Market Intelligence Cell

Fighting Financial Crime

The Market Intelligence Cell (MI Cell) was established at the Bank of Mauritius (the Bank) in December 2013 to enable it to fulfill one of the new mandate bestowed upon it, namely, to carry out investigations and take measures to suppress illegal, dishonorable and improper practices, market abuse and any potential breach of the banking laws.

The MI Cell assists the Bank in the fight against financial crime by, *inter alia*:

- Gathering information on Market abuse in line with the mandate of the Bank.
- Conducting special examinations and investigations.
- Examining fraud reports from Financial Institutions.
- Identifying risk areas in Financial Sector.
- Creating awareness and providing advice on risks areas**.**

Types of Financial Frauds

Ponzi-schemes – 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 complex investment, Ponzi Schemes, unlike pyramid schemes which involve a hierarchical structure, are promoted as investment schemes that promise to pay relatively high rates of returns for fixed term investments. They are fraudulent investment plans in which the money is not invested at all. Instead, every new investment is used to pay off earlier 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.

Identity fraud – Someone impersonates you without your knowledge or consent, or uses your personal information, such as your name, your address, your NIC number, to obtain money, goods or services. Identity fraud is becoming common **on-line**, and fraudsters use this technique to give instructions to banks for fraudulent money transfer.

Phishing – This occurs when a web page is designed to look like a legitimate site, for e.g. a financial institution's website, and from which are sent email messages that seek to trick people into handing over account login information, such as details of your account, login IDs, passwords or other information, including personal details. These details are then exploited for fraudulent purposes, mainly to steal money from your account.

Card fraud – The 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 with the card until you notify your bank of its loss and the card is cancelled.

Skimming – This 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.

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

Advance fee scams – These scams are usually perpetrated through 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 – In a fund transfer scam, 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. In so doing, you may become a party to an offence.

Fake cheque scams -In the 'fake cheque' scam (also known as a 'money transfer' scam or a 'mule job'), you are offered *'vacancies'* or *'work-from-home opportunities'.* A scammer tries to recruit people to work as 'remote managers' or 'payment processors'. The scammer claims to be a foreign company that needs help to transfer money earned abroad to their own bank, against payment of a commission on each transfer. The 'payments' that the scammer sends you will typically be forged cheques or other financial instruments.

Fake prizes – A perpetrator claims that you have won a nonexistent prize and either asks you to send a cheque to pay the taxes or asks you details about your credit card, or your account number to pay for shipping and handling charges to send you the non-existent prize.

Inheritance scams – You receive a mail from an *'estate locator'* or *'research specialist'* purporting an unclaimed inheritance or refund. You are lured into sending a fee to receive information about how to obtain the purported asset.

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 which you are instructed to deposit in your account and send the money back to the lottery committee. The perpetrator will create a "sense of urgency," compelling you to send the money before the cheque, which is counterfeit, is returned.

Wills and Legacies - 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 may claim for a fee.

Protecting yourself against Financial Crime

- ✓ **Keep** all personal information, identity cards and bank cards safe at all times.
- ✓ **Keep** your PIN numbers secret.
- ✓ **Do not** write your PIN numbers down or store them with bank cards.
- ✓ **Never** give bank account details or other security information to any person or website unless their identity and authenticity can be verified.
- ✓ **Place your money only** at authorized financial institutions**.**
- ✓ **Never** give your money to people who offer to place it with a bank on your behalf for a rate of return higher than the prevailing rate.
- ✓ **Do not allow yourself to be distracted** when using your bank card. If you notice something wrong or suspicious with an ATM, please report it.
- ✓ **Do not** let anyone else use your card**.**
- ✓ **Check** monthly credit cards statements and other bank statements carefully for suspicious transactions.
- ✓ **report promptly the theft or loss of your card** on the 24-hour telephone numbers that most issuers make available for free.
- ✓ **Exercise care when using your card to make payments on the internet.** Make sure that you disclose your Card Verification Value only in secure payment websites.
- ✓ **Be careful** when signing any financial contract. Read the small print carefully, and ask for clarifications and advice from independent sources if needed.
- ✓ **Beware** of calls, letters, e-mails or faxes asking for your help to place huge sums of money in an overseas bank.
- ✓ **Be suspicious** of any job advertised by spam or unsolicited e-mails. Legitimate companies do not send spam. If the 'job' offered involves handling money - receiving or transferring funds or payments, it could be 'fake check' scam.
- ✓ **Do not reply** to spam or unsolicited e-mails that promises you some benefit.

HELP US FIGHT FINANCIAL CRIME

REPORT FINANCIAL SCAMS ON

149

(Toll Free Number)

The MI Cell can be easily reached.

Call us : 149 (Toll-free number)
E-mail : micell@bom.mu

Write to us :
The Market Intelligence Cell
Bank of Mauritius
Sir William Newton Street
PORT LOUIS