



Financial Literacy Programme 2022

*Let's talk about...*

**Fighting financial fraud**

## Foreword by Mr Harvesh Seegolam, Governor of the Bank of Mauritius



Dear Reader,

The Bank of Mauritius is pleased to bring to you this first booklet on financial literacy. It has been published in the context of the nation-wide launch of the 2022 Bank of Mauritius Financial Literacy.

This inaugural edition focuses on how to protect yourself, and those around you, against financial fraud. It is the first of a series of informative documents that the Bank will be issuing on a regular basis for the benefit of the citizens of the Republic of Mauritius.

Through its Financial Literacy Strategy initiative, the Bank's objective is to provide our Mauritian youth, the active population and our senior citizens with clear information and proper tools to help them make sound financial decisions, and protect them from falling prey to financial fraud and scams.

As per its mandate, and building on the work that the central bank has been doing to promote consumer education, the Bank of Mauritius will be rolling out a series of initiatives across the Republic of Mauritius. This of course includes Rodrigues and our outer islands. These initiatives, which will be conducted in collaboration with the Mauritius Bankers Association, will endeavour to bring the concept of financial literacy to the doorstep of citizens.

In this digital era, and in line with our environmental and sustainability agenda, the Bank of Mauritius will be using social media and other online platforms as the main channels for the dissemination of information. However, to ensure that it reaches out to the greater number, the Bank of Mauritius will also be having recourse to physical sessions once the sanitary conditions permit to do so.

I have the pleasure of inviting you to join us on this financial literacy journey.

Best Regards,

**Harvesh Kumar Seegolam**  
Governor

# TYPES OF FINANCIAL FRAUD



## WHAT IS FINANCIAL FRAUD?

A fraud is an attempt to deceive another for financial gain. Financial frauds are a form of theft/ larceny which occur when a person or entity takes money or property, in an illicit manner, with the intent to gain a benefit from it.

Such crimes usually involve some form of deceit, subterfuge or the abuse of a position of trust, which distinguishes them from common theft or robbery.

High and unrealistic returns for small amounts of investment, easy and risk-free investment are some of features of financial frauds. Some types of fraud are Debit/ Credit card frauds, Identity Thefts, Insurance Frauds, Pyramid Schemes amongst others.

There are different types of financial fraud, an increasing number of which are based on technology. The following pages provide more information on the types of scams which fraudsters use, and on how to protect yourself.



## Card Fraud

This type of fraud starts with the theft of your bank card.

When your card is lost or stolen, it remains usable and makes it possible for a thief to make unauthorized purchases. Such unauthorized transactions can sometimes amount to thousands of rupees until you notify your bank of the loss of your card and until it is cancelled.

### **To protect yourself against card fraud:**

- Promptly report the theft of your card on the 24-hour telephone numbers that most issuers make available for free.
- Please exercise great care when using your card to make payments on the internet.
- Make sure that you do not share your pin code with anyone
- Always ascertain that you disclose the Card Verification Value (CVV) of your card only in secure payment sites.



## Counterfeit Cards

The fraudster uses the legitimate credit card information to make a fake card or sells the credit card information for a counterfeit card to be made.

Technology advancement has made the production of counterfeit cards that look accurate and legitimate, an easy process.

The victim rarely knows that he is being taken advantage of as he still has the real card in his possession.



## Fake Cheque Scams

In the *'fake cheque'* scam (also known as a *'money transfer'* scam ), a scammer tries to recruit people to work as *'remote managers'* or *'payment processors'*.

The scammer may claim to be a foreign company that needs help to transfer money earned abroad to their own bank. The deal is that you will receive payments in your account and you will need to send the money by transfer and, in return for your trouble, you will receive a commission on each transfer.

The *'payments'* sent by the scammer will typically be a forged cheque or other financial instruments. The cheque will be cleared and the money deposited in your account. You will then be requested to send the scammer his money, further to which you may keep a commission.

What typically happens is that a few days later, your bank detects the forgery and cancels the deposit. Suddenly, instead of earning the commission, you may have lost hundreds or even thousands of rupees.



## Advance Fee Scams

You get a letter, email or phone call offering you a large sum of money if you can help someone transfer millions of rupees or other currency out of his country.

To initiate the transaction, you are asked to send details of your bank account and an administration fee.





## Fund Transfer Scams

You are asked through an advert or email to receive a payment into your bank account, to take it out as cash, and to send it abroad in return for receiving a commission.



## Fake Prizes

A perpetrator claims that you have won a prize (which will eventually turn out to be nonexistent).

The scammer will either ask you to send a cheque to pay the taxes or may ask you details about your credit card.

The fraudster may also contact you under the pretense that your account number needs to be verified so that you can pay for shipping and handling charges.



## International Lottery Fraud

Scam operators use telephone and direct mail to notify you that you have won a lottery.

To show good faith, the perpetrator may send you a cheque. You are instructed to deposit the cheque and immediately send (via wire) the money back to the lottery committee.

The perpetrator will create a “sense of urgency,” compelling you to send the money before the check, which is counterfeit, is returned.

You are typically instructed to pay taxes, attorney’s fees and exchange rate differences in order to receive the rest of the prize.



## Identity Fraud

Someone impersonates you without your knowledge or consent, or uses your personal information to obtain money, goods or services. For example, by using one or more pieces of your personal identifying information – your name, your address, your NIC number – a perpetrator establishes a deposit or other financial account, or takes over a credit in your name.

Identity fraud may also be carried out internally by dishonest employees at your bank or financial institution. Dormant bank accounts or accounts with infrequent transactions are most at risk.



## Inheritance Scams

You receive a mail from an 'estate locator' or 'research specialist' purporting an unclaimed inheritance, refund or escheatment.

You are lured into sending a fee to receive information about how to obtain the purported asset.



## Phishing

This occurs when a web page is designed to look like a legitimate site, say a financial institution's website, and from which are sent email messages that seek to trick people into handing over account login information.

A fraudster will usually try to lure you by requesting you to submit details of your account, login IDs, passwords or other information.

You may also be directed to enter personal details on fake websites that look identical to the legitimate ones. Those details are then exploited for fraudulent purposes, mainly to steal money from your account.



## Ponzi Schemes

'Ponzi schemes' are named after Charles Ponzi who, in 1920, ran a scam in the U.S. promising a 50% rate of return in 45 days for a convoluted investment involving international mail coupons.

Unlike pyramid schemes (described on the next page) which involve a hierarchical structure, Ponzi schemes are promoted as investment schemes that promise to pay relatively high rates of returns for fixed term investments.

These Ponzi schemes are fraudulent investment plans in which the money is not invested at all. Instead, every new investment is used to pay off earlier investors. Such payouts are used by the fraudsters to build credibility for Ponzi schemes with a view to attracting more and more investors.



## Pyramid Schemes

Pyramid schemes are illegal money-making ventures that usually benefit those that started the scheme, the individuals at the top of the pyramid.

A single promoter (or small group of promoters) collects money from a certain number of friends and instructs them to collect more money from others with a promise of better returns on the initial deposit based on the number of people a participant recruits.

The cycle goes on from there and as the pyramid grows the number of people involved becomes too large to sustain it. Some people will fail to deposit their money or recruit the required number of friends and the pyramid crumbles.

Most people end up at the bottom of the pyramid and inevitably lose their initial investment, which is enjoyed by the top selected few (usually those who started the scheme). The people at the bottom of the pyramid do not get their money back because there is no one beneath them in the pyramid adding new money.





## Stock Market Scams

It starts where a person sends out, say 32,000 letters to potential investors. The letters show the company's elaborate computer model, its financial expertise and inside contacts. In 16,000 of these letters, the scammer predicts that the index will rise, and in the other 16,000 a decline is predicted.

No matter whether the index rises or falls, a follow-up letter is sent, but only to the 16,000 people who initially received the correct "prediction." To 8,000 of them, a rise is predicted for the next week; to the other 8,000, a decline. Whatever happens, 8,000 people will have received two correct predictions. Again, to those 8,000 people only, letters are sent concerning the index's performance the following week: 4,000 predicting a rise; 4,000 a decline.

Whatever the outcome, 4,000 people have now received three straight correct predictions. This is iterated a few more times, until 500 people have received six straight correct "predictions." These 500 people are now reminded of this and told that in order to continue to receive this valuable information for the seventh week they must each contribute an amount. If they all pay, the "advisor" will receive 50 times that amount.



## Share Scams

A stranger phones you out of the blue and tries to sell you shares in companies you have probably never even heard of or which do not exist at all.



## Skimming

‘Skimming’ involves stealing information off a credit card during a legitimate transaction.

The fraudster swipes the card through an electronic device known as a ‘wedge’ or ‘skimming device’ which records all information contained on the magnetic strip.

A disturbing fact about skimming is that the devices can be easily purchased at relatively low prices and it is hard to catch the fraudster since the fraud is usually noticed only after 30 or 60 days when the victim receives his/her credit card statement.



## Wills and Legacies Scams

A letter or email is sent to you claiming that someone has died and had mentioned your name in his will.

The mails usually say that one Mr. X, a citizen of Y country has mentioned your name in his last will, according to which you will receive a portion of his account in a particular currency.

Usually the scammer will claim to be the deceased's legal advisor and will ask you to proceed for a fee.