UNREGULATED SCHEMES

Financial Services Fund

operating under the

Financial Services Commission, Mauritius

Harmoney

by FSF

Financial Scams

- Financial Scams refer to dishonest, fraudulent and illegal schemes that attempt to defraud people.

- The fraudsters will often target vulnerable victims who are in urgent need of money (for example, unplanned retirement – the senior citizens are particularly vulnerable) and/or those who cannot recognise the signs of a fraud.

Questions and Answers

How can scams be identified?

- Promise of excessively high returns in a very short time when compared to what is being offered in the market;
- Request to the potential victim to provide personal details including his bank account details, pin number or internet banking log-in credentials; and
- Pressure on the potential victim to act rapidly.

What do scams and swindles mean ?

A scam is a term used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person.
A swindle is described as the act of getting money dishonestly from someone by deceiving or cheating him.

How does the FSC assess its procedures and processes

Keeping abreast of and meeting international standards and norms have become a necessity for regulators. The FSC Mauritius is a member of international standard-setting bodies namely the International Organisation of Securities Commissions (IOSCO), the International Association of Insurance Supervisors (IAIS) and the International Organisation of Pension Supervisors (IOPS). The FSC Mauritius continuously adheres to these international norms and standards to foster transparency, market efficiency, and the effectiveness of its supervision.

What should a person do if he is a victim of a scam

If someone believes that he/she is victim of a scam or has been contacted by perpetrators of scams, there are steps that he/she can take:

- **Step 1:** Report the scam to the police immediately. The police has the power to stop and arrest any person indulging in a fraudulent/criminal activity.

- **Step 2:** Stop giving money

  The person should stop giving money to the company or individuals involved. If he/she has given them his/her bank account details, the bank should be informed immediately.

- **Step 3:** To get more information, contact the FSC Mauritius on 403 7000 or by mail.

  The person should provide as much information as possible on what has happened, including the company or person involved, their contact details and copies of any documents related to the transaction should be submitted.

- **Step 4:** Beware of ongoing or new scams

  The people running scams are skilled, experienced and have persuasive skills that can easily convince people to part with their money. People should refuse to listen to their arguments and report them to the police immediately.

- **Step 5:** The person should protect himself/herself from being scammed again and should verify that the company or the individual is duly registered with either the FSC Mauritius or the BOM. In case of doubts, the Regulators should be contacted. It is worth bearing in mind that authorised companies are unlikely to contact someone out of the blue with abnormally high yield offers.

Helpful Tips

- Always verify if a person, whether an individual or a legal entity, who is proposing the investment opportunity, is duly licensed by the FSC Mauritius, BoM and other relevant regulators;

- The pin number, account number and log-in credentials should not be shared with someone untrustworthy whether in person, by email or over the phone;

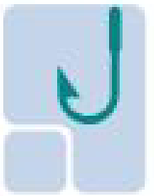
- It is very unlikely that a genuine investment will offer excessively high return in a short time period;

- Contact the police immediately if there is suspicion of a scam; and

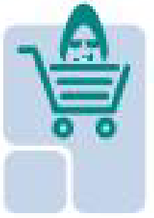
- Inform regulators (FSC Mauritius and BoM) or inform the police in case of any suspicion.

Types of scams

The different types of scams that can trick people out of their money are as follows:



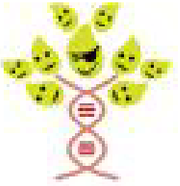
Phishing **-** It is the act of acquiring sensitive information such as username, password and credit card details by acting as a financial entity through the use of electronic communication devices. The main intention of fraudsters is to go on 'phishing expeditions' by luring and trying to hook potential victims from internet users. This process is usually conducted through the use of emails.



Scams linked to online shopping **-** Shopping on the internet is regarded as being economical and time convenient but there are also many dangers associated with it. Hackers can get possession of someone's credit card details and other sensitive information and hence misuse them.

Ponzi scheme **-** It refers to a fraudulent act where an operator convinces and attracts investors to invest their money in a scheme promising that their money will be invested and they will earn a bigger profit in a short period of time as compared to any other investment in the market. In fact, no investment is being made and the existing customers benefit from a sum of money upon the recruitment of new investors, from the deposit made by them. This type of scam relies on continuous recruitment of new investors.

Lottery Scam **-** This is when someone receives an email or text message informing him that he has won a lottery or a prize and in order to claim this prize, he should send a specific amount of money to a mentioned address. In reality, there is no such lottery and the person is merely being tricked out of the money that he is being requested to send.



Genealogy Scam **-** This refers to a situation where someone is contacted by the scammer telling him that he has inherited the fortune of a deceased distant relative. In order to obtain the inheritance, the person is requested to first settle the legal fees. In fact, there is no inheritance and the aim is to scam the person of the amount claimed as legal fees.

Website cloning **-** This refers to the copying of an existing website design or script to create a new one. The aim of such websites is to get hold of personal information such as card details, addresses and emails and eventually use such information for fraudulent purposes.

Social Media Scam - It is a fact that nowadays many people use social media to make investments and this in turn gives an opportunity to fraudsters to trick them of their money. Therefore, if someone notices a new post on their wall or receives emails from unknown people, they should be extremely cautious and not respond to these proposals. Scams in disguise of emails are being received from scammers either on personal email or office email address. In case individuals encounter such situations, they should make sure that they do not respond and report the matter accordingly. It is also important to be alert when emails are received pertaining to investment opportunities in particular projects.

Warning and Alerts

"If it sounds too good to be true, it probably is"

The public should take precautions and should be well aware and warned of the different traps that they can fall in. To inform and protect consumers and investors against illegal, dishonourable and improper practices, market abuse and financial fraud in the financial services and global business sectors, authorities are continuously trying to combat scams and inform consumers to be protected against such cases.

This Guide is for information purposes only.
You should not construe such information as legal, tax, investment, financial, or other professional advice. You should consult your professional adviser for any financial advice.
The FSC cannot be held liable for any error or omission.

Financial Services Fund

Harmoney by FSF

FSC House, 54 Cybercity Ébène. www.harmoney.mu info@harmoney.mu