

CARIBBEAN FINANCIAL ACTION TASK FORCE



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

Typology Report on Money Laundering and Terrorist Financing

© 2018 CFATF. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Requests for permission to further disseminate reproduce or translate all or part of this publication should be obtained from the CFATF Secretariat at cfatf@cfatf.org

TABLE OF CONTENTS

Contents

LIST OF ACRONYMS USED IN THE REPORT 3

INTRODUCTION 4

OVERVIEW OF PREVIOUS CFATF TYPOLOGIES 5

AIMS OF THE PROJECT 8

SCOPE OF THE STUDY 8

METHODOLOGY 8

MONEY LAUNDERING CASES..... 9

1. *Use of cheque, wire transfer and trust company service provider* 9

2. *Use of virtual currency* 11

3. *Skimming, harvesting of debit cards and illegal trade in precious metals* 11

4. *Fraud by false pretence; skimming and harvesting of bankcards* 13

5. *Skimming and harvesting of debit cards*..... 13

6. *Tax evasion* 14

7. *Fraud, wire transfers* 15

8. *Transfers along high-risk corridors and structuring of transactions* 16

9. *Fraud involving transactions in the purchase and sale of real property*..... 18

10. *Tax evasion* 19

11. *Currency exchange* 21

TERRORIST FINANCING CASES 22

1. *Jihadi funded by credit - Use of credit card;* 22

2. *Self Funded Jihadi - Use of family members or third parties, Currency exchanges/Cash conversions; Wire transfers; Credit Cards; New payment technologies (Pre-paid card)*..... 23



LIST OF ACRONYMS USED IN THE REPORT

AML/CFT	-	Anti-money Laundering/Combating the Financing of Terrorism
ATM	-	Automatic Teller Machine
BMD	-	Bermudan Dollar
BNI	-	Bearer Negotiable Instrument
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
FIA	-	Financial Intelligence Agency
FIU	-	Financial Intelligence Unit
FIUTT	-	Financial Intelligence Unit of Trinidad and Tobago
IFSC	-	International Financial Services Commission
IP	-	Internet Protocol
IRS-CI	-	Internal Revenue Service - Criminal Investigation
ISIL/ISIS	-	Islamic State of the Levant/Syria
LEA	-	Law Enforcement Agency
MSB	-	Money Service Business
POS	-	Points of Sale
PPO	-	Public Prosecutor's Office
RAS	-	Reports of Suspicious Activities
RGD	-	Registrar General Department
SAR	-	Suspicious Activity Report
SOCU	-	Special Organized Crime Unit
STR	-	Suspicious transaction report
SUDEBAN	-	Superintendent of Banking Sector Institutions
TCSP	-	Trust and Company Service Providers
UNIF	-	National Financial Intelligence Unit



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 helpful 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 2008.
5. This report is a compilation of thirteen sanitized cases received from eight CFATF member countries, two 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 TYPOLOGIES

6. Subsequent to the publication of the 2008 ML/TF update, the CFATF published typology studies on:

i. Money laundering using trust and company service providers¹

7. 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.

8. 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.

ii. Human trafficking and migrant smuggling²

9. 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.

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

² <https://cfatf-gafic.org/index.php/documents/typologies/3564-cfatf-typologies-report-on-human-trafficking-and-the-smuggling-of-migrants-1>



10. 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 lotteries³

11. 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.

12. Based on the responses from CFATF members a total of 1,070 illegal lottery related investigations were conducted by five jurisdictions resulting in only twenty-five convictions during the period under review. Only one jurisdiction (Jamaica) recorded prosecutions/convictions.

iv. Movement of cash and negotiable instruments⁴

13. 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;

14. 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 islands 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.

15. 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;

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>



- 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 a 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 share with other law enforcement counterparts overseas.

v. *The proliferation of small arms and ammunition*⁵

16. 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 possible nexus to money laundering and terrorist financing.
17. The report concluded that small arms and ammunition are the main tools used in many of today's conflicts and are the cause of the majority 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.
18. The international communities 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.
19. It would appear that the existing legislative framework and current counter-measures, for the most part, to combat the proliferation of small arms and ammunition, have proven to be insufficient. Therefore, it is incumbent upon CFATF member states to seriously consider the recommendations highlighted in this report.

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



AIMS OF THE PROJECT

20. The region has not done a compilation of its ML/TF cases since the publication of the 2008 ML/TF typologies report. 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.
21. 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

22. The target areas are the CFATF members in general including the Financial Intelligence Units (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

23. Cases will be 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. Use of cheque, wire transfer and trust company service provider

Source country: Sint Maarten

Details

24. The FIU Sint Maarten carried out an analysis of a STR which resulted in a suspicion of money laundering arising from that analysis. Consequently, the FIU made a disclosure to the the Public Prosecutor's Office (PPO) which then started a criminal investigation based on that disclosure.
25. The analysis was triggered by three subjectively reported transactions filed by a bank in Sint Maarten. According to the bank, the transactions were a-typical for the profile of the subjects, a husband and wife, who both live in Sint Maarten. The origin of the money was not clear to the bank. The first transaction involved a cheque for USD 200,000 from a car rental company based in Sint Martin. The second transaction involved the cashing of a cheque from an offshore company located in a Caribbean island, for USD 1,000,000 whilst the third transaction was the transfer USD 600,000 to the northern American continent for the cash purchase of real estate.
26. The FIU subsequently consulted various open and closed sources of informtion and the following initial findings were made. The two subjects were the signatories of three private bank accounts with the reporting bank. They are also signatories of two other bank accounts, in the name of the car rental company, which is established in Sint Martin, and a restaurant, also located in Sint Maarten. The bank accounts are all denominated in US currency. Substantial cash deposits were made by the male to one of the private bank accounts. These deposits amounted to approximately USD 4 million, followed by cash pick-ups totalling of USD 3.5 million. Checks at the business registrations at the Chamber of Commerce revealed that the subjects were connected to several car rental companies, established in Sint Maarten.
27. The tax return forms filed by the aforementioned subjects do not justify the volume of the transactions (payments) made.
28. The FIU concluded that the analysis had to be extended. Further investigation was done on the offshore company that issued the cheque for USD 1,000,000. It followed that the management of this company is carried out by a Trust company located in Sint Maarten and that the ultimate beneficial owner of the offshore company is the female subject.
29. Further analysis of obtained banking information showed that the offshore company was fed by cash deposits carried out on behalf of the various car rental companies and a cash flow was uncovered between the said offshore company and another offshore company both of which are located in Sint Maarten, but incorporated and established in another Caribbean island. The cash flows between these companies totalled USD 1,000,000.
30. Additionally, money flows were discovered in relation to a bank account in the other northern American continent.
31. Regarding the the purchase of real estate in a northern American continent, information was also requested which led to more money flows being discovered between Nothr America and Western Europe.
32. The origin of the funds remained unknown and it was recognized that there was an interruption of the paper trail through: the issuing of cheques by the offshore company to the car rental companies; the cashing of these cheques by the various car rental companies



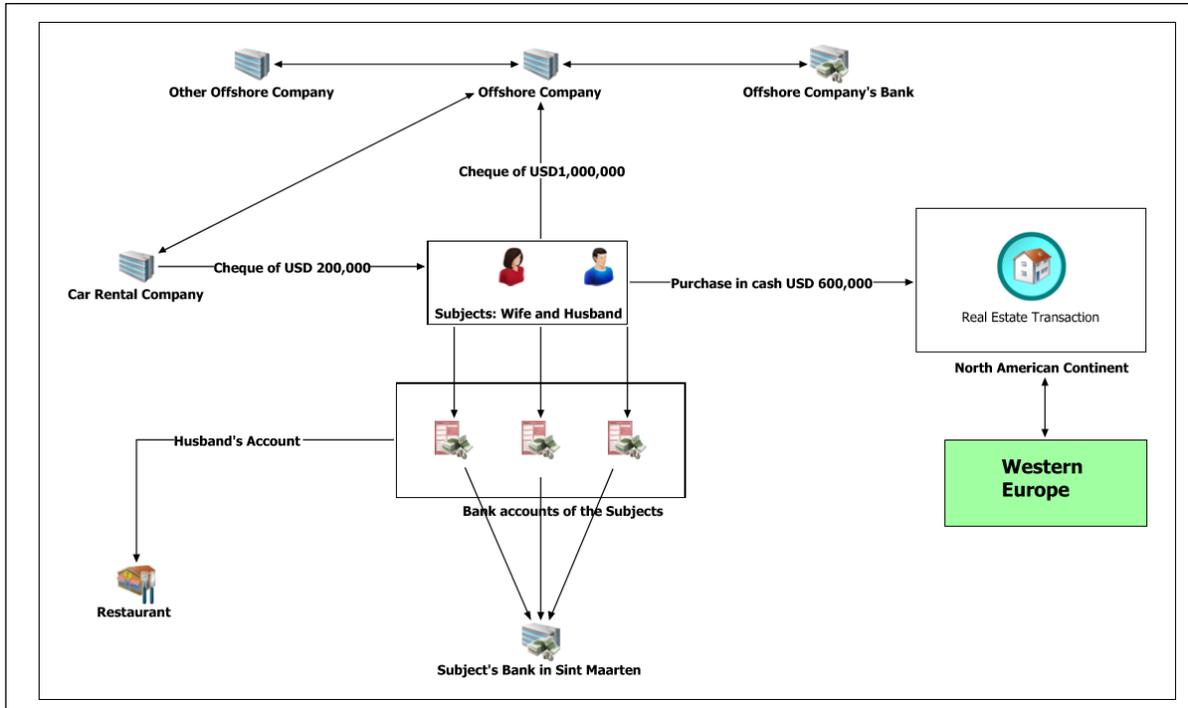
at bank A; and the subsequent deposit of these funds in the bank account of the offshore company at bank B after which transfers were made abroad.

33. It is not plausible that these funds were derived from the rental of cars. At this moment the source of the funds is being sought by the financial investigators.

Result

34. The case is in the criminal investigation stage.

Chart 1: Money laundering involving trust company service provider



2. Use of virtual currency

Source country: Belize

Details

Case 1

35. Based on enhanced due diligence (EDD), Company A, a registered agent for an international business company incorporated in Belize, submitted a report stating that a licensee, Company Z, was providing cryptocurrency conversion services⁶ to its clients. Company A indicated that it was not familiar with cryptocurrency regulation in the jurisdiction and whether the activity was permitted and thus reported the incident.

Case 2

36. Company B, a Belize incorporated international business company, purported to be engaging in international cryptocurrency exchange, made a report on its clients. Company B was not legally obligated to make a report as cryptocurrency exchange is not a regulated service and Company B is not a reporting entity. However, Company B reported that whilst conducting EDD on clients it discovered adverse information which indicated that some clients were involved in illicit activities and previously convicted of crimes such as fraud and drug trafficking. Company B indicated that it reported the matter on the basis that it is incorporated in the jurisdiction.

Result

37. Information regarding Case 1 was disseminated to the International Financial Services Commission (IFSC) which is both the regulatory authority for registered agents and the Director IFSC is the registrar general for international business companies.
38. Information regarding case 2 was disseminated, as a spontaneous disclosure, to the jurisdictions that maintained a nexus to the subjects.

3. Skimming, harvesting of debit cards and illegal trade in precious metals

Source country: Curacao

Details

39. A number of subjects of Venezuelan origin, transferred more than USD 220,000.00 predominantly via one money remitter, to various persons on six different surrounding islands. Some of the parties involved are also associated with the skimming and harvesting of debit cards and the purchase and sale of gold. According to the reports, the subjects appeared to be residing in hotels in Curaçao. About half of all the money involved was sent to the island of St. Lucia. According to the reports, the recipients of the amounts were also mostly residing in hotels. In addition, some of the senders of the amounts, via the money remitters, were also the recipients of some of the money on the other islands.
40. On the basis of several reports from a reporting entity, the jurisdiction concluded that some legal entities engaged in the trade of gold/jewelry, were also involved in this scheme. These legal entities transferred funds through a bank to persons of Venezuelan origin, residing on

⁶ The current position of the Belize International Financial Services Commission is that cryptocurrency services is not a licensed international financial services activity, notwithstanding the absence of any such specific prohibition in any Act in Belize. However, Belize has noted the recent updated FATF guidance on virtual assets (as contained in a CFATF bulletin of October 23, 2018) which encourages jurisdictions to properly regulate and supervise for AML/CFT purposes, persons engaged in such activity. Accordingly, Belize intends to update its legislation to align with such FATF recommendation and is currently consulting with the IMF to provide technical assistance in this area, as a part of a wider legislative upgrade



Curaçao. These persons then transferred the funds to other people, also of Venezuelan origin. In the descriptions of several transaction reports, a number of cases indicate 'proceeds of gold sales' and 'withdrawing funds from ATMs to purchase gold'. These transactions have been linked to the harvesting of the skimmed debit cards by Venezuelan nationals in St. Lucia and St. Vincent and the Grenadines.

41. Notable is that one subject received funds from involved legal entities and over a period of six months withdrew a total of USD 266,500.00 from his bank account followed by a deposit by cheque for USD 25,000.00 at another bank. This cheque was issued by one of the involved legal entities that provides pawning services.
42. The various transactions and statements indicate the trade in gold, with links to St. Vincent and the Grenadines. However, in St. Vincent and the Grenadines it is not permitted to purchase gold without a license. It is very likely that these subjects are involved in the illegal trade in gold which is being obscured by making use of many people and several islands. A total of 162 unusual transaction reports are represented in this case conducted by several subjects, with a total amount of USD 1,396.034,06.

Conclusion

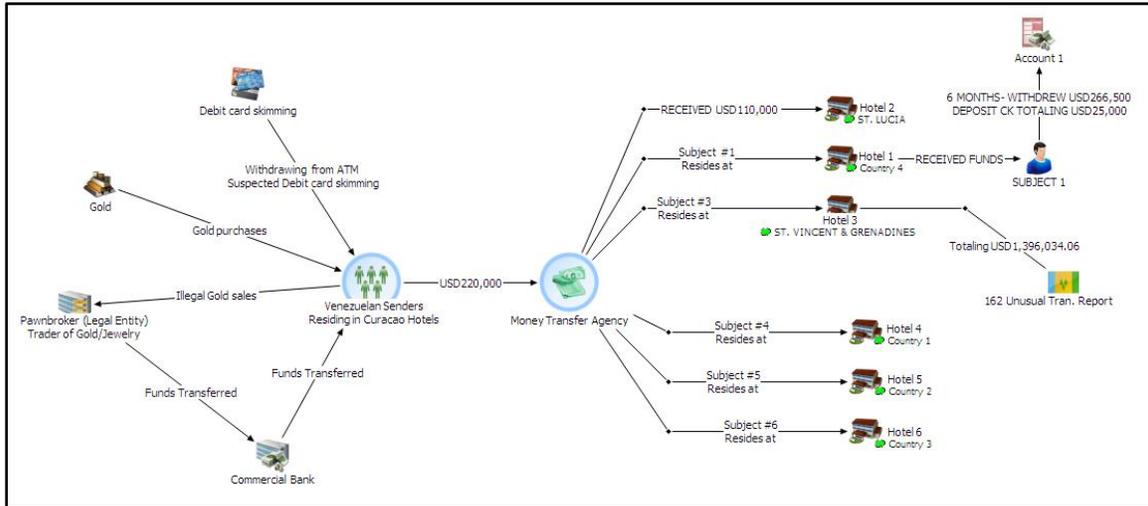
43. In a relatively short timeframe a group of non-residents transferred more than USD 220,000.00, via money remitters from Curaçao to other islands in the Caribbean. This took place by multiple persons and multiple transactions, where some of the persons involved are suspected of skimming bank cards and the harvesting thereof. In addition, the various transactions and statements indicate the trade in gold, with links to St. Vincent and the Grenadines. In St. Vincent and the Grenadines, it is not permitted to purchase gold without a license. It is very likely that these group of persons and companies are involved in the illegal trade in gold which is being obscured by making use of many people and several islands.

Result

44. On the basis of the above mentioned information, the several transactions were declared suspicious and forwarded in a intelligence report to the law enforcement agencies and public prosecutors office. It is unclear if this case turned into a criminal investigation.



Chart 2: Transfer of excessive funds via a money remitter and a bank by non-residents in Curacao to non-residents in a number of surrounding islands.



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

Source country: Grenada

Details

45. On review of a company's ATM cameras, subject A was observed making use of the machines at different locations using fraudulent cards. During the period the fraudulent cards were used, subject A received cash from the ATM machines totaling USD 7,000. A total of eighty-three cards were recovered from the Company's ATM machines. Subject A was caught at a shopping mall in the city and interviewed. He indicated that moneys were remitted overseas and there was a subject B involved who fled the jurisdiction. Subject A was subsequently, arrested and charge for the offences of Fraud by False Pretence and Money Laundering.

Result

- 46. Subject A pleaded guilty to four counts of Fraud by False Pretence and Money Laundering and was ordered to pay compensation to the bank in the sum of USD 7,000 and a fine of USD 3,745 in relation to the charge of money laundering.
- 47. A Removal Order was also granted by the court for the removal of Subject A from the jurisdiction after all monies are paid in full.

5. Skimming and harvesting of debit cards

Source country: Bermuda

Details

48. In early February 2016, an Eastern European visitor (accompanied by another Eastern European visitor) attended a local MSB with BMD 4,000 cash he wanted to send overseas. The suspects gave the MSB a local hotel address for their contact details. Suspicion was



raised because a non-Bermudian on vacation was in possession of a significant amount of Bermuda cash. The MSB had controls in place that limited the amount of wire transfers to BMD1,500 per day per customer. As a result, the MSB filed a SAR with the FIA.

49. Following an analysis by the FIA, it was confirmed that there was already an ongoing investigation by the Bermuda Police Service into the same suspects for using ‘skimmed’ cards loaded with stolen bank account information in local ATMs.

Conclusion

50. Investigations/intelligence revealed that the suspects were attempting to send funds overseas using other local MSB’s. In fact, some attempts were successful, and monies did leave the jurisdiction. A lookout was put in place which resulted in the suspects being arrested at the Bermuda international airport departure lounge where the two were found to have cash totaling \$19,833.00 made up of Bermuda and US currency.

Results

51. The two subjects were charged jointly for theft, attempted theft and money laundering offences. Both subjects plead guilty and were convicted and subsequently sentenced to two years imprisonment. Both subjects had fled the jurisdiction and one was eventually re-arrested and extradited back to Bermuda to serve his sentence. The second subject is still at large.

Other methods identified

The subjects seem to be methodical, professional criminals and launderers who came to the jurisdiction armed with several counterfeit cards. This suggests that there may be a broader network and or connected cybercriminals who steal and share the data for the fraudulent cards.

6. Tax evasion

Source country: Guyana

Details

52. Over several years several businesses were observed purchasing very large value Manager’s Cheques close to the end of the year and re-depositing these cheques early in the new year. It is believed that this practice is used to evade taxes, as at the end of the year the businesses net property value appears lower than it would otherwise be, due to the reduced bank account balances. The practice is believed to give the subjects comfort to disclose a lower bank balance in their property tax submission while disclosing an inaccurate (none or lower than actual) cash-on-hand value to the Tax Authorities.



Table 1: Showing the accumulated value for all suspicious manager’s cheque transaction and the estimated value (USD) of taxes evaded by the perpetrators for the period 2012 to 2017.

Description	2012	2013	2014	2015	2016	2017	TOTAL
Estimated Value of asset/ Cheques Hidden	2,615,116	6,717,988	6,823,776	6,400,859	7,858,140	8,549,104	38,964,982
Minimum Value of tax evaded	17,224	47,222	48,297	45,277	55,366	60,990	274,377

53. A wider review of this practice revealed it was endemic among certain businesses and was practiced for several consecutive years. It appeared to be a common method used by these businesses to cause their net property value to appear lower than it would otherwise be, due to the reduced bank account balances and non or inaccurate declaration for cash-in-hand at the end of the tax year. The manager's cheques are usually drawn in the name of the owners of the business.

Result

54. A detailed report on the activities of this group was sent to the Tax Authority. Intelligence reports were also sent to the Special Organised Crime Unit for investigation into possible money laundering.

7. Fraud, wire transfers

Source country: The Bahamas

Details

55. The FIU received a request for information from the police force with regard to a fraud matter involving a local person Mrs. Susan Cash and her husband Mr. John Cash who is a foreign national. The FIU, using its statutory powers under the Financial Intelligence Unit Act, Chapter 367, sent out production orders to various banks involved in the matter. Due to the FIU's production orders, a suspicious transaction was reported to the FIU by AA Bank & Trust Limited with regard to their client a Mrs. Cash, who is also an employee of the Bank. AA Bank and Trust stated that an unusual transaction report came to their attention alerting the bank that Mrs. Cash had been depositing and cashing several fraudulent cheques payable to companies, drawn on different banks. One of the fraudulent cheques was in the amount of USD 30,000.00 dollars. AA Bank & Trust Limited conducted further enquiries and it was revealed that several cheques and wire transfers were cashed and processed to the account of John Cash in another jurisdiction where he was residing at the time. All the information and documents received from the answered production orders, and information contained in the STR were given to the local police force to assist with advancing their investigation.

56. Based on a request from the local police force to freeze the accounts of Mr. and Mrs. Cash, the FIU froze these accounts for a period of eight days as prescribed under the FIU Act. The accounts were valued at approximately USD 154,000. The FIU was also asked by the police force to make an official request to the foreign country’s FIU to confirm the accounts of Mrs. Cash and Mr. Cash. It was confirmed by the foreign FIU that approximately USD 350,000.00 was wire transferred to Mr. Cash's accounts for educational and living expenses.



Result

57. Mrs. Cash was later arrested and charged with eighteen counts of fraud, two counts of attempted fraud, three counts of money laundering, thirty-five counts of possession of forged cheques and thirty-five counts of uttering fraudulent cheques. She pleaded not guilty before a Magistrate Court and was remanded to prison to await a bail hearing before a Supreme Court judge. Prosecution is pending.

8. *Transfers along high-risk corridors and structuring of transactions*

Source country: Guyana

Criminal dimension: Suspected laundering of proceeds⁷ of crime and structuring of transactions.

Details

58. Reporting entities observed multiple cases of persons transferring money to multiple individuals in high risk jurisdictions, in a structured⁸ manner. In some cases, multiple transactions are completed on the same day by the same individual. Some subjects resend money immediately after receiving a transfer themselves. In many instances the subjects could not demonstrate any level of acquaintance with the intended recipient which led authorities to believe that subjects were acting on behalf of a third-party. The funds are suspected to be related to the following illegal activities:
- i. Trafficking in Persons
 - ii. Drug Trafficking
 - iii. Illegal Mining
 - iv. Mail and credit card fraud
59. The subjects are recruited by individuals connected to the network of persons carrying out the illegal activities and may be paid small sums to conduct transactions on their behalf. The recruiters target persons in communities that are of lower economic status. Subjects are replaced once the reporting entity becomes suspicious, that is, the reporting entity request more CDD or EDD information. Recruiters attempt to spread their exercise across a large geographic area but despite their efforts patterns have emerged in the analysis showing clusters of activity in each of the targeted communities.

⁷ Proceeds of crime” can be defined as any property derived or realized directly or indirectly from a serious offence and includes, on a proportional basis, property into which any property derived or realized directly from the offence was later converted transformed or intermingled, as well as income, capital or other economic gains derived or realized from such property at any time since the offence

⁸ "Structured transaction" is a series of related transactions that could have been conducted as one transaction, but the customer intentionally broke it into several transactions for the purpose of circumventing the reporting requirements.



Chart 3: The activities of one sender who transferred money to various, recipients in various jurisdictions within a short period of time.

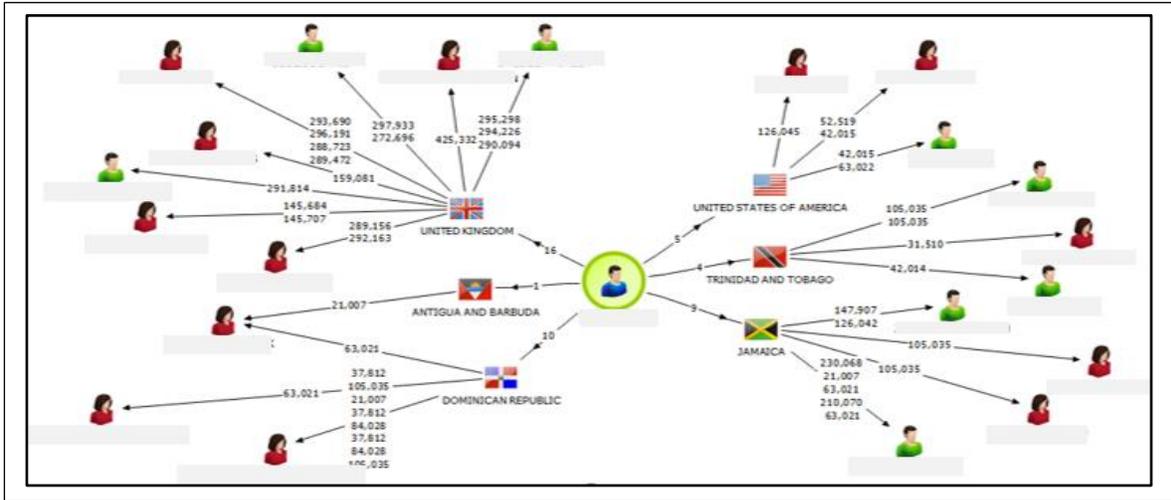
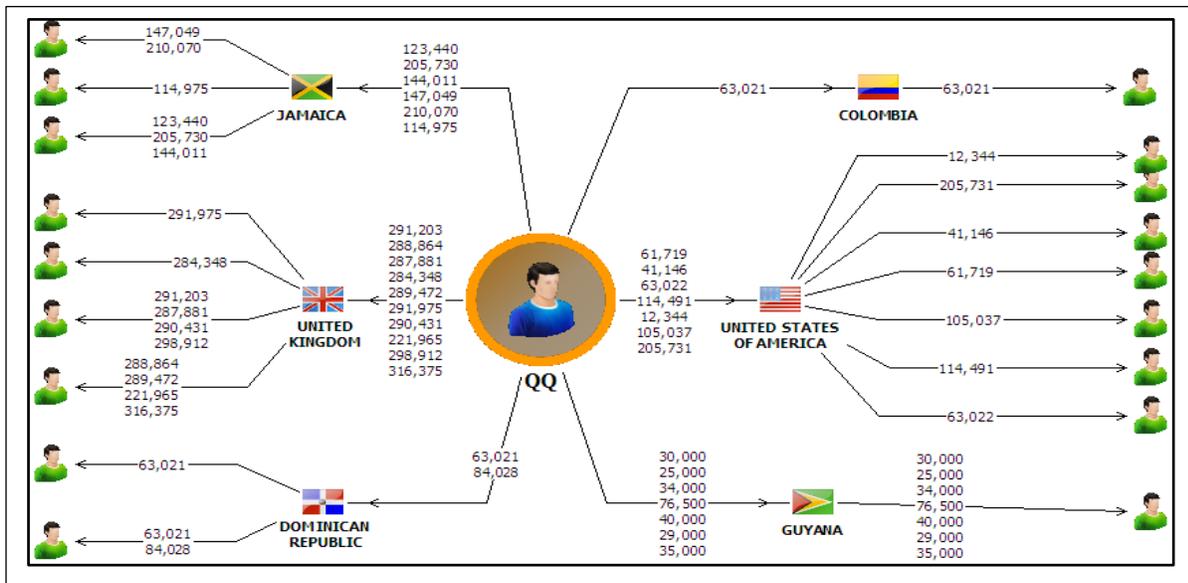


Chart 4: Activities of entity QQ by Country. The chart below shows individual QQ and his/her connection to eighteen persons through a total of thirty-four transactions valued at approximately GYD5.5M or approximately USD 26,000.



Result

- 60. The FIU prepared an analysis based on eighty STRs received from the reporting sector and concluded that there is a strong likelihood of illegal activities associated with the flow of money in the observed network of approximately 490 persons.



61. A detailed report was provided to the Special Organized Crime Unit (SOCU) for further investigation, and consideration for possible money laundering charges. Investigations are currently ongoing.

9. *Fraud involving transactions in the purchase and sale of real property*

Details

Source country: Trinidad and Tobago

62. X, purporting to be the owner of a parcel of land, enters into an agreement for sale of the land with A. Because of this agreement for sale, X provides a copy of his deed of ownership to A. This deed reflects X as the owner of the said land, having purchased the land from B.
63. A pays the down payment of more than 10% of the asking price of approximately USD 75,000.00 and seeks the services of an attorney-at-law who conducts title searches on the land for the sale to be completed.
64. Upon conducting title searches, several discrepancies were discovered including:
- The copy of the deed received from X, differed from the Deed held at the Registrar General Department (RGD), Land Registry;
 - The property description of the deed received from X differed from the Deed at the RGD, Land Registry;
 - The signature of the attorney-at-law whose name and signature appears as the preparing attorney on the copy of the Deed from X appears unusual;
 - The deed to X from B showed an extensive time lapse between the dates of execution, payment of stamp duty and subsequent registration e.g. a deed of conveyance for the sale dated December 2012 but registered with the RGD in July 2014;
 - In-depth title searches suggest a series of fraudulent deeds prior to the deed to X. The title search revealed conflicting deeds of conveyance from the previous owners to the person purporting to be the present owner of the land.
 - The deed received from X was purportedly drawn up by an attorney-at-law, stamp duty paid and then registered in the RGD - Land Registry. This deed appeared legitimate except that the signatures of the parties- the vendor (B), attorney-at-law and witnesses were all forged.

Result

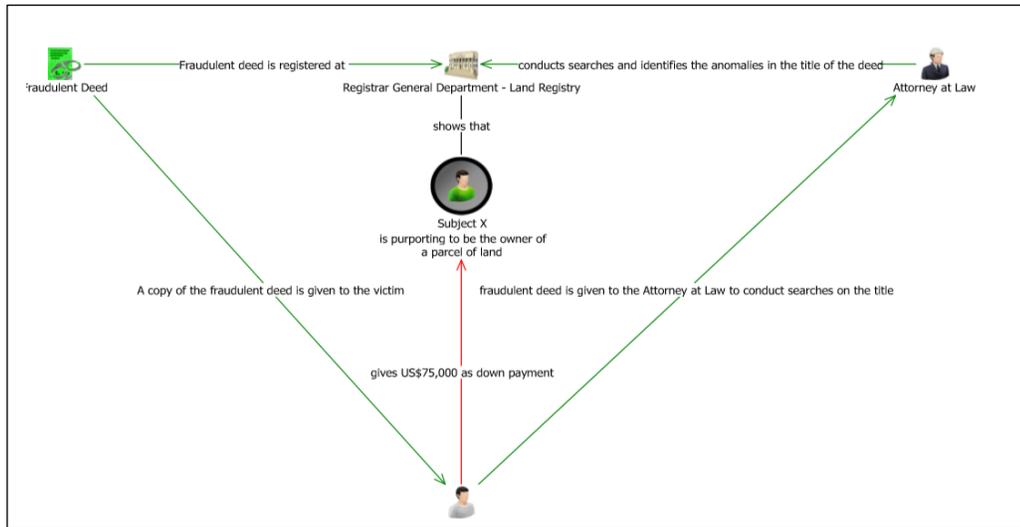
65. A strategic analysis report which detailed trends and indicators of real estate fraud was prepared by the FIUTT which also issued fraud warnings to the public, financial institutions, DNFBPs, the RGD and the Law Association of Trinidad and Tobago. An intelligence report was disseminated to LEA for investigation. After this action by FIUTT, similar fraudulent transactions were unearthed resulting in arrests and charges for fraud pertaining to real property.

66. Other methods identified

Knowledge of or access to: Unoccupied property; Unoccupied property owned by someone who has died or lives abroad; Property in which taxes and other assessments are unpaid for long periods, which suggest owner absenteeism; Official stamps of attorneys-at-law and procedures of government departments involved in the conveyancing process.



Chart: 5 Money laundering in real property using fraudulent deeds and conveyancing instruments



10. Tax evasion

Source country: Trinidad and Tobago

Details

67. The case concerns a US citizen, 'Blackjack' who created a complex scheme to avoid the payment of taxes on millions of dollars of income earned between 2009 and 2011 from a Private Members' Club (operated similarly to a Casino) registered in Trinidad and Tobago. The US IRS-CI was conducting investigations on Blackjack who was suspected of tax evasion in the USA and made an enquiry to the FIUTT. Pursuant to a request from the Internal Revenue Service - Criminal Investigation (IRS-CI) for financial information, the FIUTT conducted an analysis which revealed the following:

- A total of twelve STRs/SARs on 'Blackjack' from 2002 to 2006;
- These STRs/SARs revealed fourteen associates, including companies;
- In 2002 one of the twelve STRs/SARs, revealed that Blackjack sent a large wire transfer to a foreign jurisdiction;
- In 2006, the other eleven STRs/SARs were received in relation to frequent and large wire transfers out of Trinidad and Tobago.

68. Further financial analysis established:

- The existence of bank accounts held by Blackjack in financial institutions in Trinidad which were unknown to IRS-CI. This was deemed to be the most important piece of evidence in the investigation;
- The use of the third-parties (individuals & companies) which indicated attempts to conceal and disguise the identity of the ultimate beneficiary, Blackjack;
- That large cash transactions (for deposits, payment of insurance premiums & to fund outgoing wire transfers) were regularly conducted by employees of X1 Casino;
- That funds were moved outside of the jurisdiction by both individuals and companies.



69. A financial profile for Blackjack and his source of funds revealed financial flows amongst the suspect and his associated individuals, companies and businesses. The financial mapping identified the existence of several bank accounts in Trinidad held by Blackjack. This information was ground breaking to the investigation as it showed the full financial picture of Blackjack.

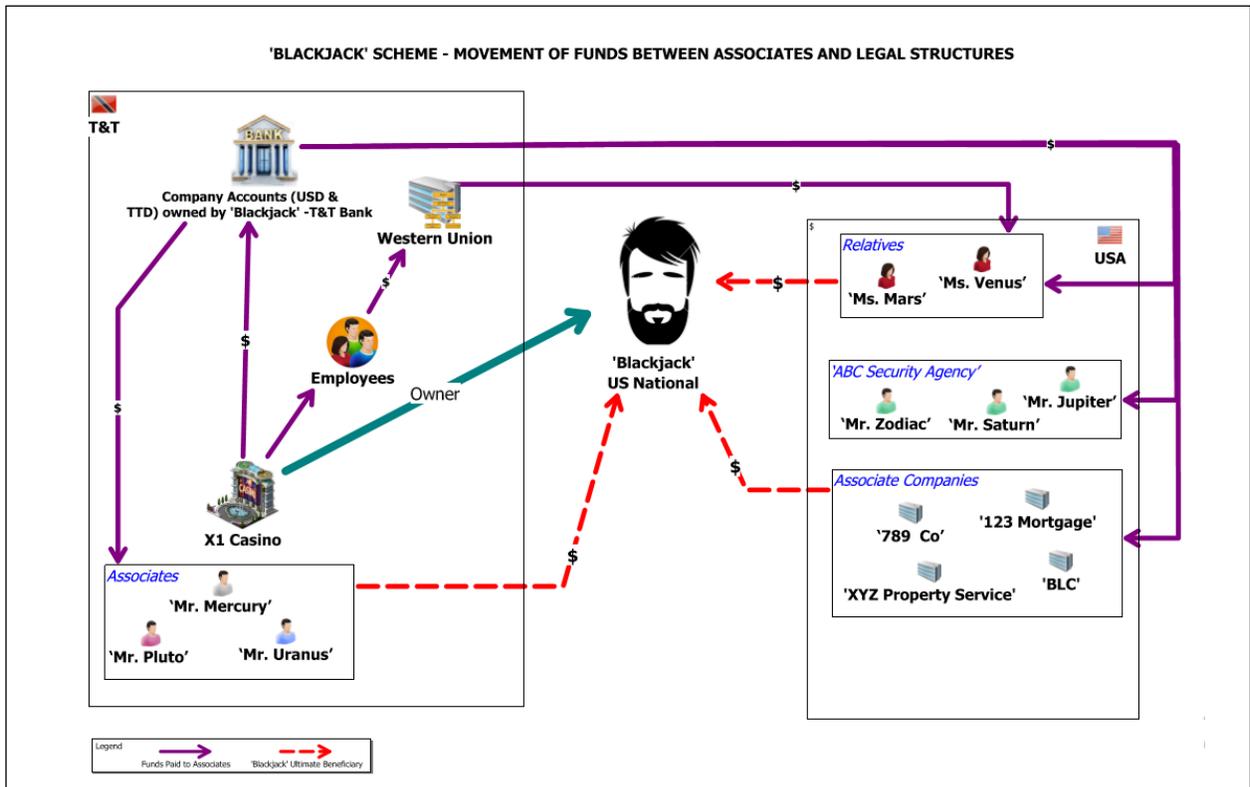
Result

70. The US authorities laid an indictment before the Grand Jury, in the District Court of New Jersey against 'Blackjack' for failing to file a U.S. Individual Income Tax Return (IRS Form 1040) for the tax years 2009, 2010 and 2011, and failing to report income that Blackjack received from X1 Casino which was registered and operated in Trinidad.

71. Blackjack pleaded guilty in the US and was sentenced to a forty-six months 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 to the IRS. Blackjack has paid all of his restitution which shows the success of this multi-jurisdiction tax investigation.

72. The U.S authorities official media release acknowledged the contribution of the FIUTT in securing the conviction.

Chart 6: Movement of funds between associates and legal structures



11. Currency exchange

Source country: Venezuela

Details

73. The Venezuelan Financial Institutions have been affected by the so-called "Banknote Mafias"; by virtue of the fact that the criminal organizations were given the task of selling Tickets, charging up to 35% of their real value as illegal commission, through cash advances through points of sale (POS), a situation that caused the shortages in the normal flow of cash, which generated an important alarm in the National Financial System and therefore in the citizenship; causing an impact on the normal development of the national economy.
74. In this sense, the Regulated Entities through the Reports of Suspicious Activities (RAS) highlighted the use of POS from Venezuelan border areas; as well as, regions of a neighboring country, through which transactions were made, an operation that could be verified by checking the Internet Protocol (IP) addresses of that country; Likewise, it was described in the detail of the motivation of the RAS natural and legal persons whose economic activities were related to the purchase and sale of products from the neighboring country.
75. In this regard, the National Financial Intelligence Unit (UNIF), through the Superintendent of Banking Sector Institutions (SUDEBAN), has implemented measures in the area of Prevention and Control of Money Laundering and Terrorist Financing (ML/ FT), to verify the proper functioning of the POS and mitigate the shortage of cash. In this sense, the Regulated Entities were urged to adopt preventive measures in order to prevent the aforementioned practice from becoming a rising typology and in a sustained manner over time, which could negatively affect the economy and the normal development in the statistics of the SARs sent to the UNIF.
76. In addition, the UNIF initiated an Inspection Visits Plan in conjunction with the Quality of Service Management for the purpose of overseeing the Institutions of the National Banking System (Public and Private Banking) to verify the daily operations regarding the availability of existing cash; as well as to the companies authorized to transport securities in the National Territory, with the purpose of taking the necessary corrective measures to mitigate the risks of said illegal practice. Among the findings found was complicity of some bank employees and some businesses; considering as a first measure to temporarily suspend the two franchises authorized to give cash advances as it was a network of auto markets and one of pharmacy. It should be noted that the businesses that incurred the improper use of the points of sale (rent, loan, among others); they were subject to sanctions, such as: the elimination of POS; as well as the closing of the associated bank account.

Result

77. It is important to know that there is feedback with the Financial Institutions with the purpose of informing them every six months about the behavior of the National Banking Sector through statistical information, based on a descriptive analysis of the Reports of Suspicious Activities received by the UNIF, related to the crimes of ML/FT or other crimes typified in the Organic Law against Organized Crime and Terrorist Financing; as well as, some outstanding typology in order to mitigate the risks.



TERRORIST FINANCING CASES

1. Jihadi funded by credit - Use of credit card;

Source country: Trinidad and Tobago

Details

78. 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 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, STRs/SARs were submitted to the FIUTT
79. *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 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.
80. *Financial Footprint*: Subject A utilized his credit card to purchase ten airline tickets to European, South American and Central American destinations. Credit card usage was also observed for living expenses along this route as well as an attempted transaction in Turkey.
81. *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 magazine 'DABIQ'.
82. *Inference*: Transactions conducted by Subject A indicates that he may have travelled to known terrorist jurisdictions and may have been financed by associates. The transactions highlighted also revealed that jurisdictions such as 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 activities.

Result

83. 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 be designated as a terrorist and assets frozen.
84. 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
85. Analysis conducted by the FIUTT also produced two Strategic Analysis Reports in (1) 2015- "Foreign Terrorist Fighters Travel Routes and Indicators" and (2) in 2017- "Foreign Terrorist Fighters and their Facilitation Networks." These reports were shared with Foreign FIUs, Law Enforcement Authorities, Financial Institutions and other supervised entities, the Central Bank of Trinidad and Tobago and members of the public.
86. Indicators to TF were identified and categorized according to the preparatory phase and travel and transiting phase as follows:

Preparatory Phase:

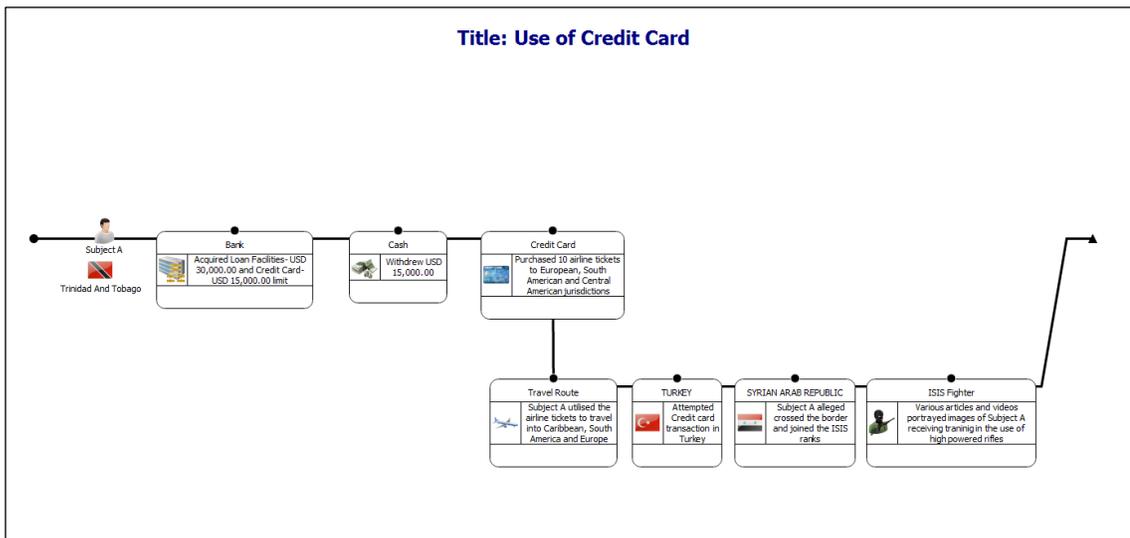


- Application of small loans and withdrawing the funds in cash shortly before departure;
- Sudden sale of possessions (e.g. car, house, jewelry);
- Sudden depletion/closure of accounts via cash withdrawals;
- Travel related purchases linked to conflict zones (e.g. purchase of airline tickets).

Travel and transiting phase:

- Transactions in jurisdictions suspected of being transit routes;
- Cash withdrawals at ATMs in recognized ‘hotspots’ in border areas close to conflict zones;
- Evidence of ‘broken travel’.

Chart 7: Jihadi funded by the use of credit card



2. Self Funded Jihadi - Use of family members or third parties, Currency exchanges/Cash conversions; Wire transfers; Credit Cards; New payment technologies (Pre-paid card)

Source country: Trinidad and Tobago

Details

87. 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 the then Prime 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 hit the headlines again in 2016, when he was featured in a lengthy interview in ISIS Dabiq magazine in which he encouraged sympathizers to "attack the interests of the crusader coalition, including embassies, businesses and civilians".



88. *Financial Activity*: 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 cash advances totalling 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 a total of USD 4,500.00 into the account of Subject T.
89. 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 the cash obtained by the said relative from Subject T's account remains unknown.
90. *Pre-Paid Card Purchases*: Subject T's pre-paid card was used to make purchases from Google Store for several gaming applications, which are strategy/tactical and weaponry based. The Subject 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.
91. The travel footprints of Subject T corroborated the existence of a known route utilized by suspected foreign terrorist fighter.
92. Intelligence received by the FIUTT also indicated that Subject T sold all his possessions such as motor vehicle and television for cash in an attempt to raise funds to facilitate the travel to Syria.
93. *Money Value Transfers*: During the years 2009 to 2011 Subject T sent several transactions totaling 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 a total of 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.
94. *Online Presence*: Subject T was also a central figure seen in videos and various media prints issued by or on behalf of ISIS. Subject T was described as a sniper and an English propagandists for ISIS and was tasked with encouraging sympathizers to support ISIL/ISIS and commit acts of terrorism/rebellion in their respective home countries.
95. *Inference*: The transfer of funds to persons within the high-risk Middle-Eastern jurisdictions and surrounding African territories as well as Subject T's participation in terrorist activities in Syria and his close affiliation with the other senders and persons suspected of traveling to join ISIS, all point to the possibility of terrorism financing.

Result

96. The U.S. Department of the Treasury listed Subject T on the Office of Foreign Assets Control, Specially Designated Nationals List in March 2017.
97. 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" ISIL.



98. 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.

99. Other methods identified

- Numerous low value wire transfers;
- Several senders to a common receiver in high risk jurisdictions known for terrorist activities;
- Transactions between unrelated parties.

Chart 8: Use of third-parties and wire transfers by for self-funded Jihadi

