RISK GUIDE: Scams reported to the FIU

October 2025

The purpose of this guide is to inform and assist financial institutions in making informed decisions on strategies on scam prevention in Fiji.

Introduction

There were 77 scam related suspicious transaction reports received from banks and payment service providers from **January 2024 to July 2025**. 22 reports were received for the year 2024 and 55 reports were received for the year 2025 (3 January to 23 July 2025), showing a possible increase in scam activity in the country.

This guide aims to present patterns and trends observed in scams being reported to the FIU by financial institutions.

What were the type of financial products and platforms used in these scams?

The types of scams observed during the period included romance scams, investment scams and parcel scams. The scammers used various financial products and platforms to obtain funds. We have classified the reports into the following categories:

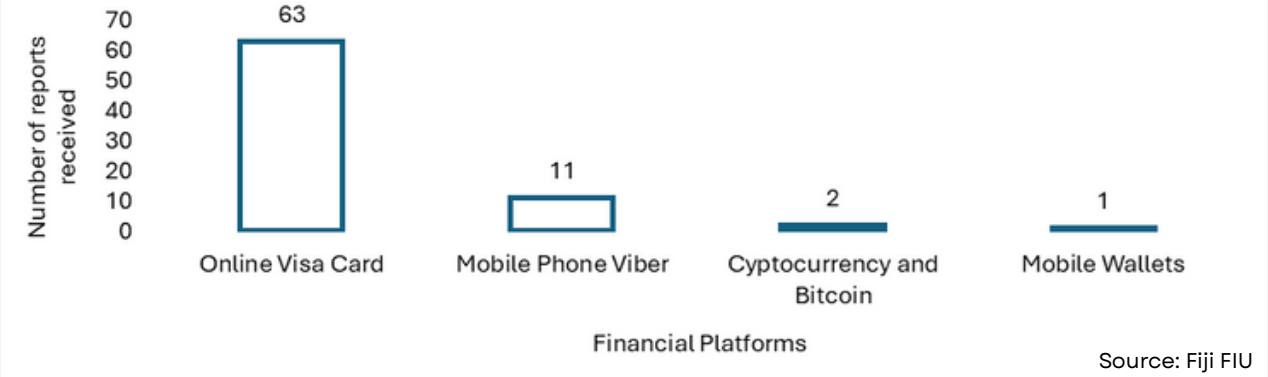
1. **Visa Debit card;**
2. **Mobile phone messages and Viber scams;**
3. **Cryptocurrency and Bitcoin; and**
4. **Use of mobile wallets.**

From 2024 to July 2025, 82% of scams reported to the FIU involved the use of Visa Debit cards issued by banks. These scams typically involved a person falling victim to an overseas based scammer and sending his/her Visa Debit card and PIN to the scammer to use. The scammer controls the account and uses the account as a mule account. Withdrawals from these accounts primarily take place in **Kenya, Malaysia, Indonesia, West Africa, Nigeria, Cambodia and United Arab Emirates.**

The second (14%) most common scam method is the use of the mobile phone messaging app Viber. Several victims are lured to deposit funds into another victim or mule account. The funds are then accessed by the overseas based scammer through a Visa Debit card that has been sent abroad.

The FIU notes that there was only one report involving the use of mobile wallets in a scam. This is due to the mobile wallet providers reporting scam activity directly to the National Scam Taskforce and Fiji Police Force.

Types of financial platforms or facilities used in scams reported to the FIU



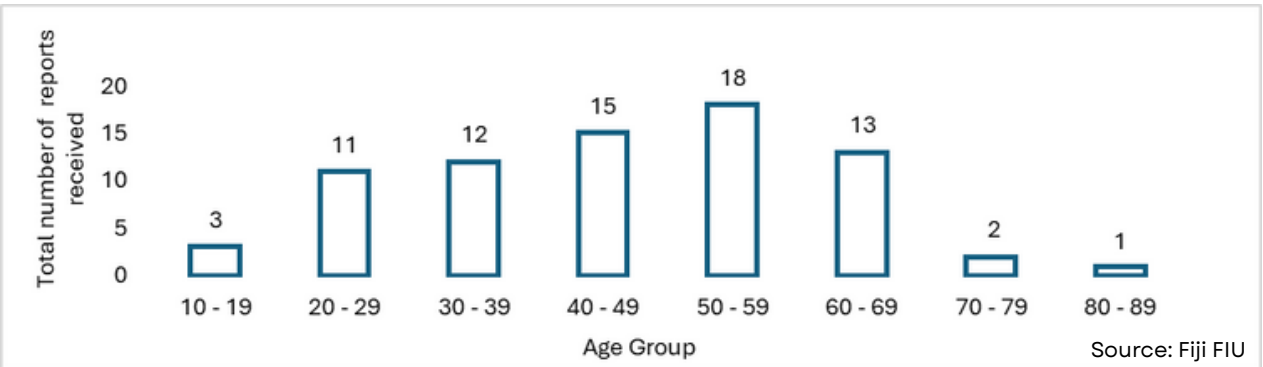
Source: Fiji FIU

What were the affected victims age group and occupations?

We identified that majority (60%) of the victims were between the ages of 40 and 69 with the largest (23%) subset of victims falling in the 50 – 59 age group.

Analysis of the reports also showed that scammers target victims who are vulnerable and on the verge of retirement. Most of these victims are retired, unemployed or low-income earners such as drivers, security officers, cleaners, machinists, and farmers.

Age Group of Scam Victims

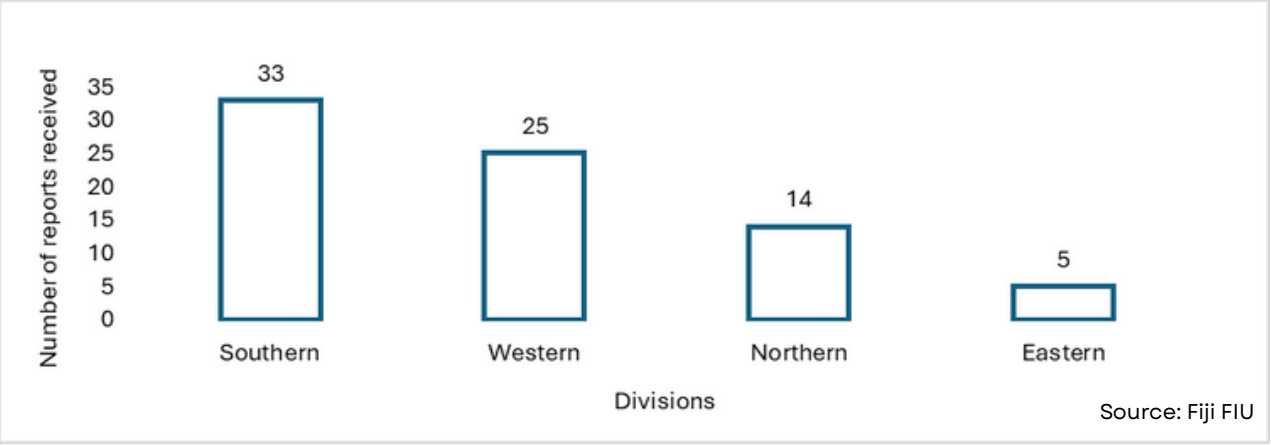


Source: Fiji FIU

Where were most of the affected victim of scams located?

43% of the reported victims live in the Southern division (Rotuma, Kadavu, Lau, Beqa and from Navua to Nasinu) followed by 32% from the Western division. The victims are also generally located in informal settlements within larger urban centers.

Location of Scam Victims



Source: Fiji FIU

What are some common trends of these scammers?

- Scammer promises large payouts after receiving the Visa Debit card;
- Scammer promises the shipment of items or parcels and requests for upfront payment of fees (processing fees, legal fees, customs fees);
- Scammers hack Viber accounts and impersonate users to solicit money from friends and colleagues, claiming family emergencies.
- Scammers create fake Facebook profiles, send friend requests to victims, gain their trust, and then request bank details under the pretense of sending money.
- Scammer targets low-income individuals to open bank accounts under their name where scammers can send money and with a promise of the victim gaining from the money deposited;
- Victims are primarily recruited/ contacted/ lured through social media.
- Victims provide their Visa Debit cards to overseas scammers, lured by the false promises of marriage, overseas travel or investment opportunities.
- Victims are mostly between the ages of 40 to 69 years and on the verge of retirement.
- Many victims are low-income earners such as drivers, security officers, cleaners, machinists and farmers.
- Visa Debit Card withdrawals often occur in countries known for high scam activity.
- Narrations of the transactions are normally abbreviations or contain a code.
- Transaction values were normally less than $1,000 with some transaction values as low as $2.

What is an emerging trend for scams?

In 2025, the FIU observed a new trend, where scammers are using artificial intelligence (AI) to create fake videos. A recent example was the fake video that falsely portrayed the Governor of the Reserve Bank of Fiji endorsing a fraudulent investment platform.

The video, generated using AI and deepfake technology, mimicked a legitimate news broadcast and claimed users could earn $18,000 per month from an initial investment of just $500. The incident highlights the growing sophistication of scams and highlights the challenges of combating AI-driven misinformation.

Conclusion

Scams continue to evolve in sophistication, exploiting vulnerabilities across our country. While anyone can fall victim, certain groups remain disproportionately at risk. Older adults, who may be less familiar with digital technologies and individuals facing financial hardship or social isolation are more likely to be deceived by promises of quick money or companionship.

Recognizing these at-risk populations is essential for developing targeted education, prevention strategies, and support systems. By raising awareness and fostering a culture of vigilance, we can better protect our communities from the far-reaching consequences of scams.

How to use this information?

- Share this information to improve awareness of your staff of these scams.
- Use your internal reporting systems and procedures to identify and report on any scam.

How to contact us?

Email: info@fijifiu.gov.fj; fijifiu-intel@rbf.gov.fj or fijifiu-compliance@rbf.gov.fj
Phone: (679) 322 3333
Website: www.fijifiu.gov.fj

Source:

1. Suspicious Transactions Reports (STR) reported to the FIU.