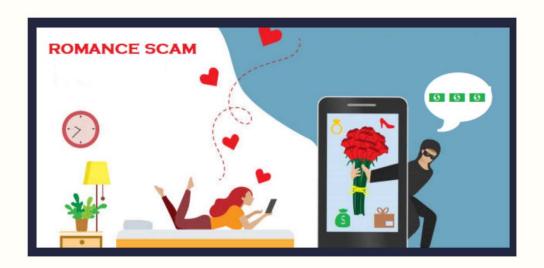


Government of the Republic of Trinidad and Tobago
MINISTRY OF FINANCE



STRATEGIC ANALYSIS REPORT - SA/001/2023-v3

THE ROMANCE SCAM/FRAUD PHENOMENON IN TRINIDAD AND TOBAGO







All rights reserved. This Report or any portion thereof may not be copied for commercial redistribution, republication or dissemination without the explicit written consent of the Director of the Financial Intelligence Unit of Trinidad and Tobago.

©Financial Intelligence Unit of Trinidad and Tobago, 2023

Website: Financial Intelligence Unit – Trinidad and Tobago (fiu.gov.tt)

Date of completion: July 2023

TABLE CONTENTS

LIST OF ACRONYMS	
EXECUTIVE SUMMARY	5
CHAPTER 1 – INTRODUCTION	6
• SCOPE	7
METHODOLOGY	7
ROMANCE SCAM – A DEFINITION	8
CRIMINALITY IN ROMANCE SCAMS	8
SOCIO ECONOMIC CONTEXT	9
A PSYCHOLOGICAL PERSPECTIVE	10-11
CHAPTER 2 – KEY FINDINGS	12
FINANCIAL INSTITUTIONS	12
STRs/SARs OVERVIEW	13-14
REPORTING ENTITIES	15
TTPS FRAUD SQUAD	15
VICTIMS' PROFILE	
PERPERTRATOR PROFILE	
ROMANCE SCAM STUDIES (CASE I)	
ROMANCE SCAM STUDIES (CASE II)	
OVERVIEW OF ROMANCE SCAMS (DIAGRAM)	
CHAPTER 3 – INDICATORS	27
INITIAL CONTACT WITH VICTIMS	
QUICK LOVE AND ISOLATION	27
PROMISES OF GIFTS, MONEY AND MARRIAGE	28
REQUEST FOR MONEY FROM VICTIM	28
REQUESTS FOR SECRECY	29
CHAPTER 4 – RECOMMENDATIONS	30
PREVENTION	30
DETECTION	31
SHARED NETWORK OF INFORMATION	31
CONCLUCION	22

LIST OF ACRONYMS

AML/CFT

Anti-Money Laundering/Countering Financing of Terrorism

CFATF

Caribbean Financial Action Task Force

FATF

Financial Action Task Force

FIUTT

Financial Intelligence Unit of Trinidad and Tobago

LB

Listed Business

LEAs

Law Enforcement Agencies

ML/FT

Money Laundering/Financing of Terrorism

STR/SAR

Suspicious Transaction/Activity Report

TTPS FRAUD SQUAD

Trinidad and Tobago Police Service/Fraud Squad



EXECUTIVE SUMMARY

This strategic intelligence report examines the escalating trend of suspected Romance Scam cases which were submitted through Suspicious Transaction/Activity Reports (STRs/SARs), to the Financial Intelligence Unit of Trinidad and Tobago ("the FIUTT"). The FIUTT noted an increase in STRs/SARs related to suspected Romance Scams at the onset of lock-down measures (2020), as a result of the Covid-19 Pandemic. As a consequence, the increase in the submissions of STRs/SARs, together with the nature of the suspected perpetrators within what appeared to be organised criminal networks, prompted an in-depth analysis aimed at presenting the indicators of Romance Scams, the monetary value of transactions examined during the period, related to the scams, cumulative value of losses to victims and the possible identification of international links of the local organized criminal network.

The views of professionals in the fields of economics, psychology and regional intelligence agencies, as well as, statistics from the Trinidad and Tobago Police Service/Fraud Squad ("TTPS/Fraud Squad"), revealed that there has been a significant loss to victims (nationals of Trinidad and Tobago), through this type of activity. The findings on the nature and impact of Romance Scams in Trinidad and Tobago, as well as other information which will be applicable to FIUTT stakeholders are also included. Recommendations for the prevention and detection of this trend and information on financial losses to the victims are also featured. Producing this Strategic Analysis Report is ultimately intended to assist in identifying and dismantling the organized criminal network.

~~~~~

#### **CHAPTER 1 – INTRODUCTION**

Romance scams, sometimes referred to as Social Media Fraud, lonely-hearts and/or friendship scams involve perpetrators expressing false romantic intentions toward their victims, to gain and then take advantage of their trust and affection to access financial assets such as cash, bank accounts and credit cards. This type of fraud has been in existence for some time and has become a significant risk and threat within Trinidad and Tobago. Social media usage soared exponentially during the period of the pandemic, which gave rise to the increase of Romance scam activity in society. This activity evolved into online dating apps, emails, instant messaging and social media platforms which makes it arduous to trace, investigate and/or prosecute offenders. Fraudsters take advantage of victims' desire for a relationship to manipulate them into releasing their earned income and savings to them.

Trinidad and Tobago was not impervious to the effects of the COVID-19 pandemic and the global economic downturn. Many persons suffered great losses in losing their jobs, life earnings, loved ones, and having their movements restricted. As a result, citizens sought alternative means of earning income and pursuing love relationships.

Over the years, the FIUTT received suspicious financial reports where citizens submitted claims of being financially scammed via "romance relationships" in Trinidad and Tobago. The FIUTT produced its initial report on the Romance Scam phenomenon in December 2019. However, due to the onset of the COVID-19 pandemic in Trinidad and Tobago, this trend amplified based on the reports analysed for the period 2020 – Sept 2022. It resulted in a loss of approximately TTD6.7 million and according to statistics on romance scams reported to the TTPS/Fraud Squad, for the same period, there were reported financial losses in the estimated amount of TTD4.6 million.

The FIUTT's mission is to effectively detect and deter money laundering and financing of terrorism, in collaboration with local law enforcement, regulators and international counterparts. Thereby contributing towards a safe and stable financial, social and economic environment within Trinidad and Tobago.

As such, this report is intended to strategically analyse available information with the aim of identifying the trends and indicators of Romance Scam activities, assessment of gaps highlighting risks, threats, vulnerabilities, and provide FIUTT's perspective on the phenomenon of Romance Scam in Trinidad and Tobago with recommendations to assist the relevant authorities to dismantle the apparent Organized Criminal Network behind this scheme.



#### **SCOPE**

The FIUTT conducts strategic analysis using data from STRs/SARs submitted by Reporting Entities to identify Money Laundering along with predicate offences and the related trends and patterns.

Statistical data utilized for this Strategic Analysis report mainly originated from **96** STRs/SARs submitted by FIs, LBs and Money Remittance Agencies to the FIUTT. The consistent development of this trend shows a pattern of activity noted by the individuals involved and provides a guide of specific indicators for investigations into an apparent Organized Criminal Network. More specifically, data on romance scam reports received by the TTPS/Fraud Squad will be highlighted for the period 2020 –2022.

#### **METHODOLOGY**

The STRs/SARs were submitted on the basis of suspicious transactions and/or suspicious activities related to fraud/romance fraud. In addition, the FIUTT received STRs/SARs from various Reporting Entities with regard to transactions related to the **clearing of alleged packages from individuals purporting to be romantically invested in unsuspecting individuals**. The FIUTT utilized various analytical tools and methods in the collation and evaluation of reported STRs/SARs specific to this Strategic Analysis Report. The observations from these reports led to the development of strategic financial analysis data which was used as the primary source of this report.

In addition, the FIUTT accessed a wide range of information sources which included non-public sources, local Law Enforcement Authorities and the Registrar General's Department. Not to mention, Open Source Intelligence was used to identify potential links to individuals or groups which may be affiliated to or have a nexus to the apparent Organized Criminal Network. The perspectives from experts (local and foreign) in the fields of Economics, Psychology, Law Enforcement and Intelligence were incorporated into this Strategic Analysis Report, to gain a wider understanding of the fundamentals of Romance Scam both on a domestic and international outlook.

#### **ROMANCE SCAM - A DEFINITION**

A Romance scam involves perpetrators expressing false romantic intentions towards victims, to gain and then take advantage of their trust and affection with the aim of extorting money from them. It is an online scam that typically begins on social media platforms and/or dating apps.

Fraudsters usually take on a false identity by creating a fake online profile to gain the victim's interest and trust. The fraudster then builds a relationship with the victim, using the illusion of a romantic or emotional connection, in an attempt to manipulate or steal from the victim. The fraudster convince the victim that they are "in love" with them and will give many different reasons why they cannot meet. After the fraudster spends many weeks or months developing the relationship with the victim, he/she requests money from the victim for critical reasons such as medical purposes, living costs, investments, courier fees, and transaction costs for high-value packages. Victims can be of any age or gender to fall as prey into this activity. However, women are generally the targets of these fraudsters. The fraudsters appear to be associated with a network of Trinidad and Tobago nationals who facilitate the payments requested of the victims into local bank accounts.

#### **CRIMINALITY IN ROMANCE SCAMS**

In Trinidad and Tobago, Romance scams can be captured under section 7 of the Criminal Offences Act, Chapter 11:01 which states:

Any person who is convicted on indictment of any of the following offences, that is to say, any cheat or fraud punishable at common law; any conspiracy to cheat or defraud, or to extort money or goods, or falsely to accuse of any crime, or to obstruct, prevent, pervert or defeat the course of public justice; .... is in respect of any of the above convictions liable to imprisonment for any term warranted by law, and also to be kept to hard labor during the whole or any part of such term of imprisonment

#### and also section 34 of the Larceny Act, Chapter 11:12 which states:

- (1) Any person who, by any false presence, with intent to defraud, obtains from any other person any chattel, money, or valuable security, or causes or procures any money to be paid, or any chattel or valuable security to be delivered, to himself or to any other person for the use or benefit or on account of himself or any other person, is liable to imprisonment for five years.
- (2) Any person who, by any false presence, with intent to defraud or injure any other person, fraudulently causes or induces any other person
  - a. to execute, make, accept, indorse, or destroy the whole or any part of any valuable security; or
  - b. to write, impress, or affix his name or the name of any other person, or the seal of anybody corporate or society, upon any paper or parchment in order that the same may be afterwards made or converted into, or used or dealt with as, a valuable security, is liable to imprisonment for five years.

#### SOCIO ECONOMIC CONTEXT

As a result of the Covid-19 pandemic, the Government of Trinidad & Tobago implemented many strategies to curb the social contact of people in the general public. These strategies included, but were not limited to, the closure of schools, tertiary institutions, bars, restaurants, air and sea ports, and non-essential services and activities. These measures had an adverse effect on the country significantly. In 2022, academics highlighted that the retrenchment notices registered with the Ministry of Labour increased from 1528 in 2019 to 2775 in 2020, which became the highest number of retrenchment notices recorded within the period January 2018 to June 2022. In tandem with retrenchment notices registered, was the indication that inflation also increased during this period. The retail price of food increased from 115 in 2019 to 128.2 in 2020. Additionally, it was suggested by researchers the fact that the following factors should be considered as it relates to the changing nature of crime in Trinidad and Tobago:

- Aging population as more of the population is aging, more persons are at home and may seek relationships via online dating, etc. This allows for them to become susceptible to Romance scamming;
- **Employment and unemployment trends** including unemployment by sector, and the work-from-home system;
- **Gender dimensions** (male perpetrators and male victims; female perpetrators and female victims);
- "Seasonality" of scams (potential increase of scams during particular seasons of the year (Christmas, carnival, valentine, etc.);
- Migrant population migrants may be more vulnerable to romance scams, but may be considered as possible sources of knowledge into fraud/scams which may have been derived from criminal knowledge of their country of origin.

The nature of criminal activity is changing as the socio-economic circumstances changes. It should be noted that online dating scams happen all over the world but certain demographics tend to be more vulnerable than others. As such, more data, research, resources (and training) are needed on how to manage crime trends. Furthermore, significant training and education (socialization) is needed on digital footprints.



### A PSYCHOSOCIAL PERSPECTIVE

The Covid-19 pandemic has fast-tracked the establishment of the digital world in Trinidad and Tobago. There was an increase in the usage of technology and the digital ecosystem as schools and workplaces were required to go online/digital to conduct their classes and services respectively. Romance scams have become easier to conduct through social media and online dating platforms as fraudsters can hide behind fake profiles.

#### A PSYCHOSOCIAL PROCESS - GROOMING

Grooming is the predatory act of maneuvering another individual into a position that makes them more isolated, dependent, likely to trust, and more vulnerable to abuse. As in the case of the romance scam fraudster, he or she engages in the five common stages of grooming which are:

- 1. Victim selection
- 2. Access & Isolation
- 3. Trust development
- 4. Desensitization
- 5. Post-Abuse maintenance

Within these stages, the fraudster would display the following techniques:

- Regular/ intense contact with the victim
- Kindness and flattery
- Be a sympathetic listener
- Use deception (for example, false profile picture or false location)
- Secrecy (for instance, the fraudster would ask the victim not to tell anyone about their relationship)

#### **SOCIAL ENGINEERING**

Social Engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to make users become gullible into making security mistakes or giving away sensitive information. The techniques include but not limited to:

- Baiting
- Scareware
- Pretexting
- Spear-phishing

Here, the fraudster would use the highlighted techniques to identify his/her victim(s), deceive the victim(s), obtain the relevant information needed over perhaps a few weeks or even months and when



the crime has been committed, remove all traces of themselves (done by discarding phone numbers and deleting their profile pages).

Researchers suggests that there are two different realities as it relates to the romance scam transaction. There is the scammer's perception and the victim's perception to be considered. The Scammers perceive the virtual world as a recruitment hub; the various stages of a Romance scam is merely a financial transaction. It is just business for them while the victim believes that they are in an intimate, promising relationship. The victim's actions and decisions are motivated by love and it is an affair of the heart. Here the transaction entails emotions, the currency is love, the investment is time, hope, and care and the outcome is emotional bankruptcy resulting in extensive psychosocial loss.

THIS SPACE WAS INTENTIONALLY LEFT BLANK

#### **CHAPTER 2 – KEY FINDINGS**

The analysis of the financial activity relative to Romance Scam Fraud produced insightful intelligence which is presented in the following categories:

- i. Financial Institutions
- ii. Victims' profile
- iii. Perpetrator profiles
- iv. Social media platforms
- v. Financial loss to victims
- vi. Romance Scam case study

#### **FINANCIAL INSTITUTIONS**

Over the period **October 01, 2019 to September 15, 2022,** FIUTT received a total of **96 STRs/SARs** related to Romance Scam Fraud submitted by **Reporting Entities**<sup>1</sup>.In the first quarter of fiscal 2021, the FIUTT noted a significant escalation in STRs/SARs, which contained a similar modus operandi, and was categorized as Romance Scam. These STRs/SARs presented one or more of the following characteristics:

- a. **Perpetrators** using a fictitious name, or falsely takes on the identities of real, trusted people such as military personnel, aid workers or professionals working abroad. A fake online profile is created on social media, the platform for luring unsuspecting victims into a cyberspace friendship.
- b. Perpetrators will express strong emotions for their victims in a relatively short period of time, and will suggest moving the relationship away from the website to a more private channel, such as phone, email or instant messaging. Perpetrators will go through great lengths to gain their victims' interest and trust, such as showering them with loving words, sharing personal information and promises of sending gifts.
- c. Once they have gained their victims' trust, the Perpetrators will send photos of gifts such as clothing, jewelry, perfumes and accessories. These intended gifts will be offered to their victims.
- d. Victims are then contacted by someone claiming to be from a courier/shipping company, who instructs them **to send money** to cover 'shipping fees', 'AML clearance certificates' and other 'fees'. The **Perpetrator** assures these victims that she/he will be compensated with the high value cash inside the package.
- e. Victims are provided **account numbers** for various **third parties** at **local banks** and are directed by the **shipping agent** to pay the **fees for the release of the package**. After the

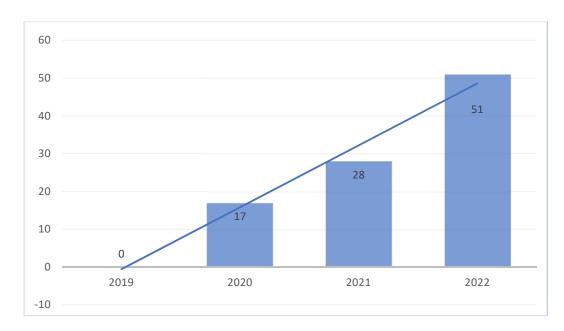
<sup>&</sup>lt;sup>1</sup> Financial Institutions and certain businesses and professionals (the "Listed Business"), collectively called, **Reporting Entities**, are designated to detect and deter ML and FT.

initial payment, victims are approached with **further requests** for money to cover some other **unforeseen fees**. These payments are often made in **cash direct deposits**, **interaccount or internet transfers**.

#### **STRS/SARS OVERVIEW**

The 96 STRs/SARs reviewed from Reporting Entities, spanned fiscal years 2020 to 2022 with significant increases, indicating a proliferation of Romance Scams in Trinidad and Tobago. In fiscal year 2020, a total of 17 STRs/SARs or 18% of the totals STRs were received. This figure increased to 28 submissions; or 29% of the totals STRs received in fiscal 2021, accounting for a 68% increase in STR/SAR submissions as it relates to Romance Scam Fraud. In fiscal 2022, a total of 51 STRs/SARs or 53% of the totals STRs were received, accounting for an 82% increase in STR/SAR submissions related to Romance Scam Fraud.

Diagram 2
STR/SAR Submissions to the FIUTT on Romance Scams for the period October 01, 2019 to September 15, 2022



Analysis of the dollar value of the 96 STRs/SARs showed, the total monetary value of the 17 STRs/SARs received in fiscal 2020 amounted to TTD 979,759.00. In fiscal year 2021, the monetary value of the 28 STRs/SARs received amounted to TTD 2,933,110.00, representing a 200% increase when compared to the 2020. In fiscal year 2022, the total monetary value amounted to TTD 2,821,741.00, a 4% decline when compared to 2021. It should be noted that despite an 82% increase in the number of STRs/SARs received in 2022, the dollar value was not commensurate. A breakdown of the yearly submissions and dollar value are presented in Table 1.

Table 1
Breakdown of the yearly STRs/SARs submissions and dollar value

| Dicardonii oi tiic yeariy oi iio oaanii oo oo ahaa aana aana talaa |                  |              |  |
|--------------------------------------------------------------------|------------------|--------------|--|
| Fiscal Year                                                        | No. of STRs/SARs | Amount (TTD) |  |
| 2019                                                               | 0                | 0            |  |
| 2020                                                               | 17               | 979,759.00   |  |
| 2021                                                               | 28               | 2,933,110.00 |  |
| 2022                                                               | 51               | 2,821,741.00 |  |
| Total                                                              | 96               | 6,734,610.00 |  |

THIS SPACE WAS INTENTIONALLY LEFT BLANK

#### **REPORTING ENTITIES**

The FIUTT received a total of **96 STRs/SARs** for the period October 2020 to September 2022. **Financial Institutions** submitted **95%** (91 requests) of the total requests received while **5 requests or 5%** were submitted by **Money/Value Transfer Service Providers**. Given the wider nature of products offered by Financial Institutions, it is expected that the Banks would have been faced with a higher risk resulting in the large number of suspicious activities and/or transactions being detected which subsequently give rise to a higher percentage of STR/SAR submissions. A breakdown for these submissions are presented in **Table 2**.

Table 2
Breakdown of Reports submitted to the FIUTT by Reporting Entities

| Reporting Entity | No. of STRs/SARs | % of Submissions |
|------------------|------------------|------------------|
| Bank 1           | 41               | 43%              |
| Bank 2           | 25               | 26%              |
| Bank 3           | 12               | 13%              |
| Bank 4           | 9                | 9%               |
| Bank 5           | 4                | 4%               |
| MVTS 1           | 3                | 3%               |
| MVTS 2           | 2                | 2%               |
| Total            | 96               | 100%             |

#### TRINIDAD AND TOBAGO POLICE SERVICE/FRAUD SQUAD

The Fraud Squad of the Trinidad and Tobago Police Service recorded a total number of 124 reports from victims of suspected Romance Scams. These reports were received over the three (3) year period 2020 to 2022 and accounted for an estimated TT\$4,614,086.00 loss to victims. Table 3 details the yearly figures related to Romance Scam reports for the three (3) year period. While the <u>number of reports</u> for each year from 2020 to 2022 declined, the <u>dollar value</u> for the years 2021 as compared to 2022 showed a 30.2% increase. This increase in dollar value may suggest that there was a demand for larger sums of money by perpetrators, and/or, an occurrence of multiple high value transactions related to each report by a victim.



Table 3
Romance Scam Reports made to the
Trinidad and Tobago Police Service/Fraud Squad

| Year  | Number of<br>Reports | Dollar Value<br>(in TT\$) |
|-------|----------------------|---------------------------|
| 2020  | 52                   | 1,612,688.00              |
| 2021  | 44                   | 1,304,068.00              |
| 2022  | 28                   | 1,697,330.00              |
| TOTAL | 124                  | 4,614,086.00              |

Source: Trinidad and Tobago Police Service/Fraud Squad

#### **VICTIMS' PROFILE**

Limited information was obtained on the identity of the victims of the Romance Scam cases. However, in some reports the FIUTT gleaned reasons for the victims' hesitance to report to law enforcement, included, they were apprehensive of family members finding out about their actions, or, they were ashamed, as well as, they exchanged intimate photographs of themselves with the perpetrators. In addition, some of the victims were in committed relationships and became involved in secret affairs with their online 'lovers'. Further to this, persons are not always required to produce identification at Reporting Entities when depositing funds and therefore, the identity of victims were not always captured.

The analysis of this strategic analysis report showed a total of **268 victims**, of which **66% or 177** were listed as females, while **24% or 64** victims were males and **10% or 27** victims' gender remain unknown<sup>2</sup>. The **prevalence of female victims** is thereby confirmed as **a major target group** in the social engineering of a **hidden Organized Criminal Network**. Although lower in numbers, **male victims** were also targeted and fell for a **similar pattern in being scammed** as their female counterparts.

<sup>&</sup>lt;sup>2</sup> Unknown gender refers to the absence of information on gender on respective victims' reports.



Diagram 3
Number of Victims by Gender

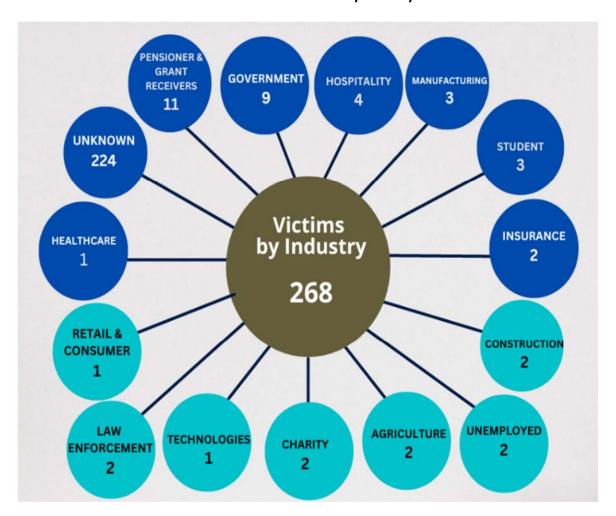


Due to the said **limitation in obtaining information on victims' identity**, **81%** of the victims' **ages were not captured**. The identified target victims' ages ranged from **23 to 78** years old and of the ages captured, persons between **40-59 years old** were **more susceptible to have fallen prey** to Romance scams in Trinidad and Tobago.

From the **restricted** available **information** on the **victims**, analysis of their **occupation/profession** to determine their **likely source of income** and **lifestyle**. Analysis revealed that victims held **varying occupations/professions** across industries. Some of these occupations/professions included but not limited to **clerks**, **healthcare providers**, **law enforcement officers**, **market vendors**, **and teachers**. Some were unemployed and even **pensioner's/grant recipients**. **Diagram 4** below gives a list of the victims' occupations/professions.



Diagram 4
Romance Scam Victims by Industry

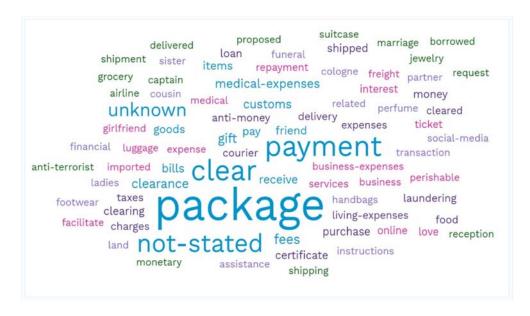


#### THIS SPACE WAS INTENTIONALLY LEFT BLANK

#### **VICTIMS' REASONS FOR BANK DEPOSITS**

Once the **Perpetrator** and his/her associate are successful in convincing their victim to pay in advance for the package or whichever arrangement linked to the 'romantic relationship,' the victims provide a variety of reasons for depositing large sums into the accounts of third party account holders at local Financial Institutions. The most common reason for the deposits was, to 'clear a package', for 'medical-expenses' or 'shipping/courier fees'. Notwithstanding, a significant amount of victims' reasons for deposits were not recorded likely due to online banking transactions or refusal by victims to make a declaration. **Diagram 5** depiects the various reasons given by victims.

Diagram 5
Reasons Given by Victims of Payments



#### **FINANCIAL LOSS TO VICTIMS**

The aggregate **loss** to the **268 victims** which were identified amounted to approximately **TTD\$3,353,114.00**. While the completed transactions totaled **TTD\$3,587,257.00**, the difference of **TTD\$146,858.00** accounted for attempted transactions, where either due to the Reporting Entities' internal monitoring systems, the victim was turned away due to the suspicious nature of the transactions, or the victim decided not to follow through with the transactions. The cumulative total of transactions conducted by the victims amounted to **TTD \$7,174,514.00**.



#### **PERPETRATOR PROFILES**

In the analysis of Romance Scam cases, perpetrators were identified as persons who aided in various stages of the scam against the victims. These perpetrators were categorized as 'online friends/lovers', 'shipping agent/courier' and 'third party account holders.' Since most of the communication with the victim was made online and over the telephone, the identities of the online friends/lovers and shipping agents were fictitious in nature, with limited evidence of verifying their identities. Furthermore, as mentioned, not many victims were forthcoming with full details of their perpetrators' identities, due to an apparent fear of the personal consequences to themselves and their families.

The FIUTT's analysis of the 96 STRs/SARs related to Romance Scam, identified 128 third parties as the holders of bank accounts at five (5) major banks in Trinidad and Tobago. Based on this analysis, a total of 163 deposit transactions were distinguished as being from the victims of Romance Scams. It is likely that there may be more such victim deposit transactions on the identified accounts, which were not clear enough to be classified as Romance Scam transactions. Notwithstanding this, the following is considered: Bank #1 reported seventy (70) deposit transactions by victims. This was followed by Bank #2 with thirty-nine (39) deposit transactions, while Bank #4 recorded twenty-five (25) deposit transactions. Banks #3 and #5 recorded thirteen (13) and seven (7) deposit transactions respectively, into third parties' accounts.

Of the 128 third party account holders, 74 or 57% were females and 54 or 43% were males. These individuals were recorded as residing in communities across Trinidad and Tobago. Conversely, there was a gap in the records provided, since, thirty-six (36) account holders' addresses were not provided. Of the available data, 11 account holders resided in Arima, followed by 6 in Gasparillo and Laventille and Carapichaima with 5 each. The remaining individuals were from random addresses throughout Trinidad and Tobago. Employment history of the account holders' spanned Government Ministry workers, Security Officials, Professionals, Self Employed persons, sales representatives, food and beverage workers as well as recipients of Government grants and unemployed persons.

6 Nigerian nationals were noted as a subset of the 128 third-party account holders. These individuals all held accounts at Bank #1 and were noted to reside mainly along the East/West Corridor, Santa Cruz and Arima. They were recorded as being employed as security officers, construction workers, a business owner and an optometrist at a known optical establishment in Arima. Both the optometrist's personal and business accounts featured as accounts used by victims of Romance Scams to deposit money.

Due to the nature of the Romance Scam, the names given by persons purporting to be 'shipping agents/couriers' were deemed to be fictitious, as were the companies from which they claimed the 'packages' were said to be held, pending the victims' payments. From the available information provided by victims the following (fictitious) shipping agents/ couriers were reported named:

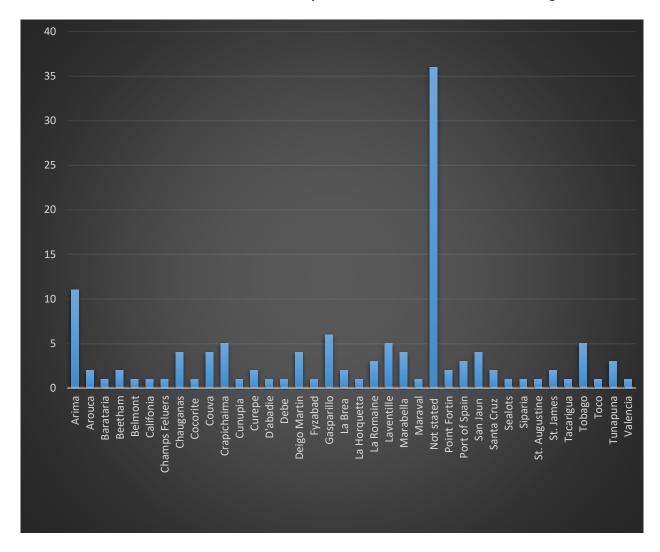
- Emerald Courier Delivery Service
- Sapphire Delivery Courier Service
- Garnet Couriers
- Garnet International Courier Service
- Ruby Diplomatic Courier Delivery Service
- Onyx Shipping Limited
- Onyx Cargo International Courier Delivery Service
- Peridot Delivery Service
- Quartz Company- Nationwide Diplomatic Delivery

Note that variations of the names 'Garnet' and 'Onyx Shipping' were featured in several cases.

Persons pretending to be 'online friends/lovers' of the victims gave false names and possibly stole the cyber identities of real persons, to deceive their victims into fake love. Of the 96 STR's/SARs analyzed, 40 names were identified as those of 'online friends/lovers', 26 or 65% were identified as males, while 8 or 20% were females. 6 or 15% of the named 'online friends/lovers' gender could not be determined from the available information. The female 'online friends/lovers' claimed to be from Syria, Dubai and the USA, and purported to be employed in the USA Army as a Captain, Officer, or Marine. Male 'online friends/lovers' claimed to be from Dubai, Canada, England, United Kingdom, USA, Syria and the United Arab Emirates. Occupations for the male 'online friends/lovers' were said to be mostly under the job title 'Carnival Cruise Ship Captain'.



Diagram 6
Districts of Residence of Third Party Account Holders in Trinidad and Tobago





#### **ROMANCE CASE STUDIES**

#### **CASE STUDY I**

Mr. White is a forty-eight (48) year old male Trinidadian who lives in Arima. He is a construction contractor. In September 2021 Mr. White visited the Arima branch of MNM Bank to deposit TT\$7,500.00 into the account of Ms. Red. Mr. White advised bank officials that he met a woman on Facebook and she told him she is an Army Captain. The unnamed woman, sought Mr. White's assistance to mail \$1.6 million cash to Trinidad in packages, which she would send to him. She would then come to Trinidad to meet him and they would continue their romance in Trinidad. He was told that he would have to pay 'Customs taxes' to 'clear the packages'. Mr. White stated that he was initially given an OPL Bank account in the name of Ms. Yellow into which he was to deposit the said TT\$7,500.00. However, OPL Bank refused the transaction. Mr. White then visited the Arima branch of MNM Bank and made deposits amounting to TT\$35,000.00 on three (3) separate occasions into accounts of Ms. Red and Ms. Green.

Mr. White became suspicious when he did not receive the packages, he subsequently made a report to the Police.

Ms. Red is a forty-nine (49) year old Trinidadian national who lives in Valencia. She is employed as a personal care assistant and earning a monthly income of TT\$1,500.00. She maintains an account at the Arima Branch of MNM Bank. A review of her account revealed a high credit turnover since the account was opened in January 2021. Credits amounted to TT\$147,300.00 of which TT\$114,250.00 (78%) was cash which were made as transfers from other third party accounts. Among the depositors were, Mr. Grey who, similar to Mr. White stated that he made deposits to clear packages sent by a friend whom he met on Facebook. The package was never received. Also making deposits was Ms. Black who was given the account of Ms. Red, to send money to assist a friend she met on Facebook with the purchase of an airline ticket. Ms. Black indicated that sometime after making the payment she realized that she was scammed and ended all communication with the Facebook friend.

Ms. Green is a forty-two (42) year old Trinidadian national whose addresses were identified in Laventille and Charlieville. She is currently unemployed and previously worked at a children's nursery. A review of activity on the account of Ms. Green held at MNM Bank revealed deposits for the month of September 2021, totaled TT\$74,400.00 of which TT\$57,400.00 (76%), was cash. These cash deposits ranged from TT\$2,000.00 to TT\$20,000.00 and were below the reporting threshold of the bank. The account also reflected an internet banking transfers of TT\$27,000.00 from a third party account. Deposits into this account were made by six (6) individuals other than the account holder. Among the depositors were Mr. White and Ms. Pink, both of whom indicated that the deposits were made to clear packages which were sent to them by a friend they met on Facebook. Both Mr. White and Ms. Pink never received the promised packages.

Ms. Yellow is a thirty-five (35) year old female Trinidadian national who resides in D'abadie. She is employed with AZ Roti Shop and earns a monthly salary of TT\$3,600.00. Ms. Yellow is the holder of a Savings Account at OPL Bank. She was noted to have suspicious financial links to a Nigerian national referred to as Mr. Blue, who appears to be expertly involved in an elaborate fraud scheme. A review of the account held by Ms. Yellow revealed the between August to September 2021, cash and online credits into her Savings Account amounted to TT\$119,600.00. Of this amount TT\$107,000.00 was transferred to an account held by Mr. Blue. Mr. Blue, is the holder of a Savings Account at OPL Bank. He was called in by OPL Bank officials for suspected comingling of funds. It was noted that in January 2020, several cash deposits totaling TT\$64,200.00 were made to his account. Mr. Blue claimed to be a pastor and the funds represented gifts and payments from church members. Checks revealed that he was the owner of a Pharmacy. Due to the suspicious activity, bank officials counselled Mr. Blue on the comingling policy. Restrictions were placed on his account pending the completion of Source of Funds and provision of supporting documents for all deposits. Following this there was minimal activity on the account and it was subsequently closed.

THIS SPACE WAS INTENTIONALLY LEFT BLANK

#### **CASE STUDY II**

Ms. Hibiscus is a 34-year-old school teacher who lives in East Trinidad. She is single and lives with her parents and younger siblings. Due to the pandemic, Ms. Hibiscus has been spending more time at home since her classes now require her to conduct virtual classroom sessions. With very limited opportunities to socialize, Ms. Hibiscus resorted to technology, through social media for most of her social interactions. She uses Facebook, Instagram, Twitter and Whatsapp, to frequently chat with friends, keep abreast of current affairs and for commercial and entertainment activities.

During the last lockdown, Ms. Hibiscus made a new friend from Austria, named Andre Scamp. Mr. Scamp says he is 37 years old and works with the United Nations Peacekeeping Corps and is stationed in North Africa. Andre Scamp initially reached out to Ms. Hibiscus with a Facebook friend request. After checking out his Facebook Profile, complete with photos of himself and colleagues in the UN, and other friends, she decided to accept the friend request. The two started chatting once a week, a friendship developed as Andre Scamp was very charismatic and soon they were chatting on a daily basis. Soon Mr. Scamp told Ms. Hibiscus that he found her irresistible and a romantic relationship developed. Ms. Hibiscus willingly shared details of her life in Trinidad, including how frustrating it has been as a single female professional in finding a man.

During the romance, Andre Scamp told Ms. Hibiscus that he wanted to show his appreciation for her by sending gifts through the mail. He sent her photos via Whatsapp and Facebook of these intended gifts including expensive perfumes, clothing, shoes, and jewellery. Ms. Hibiscus grew excited about the positive upturn in the relationship and shared her mailing address and telephone numbers to facilitate the package. Two days later Ms. Hibiscus received a telephone call from Mr. Dan Tricks from a local shipping company. Mr. Tricks told Ms. Hibiscus that there is a package for her, however she must first pay a 'clearance fee' for it to be processed and cleared. Mr. Dan Tricks provided Ms. Hibiscus with the account number of Ms. Gloria Glutton at AVM Bank and told Ms. Hibiscus to deposit TT\$8,900.00 into the account and keep the receipt as proof of payment to be presented upon delivery. Ms. Hibiscus did as instructed.

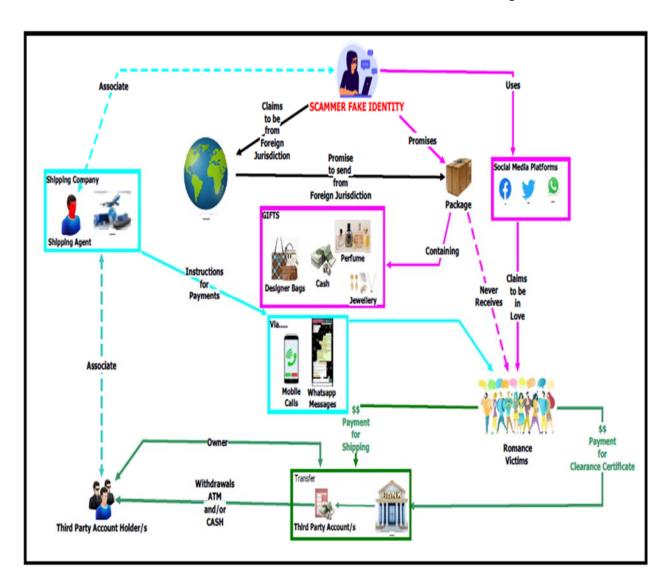
The following day, Ms. Hibiscus received a telephone call from Mr. Dan Tricks telling her that her package was scanned a second time and was found to contain US currency cash inside. As such, the shipping company would now require a further TT\$5,000.00 to acquire an 'Anti-money Laundering Certificate'. Ms. Hibiscus was given another bank account number at AVM Bank to make the deposit. She was hesitant to make this deposit, but after talking to her lover Andre Scamp, who explained that he did not mean to cause her any panic, but only wanted to surprise her with the US cash, she agreed and deposited the additional funds.

Soon after Ms. Hibiscus called Mr. Dan Tricks, however all calls went unanswered, this continued for several days. She became anxious and tried to contact Andre Scamp about the issue and found that all his Social Media accounts no longer existed. Ms. Hibiscus only then realized that she had been tricked. She spoke to a friend about it and was accompanied to the Fraud Squad of the TTPS to make a report.



Diagram 1 depicts the general overview of the standard activities which normally occurs in the creation, development and execution of a romance scam as related to the case studies above.

Diagram 1
Overview of Romance Scams in Trinidad and Tobago





#### **CHAPTER 3 – INDICATORS**

During the **fiscal years 2020 to 2022**, the FIUTT noted significant increases of Romance Scam cases targeted at vulnerable nationals. Certain commonalities exist in these cases. **Indicators of Romance Scams in Trinidad and Tobago** may include:



#### **INITIAL CONTACT WITH VICTIMS**

Romance Scams often take place through online dating websites but scammers more frequently use social media or email to make contact. Scammers have been known to make telephone contact with their victims, whose initial contact with the Scammer is via a fake online profile designed to lure the victims in. The Scammer usually uses a fictitious name, or falsely takes on the identities of real, trusted people such as military personnel, aid workers or professionals working abroad. Fraudsters portray themselves as being wealthy and generous and send photographs and videos showing their purported wealth.

#### **QUICK LOVE AND ISOLATION**



Romance Scammers will express **strong emotions** for the victims in a relatively **short period of time**, and will suggest moving the relationship away from the website to a more **private channel**, such as **phone**, **email or instant messaging**. Scammers will go through great lengths to **gain the victim's interest** and **trust**, such as showering their victims with **loving words**, and sharing of **personal information**.



#### **PROMISES OF GIFTS, MONEY AND MARRIAGE**



The Scammer gives promises of relationships, gifts and visits to Trinidad and Tobago to get married or become engaged. The Scammers will send photos of gifts such as clothing, jewelry, perfumes, accessories and money to the victims.

Promises are made to the victim to **receive large sums of money** for little or no effort on the part of the victim.

#### **REQUESTS FOR MONEY FROM VICTIM**



The intended gifts will be offered to the victim who will then be required to send money to cover 'shipping fees', 'AML clearance certificates' and other 'fees'. The scammer assures the victim that she/he will be compensated with high value cash in the package. The victim is given account numbers for various third parties at local banks and is directed by someone posing as a shipping agent to pay the fees for the release of the package. The victim receives phones calls from third parties claiming to be from shipping companies/brokers. After the initial payment, the victim is approached with further requests for money to cover other unforeseen fees.

These payments are often made in cash direct deposits, interaccount or internet transfers. Claims of mandatory fee payments to be made for **anti-money laundering clearance**. In some cases, scammers may request for assistance for **medical costs**, **tuition**, **courier fees**, **transaction cost etc.** 



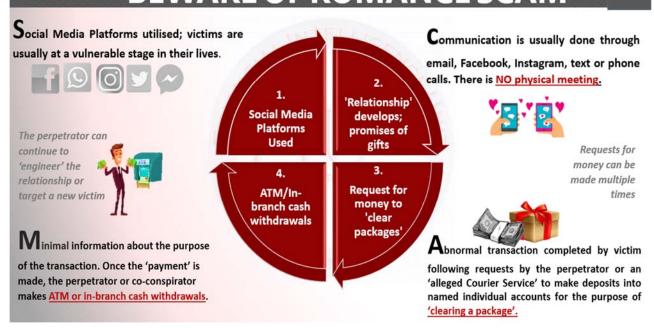
#### **REQUESTS FOR SECRECY**

The fraudster **requests confidentiality** in their transactions and in providing their names. Many different reasons are given for **why they cannot meet the victims**. It may be due to being **stationed at a distant overseas military base** or due to some job that requires **long distance travel**. Victims are encouraged to keep the **relationship hidden** from **family members and friends**. The payments are requested to be made through Money Service Businesses, or local bank accounts. The fraudster will claim to be sending large amounts of cash with a gift and Customs has held it until a fee is paid, or even claims that the personal gift and cash is being shipped through Diplomatic channels.

#### THIS SPACE WAS INTENTIONALLY LEFT BLANK



## **BEWARE OF ROMANCE SCAM**



#### CONCLUSION

The steady and rapid increase in Romance Scam cases in Trinidad and Tobago has caused significant financial losses to both female and male victims. The onset of the Covid-19 pandemic in 2020 resulted in restrictions in social interaction and an increase in the amount of time persons spent online seeking social connections on social media, dating websites and on mobile phone calls. Fraudsters took advantage of the increased cyber space traffic by unsuspecting and vulnerable persons.

This report is intended to assist our stakeholders (Competent Authorities, Financial Institutions, Law Enforcement Authorities and policy makers) in the prevention of future occurrences of Romance Scams. In addition, it is also intended to assist with the detection of perpetrators involved in this organised criminal network, to curb the loss of funds to victims and stop the negative impact of this social engineering crime on the families and associates of the victims.

To submit any reports or enquiries on potential acts of Romance Scams, persons can contact:

The Fraud Squad Trinidad and Tobago Police Service Level 6 – 7 Government Campus Plaza Ajax Street, Port of Spain

Tel. No.: 1-868-625 - 2310 or 624 - 0323





Enquiries relating to this report should be addressed to:

#### The Director

Financial Intelligence Unit of Trinidad and Tobago Level 25, Tower D International Waterfront Complex 1A Wrightson Road, Port of Spain





+ (868) 627-7018



fiufeedback@gov.tt



www.flu.gov.tt