in known high-risk terrorists related jurisdictions. Additionally, the true purpose/origin of the funds could not be determined as having been derived from legitimate sources or to be used for legitimate reasons. As such, the intended purpose, use and ultimate beneficial owner of the funds transferred remains highly obscured.

Typology

26. Financial Flows – A Human Trafficking Perspective

Suspected Offence	Human Trafficking
Customer Type	Individual; Group
Industry	MVTS
Channel	Electronic
Jurisdiction	Local; Foreign

Modus operandi of the criminal group: Jane Doe is a known human trafficker operating in Jupiter, an HT high risk jurisdiction. Jane Doe together with other persons located in other high risks HT territories, (Uranus, Pluto, and Mars), used the local Money Service Businesses (MSBs) to send high volumes of cash to a person (Mrs Z) resident in Saturn. The cash was suspected to be laundered funds derived from the predicate crime of HT.

The ML/TF schemes employed by the group: Jane Doe and other persons from multiple jurisdictions, sent high volumes of cash to Mrs Z resident in Saturn. None of the senders seemed to have any relations with the receiver. Mrs Z was a national of Saturn, a country known to be source country for HT.

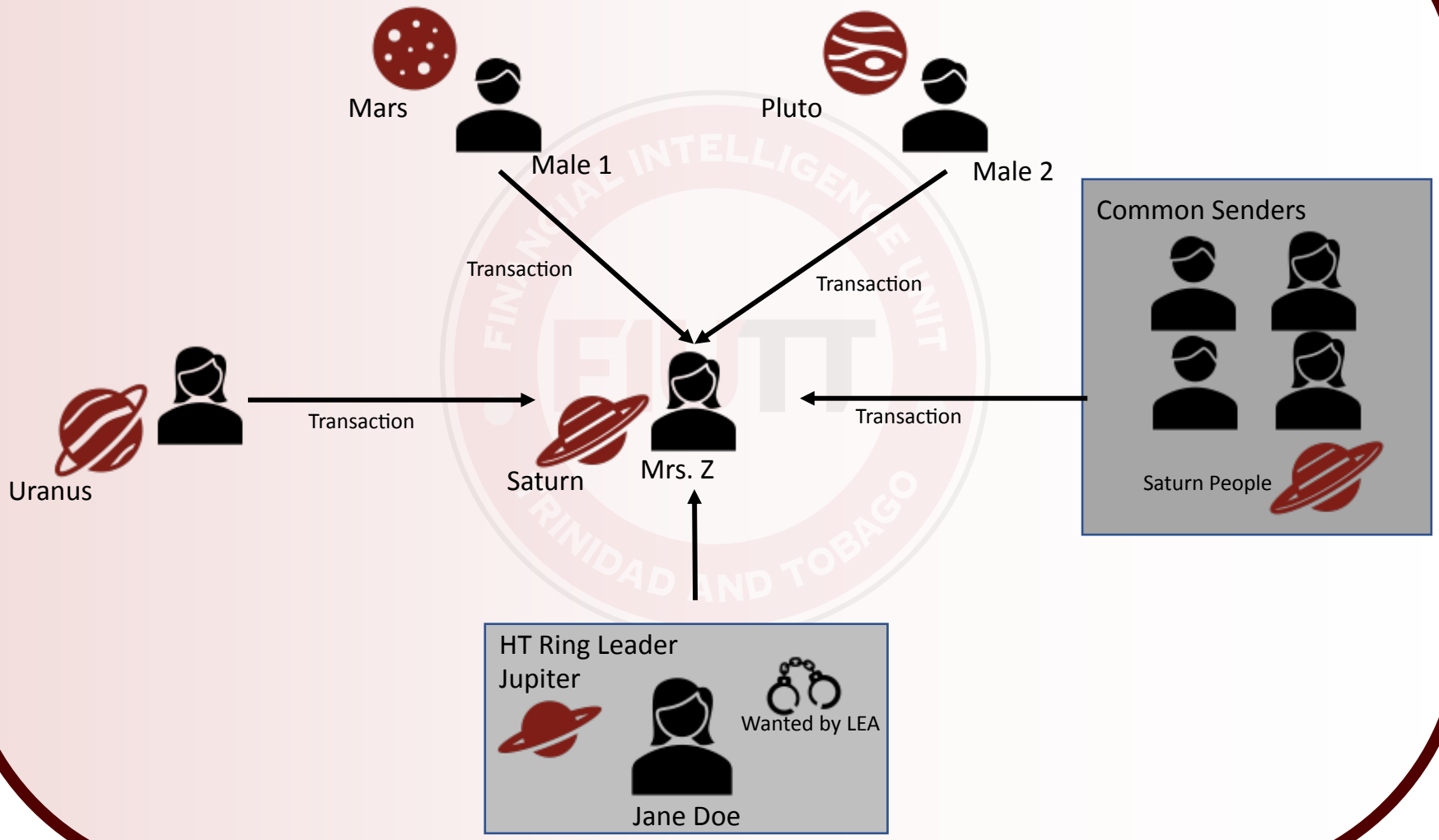
How the group's predicate criminality and ML/TF activities were detected and investigated: Analysis was conducted by the FIUTT and intelligence reports forwarded to Law enforcement for investigation.

Suspicious Indicators

- Transfers of high volumes of cash, below the reporting threshold;
- Use of third parties to move criminal proceeds;
- Transfers from several persons to one common receiver with whom they appear to have no discernible relationship;
- Use of intricate networks to hide the true source of funds;
- Transfers sent by a person who is known to be involved in the HT trade.

DIAGRAM 23

HUMAN TRAFFICKING FLOWS



Glossary

BENEFICIAL OWNER

Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Source: Glossary of the FATF Recommendations

FINANCING OF TERRORISM

Financing of Terrorism may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organisations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. Therefore, funds derived from legitimate, as well as illegal activities, can be used for or to facilitate terrorist activities.

MONEY LAUNDERING

Money Laundering is the process by which illegally obtained funds are given the appearance of having been legitimately obtained. The process may involve one or more of the following methods:

- **Placement**

Illegal funds or assets are first brought into the financial system. This 'placement' makes the funds more liquid using a variety of techniques, which include depositing cash into bank accounts and using cash and other instruments to purchase assets.

- **Layering**

To conceal the illegal origin of the placed funds and thereby make them more useful, the funds must be moved, dispersed, and disguised. The process of distancing the placed funds from their illegal origins is known as 'layering'. These include using multiple banks and accounts, having professionals act as intermediaries and transacting through corporations and trusts. Funds may be shuttled through a web of many accounts, companies and countries in order to disguise their origins.

- **Integration**

Once the funds are layered and distanced from their origins, they are made available to criminals to use and control as apparently legitimate funds. The laundered funds are made available for activities such as investment in legitimate or illegitimate businesses, to fund further criminal activity or spent to enhance the criminal's lifestyle. At this stage, the illegal money has achieved the appearance of legitimacy.

POLITICALLY EXPOSED PERSONS

i. Foreign PEPs are individuals who are or have been entrusted with prominent functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials.
ii. Domestic PEPs are individuals who are or have been entrusted with prominent functions in Trinidad and Tobago, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials.
iii. Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management such as directors and members of the board or equivalent functions.
iv. Family members are individuals who are related to either a Foreign or Domestic PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.
v. Individuals who are closely connected to or associated with a PEP as defined in i, ii and iii above, either personally or professionally.

PROLIFERATION OF WEAPONS OF MASS DESTRUCTION AND ITS FINANCING

The FATF Recommendation 7 requires Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

What is proliferation of weapons of mass destruction?
Proliferation is the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services or expertise.

REPORTING ENTITIES

Reporting Entities are FIs, and certain businesses and professionals (the "Listed Business") which are designated to detect and deter ML and FT. These obligations include the development and implementation of a compliance programme which includes policies, procedures and controls such as the appointment of a Compliance Officer, reporting suspicious transactions, customer due diligence, retention of records and training for staff.

Source: Glossary of the FATF Recommendations and FIUTT

TARGETED FINANCIAL SANCTIONS

The term targeted financial sanctions means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

Source: Glossary of the FATF Recommendations

TERRORIST

The term terrorist refers to any natural person who:

i. commits a terrorist act by any means, directly or indirectly, unlawfully and wilfully;
ii. participates as an accomplice in terrorist acts or Financing of Terrorism;
iii. organises or directs others to commit terrorist acts or the Financing of Terrorism; or
iv. contributes to the commission of terrorists' acts or the Financing of Terrorism by a group of persons acting with a common purpose. The contribution is made internationally, with the aim of furthering the terrorist act or the Financing of Terrorism, with the knowledge of the intention of the group to commit the terrorist act or the Financing of Terrorism.

Source: Glossary of the FATF Recommendations

TERRORIST ORGANISATION

The term terrorist organisation means a Legal Entity or group of terrorists that:

i. commits a terrorist act by any means, directly or indirectly, unlawfully and wilfully;
ii. participates as an accomplice in terrorist acts or the Financing of Terrorism;
iii. organises or directs others to commit terrorist acts or the Financing of Terrorism; or
iv. contributes to the commission of terrorist acts or the Financing of Terrorism by a group of persons acting with a common purpose. The contribution is made internationally, with the aim of furthering the terrorist act or the Financing of Terrorism, with the knowledge of the intention of the group to commit the terrorist act or the Financing of Terrorism.

Source: *Glossary of the FATF Recommendations*

VOLUNTARY INFORMATION REPORTS (VIRs)

If any member of the public would like to provide information about suspicions of money laundering or of the financing of terrorist activities, a Voluntary Information Report (VIR) can be submitted via post or email to the FIUTT. If you believe that the information you provide is serious and requires an immediate law enforcement response, then you may also wish to provide this information directly to your local law enforcement agency.

- END -