FijiFIU
Fiji Financial Intelligence Unit

Breaking Barriers in Digital Finance
World Consumer Rights Day 2022 Celebration
Suva, Fiji
15 March 2022

Digital Financial Scams Prevalent in Fiji
Speech by Razim Buksh
Director
Financial Intelligence Unit

A. Introduction

Bula Vinaka and good morning.

Thank you CEO for inviting me to be part of our national celebration of 2022 World Consumer Rights Day.

I am indeed very pleased to be part of the panel discussion. I'll be speaking on the topic *digital financial scams prevalent in Fiji*.

We live in the day and age where people are online social ego-centric. The modern-day digital space has the ability to connect anyone anywhere and has the widest possible reach, network and global audience.

The digital space is amazing and equally dangerous.

With the never filling appetite to explore the online space, most times people get carried away. We are tempted to open unneeded online accounts, download unnecessary apps, join all the many different social networking groups, the endless *Viber*-based marketing groups to describe a few.

Criminals also use the same digital space.

Most times they exploit your economic and social condition.

Once the criminals gain your trust, they manipulate and condition you to believe that they are the saviour you have been waiting for. From online romance, property inheritance, lotteries, investment, employment to every other possible means of removing your hardship you even cannot think of, you become their next target of financial scam.

Always remember that may end up in serious trouble if you click on everything that pops-up on your screen, open unsolicited attachments, click on web links, and when you begin to chat and socialise online with complete strangers.

B. Overview of Financial Scams reported to FIU

There are many types of financial scams that have been detected in Fiji by the FIU.

These include:

- Investment scam;
- Loan scam;
- Lottery scam;
- Inheritance scam;
- Pyramid scam;
- CEO/CFO scam;
- Shopping scam;
- Business Email Compromise scam;
- Romance scam;
- Scholarship scam;
- Immigration scam;
- Employment scam;
- Blessing/Prayer scam;
- Cryptocurrency scam;

The **top three scams in Fiji** in the 12 to 24 months would be the following:

1. **Romance Scam**;
2. **Loan/Investment Scam**;
3. **Pyramid/Multi-Level Marketing Scam**: (purchase of product not of any value, resell, gifting, training courses, the more people you get the more money you make!)

The FIU received 132 reports on advance fee fraud type scams in 2020 and 2021.

60 percent (around 80 reports) were related to **romance scams**.

C. Romance Scam

The most common element seen in these scams is the existence of some form of social engineering where fraudsters identify ways to gain the trust of the victims to ultimately send money to them.

This is clearly seen in romance scams where victims are led to believe that they are in a romantic relationship usually with a Caucasian person from *Facebook*.

The fraudster lies about sending a package to them – this normally "includes" jewellery, cash, electronics, and clothing. The package is then "stuck" in customs in another country and the victims will try and send funds to have their package released. Many other reasons are given by the fraudsters, in addition to the promise of parcel, such as, airfare to travel to Fiji and spend time with the Fijian "partner", leave fees, blocked bank account, health condition, stranded, etc.

D. Loan/Investment Scam

There have been a number of reports and queries made to the FIU regarding potential loans and investments from foreigners to local businesses.

The value of the supposed loans and investments are quite high – in the million dollar range.

Fijians are normally approached by the "lender" or "investor" via social media or email.

They submit bank account details, copies of company registration, copies of ID as part of the loan negotiation before being asked by the “lender” or “investor” to pay for “AML/CFT Certificate”, “release of funds from the FBI”, fees for the release of loan funds, insurance fees, disbursement fees, commission, etc.

In some cases these businesses do pay the funds and incur a loss. It is also highly likely that the fraudsters will use the information submitted by the victims – bank account details, copies of company registration and ID for their next scam.

E. Business Email Compromise

BEC is a common scam observed globally.

In all cases the fraudsters either mimic the email address of a CEO/Financial Controller/Accountant to a Junior level staff and instruct them to urgently send funds to them.

In other cases fraudsters would mimic the email address of a legitimate supplier and request local businesses to make payments to a bank account held by the fraudster or a mule.

Funds are quickly moved through a series of other accounts in other countries to continue to hide the trail. Businesses do not realize they have been swindled until the supplier follows up on the payment a few weeks later.

In 2022, the FIU received two such reports on this matter. Two Fijian businesses have already lost more than FJ$400,000.00 in 2022.

There are 32 cases on BEC scam from 2016 to 2022 totalling $6.2 million.

F. Lottery Scams

In the cases we have seen recently, individuals are advised that they have won a lottery and are required to provide ID documents and send funds to a third party for the administration fee of the lottery.

The FIU recently dealt with a case where a member of the public was referred to the FIU by a financial institution because the transaction was suspected to be a scam.

The member of the public provided the FIU with a copy of a remittance that the fraudsters claimed to be winnings from a previous lottery. The FIU identified the beneficiary in the copy of the remittance as being associated with another advance fee fraud scam in January. The member of the public was advised not to send any funds to the fraudsters and to cease communication with these fraudsters.

G. Virtual Assets – Cryptocurrencies

There have been a few cases where virtual assets are marketed and promoted through social media platforms. It is important to note that some of these individuals are doing this via multi-level marketing. They are encouraged to recruit more individuals to obtain more returns – which has some similarities to pyramid scams. It is important to note that the purchase of cryptocurrency by Fijian nationals is currently not permitted under the RBF Exchange Control Guideline. If individuals are purporting to be able to purchase on your behalf you must carefully weigh how they will purchase the cryptocurrency given the current restrictions in place.

H. Examples of Recent Scams:

1. **Investment Loan Scam**
   - Victim was offered a loan of $9,000,000.00 by a foreign entity.
   - The loan agreement stated that a third party offering business advisory would disburse the loan and liaise on their behalf.
   - The third party was located in another country and was mentioned in a scam forum for conducting job scams earlier this year.
   - Two potential websites were identified and were set up in 2021 from the same domain provider.
2. **Online Shopping Scam**
   - Victim decided to purchase an outboard engine online from offshore.
   - Victim made multiple transfers to a foreign entity for the purchase of the outboard engine.
   - The outboard engine was not received and funds were not recovered.
3. **Inheritance/Blessing Scam**
   - The victim in this case had spent few months communicating with a friend/fraudster.
   - They had developed a close relationship based on shared religion/spirituality.
   - The fraudster was alleged to be terminally ill and seeking prayers from the victim.
   - The fraudster claimed that she was dying and would like to bless her with funds of a few million USD.
   - The fraudster then advised that the victim would need to pay for AML certification to the bank and from the FBI.
   - The victim was advised not to send the funds but insisted on sending the funds as she had been communicating with her friend for some time.
4. **Loan Scam**
   - Victim received an email from a "UN Special Agent" requesting that £1,700.00 be sent for the legalization/affidavit of claim/title form by the UK Judiciary at the Crown Court Registry.
   - The email was sent from a gmail account and contained spelling errors.
   - The victim was advised that it was a scam and not to proceed any further.
5. **RBF Lottery Scam**
   - Fraudsters used the RBF logo to attempt to scam victims into paying a fee/other funds to release the lottery funds.
6. **Facebook Romance Scam - Male**
   - Facebook profile photo of a European lady in her mid-50's;
   - Cover photo of a brown skin hands holding 7 x $FJ50.00 notes;
   - Targeting Fijian men in their 40's to 50's;
   - Offering FJ$10,000 loan to Fijian men;
   - Send few hundred dollars before loan funds will be released;

I. Quick facts about Scams in Fiji:

- Victims of above scams are from all backgrounds and ages, including business entities;
- Victims are first contacted by scammers/perpetrators via social media platforms;
- Ongoing communication via messaging platforms such as “messenger”, WhatsApp, Viber, or email;
- Often there is no recovery of funds lost;
- Victims are not easily dissuaded or convinced that these are scams until they become aware that they have lost their funds;
- Awareness of consumers on online risk of fraud and scam.

J. AML Preventive Measures and Impact

- Financial institutions (FI) are required to implement preventative measures such as CDD, monitoring of accounts or transactions and reporting transactions to the FIU under the FTR Act.
- CDD is undertaken when a person first enters into a business relationship with a FI such as when opening a bank account. During the CDD process, the FI will seek to establish the identity of the customer, the nature/type of the account, nature of business activity undertaken and source of income.
- These CDD processes are to ensure that FIs know their customers. These requirements are not meant to be a hindrance to people accessing bank accounts and other financial services.
- FIs use information collected during the CDD process to monitor accounts and customer transactions. Transactions that do not match the known personal background of the accountholder (example business type deposits into a personal account) are flagged and subject to great scrutiny for possible reporting as a suspicious transaction to the FIU.
- Persons and entrepreneurs must ensure that they declare this information to the bank when opening a bank account.
- The bank must have up-to-date information on an existing customer, thus persons wishing to engage in business activities must ensure that their banks are informed of the change in their business activity or background information.
- AML/CFT preventive measures are not aimed at restricting people’s access to financial services. These measures are aimed at preventing people from abusing financial services/products for laundering/hiding/storing proceeds of illegal activities.

K. Some Tips to Detect Scams and Fake Online Proposals

Tips to stay safe online:

1. Always double check the name and particulars of sender of email or person you are communicating with on the online platform. You can be easily tricked as email addresses can be easily spoofed and the domain name could have slight spelling alterations (to trick you).
2. Typos and spelling errors can be a good indication that the message you are receiving is not genuine.

3. Do not share personal and sensitive information including any copies of ID without thinking twice. For example, a bank will never ask for personal information over an email. You should call your bank directly to ascertain if an email is genuine or not.
4. Be careful with messages that require you to act urgently or asks you to take immediate action. For example, the online offer/discount will expire in 24 hours, or send cash immediately to secure the deal.
7. Do not click on any link button, icon or URL. The displayed text may not match the actual URL link, if it seems strange, do not click.
8. Attachments can be dangerous, especially if the sender is unknown and download looks suspicious.
5. Is it too good to be true? If it sounds too good to be true, chances are it is! It is merely to attract your attention and tempt you to take action. It is definitely a fake offer/proposal/investment/reward/lottery/etc. Remember, you cannot win a lottery if you never participated.
9. Ensure that your devices up to date. Regularly check for your antivirus and software updates.
6. Check your accounts regularly (to ensure that no changes have been made without your knowledge).
10. Ask for assistance when in doubt.

L. Conclusion

The FIU has not only contributed towards the successful investigation and prosecution of complex financial fraud cases in Fiji, it has also proactively engaged with its stakeholders to ensure the safety and protection of Fijians and our financial system from money laundering and other financial crimes.

I look forward to working with the Consumer Council of Fiji, regulators, policy makers, businesses and other stakeholders to further discuss and develop action plan to strengthen and modernise Fiji's online, digital and technology based systems and solutions and to ensure that financial transactions are conducted by consumers safely and securely in Fiji.

Thank you for listening.

Vinaka Vakalevu.

Razim Buksh
Director
Financial Intelligence Unit
Tower Level 5, RBF Building, Suva.
Phone: +679 322 3333 | Fax: +679 331 6454 | Mobile: +679 992 8303
Email: razim@rbf.gov.fj
Website: www.fijifiu.gov.fj
15 March 2022