CARIBBEAN FINANCIAL ACTION TASK FORCE

REPORT: CFATF Risk, Trends & Methods Group (CRTMG)-Rev 1

Money Laundering and Terrorist Financing Cases Update 2020

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
CDD	-	Customer Due Diligence
CFATF	-	Caribbean Financial Action Task Force
CRTMG	-	CFATF Risk Trends and Methods Group
FATF	-	Financial Action Task Force
FI	-	Financial Institution
FIU	-	Financial Intelligence Unit
LEA	-	Law Enforcement Agency
SAR	-	Suspicious Activity Report
STR	-	Suspicious Transaction Report
TCSP	-	Trust and Company Service Providers
USD	-	United States Dollar
VA	-	Virtual Asset
VASP	-	Virtual Asset Service Provider

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 2019.
5. This report is a compilation of thirteen (13) sanitized ML cases received from seven (7) CFATF member countries[1]. No TF typology cases were submitted. 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.

[1]British Virgin Islands, El Salvador, Guyana, Jamaica, Montserrat, St. Kitts-Nevis and Trinidad and Tobago.

OVERVIEW OF PREVIOUS CFATF CRTMG TYPOLOGIES AND OTHER STUDIES

i. Money laundering using trust and company service providers[2]

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.

ii. Human trafficking and migrant smuggling[3]

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

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

[3] https://cfatf-gafic.org/index.php/documents/typologies/3564-cfatf-typologies-report-on-human-trafficking-and-the-smuggling-of-migrants-1

conducted within the human trafficking category. The responses also indicated that human trafficking activities are associated with "Sexual Exploitation."

iii. Illegal lotteries[4]

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[5]

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 the CFATF member countries have declaration systems at their legal ports of entry. However, the majority of countries 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.
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;

[4] https://cfatf-gafic.org/index.php/documents/typologies/6949-illegal-lotteries-typology-project-report
[5] 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 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[6]

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.

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

20. With respect to licensed entities, 227 financial institutions were surveyed[7]. 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

AIMS OF THE PROJECT

21. The region completed its last ML/TF cases publication in 2019. 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.

[7] 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.

COVID-19-Related Cases

25. The COVID-19 pandemic has undoubtedly impacted the landscape upon which services are delivered, business is conducted, and illicit actors operate. Numerous jurisdictions within the FATF global network have reported changes in their national threat profile because of the pandemic. In some instances, the procurement process of critically needed Personal Protective Equipment (PPE) were targeted and payments diverted by criminal actors. In other cases, the delivery of targeted social services to those most vulnerable have been abused to facilitate fraud and ML whereby illicit actors capitalized on vulnerabilities created by the speedy delivery of financial relief. Although the use of new technologies, digital customer onboarding and delivery of digital financial services presents opportunities to ensure the continuity of the financial system whilst implementing required social distancing, it does come with inherent risks that must be effectively mitigated.
26. CFATF members have also detected COVID-19 related ML cases. This update features three (3) cases related to scams.
27. Additionally, several members have issued advisories warning of scams related to COVID-19.

Anguilla
https://www.facebook.com/1544774132458879/photos/a.1550892088513750/2656699564599658/?type=3&theater

Antigua and Barbuda
http://ondcp.gov.ag/ondcp-public-advisory-covid-19-fraud-alert/

Barbados
https://gisbarbados.gov.bb/blog/police-issue-caution-against-fraud/

Belize
http://fiubelize.org/wp-content/uploads/2020/06/Covid-19-Fraud-Alert.pdf

Cayman Islands
https://www.rcips.ky/rcips-fciu-highlights-increases-in-fraud-and-cybercrime-due-to-covid-19

Curacao & Sint Maarten
https://cdn.centralbank.cw/media/press_releases/covid-19

Eastern Caribbean Securities Regulatory Commission
https://ecsrc.com/gallery/NewsItems/detail/150

Eastern Caribbean Central Bank
https://www.eccb-centralbank.org/news/view/ecsrc-advisory-on-investment-scams

El Salvador
https://www.fiscalia.gob.sv/medios/2020/10/Ponentes-002.jpg

https://www.fiscalia.gob.sv/jefes-de-unidades-de-investigacion-e-inteligencia-financiera-de-la-region-ponen-en-perspectiva-los-retos-en-la-prevencion-de-lavado-de-activos-y-financiacion-de-terrorismo-en-tiempos-de-covid/

St. Kitts-Nevis https://www.fsrc.kn/documents/Advisory-Warning-to-the-Public.pdf

Trinidad and Tobago
https://www.fiu.gov.tt/wp-content/uploads/COVID19-SCAM.pdf
https://www.fiu.gov.tt/wp-content/uploads/ADV005_2020_Alert_for_the_Business_Community.pdf
https://www.central-bank.org.tt/sites/default/files/press_releases/joint-media-release-pyramid-scheme-alert.pdf

MONEY LAUNDERING CASES

1. Purchase of portable valuable commodities

Source country: British Virgin Islands (BVI)

Details

28. Mr. X was the subject of a Suspicious Activity Report (SAR) filed by a DNFBP operating in the BVI and supervised by the Financial Investigation Agency (FIA). The suspicion arose after the subject purchased a wristwatch priced at $60,500.00 on a layaway plan. The purchase was made by four (4) separate cash payments which took place over a four-day period as follows:

9th Jun 2020	Cash	$9,500.00
10th Jun 2020	Cash	$9,500.00
11th Jun 2020	Cash	$9,500.00
18th Jun 2020	Cash	$32,000.00

Results

29. A spontaneous disclosure was made to the Royal Virgin Islands Police Force Financial Crime Unit following an analysis by the FIA. The police investigations are ongoing.

2. Identity fraud; Use of non-domestic bank account; Wire transfers

Source country: British Virgin Islands

Details

30. A foreign couple from Country A was interested in constructing a vacation home in the BVI. Having been referred by acquaintances, the couple contacted a builder in the BVI. After much discussion, it was verbally agreed that the BVI builder would commence construction of the home once funds were received by the said builder. Email addresses were exchanged between the BVI builder and the interested couple and correspondence took place via email.

31. Some instructions on the transfer of funds to construct the home were provided to the foreign couple supposedly by the BVI builder. The funds were wired to a bank account in Country C.

32. During one of the email exchanges, the foreign couple, having sent the funds via wire transfer, enquired of the local builder what progress was being made on the construction of the home. The local builder denied receiving any funds from the foreign couple. He also denied providing instructions for the funds to be wired to an address in Country C.

33. After reviewing the exchange of emails, the foreign couple were convinced that the email of the local builder was possibly hacked. A report was made to law enforcement in Country A. However, law enforcement in Country A was unable to consider the matter and advised the couple to contact the authorities in the BVI. A subsequent report was made to the BVI FIA and an investigation was conducted.

34. The BVI FIA were able to contact the authorities in Country C to determine the recipient of the wire transfer. It was disclosed that the funds were received at a bank in Country C and cleared by an individual in said Country C who did not appear to have any connections to the BVI or to the BVI builder.

Results

35. The BVI FIA believes that the couple who were interested in constructing the home in the BVI was subject to a Nigerian 419 fraud scam. As a result, information was shared with the authorities of Country C as the monies were transferred from Country A by the couple who were citizens of Country A to Country C, rather than to the BVI to pay the BVI based contractor for the construction of the home.

36. The amount of money involved was approximately $150,000.00 USD.

3. Large Cash Deposits

Source country: El Salvador

Details

37. In this case, the installed capacity of the business has been used to try to justify cash deposits, product of the sale to the informal sector and their structuring; as well as the use of regional banks and exchangers for the transfer and payment of funds to final beneficiaries.

38. Person X dedicated to the importation of fruits and vegetables, mobilized the amount of US $34.7 million through various banks, by structuring 95% of cash deposits (remittances below the authorized threshold), according to current law, whose funds were transferred and collected in another jurisdiction by issuing cheques to different people, with values below the threshold established by law. It is important to note that Person X presented statements to a bank for the sales of the month, whose income coincided in part with the amount of imports, operating expenses and with the profit margin that it generated, except that simultaneously it was operating with another bank, which did not generate any greater suspicion for the first bank, except that on occasions the limit determined in its client profile was exceeded.

39. Another modality observed in the operation is the withdrawal of funds. Cheques began to be issued in the name of different people for significant amounts, who endorsed them to local money changers, and the latter deposited them in local bank current accounts; to later transfer said funds to a branch that they managed in another jurisdiction for payment to final beneficiaries, with which the traceability of the transaction was partly lost, the practice of which was done on a daily basis.

40. It is worth mentioning that even when Person X made real imports for the acquisition of products and local sales through informal merchants, what is observed is the attempted justification of the cash deposits that were made in accounts of different banks. According to Person X, most of his clients come from the informal sector.

41. The balances presented by the bank accounts in the name of Person X tripled the amount of the declared income, so there were also strong signs of tax evasion.

Results

42. The intelligence report was disseminated to the Public Ministry for its judicial process.

4. Use of Credit Cards, cheques, promissory notes

Source country: Montserrat

Details

43. Individual A is the owner of Business Y, a transportation service in County Z, which provides tour transportation and vehicle rentals. A review of individual A accounts shows a number of issued cheques being returned "NSF" (Not Sufficient Funds), consistent with cheque-kiting[8]. Additionally, according to information received by Institution X's Corporate Investigation Services the activity on the accounts was considered unusual reflecting an abuse of the facilities over a period of time and it was reportedly revealed that Individual A usually issues cheques to businesses and individuals in exchange for cash.

44. Individual A's business and personal accounts were closed by Institution X in 2018.

45. An analysis of Individual A's financial affairs revealed that over a period of time Individual A was writing cheques for amounts that were not available in his account.

46. While the FIU was in process of carrying out its inquiry, Individual A migrated. As a result, the investigation is still on going.

Results

47. Pending prosecution

5. Advance Fee Fraud/Trade-Based Related Fraud

Source country: St. Kitts and Nevis

Details

48. A Suspicious Transactions Report (STR) received from a local commercial bank indicated that approximately US$12,000.00 was fraudulently wired from Company A's bank account to a bank account in Country Y located in the North American region. The funds were sent in two (2) transactions seven (7) days apart. The beneficiary account was in the name of Individual X.

49. According to the STR, Company A placed an order for the supply of office equipment via email. An invoice purporting to come from a representative of Supplier W was received and Company A sent the payment. There was no confirmation of receipt of funds by Supplier W and Company A made contact with Supplier W via telephone.

50. Supplier W informed Company A that no payments were received, and the wiring instructions and email were not familiar to Supplier W.

51. Individual X is not featured in the FIU's database. Individual X might be a perpetrator or an unknowing participant of this fraudulent activity.

[8] Cheque kiting is a form of cheque fraud, involving taking advantage of the float or cheques clearance hold period to make use of non-existent funds in a chequing or other bank account.

52. Individual X's account is being used to facilitate a Trade-Based Related fraud. This information was shared with domestic LEA; and the FIU and relevant LEAs in the North American region.

Results

53. None given.

6. Unusual Large Cash Deposits

Source country: St. Kitts-Nevis

Details

54. An STR submitted by a commercial bank indicated that Company E's account received over US$200,000 in cash deposits during a 3-month period. There were multiple deposits.

55. Subject S is the recorded owner of Company E.

56. The frequent/unusual/large cash deposits far exceeded expected account activity especially during a period where there was limited to no economic activity island-wide in this business sector due to COVID-19 Pandemic.

57. A review of the FIU's database revealed that bank accounts of businesses located in the same area and owned by persons of the same ethnicity have been featured receiving frequent/unusual/large deposits.

58. Additionally, a Request for Assistance received from a domestic LEA, to aid with a financial investigation related to suspected smuggling of foreign currency, features individuals involved in suspicious smuggling who also operates a similar business in same location as Subject S. Data gathering was conducted, and findings shared with LEA to assist with investigation.

59. ML activities suspected in the cash deposits of over US$200,000 - source of funds unknown.

60. It is suspected that Subject S may actively be comingling laundered funds with those of legitimate business operations. Subject S might be in operation on his/her own or might be assisting others to launder funds by using his/her business place.

Results

61. FIU shared this matter with the domestic LEA responsible for conducting ML investigations.

7. Suspected Fraud – Romance Scam 1

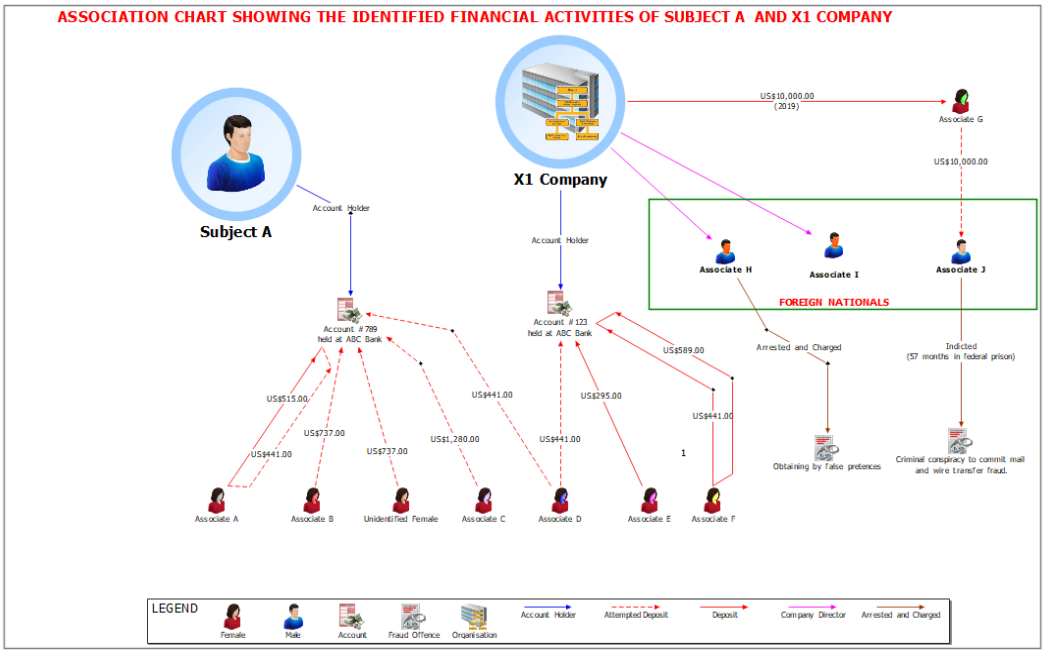
Source country: Trinidad and Tobago

Details

62. X1 Company Limited is owned by two (2) foreign Nationals. In mid-2020 four (4) deposit transactions were conducted into a USD Business account held in the name X1 Company Limited (one of the four deposits, was declined by the financial institution). The four (4) deposit transactions were made by three (3) women who claimed to have developed romantic relations with men over the internet, via social media. The women all claimed that they were promised gifts of jewelry, handbags, clothing and phones, which were to be mailed to them from various overseas locations. The women also indicated that their 'male friends' would ask them to deposit money into a local account held in the name of X1 Company Limited, to cover custom taxes on the packages. Once the initial deposit was made, the women would again be contacted by another person purporting to be from a shipping company, requesting additional funding for clearing packages or other taxes, to be deposited into the X1 company account.

63. One of the three (3) female depositors to the bank account of X1 Company, also attempted to deposit money into the account of another customer (Subject A) of ABC Bank. Subject A started banking with ABC Bank in July 2018. In December 2018 it was noted that deposits were being made to clear packages said to contain gifts. These depositors were females claiming to have met their 'male friends' online. Similarly, in June 2020, five (5) women made six (6) deposit transactions into Subject A's account, of which only one (1) was successfully deposited. The account holders of X1 Company Limited, were requested to explain the purpose of the deposits. The directors of X1 Company Limited was unable to provide a reasonable explanation for the deposits.

Chart 1:



Results

64. Disseminated to the relevant Law Enforcement Authority for investigations. The total value of funds deposited: US$66,926.45. The total value of attempted deposits: US$24,629.37

8. Suspected Fraud – Romance Scam 2

Source country: Trinidad and Tobago

Details

65. A female person (TZ), began interacting with a male individual (AB), whom she met on Facebook. TZ admitted that she was bored during the COVID-19 lockdown and developed a friendship with AB, who gave his identity as a foreign national. As the relationship progressed, AB offered to send gifts to TZ and sent photos of the items to her (see photos at Image 1, 2 and 3 below). TZ provided AB with her mobile telephone number and was subsequently contacted via WhatsApp by a third-party (XY), purporting to be from a shipping company. XY sent to TZ, bank account details via WhatsApp of a person (P1) who lives in the same country as TZ. TZ was asked to make a deposit to P1's account number in order to have the items from AB, shipped to her.

66. A SAR was filed to the FIU. It was discovered that seven (7) atypical deposits were made into P1's account by females at various branches of a financial institution. The funds were withdrawn immediately after deposit, either via ATM or over the counter. The suspicious transactions on the account showed: that the deposits were recent; the deposit activity was outside of P1's usual pattern of activity and did not fit P1's known income profile.

67. The total value of the funds acquired by perpetrators: US$3,885.74

Image 1: **Facebook Profile of AB**

Image 2: **Instagram Profile of AB**

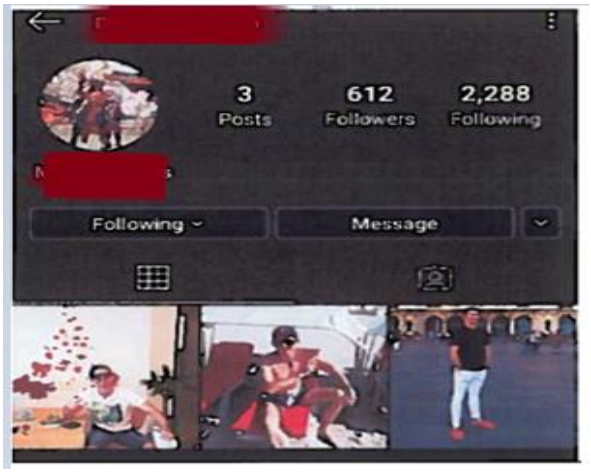


Image 3: **Composite pictures of items purported to be sent to TZ**

Results

68. Disseminated to Law Enforcement Authority for investigation. The total value of funds deposited: over US$3,880.00

69. Although the Romance Scam phenomena was observed in previous years, there was an increase in this activity at the onset of COVID-19. This event appeared to coincide with Government's travel and other restrictions on the movement of the population.

70. The most used social media platforms in the cases of romance scam, were Facebook and WhatsApp. It was observed that the relationship was engineered/initiated on Facebook and later progressed to WhatsApp. Facebook was used in most instances as the 'grooming tool' in the beginning of the relationship, where the 'trust' was gained.

71. As the 'relationship' progressed, the victims shared their mobile numbers, allowing the scheme to continue via WhatsApp. Through the mobile numbers, the perpetrator and third-parties, (who were part of the scheme), communicated with the victims.

72. **Consider:**

    a. Whether there may be a social/psychological impact - persons who may have lost funds but are embarrassed to report.

    b. Under reporting to LEA.

9. Conspiracy to defraud involving a politically exposed person

Source country: Jamaica

Details

73. Subject YZ, who is an officer employed in a senior position within a government agency, appeared to be living a lavish lifestyle, not commensurate with his remuneration. His lavish lifestyle was partly evidenced by the acquisition of assets, with no liens against them, which included four (4) motor vehicles and real property estimated to be valued at US$130,000.00. A STR filed by a FI also disclosed an account balance of at least US$48,000 in an investment account.

74. Analysis showed Subject YZ made credit card deposits and reported that the source of funds was from construction work done, however further interrogations indicated that Subject YZ was not associated with any registered businesses neither was there any evidence of income declaration to the Tax Authority. Additionally, Threshold Transaction Reports/Large Cash Reports, which were mainly cheque encashments, were triggered by Subject YZ, from the account of the government agency for which he worked. The purpose of the cash encashments was described as 'to pay workmen employed with the government agency'. The total value disclosed over a three-month period was at least US$172,270.

75. Investigations were conducted, resulting in evidence uncovering schemes devised to defraud the government agency's funds of over US$3.2M. The scheme included: the falsification of cheques and invoices and payment vouchers generated in the name of 'purported contractors' that carried out work on behalf of the government agency. Such contractors could not be verified.

Results

76. In 2019, Subject YZ and six (6) co-accused were charged with: Conspiracy to defraud; Possession of Criminal Property; Obtaining Money by Means of False Pretence; Uttering Forged Documents; and Engaging in a Transaction that involves Criminal Property, among other

charges. In 2020 Subject YZ and five (5) of the co-accused were found guilty of committing the offences.

77. Jamaica's Supreme Court ordered the restraining of property and other assets valued at approximately US$1.8M, which Jamaica's Financial Investigations Division is now taking steps to forfeit.

78. The investigation was carried out by personnel from the Financial Investigations Division and other of local law enforcement agencies namely, Major Organized Crime & Anti-Corruption Agency and Office of Contractor General.

Identified factors:

i. Association with corruption;
ii. Purchase of valuable assets;
iii. Use of forged documents;
iv. Abuse of client/customer relationship with a FI;
v. Use of family members & third parties.

Additional Factors to consider:

79. Corruption and the identification of a politically exposed person early in a banking relationship and the activation of enhanced due diligence procedures.

10. Money laundering involving the use of stolen identities

Source Country: Jamaica

Details:

80. Subject X, after adverse media reporting, established bank accounts, with several FIs, using different unique identification inclusive of ID numbers and dates of birth.

81. Some years after the adverse media report, Subject X received large wire transfers to his US$ accounts which were maintained at several FIs. The source of the funds was stated as being from bitcoin exchange/ online crypto currency trading and exchange service. A STR was filed.

82. Investigations revealed that Subject X had stolen the identities of US residents which was used to establish banking relationships and obtain banking facilities, including credit cards, in the names of the stolen identities. The credit cards, which were shipped to Jamaica, were then used locally to: withdraw funds; purchase a motor vehicle; purchase virtual assets (VAs) and other items. Funds were also transferred to the accounts of and for the benefit of Subject X's girlfriend and cousin.

83. The incoming wire transfers that were received represented the proceeds from the sale of the VAs which were purchased with the fraudulently obtained credit cards. Some wire transfers were returned to the virtual assets service provider (VASP) because Subject X was unable to adequately justify his source of funds to the FI. The FI was unaware of his fraudulent activities.

Results

84. In 2018 Subject X was charged with: engaging in a transaction involving criminal property; possession of criminal property; fraud; and money laundering.

85. In July 2020 Subject X pled quilty to the 14 fraud-related offences and was sentenced to a three-year suspended sentence and fined approximately US$45,000, which was paid the following day.

86. Several properties including real estate valued at approximately (US$385,000), bank accounts containing US$262,000 and motor vehicles valued at US$75,000 have been restrained pending the outcome of a civil suit against Subject X and his associates. Investigators are working alongside their overseas partners to obtain more information on the value of the VAs and the duration of the criminal activities. At least two (2) VASPs were identified through the wire transfers. The total value of Subject X's benefit is yet to be determined.

87. The criminal charges relating to money laundering, possession of criminal properties and engaging in criminal properties charges are still pending before the Court.

88. The investigation that lead to the successful prosecution so far, are as a result of the collaorative efforts of law enforcement officers from Jamaica and the United States, supported by the STRs filed by several FIs.

Identified factors:

i. Use of credit cards;
ii. Purchase of valuable assets;
iii. Wire transfers;
iv. Identity fraud;
vi. Use of VAs

Additional Factors to consider:

i. Use of third parties to receive funds in their accounts;
ii. The emerging and varied use of VAs

COVID-19 RELATED MONEY LAUNDERING CASES

1. COVID-19 related Fraud - Pyramid Scheme

Source country: Guyana

Details

89. Analysis of information received from licensed financial institutions reveals a growing trend of persons depositing funds into accounts of third parties, not known or hardly known to them. In most instances, the purpose of the deposit is stated as 'fees for clearing packages consigned to the depositor'. In other cases, it's indicated that the funds were for 'family assistance' or 'Payment for Box-Hand'.

90. Acquaintances are reported to have been established through communication on social media platforms such as Facebook and WhatsApp, by random telephone calls and through social engineering.

91. Some subjects were promised special assistance to relieve hardship caused by the COVID – 19 Pandemic and therefore completed and submitted documents (such as forms) containing their personal information, to questionable sites/domains.

92. The scammer persuades victims to send them money or deposit it their account to cover fictious Brokerage Fees, Customs Duties and/or Shipping Charges for package(s) containing valuable items which is about to be shipped to the victim or has to be cleared at customs.

93. The victim is sometimes persuaded to provide false information to the MTA concerning the purpose of the transaction, to ensure the transaction is not delayed, flagged or to cause the MTA to file a Suspicious transaction report. The MTAs appear to be aware of the 'package delivery scam' and have been flagging transfers which purpose is to clear packages.

94. A few persons attempted to reclaim the funds they deposited upon realizing they have been scammed. It was however observed that the funds were immediately withdrawn from the account by the scammer/s after which they discontinued all contact and communication with the victim.

95. With respect to persons who made deposits and claimed they were for box-hand payments, the banks recognized that none of the persons who made deposits received payouts, as is the custom in box-hand arrangements.

Results

96. These incidents are currently under investigation by law enforcement agencies (LEAs).

2. Mass Marketing Foreign Cheque Fraud - COVID-19 Pandemic

Source country: St. Kitts-Nevis

Details

97. An STR submitted by a commercial bank indicated that its client, a media house, was the target of a "Mass Marketing Foreign Cheque Fraud" scheme.

98. According to the STR, the media house was contacted via email by Subject B who claimed to be acting on behalf of Company P. The email stated that Company P sought the price rate to advertise an "Online Seminar Program" that it was planning to offer due to the COVID-19 Pandemic.

99. The media house provided an invoice for the advertisement services at a cost of US$2,215.00, in addition to bank wiring instructions.

100. Later that month, the commercial bank received a cashier's cheque, via mail, in the amount of US$22,150.00. The next day, Subject B contacted the media house stating that Company P had erroneously issued a cheque in the amount of US$22,150.00 instead of US$2,215.00 and therefore would like the difference to be reverted to him.

101. The media house informed the commercial bank that it only anticipated receipt of US$2,215.00 via wire transfer and not to deposit the cheque that far exceeded the quoted price to its account.

102. It was later determined that the cheque was a fraudulent document.

103. Neither Subject B nor Company P were previously featured in the FIU's Database.

Results

104. The FIU issued a Non-Public Advisory to media houses (print & broadcast) and financial institutions to assist with the identification of potential fraud. The information was also shared with domestic LEA and AML/CFT Regulators.

3. COVID-19 related Fraud - Pyramid Scheme

Source country: Trinidad and Tobago

Details

105. The Subject is an administrative professional employed with a Government Ministry in Country A1. The Subject established a personal savings account with XYZ Bank in mid-2011. The Subject's main 'known source' of income is salary of US$2,060.00 per month.

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

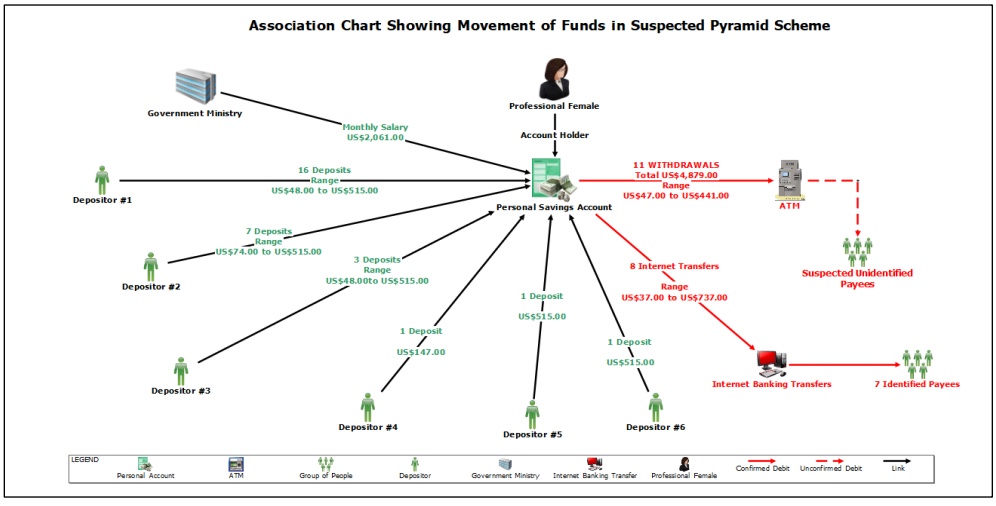
107. Over a one (1) month period, 29 deposits were made to the Subject's account. These payments were made by six (6) different third-party depositors (not the same depositors noted above). Of the six (6) depositors, one (1) individual made a total of 16 deposits of amounts ranging from over US$45.00 to over US$500.00. The total amount deposited into the account by the six (6) depositors was over US$10,000.00. Conversely, withdrawals from this account amounted to over US$62,500.00. These withdrawals were conducted either via ATM withdrawals (over 18 transactions ranging between US$40.00 to US$440.00), or via internet transfers (over seven (7) transactions ranging between US$35.00 to US$735.00). The payees of the internet transfers were seven (7) identified individuals.

108. The Subject indicated that the credits represented "gifts FROM friends" and the withdrawals were for the "purchase of gifts" FOR friends. The Subject did not provide any documents to support the claim, nor did the subject offer any further explanation, as the transactions were deemed personal by the Subject. Additionally, the Subject advised XYZ Bank that there was no current involvement in any business activity.

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

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

110. Chart 2: **Suspected Fraud – Pyramid Scheme**



Results

111. FIU shared this matter with the domestic LEA responsible for conducting ML investigations. This case, along with others of a similar nature, are pending investigation by law enforcement.

Value in this case: US$19,517.77