GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT
OF TRINIDAD AND TOBAGO
MINISTRY OF FINANCE

FIUTT REFERENCE: TYP/004/2024

TYPOLOGY
SCAMMERS' USE OF SOCIAL MEDIA PLATFORMS

The Financial Intelligence Unit of Trinidad and Tobago ("the FIUTT") is publishing this Typology in accordance with *Section 17(1)(b) of the Financial Intelligence Unit of Trinidad and Tobago Act, Chap. 72:01, and Regulation 26(1)(d)(ii) of the Financial Intelligence Unit of Trinidad and Tobago Regulations.*

PURPOSE OF THIS TYPOLOGY

This Typology is intended to provide the public with information on scammers' use of social-media to defraud unsuspecting persons of their money. The Financial Intelligence Unit of Trinidad and Tobago ("the FIUTT") anticipates that this Typology will assist the citizens of Trinidad and Tobago in identifying and reporting suspicious activity involving persons who attempt to exploit social-media platforms for money laundering and other illicit activities, and thereby take the appropriate steps to detect and deter such activity.

GENERAL INFORMATION

In recent times, the FIUTT has noted a significant increase in Suspicious Transaction/Activity Reports (STRs/SARs) involving fraud occurring via social-media platforms. While legitimate sales and purchases are conducted via social-media platforms such as Facebook, Instagram and WhatsApp, these platforms are increasingly used to lure unsuspecting victims into the 'scammers trap'. Fraudsters lurk on popular social-media channels targeting individuals who are interested in vehicle purchases, phone purchases, and other goods. Anyone can be targeted by social-media fraudsters.

Scammers employ various tactics to steal a person's money. The following are some patterns to be aware of: **Observed scenarios of social-media scammers targeting persons seeking loans and investment online and buyers of goods *(particularly vehicle buyers):***

1. Scammer fake profile:

A scammer creates a fake profile with stolen pictures of a vehicle or generic vehicle pictures, which is often a popular vehicle model. They advertise the vehicle at an attractive price to entice potential buyers. The seller's profile information is very limited; they avoid phone calls but prefers text messaging. The scammer may also emphasize the urgency to close the deal and instructs the buyer to deposit funds into an account via online transfers or over the counter deposits and in some instances by way of wire transfers, before the buyer sees the physical vehicle. The buyer loses their money and, the scammer disappears.

2. "Rent-to-own or "Work-to-own" arrangement:

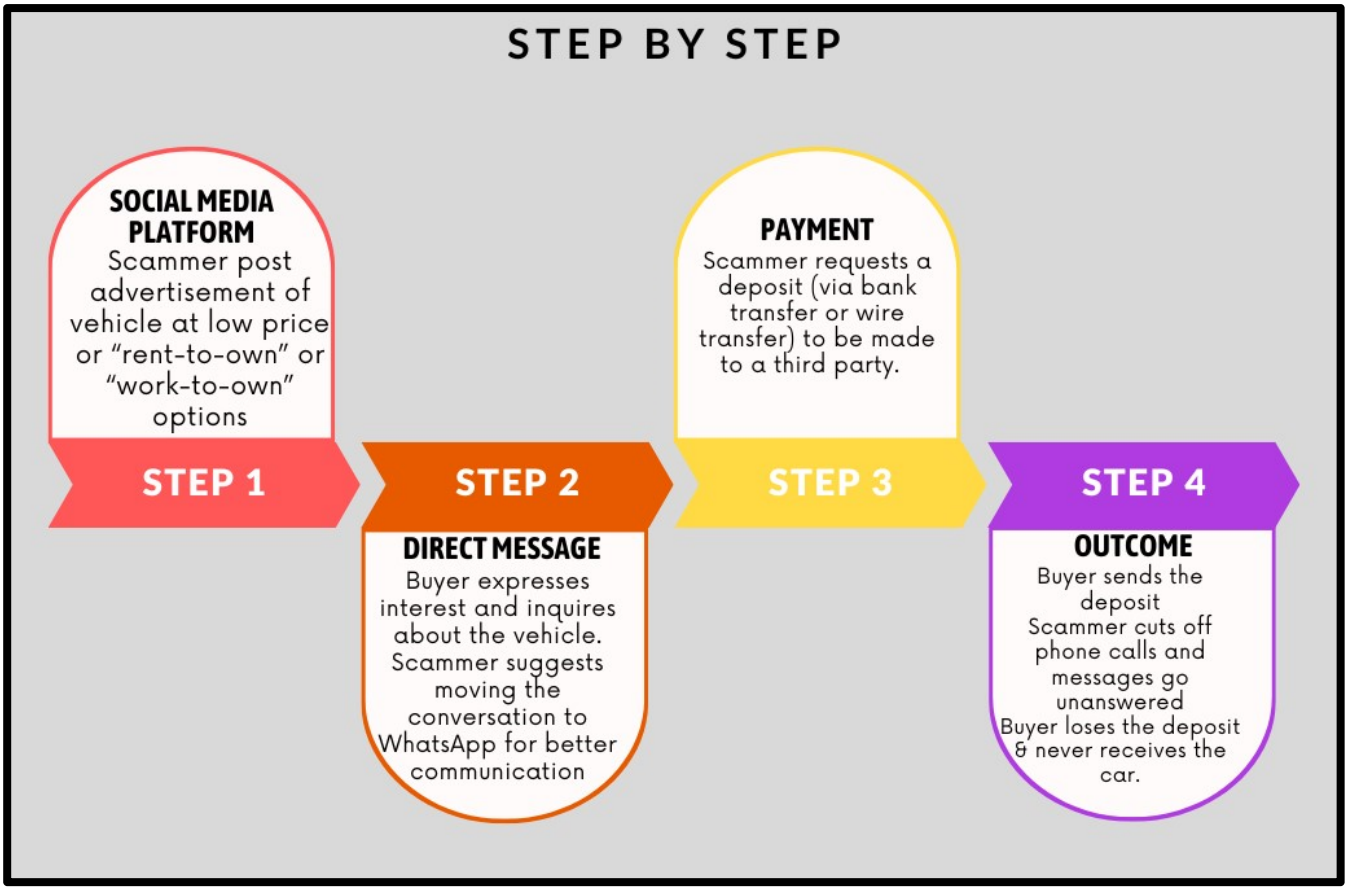
A scammer posts on a social-media platform, particularly Facebook Marketplace, about selling a well-maintained vehicle. He/she advertises the vehicle as a "**rent-to-own" or "work-to-own"** to entice potential customers. Once a potential customer communicates interest in the advertisement, the seller then moves the conversation to WhatsApp and instructs the customer to speak to another person via WhatsApp to arrange payment. The customer is then instructed to deposit funds to the scammer's account through online transfers or; wire-transfer to a third-party before seeing the physical vehicle. In some instances, the customer would make the deposit over the counter to the third-party's account. The scammer would even inform the customer that the vehicle would be delivered to a Police Station of the customer's choosing. After the customer makes the deposit, the customer tries to contact the vendor which proves to be unsuccessful.

3. Scammer utilises existing vehicle listing:

A scammer finds an existing vehicle listing (often on a legitimate platform), and copies the details, creating a replica listing on a social media platform. They may alter the information slightly (e.g. lower the price and add different contact details). The scammer pretends to be the seller and tries to convince the buyer to send them money. The buyer loses their money and the scammer disappears.

This advisory highlights the prevalence of social media scams that have been reported to the FIUTT. Scammers are using social media platforms to defraud people of their money. It also highlights the red flags associated with the scam so that persons can mitigate their risk.

HOW THE SOCIAL MEDIA SCAM WORKS? Persons who utilises social-media platforms to perpetuate scams, may appear in various forms. These scams may typically follow a similar pattern to reel-in potential scam victims, and steal money. Here's a breakdown of how they might work:



RED-FLAGS/INDICATORS TO THE PUBLIC: *EXERCISE CAUTION*

Citizens of Trinidad and Tobago can play key roles in identifying suspicious activities as it relates to social-media fraud, through the recognition of certain red-flags/indicators of illicit conduct. Many of the red-flags/indicators considered in isolation, are not necessarily indicative of scammers use of social-media platforms, to commit fraudulent activity. As such, additional contextual information should be considered, including the operating environment (the facts and circumstances). The following are some red flags:

- **Unrealistic prices:** The price of a vehicle, phone or other item is priced unbelievably low, or appears to be a great bargain. In some instances, persons may offer the vehicle as "rent-to-own" or "work-to-own".
- **Pressure tactics:** Fraudsters often try to create a sense of urgency, pressuring the customer to buy quickly; or, make a deposit before someone else does.
- **Fake profiles and advertisements:** Scammers create fake social-media profiles posing as legitimate sellers. Some sellers may have new or incomplete social-media profiles which are often used by scammers to appear much more convincing. They use stolen pictures of desirable vehicles or phones and advertise them as their own at low prices or at bargain prices.
- **Requests for upfront payment:** Scammers may request money upfront including deposits, especially through transfers at financial institutions or through money value service providers. They may even agree to deliver the item, but, disappear after receiving the payment.

- **Vague or missing details:** Photos may be blurry and unoriginal. The description of the products lacks information.

RECOMMENDATIONS:

- **Do your research**: Before contacting a seller, check their profile for reviews or mutual friends. Search for the item elsewhere online to compare prices and identify potential scams. Don't rely on profile pictures. Ask for additional photos showing specific details or request a video call to see the item in real-time. Be cautious if the seller avoids answering questions about the item or their location.

  Where possible, arrange to meet the seller in-person to inspect the item before handing over any cash, but be careful of potential robbery when dealing with cash-on-delivery. Also request a detailed vehicle history report and the vehicle's registration documents.

- **Meet in a secure location:** Opt for well-lit public spaces during the day and preferably with someone else present and consider meeting at a nearby Police Station if you feel unsafe.

- **Report Suspicious Transaction/Activity:** If you encounter a suspected scam, report the 'seller' to the social-media platform, and the Trinidad and Tobago Police Service (TTPS).

The public: If any member of the public would like to provide information about suspicions of money laundering, financing of terrorism activities, or any other predicate offence, a written Voluntary Information Report (VIR) [*anonymous if desired],* can be submitted:

- via email, addressed to the Director of the FIUTT at fiutt@gov.tt, or;
- if you believe that the information is serious and requires an immediate law enforcement response then you may provide this information directly to the Fraud Squad of the Trinidad and Tobago Police Service (TTPS) at telephone numbers: 1(868) 625-2310 or 1(868) 623-2644 or Fraud Squad South office at 1(868) 652-8594, or by email: Fraud.Squad@ttps.gov.tt.

Financial Institutions, Non-Regulated Financial Institutions and Listed Businesses are reminded that any transaction/activity suspected to be fraudulent or related to money laundering, financing of terrorism or any other predicate offence, should be reported:

- by the immediate submission of STRs/SARs, to the FIUTT, and;
- immediately to the Fraud Squad of the TTPS at Telephone numbers: 1(868) 625-2310 or 1(868) 623-2644 or; Fraud Squad South office at 1(868) 652-8594; or by email: Fraud.Squad@ttps.gov.tt.

Stay vigilant and stay safe.

Dated: September 10, 2024
Financial Intelligence Unit of Trinidad and Tobago