CARIBBEAN FINANCIAL ACTION TASK FORCE

REPORT: CFATF Risk, Trends & Methods Group (CRTMG)

Money Laundering and Terrorist Financing Cases Update 2019

TABLE OF CONTENTS

Contents

LIST OF ACRONYMS USED IN THE REPORT

AML/CFT	-	Anti-money Laundering/Combating the Financing of Terrorism
ACH	-	Automated Clearing House
ATM	-	Automatic Teller Machine
CAYFIN	-	Cayman Islands Financial Reporting Authority
CDD	-	Customer Due Diligence
CFATF	-	Caribbean Financial Action Task Force
CRTMG	-	CFATF Risk Trends and Methods Group
EDD	-	Enhanced Due Diligence
FATF	-	Financial Action Task Force
FI	-	Financial Institution
FIU	-	Financial Intelligence Unit
FIUTT	-	Financial Intelligence Unit of Trinidad and Tobago
LEA	-	Law Enforcement Agency
MSB	-	Money Service Business
NPO	-	Non-Profit Organisation
OFAC	-	Office of Foreign Assets Control
SAR	-	Suspicious Activity Report
STR	-	Suspicious Transaction Report
TCSP	-	Trust and Company Service Providers
TTD	-	Trinidad and Tobago Dollar
USD	-	United States Dollar

INTRODUCTION

1. The Caribbean Financial Action Task Force (CFATF) is the regional anti-money laundering/combating the financing of terrorism (AML/CFT) body, comprising of twenty-five states, which have agreed to implement common AML/CFT countermeasures.
2. The CFATF Risk Trends and Methods Group (CRTMG) is a working group of the CFATF and is responsible for conducting typologies research to identify and analyse money laundering (ML), terrorist financing (TF) and other threats to the integrity of the financial system, including the methods and trends involved.
3. Typologies studies assist CFATF members in the implementation of their strategies to counter ML and TF and can be a great aid when designing and implementing AML/CFT systems. Generally, when ML or TF activities are conducted in a similar manner they are classified as a typology.
4. The CFATF last published an update on regional ML typologies in 2018.
5. This report is a compilation of thirteen (13) sanitized cases received from seven (7) CFATF member countries, two (2) of which show clear elements related to terrorist financing. The cases, as compiled, enables the CRTMG to have an updated categorized list of regional ML/TF activities from which future projects may be selected.

OVERVIEW OF PREVIOUS CFATF CRTMG TYPOLOGIES AND OTHER STUDIES

i. Money laundering using trust and company service providers[1]

6. This joint Financial Action Task Force (FATF) and CFATF study considered how the effectiveness of the international standards, as applied to Trust and Company Service Providers (TCSPs), could be enhanced by evaluating the following:

   - The role of TCSPs in the detection, prevention and prosecution of money laundering and terrorist financing;
   - The effectiveness of the FATF Recommendations as they apply to TCSPs; and
   - The potential need for additional international requirements or sector-specific international standards for TCSPs.

7. Some key findings of the project report were that:

   - Some jurisdictions do not recognise trusts in their laws, nevertheless case studies show that persons providing the services of a TCSP are able to provide trust vehicles to clients using the laws of other countries to do so. This can make it difficult for the authorities in the TCSP's home country to provide oversight for a legal structure established under foreign law thereby creating a vulnerability that criminals/money launderers capitalise on.

   - TCSPs incorporate pre-constituted companies which they hold as assets for sale or transfer to clients. After the company is sold there may be no requirement for the information on the new owners to be collected and submitted to the authorities to update the information on the corporation. Jurisdictions that allow TCSPs or professional intermediaries to establish pre-constituted companies, without the need for the ownership structure of those companies to be updated after the company has been sold to clients, might provide a cover to criminals and other persons who wish to use corporate structures to obscure beneficial ownership and thereby hide assets.

   - As the creation of complex structures can often generate higher fees for TCSPs, this can make such structures more attractive to TCSPs thereby potentially reducing their ability to associate an increased use of complex structures with a higher money laundering risk.

   - TCSPs operating in highly competitive environments, both regulated and unregulated, may also experience additional challenges in obtaining adequate CDD, where there may be no minimum standard that has been clearly communicated or otherwise established that is in keeping with the FATF Recommendations.

[1] https://cfatf-gafic.org/index.php/documents/typologies/2185-money-laundering-using-trusts-and-company-service-providers

ii. Human trafficking and migrant smuggling[2]

8. This study sought to identify ML/FT risks associated with human trafficking and migrant smuggling activities within the Caribbean region and to increase the understanding and raise regional awareness of the related activities.
9. The report concluded that during the period 2007-2011, a total of 508 related investigations were conducted within the region resulting in ninety-five convictions. Most of the investigations were conducted within the human trafficking category. The responses also indicated that human trafficking activities are associated with "Sexual Exploitation."

iii. Illegal lotteries[3]

10. This typology exercise was pursued with the aim of countering the threat of illegal lottery schemes and related ML and TF activities by effectively providing a regional overview; warning signs; and the modus of the perpetrators.
11. Based on the responses from CFATF members a total of 1,070 illegal lottery related investigations were conducted by five jurisdictions resulting in twenty-five convictions during the period under review. One jurisdiction (Jamaica) recorded prosecutions/convictions.

iv. Movement of cash and negotiable instruments[4]

12. This project sought to identify:
    - The extent of enforcement within the CFATF region;
    - The scope of legislation and other control measures in place among CFATF member jurisdictions;
    - The concealment methods being employed;
    - The characteristics of the persons doing the transporting;
    - The origin, destination and application of the cash/negotiable instruments;
    - Enforcement successes; and
    - Challenges faced in the implementation of policies to counter these activities.
13. This report found that the majority of CFATF member countries are predominantly cash based economies. All of the CFATF member countries have declaration systems at their legal ports of entry. However, the majority of coutries had varied challenges. To effectively disrupt the illegal movement of cash and negotiable instruments competent authorities both domestically and internationally must enhance cooperation (through effective mechanisms such as laws, regulations and MOUs) and make a sustained effort to share information and intelligence amongst all stakeholders.

[2] https://cfatf-gafic.org/index.php/documents/typologies/3564-cfatf-typologies-report-on-human-trafficking-and-the-smuggling-of-migrants-1
[3] https://cfatf-gafic.org/index.php/documents/typologies/6949-illegal-lotteries-typology-project-report
[4] https://cfatf-gafic.org/index.php/documents/typologies/7171-movement-of-cash-and-negotiable-instruments-september-2016

14. Some common features and trends which have emerged from the analysis of the information gathered during the compilation of this report are as follows:

- The currencies most frequently encountered in criminal cash seizures is the US dollar, followed by the Euro;
- The predominant origin and destination of seized cash is the United States of America;
- The couriers are predominantly males between the ages of 26-40;
- The bulk of the cash seized is linked to drug trafficking;
- Airports are the preferred choice of couriers followed by sea and land borders;
- There are existing legislative frameworks comprising of disclosure/declaration mechanisms within the jurisdictions surveyed, however, enhanced enforcement is carried on passengers entering respective jurisdictions as opposed to those exiting;
- An increase in the use of civil forfeiture/seizure procedures in the administration of cases as compared to criminal forfeiture/seizure notwithstanding that 94.1% availability of criminal cash/BNI seizure legislations as compared with 76.5% availability of civil cash/BNI seizure legislation;
- Declaration forms exist, and the information particularized are used by LEAs. However, the majority of these declaration forms are still physically filed by LEAs (in particular Custom agencies);
- The majority of the jurisdictions surveyed lacked a national database housing cash and BNI seizure information which is shared among law enforcement and other authorities;
- All jurisdictions surveyed have threshold reporting provisions within their respective statutes;
- Jurisdictions surveyed identified the need for regional type real-time information sharing mechanism within which cash seizure information can be shared with key LEAs;
- Limited sharing of the information recorded on the declaration forms; and
- 52.9% of the countries surveyed cited the need for an MOU prior to information share with other jurisdictions. However, they all cited alternate methods that can be used to facilitate information sharing with other law enforcement counterparts overseas.

v. The proliferation of small arms and ammunition[5]

[5] https://cfatf-gafic.org/index.php/documents/typologies/7585-the-proliferation-of-small-arms-and-ammunition-october-2016

15. The main objectives of this project were to develop a regional report on typologies related to the proliferation of small arms and ammunition and identify the effects that these activities have on member jurisdictions, including any nexus to money laundering and terrorist financing.

16. The report concluded that small arms and ammunition are the main tools used in many of today's conflicts and are the cause of most of deaths from armed violence in the region. The attention drawn to the proliferation of small arms and ammunition will assist CFATF member countries in the development of anti-gun crime related policies and strategies.

17. The international community have assisted by creating the various conventions and treaties and making it mandatory for states to do their best to alleviate the proliferation of small arms and ammunition.

18. It would appear that the existing legislative framework and current countermeasures, to combat the proliferation of small arms and ammunition, have proven to be insufficient. Therefore, it is incumbent upon CFATF member countries to seriously consider the recommendations highlighted in this report.

vi. De-risking stocktaking exercise

19. The study was conducted in two (2) phases over the period June 2018 to April 2019, with the goal of highlighting the negative impact of 'de-risking' on the region.

20. With respect to licensed entities, 227 financial institutions were surveyed[6]. Of this number, 68.2 percent indicated that their operations were negatively affected by de-risking. FIs are equally divided as to whether 'de-risking' poses as great a threat as it did in 2015. This division in opinion reflects the uneven impact of 'de-risking' on countries in the Caribbean. Only 55 banks representing 24 percent of respondents reported that their correspondent banking relationships had been terminated within the past 3 years (2015-2018). Of this number, 80 percent (44 banks) lost between one and three relationships while 14 percent (8 banks) lost between 4 and 10 relationships. In some instances, no reason was provided for the termination of the correspondent banking relationship. Where feedback was provided by the respondent bank, the following reasons were given for the termination/restriction of correspondent banking relationships:

    i. low/small profit margins
    ii. the cost of compliance
    iii. issues with AML/CFT procedures
    iv. the product/service was no longer offered
    v. the perceived risk of the jurisdiction
    vi. fear of regulatory sanctions in the home country

[6] The respondents included commercial banks, private offshore banks, insurance companies, money service businesses, trust and company service providers, credit unions, broker/dealers, bank and trusts, asset manager, fund administrator, trustee.

AIMS OF THE PROJECT

21. The region completed its last ML/TF cases publication in 2018. The finalised fourth-round mutual evaluation reports together with: the updates given by financial intelligence units (FIU) Heads at the CFATF Heads of FIU meetings; the available annual reports of regional FIUs; and media reports; have indicated that the region is making strides in the investigations and prosecutions of money laundering. However, the non-compilation and categorisation of these cases obfuscates the region's ability to benefit from this through the publication of trends (emerging, declining or continuing) and typologies.

22. This project will compile and categorize regional ML and TF cases (investigations and prosecutions) and will also enable the CRTMG to have a categorised list of ML/TF activities from which future projects may be selected for further study.

SCOPE OF THE STUDY

23. The target areas are the CFATF members in general including the FIUs and other law enforcement Financial Investigations Units. The cases selected for inclusion in the project report will be based on regional ML/TF investigations and prosecutions. The FIUs submissions are based on the analyses of suspicious transactions reports (STRs) which the FIUs receive from their reporting entities.

METHODOLOGY

24. Cases were compiled from primary sources of information using a standard data collection template which includes sanitization guidance**.** Additionally, internet research and FIUs annual reports were used where applicable.

MONEY LAUNDERING CASES

1. Association with corruption;

Source country: Cayman Islands

Details

25. A local bank reported that it held four investment accounts: one for company F, and three accounts A, B and C on behalf of members of a family of foreign politically exposed individuals. Over the course of a 2 year period, Company F received funds from an overseas company, which it immediately transferred to the investment accounts for A, B and C. The bank filed a defensive SAR indicating that while there was negative media concerning the individuals and the investment manager managing the accounts, it had no reason to suspect criminal activity.

26. In reviewing the SAR, Financial Reporting Authority (CAYFIN) obtained copies of the investment account activity and the bank's internal risk and compliance reviews concerning the business relationships, including the account opening and remediation documentation. A review of the account activity showed that substantial high value incoming wire transfers received into the account of company F were from a company that had been linked to state level corruption in a foreign jurisdiction, as well as from one of the individual's employment with a state owned corporation that had undergone privatization. It was also identified that while subscriptions and redemption activity was observed in the investment account, there was very limited information as to what the actual investments related to. The accounts in question were being managed entirely by an indivdual investment manager, a lawyer in Jurisdiction A, who has been identified in open source media as being a front man and money launderer for the family in question.

27. Further reviews also revealed that the accounts were previously administered by the bank's parent company, a private bank in Jurisdiction A. The accounts were transferred to the management of the Cayman Islands bank, but certain indivduals at the parent bank were still actively involved in all decision making on the business relationships in question. There were also indicators that the Cayman Islands bank had failed to adequately risk assess and monitor the accounts in question due to the parent bank having waived and/or made exemptions to certain CDD requirements.

28. CAYFIN determined that there was basis to suspect that the funds held in the accounts were likely proceeds of corruption. The matter was disclosed to domestic law enforcement agencies, the Cayman Islands bank's regulator and relevant overseas financial intelligence units.

29. An update subsequently reported that the investment manager had requested that the monies held be transferred to another jurisdiction, where the individuals already held business relationships. A disclosure was made to the FIU in this jurisdiction to alert them that CAYFIN believed the funds to be proceeds of crime.

Result

30. Disclosures to local law enforcement and an overseas FIU.

2. Structuring of illegal proceeds; currency exchanges;

Source country: Cayman Islands

Details

31. Media reports identified that Customer G had been been arrested in Country X for attempting to smuggle an illegal substance internationally. Customer G subsequently pleaded guilty to a charge of illegal drug exportation in an overseas federal court. It was speculated that another individual, Mr. A, was an accomplice of Customer G but those allegations had been denied.

32. The Financial Reporting Authority (FRA) issued directives for Customer G's remittance activity. A review of the remittance activity noted that Customer G was sending funds to Mr. A, thus demonstrating a material financial connection. Further research by the FRA indicated that Mr. A had visited the Cayman Islands on several occasions and that Customer G provided him with accommodations during those visits.

33. The FRA also issued directives for Customer G's banking records. A review of the bank statements identified substantial cash deposits into Customer G's account that appeared to be inconsistent with his customer profile. In addition, Customer G had made multiple ATM cash withdrawals.

34. In addition, the FRA was able to establish financal links between Customer G and other individuals in the overseas country, which led the FRA to suspect that they could be Customer G's co-conspirators in a larger drug trafficking enterprise.

35. The information in the SARs and the results of the FRA's research was disclosed to domestic law enforcement agencies and the overseas Financial Intelligence Unit of Country X on the basis of Customer G's involvement in drug trafficking.

Other methods identified:

- Use of different locations of the MSB to send remittances to avoid detection
- Excessive cash deposits not in line with expected account activity

3. Identity fraud; use of false identification

Source country: Grenada

Details

36. On March 23rd and 24th 2016, a Spanish national withdrew US$38,700 from an account at two local banks. While conducting transactions at one of the banks, the police arrested the Spanish national. EC$8,010 and US$15,620 respectively were recovered from her possession.

37. Investigations revealed that sometime in 2016, the Spanish national, accompanied by an accomplice, departed a South American country. The pair visited the Dominican Republic where they met with another accomplice who gave them

money, an account statement for a bank account in Grenada, and a fake passport bearing the Spanish national's photograph in the name of the account holder.

38. Using the fake passport which carried her photograph but has the name of a real customer of that bank, both the subject and her accomplice sent a quantity of the stolen monies to the Dominican Republic, via two money remitters.

Result

39. The Spanish national was charged with fraud and money laundering, pleaded guilty and was fined the sum of US$7,361.33 on summary conviction. The fine was subsequently paid, and she was deported. Her accomplice was able to elude capture.

4. ATM fraud

Source country: Grenada

Details

40. In late October 2016, an East Asian national arrived in Grenada from a Caribbean country. On November 7, 2016, information received led police (FIU) to carry out a search of his hotel room. That search revealed a large quantity of US and EC cash, one laptop computer, sixteen dummy ATM cards, one router, two flash drives, one external drive, one ATM card reader and two USB cables.

41. The subject was interviewed under caution and he confessed to cloning ATM card holders' information onto dummy cards in his possession and using those cloned cards to make cash withdrawals from persons' accounts through ATMs in Grenada.

42. It turned out that the subject was in Grenada and receiving information from an accomplice in East Asia who was stealing information from persons in that region who used ATMs. That information he then cloned onto the dummy cards he possessed and used the cards to make withdrawals at ATMs.

Results:

43. He was subsequently charged with fraud and money laundering offences. He pleaded guilty and was fined the sum of US$7,361.33 on summary conviction. The fine was paid, and he was deported from Grenada as ordered by the Court.

5. Structuring

Source country: Guyana

Details

44. A few cases involving subjects who had each received numerous transfers from a single sender in the USA were reported. The recipients often visited the Money Transfer Agency (MTA) together to receive the transfers. Some recipients exhibited uncooperative attitudes towards the MTA agents when Customer Due Diligence (CDD) information was requested. The pattern of transactions suggests that the individuals are part of a smurfing network connected to the senders in the USA. Information collected suggests that receivers are recruited to facilitate collection and/ or transmission of funds between the parties. The patterns also suggested that recipients are being replaced as soon as the risk of detection

increases, facilitating the continuation of the suspected laundering scheme. These currency movements (volumes and jurisdictions involved) are suspected to be connected to illegal activities, such as drug trafficking and/ or human trafficking.

Result

45. The information was shared with the relevant law enforcement agency for further investigation.

6. Fraud by false pretence; skimming and harvesting of bankcards

Source country: Montserrat

Details

46. An analysis showed that several cheques which were issued by Subject A were being returned as a result of 'Non-Sufficient Funds', along with unusual activities which reflected an abuse of the financial services being provided to Subject A. Additionally, over a period of time Subject A had been issuing cheques to business places and individuals in exchange for cash.

47. Further analyses of Subject A's financial records showed that he is in a poor financial state and as a result, Subject A tried to manipulate the banking system by "Cheque Kiting[7]" to sustain himself, his business and his family, financially.

48. Subject A's behavior is consistent with Cheque Kiting Cheque Kiting is a fraud scheme that usually involves several Cheque accounts at several different banks. It is done by the deliberate issuance of a Cheque for which there is not sufficient cash to pay the stated amount. The purpose of Cheque Kiting is to falsely inflate the balance of a chequing account in order to allow written cheques to clear that would otherwise bounce), hence the reason for the report.

Result

49. Pending further action.

7. Fraud

Source country: St. Kitts-Nevis

Details

50. A suspicious transaction report (STR) from a bank in Country A revealed Law Firm "L" in Country A was contacted, via email, by unknown person(s) "U" whereabouts unknown, seeking legal consultation services.

51. U (Creditor) informed L that legal assistance is sought to obtain an outstanding amount on a US$450,000 loan that U advanced to Debtor D and the balance is due and payable.

[7] Cheque Kiting is a fraud scheme that usually involves several Cheque accounts at several different banks. It is done by the deliberate issuance of a Cheque for which there is not sufficient cash to pay the stated amount. The purpose of Cheque Kiting is to falsely inflate the balance of a chequing account in order to allow written cheques to clear that would otherwise bounce), hence the reason for the report.

52. U provided L with copies of documents purporting to be a Loan Agreement between U and D; US$450,000 loan Cheque payable to D from U; and partial payment Cheque payable to U from D.

53. U obtained L's contact details e.g. address, under the guise that the information would be shared with D to inform that L has been authorised to act on U's behalf to obtain outstanding amount.

54. A couple of days later U told L that D would be making a partial payment "without delay" to avoid litigation. Soon thereafter L received what appeared to be a cheque (purportedly issued by a bank in North America) via registered post. U instructed L to deduct legal fees and forward the remainder to U. It was later discovered that it was a dishonored cheque as the payee, date and amount were altered.

55. This was an attempt by U to fraudulently obtain funds from L's bank account via foreign cheque fraud scheme. It is observed that U only communicated with L via email.

Results

56. FIU issued an advisory to the legal and financial sectors to alert them about the scheme and assist in the identification of potential fraud aimed at depleting unsuspecting person's bank account. Information was also shared with law enforcement and the AML Regulator.

8. Suspicious cash deposits associated with illicit drug trade

Source country: St. Kitts-Nevis

Details

57. Individual X, in Country A, deposited approximately US$7,000 cash (in local currency equivalents) to X's bank account immediately followed by US$14,000 withdrawals - two (2) foreign currency purchases on X’s behalf collectively valued at US$7,000; and three (3) wire transfers, collectively valued at US$7,000 to Company A in North America.

58. X stated that the cash deposit was income from X’s business, located in Country A, that was being saved over a period of time. It was noted that the deposited funds mostly comprised small denominations (US$5, US$20-dollar bills).

59. An STR indicated that X was convicted for possession and intended sale of illicit drugs in Country A.

60. X was previously featured in the FIU's database in a request for assistance from the police in Country A. The FIU was requested to assist with an illicit drug investigation where X was charged for possession and intent to supply.

61. Enquiries revealed that X was recorded as sending funds, via money remitters, to individuals in Europe, Caribbean and North America. These countries have been associated with the illicit drug trade.

62. Based on X's previous conviction and small denominations of funds, X might currently be involved in illicit drug trade and the deposited funds are proceeds of this activity.

Result

63. FIU's Case Disclosure forwarded to law enforecement agency.

9. Structuring via wire transfers

Source country: St. Kitts-Nevis

Details

64. STRs revealed four individuals (A, B, C and D) in Country X sent funds to the same individual, Recipient E, in Country Y. It is noted that over a 3-month period the Senders collectively remitted US$35,000 in 14 transactions via money remitters. Some of the Senders were featured sending funds on the same day.

65. The senders are listed in the low-income category. Individuals A, B, and C are identified as being employed in the "services/sales industry" earning minimum wage. Individual D's listed employment was "in construction industry".

66. Source of funds unknown. The amount of funds sent by individuals over the short time span does not fit their financial profile low income category.

Result

67. FIU's Case Disclosure forwarded to law enforecement agency.

10. Government salaries fraud

Source country: Trinidad and Tobago

Details

68. Following LEA enquiries and negative media publications, SARs were filed which triggered investigations. They involve 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.

69. 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'.

70. Through the manipulation of payroll information by the payroll officer at X1, unauthorised 'salary payments' were moved from X1 payroll account to:

- multiple personal accounts,

- multiple (personal) loan accounts, and
- several accounts of 'shell' structures.

71. 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.

72. The criminal activity identified in this case were: conspiracy to defraud; falsification of accounts and unauthorised payment of salaries.

73. The FIU received several STRs/SARs from multiple FIs. Analysis of the STRs/SARs 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 shell structures 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 laundered over TT$ 3 million from his account, illicitly obtained from X1.
    - Two Subjects in the criminal network were flagged for remittance of funds to countries with high risks for human trafficking.

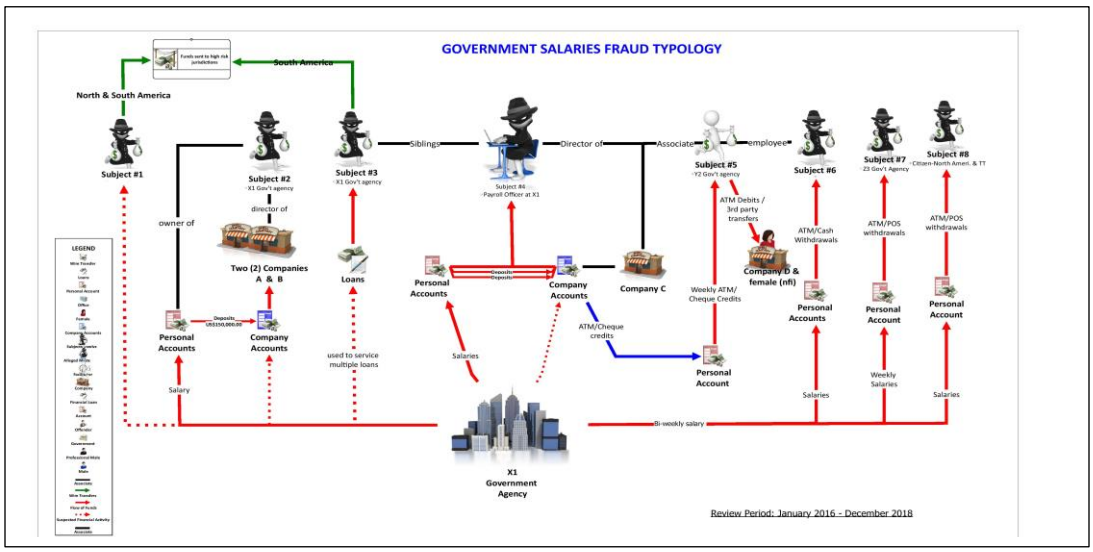
Result

74. Over 100 money laundering charges were brought against 11 Subjects for TT$ 22 million (US$ 3.5 million) which was laundered through this criminal network.

    Identified factors:

    - Association with corruption
    - Structuring
    - Wire transfers
    - Co-mingling of funds
    - Use of shell companies
    - Use of family members and third parties
    - Identity fraud
    - Revolving loan payoffs, cheque payment to legitimate companies

Chart 1: Government salaries fraud



11. Fraud through the use of shell company

Source country: Venezuela

Details

75. A natural person who, through a company that he/she owns that was not registered in the National Contractor Registry, manages to establish business relationships with other companies, signing contracts with markups up to 200%, and earning profit of considerable value.

76. A Trading Company with little trading history, no Income Tax Declaration and no employee payroll record (shell company), managed to establish business relationships with companies in the production sector of the country and other related business, to sign contracts with markups. This company was also able to fraudulently obtain large sums of money, using as instruments cash (Bolivars and foreign exchange), cheques, bank accounts, foreign currency accounts, goods of all kinds and credit cards. The contracts which were established with companies in the production sector of the country and other related companies exceeded US$27 million.

Results:

77. The natural person (the shareholder) was sentenced to a term of imprisonment for four (4) years and four (4) months for crimes enshrined in the laws against Corruption, and the Organic Law against Organized Crime and Terrorism Financing, as well as house arrest and a fine valued at forty (40) % of the property damage to other natural and legal persons involved in the case.

Identified factors:

- Association with corruption
- Currency exchanges
- Use of credit cards
- Purchase of valuable assets
- Investing in capital markets
- Co-mingling (business investments)
- Criminal knowledge of and response to law enforcement/regulations

TERRORIST FINANCING CASES

1. Funds bearing linkages to Individual suspected of terrorism activities

Source country: St. Kitts-Nevis

Details

78. STRs filed by two banks identified funds wired from a Middle Eastern country to bank accounts in Country B located in the Caribbean. Incoming funds were sent on behalf of Individual A, a Middle Eastern national believed to be residing in the Middle East region.

79. While undertaking due diligence requirements, Country B's banks discovered Individual A was identified on the USA's Sanctions list - Office of Foreign Assets Control (OFAC) Specially Designated Nationals List for suspected terrorist activities. According to the "List" it is alleged that A supplied equipment to the Islamic Revolutionary Guard Corps (IRGC)-.

80. The FIU in Country B issued freeze directives over incoming funds - approximately US$621,000 bearing linkages to Individual A, at two banks in Country B.

2. Suspected abuse of NPO

Source country: Trinidad and Tobago

Details

81. A faith-based charitable organization ("YZ") was established in the early 2000's and established a banking relationship with Bank A ("the Bank") the same year. The principals of the YZ, stated that YZ was formed to fund the renovation of local places of worship of the same faith as the YZ. Accounts were opened at Bank A to facilitate the collection of donations from local persons of the same faith; with the signatories being four members of the board of the YZ.

82. Subsequent to a natural disaster in a Caribbean territory in the late 2000's, the YZ sought to provide aid to the victims of the territory with one of their main goals being to build a place of worship on the said territory. The YZ solicited (via telethon) and received donations from the public for the purpose of assisting the Caribbean territory. In or about 2011-2012, another telethon was hosted to raise funds for the victims of a natural disaster in a Middle Eastern country. In the preceding twelve months, cash deposits to the YZ's account was approximately TT$1,500,000.00 (US$221,306.50); the volume and value of these cash deposits were deemed not to be consistent with that of a charitable organisation and what the account was initially established for. Bank A was later contacted by a representative of the YZ, Mr. T, whom advised Bank A that the YZ would be partnering with other foreign NPOs to provide relief to those affected by natural disasters in the Middle East jurisdictions.

83. At that time, the Middle Eastern jurisdiction was deemed as high-risk by the FATF, as deficiencies in the jurisdiction's AML/CFT system constitutes a ML/FT vulnerability in the international financial system. As a result, enhanced due diligence was carried out by the Bank A on the foreign NPO to whom funds were

to be transferred. Online open source revealed that the foreign NPO was a well-established charity in Europe which was undertaking extensive humanitarian work in a Middle Eastern jurisdiction. However, unconfirmed information was also unearthed which alluded to the foreign NPO being designated by another jurisdiction in the Middle East for operating under the guise of a tithing system but suspected of illicitly financing terrorism. Mr. T vouched for the legitimacy of the foreign NPO to Bank A. Checks also revealed that funds were remitted to another foreign-based NPO, headquartered in a North American city. Unconfirmed media open-source information also indicated that this foreign NPO had ties with a large terrorist organisation based in the Middle East and was allegedly financing terrorist activities. These allegations of terrorist ties were not confirmed by the competent authority in the North American jurisdiction.

84. In the late 2000's, the YZ indicated that donations would be sent to a jurisdiction located in eastern Africa to assist with relief efforts. Funds were again transferred via the two foreign NPOs identified previously.

85. In the mid-2000s funds were also transferred to a disaster relief fund for a jurisdiction in the Southern Pacific Ocean but was subsequently returned by the foreign financial institution. In the late 2000s, the YZ requested the transfer of funds to a third foreign NPO based in Europe. Enhanced due diligence conducted by the Bank revealed that this foreign NPO was linked to several suspected global terrorist organisations and the transfer was declined.

86. Media scanning reports also indicated that Mr. T has been making statements which sympathised with the suspected actions taken by some of jurisdictions' X nationals to support a designated entity in a conflict zone. Open source intelligence also revealed that Mr. T is also listed as a principal party to other NPOs within jurisdiction X. Subsequently, Mr. T was identified as travelling to an unidentified foreign jurisdiction, via Europe, he had approximately TT$ 339,000.00 (US$ 50,000.00) cash, which he claimed had been collected from charity donations. The ultimate destination and/or beneficiary of these funds could not be verified.

CONCLUSION:

87. Whilst it may be possible that the YZ is involved in legitimate charitable works and the funds collected and transferred were transacted with the intent of legitimate charitable activity, it is highly probable that the NPO could have facilitated the suspected financing of terrorism based on the following:

- The sudden change in the type of charity activity from local to international;
- Significant cash deposits being made within a short period of time where the true source and legitimacy of the source(s) could not be determined;
- One of the foreign NPO being from a country listed as a high-risk jurisdiction by the FATF;
- Large wire transfers to foreign NPOs whom are suspected of being involved in the financing of terrorism;

- Open source media comments by an associate of the YZ sympathising with the cause of nationals suspected of travelling to conflict zones;
- Mr. T of the YZ being identified as a principal party of two other local faith based NPOs;
- Mr. T travelling to foreign jurisdictions with large amounts of foreign currency on his person to possibly avoid scrutiny by banking officials and circumventing the tracing of funds via the financial system.

Chart 2: Suspected abuse of NPO