SPLOCA Awareness Guidelines for Public

CONTENTS

1. PRUDENCE IN INVESTMENT

This chapter introduces the citizen to need for prudence and understanding in investing their hard-earned money and the availability of safe savings and investment channels.

A. IMPORTANCE OF OPENING A BANK ACCOUNT

Function of Banks

A bank is an institution authorized by the Government, to accept deposits from the public and companies, and pay a certain interest rate on them, clear cheques and provide loans with certain terms and conditions. Banks also carry out monetary transactions and provide other financial services to its customers. Banks play an important role in the budgetary process and economy of the country.

Benefits of placing funds with banks

The first step in the investment process is to open an account with a bank to keep your funds secure, and also to earn a rate of interest on them. You can also place your savings in a fixed deposit with a bank for a higher interest rate.

Opening an account with a bank

You should have identification documents, a document confirming your address as well as 2 passport sized photographs. Banks identify individuals through documents such as – voter ID card, Aadhar card, PAN Card, passport, driving license, I-cards in the case of persons working in Government organizations and identification documents issued by certain approved or authorized schools.

Banks accept confirmation of address by considering the proof or documentation provided by the individual, such as – Aadhar card, ration card, certificate, original domicile certificate, electricity or water bills of the previous 3 months.

At the time of opening an account a guarantor who has been associated with the bank for more than 6 months is necessary. Such a person has to have been operating his account in a satisfactory manner.

What do you get when you open an account with a Bank?

A free passbook, which contains details of funds deposited/ withdrawn in the course of operation of the account.

An ATM card and password, which enables you to withdraw specific sums of money from anywhere

Mobile banking and internet banking facilities.

After you open an account with a Bank, you can also benefit from several social security schemes that are available.

Your rights

When you open an account with a bank, you have the right to operate the account in the branch you have opened the account in.

After the bank account is opened, the bank is bound to honour your instructions in operating the account to the extent possible, and they cannot deny you your rights to do so.

You can issue as many cheques as you want on the funds in your account.

Banks must pay you interest on the funds in the account.

You can pay bills from the funds in the account.

B. SAFE INSURANCE AND PENSION PRODUCTS

Insurance

An insurance policy is a contract that promises to pay the policy holder a specified amount in the future in the event of any accident, incident or damage.

What is premium?

Premium is the amount that the policy holder pays, either at one time or periodically, in order to insure himself against the risks and receive compensation. In return for this premium, the policy holder or their family or both are provided insurance coverage.

Types of Insurance

A. Life Insurance

This includes policies which are directly related to the life of a person. These policies provide for a specified amount to be paid to the insured person, or to their beneficiaries or family members in the event of a particular accident or occurrence taking place. This type of policy is the best way of ensuring financial security for the family of the deceased, so that the family can continue with their lives with self-respect. There are several types of such policies:

Onetime payment policy: This type of life insurance policy has a contract wherein one-time premium amount has to be paid by the policy holder such that for the rest of the holder's life or for a specified time period, the holder is under insurance cover without having to pay any additional amounts as premium.

Money back policy: This is a policy which pays back the premium amounts. In such a policy, instead of receiving a lump sum amount at a particular point in time, amounts can be received periodically. Such a policy is ideal for those who invest their funds for a smaller duration of time and in instruments that grow faster in return terms.

ULIP (Unit Linked Insurance Policy): ULIPs include both risk cover as well as investments. The movement in capital markets has a direct impact on the performance of ULIPs. Most insurance companies make different kinds of funds available on the basis of the policy holder's investment objectives, risk profile and time horizon. These fund products have different kinds of risk profile. The prospective returns may vary from one fund to the other. ULIP plans offered by insurance companies have risk profiles that are different from each other.

Pension: Pensions are a type of life insurance. Pensions are a periodic and regular payment made by states to officials who have crossed the age of retirement or to their widows, disabled or differently abled persons.

B. General Insurance

Include policies which are not directly related to the life of individuals. Such policies insure the policy holders against risks to their wealth and health. Such policies are of the following type:

Medical insurance: This is a type of insurance policy that covers the policy holder or their family against the risks of expenses incurred due to hospitalization or for surgery etc. Such policies are issued under health insurance schemes and provide immediate monetary relief to holders who suffer unexpected health related ailments. A specified insurance premium amount covers the policy holder for expenses incurred during hospitalization and other medical costs like medicines etc.

Accident insurance: Such policies are part of general insurance. Such policies are annual in duration and cover risks of critical illness, disability and accidental death and are not applicable for other situations. These policies are therefore somewhat different from medical, life and health insurance.

Crop Insurance: Such types of policies are intended to provide farmers insurance cover and financial assistance in the event of risks such as loss or damage to crops, drought, floods, unseasonal rains, infestation of pests or other diseases or other natural disasters. These policies are also intended to provide aid to farmers to plant crops for the next harvest even as compensation is paid for damage to crops from the risks enumerated above. National Crop Insurance Scheme (RKBY) is the scheme implemented at the national scale in India.

Things to remember while purchasing an Insurance Policy:

i. Be clear on your aims and objectives
ii. Understand the details of your insurance coverage and review it carefully
iii. Keep in mind the amount of insurance that you need and the premium that you can afford to pay
iv. Carefully study and compare the various insurance policy options available
v. Choose the policy option that best suits your insurance needs and capacity to pay premium
vi. Before finalizing your insurance policy, verify the various schemes, conditions and premium
vii. It is always better to choose policies with two single covers rather than one with joint coverage
viii. Check your policy on a regular basis and update it
ix. Pay your premium amounts on time

Things to avoid:

i. Don’t buy insurance policies without full understanding
ii. Buy life insurance only if necessary
iii. Don’t ignore the risks involved in an effort to buy the cheapest policies
iv. Do not forget to periodically check the benefits payable in case of illness
v. Do not restrict yourself to only one agent when buying insurance policies
vi. Don’t buy insurance policies with premiums that are beyond your capacity to pay
vii. Don’t trust online information about insurance policies blindly
viii. Do not withhold information at the time of the medical examination

Government schemes for savings

The Government has various schemes to promote savings and investments by the citizens.

National Savings certificate (NSC)

This is a popular savings scheme, available at post offices all around the year. These are available in denominations of 100, 500, 1000, 5000 and 10,000 Rupees. The interest rate on these certificates is 7.7% per annum (in 2024). It is possible to borrow money against these certificates.

National Savings Certificate-VIII Issue

Account matures in 5 years

Minimum deposit ₹1000/- and thereafter in multiple of ₹100.

No maximum deposit limit.

A single holder type account may be opened by an adult for himself or on behalf of a minor.

A single holder type account may also be opened by a minor on attaining the age of 10 years.

Joint 'A' Type account may be opened by up to three adults payable to both the holders jointly or to the survivor.

Joint 'B' Type account may be opened by up to three adults payable to either of the survivor.

Loan facility available by pledging with the banks.

Public Provident Fund (PPF)

Such accounts can be opened at any authorized post office or bank branch. The interest rate on such accounts in banks is 7.1% per annum (2023-24). A minimum of 500 rupees and a maximum of 1,50,000 Rupees can be annually invested in this scheme. The tenor for such investments is 15 years. Loan can be availed in the third year after opening such an account and 25% of the amount deposited till then can be withdrawn at the end of the 1st year. A loan taken against such an investment can be repaid in 36 instalments.

Public Provident Fund Account

Minimum deposit ₹ 500/- & Maximum deposit ₹ 1,50,000/- in a Financial year.

Loan facility is available from 3rd financial year upto 6th financial year.

Withdrawal is permissible every year from 7th financial year.

Account matures on completion of fifteen complete financial years from the end of the year in which the account was opened.

After maturity, account can be extended for any number for a block of 5 years with further deposits.

Account can be retained indefinitely without further deposit after maturity with the prevailing rate of interest.

The amount in the PPF account is not subject to attachment under any order or decree of a court of law.

Deposit qualifies for deduction under Sec.80-C of I.T.Act.

Interest earned in the account is free from Income Tax under Section -10 of I.T.Act.

Post Office Savings Scheme (POS)

The post office savings scheme is also known as the Small Savings Scheme. This is the best tax saving scheme available. This scheme is available all year round. Post Office schemes vary by the type of investment and tenor. The types of such scheme are monthly deposit, savings deposit, time deposit and recurring deposit. Interest rate is 7.1% per annum (2023-24).

Kisan Vikas Patra (KVP)

Your money is doubled in 8 years and 4 months (i.e. 100 months). This scheme is available all year round in post offices and bank branches. This scheme is available in denominations of 100, 500, 1000, 5000 and 10,000 Rupees and there is no maximum limit on the investment. It is possible to transfer these certificates from one holder to another or from one post office to another. Interest rate is 7.5% per annum (2023-24).

Minimum ₹ 1000/- and thereafter in multiples of ₹100.

No maximum deposit limit.

A single holder type account may be opened by by an adult for himself or on behalf of a minor.

A single holder type account may also be opened by a minor on attaining the age of 10 years.

Joint 'A' Type account may be opened by up to three adults payable to both the holders jointly or to the survivor.

Joint 'B' Type account may be opened by up to three adults payable to either of the survivor.

Account can be opened in Post offices and in authorised banks.

KVP can be transferred from one person to another and from one post office to another.

KVP can be encashed after 2 and half years from the date of investment at the following rates.

Money Doubles on Maturity.

Kisan Credit Card

The Kisan Credit Card is a scheme launched by the Government of India. This offers farmers access to credit via Kisan credit cards. The Kisan Credit Card (KCC) scheme had been launched in 1998. The aim of the scheme is to provide short-term credit to all farmers in India. The scheme was created by NABARD (National Bank for Agriculture and Rural Development).

Using this scheme, it is possible for farmers to easily borrow funds for agricultural purposes. This enables farmers to buy tools, seeds and other essential items in a timely manner. Under this scheme, farmers are provided with a credit card and a passbook. This contains the borrowers name, address, land details, duration of the loan, tenor together with passport sized photographs of the borrower. This card can also be used as an identity document.

Benefits of a Kisan Credit Card

Illiterate or uneducated persons can also use this card. This card ensures that the farmer does not have to execute loan documentation and formalities every year, but the same is done on a one-time basis. Thus, the farmer is spared the time, effort and the stress involved. The tenor of the loan granted under the Kisan Credit Card is until it is possible for the farmer to being repayments, i.e., until after the harvest is sold. The farmer can draw a loan under the Kisan Credit Card from any bank branch. Farmers can avail short-term loans and they can purchase equipment for their land and meet other expenses.

Kisan Credit Card Interest Rates with Banks

Bank	Kisan Credit Card Interest Rate
SBI Kisan Credit Card	Up to 7% p.a.
PNB Kisan Credit Card	7%
HDFC Bank Kisan Credit Card	9%
Axis Bank Kisan Credit Card	8.85% to 13.10%
Indian Overseas Bank Kisan Credit Card	7% (interest subvention provided)
UCO Bank	7% (interest subvention provided)

Eligibility Criteria for Kisan Credit Card Interest Rates

You can get the Kisan Credit Card if you are engaged in in the agriculture and other related activities. Even if you are involved in non-farming activities, you can get a Kisan Credit Card. You or/and the co-borrower should be between 18 and 75 years old.

Documents Required

PAN Card

Aadhaar card

Driver's licence

Passport

Voter's ID

Overseas Citizen of India Card

Person of Indian Origin Card

Job card issued by NREGA

Letters issued by the UIDAI

Latest salary slip (not over 3 months old)

Latest Form 16 (available on website of Income Tax department)

Last 3 months' bank statement

FAQs on Kisan Credit Card Interest Rates

Senior Citizens' Savings Scheme

Minimum deposit ₹1000/- & in the multiples thereof with maximum deposit of ₹30 lacs.

An individual who has attained the age of 60 years or above on the date of opening of an account or an individual who has attained the age of 55 years or more but less than 60 years and has retired under Superannuation, VRS or Special VRS, can open an account.

Retired personnel of Defence Services (excluding Civilian Defence employees) may open an account on attaining the age of fifty years subject to the fulfilment of other specified conditions.

A depositor may open an account individually or jointly with spouse.

Interest shall be payable from the date of deposit to 31st March/ 30th June/30th September/31st December on 1st working day of April/July/October/January as the case may be, in the first instance and thereafter, interest shall be payable on 1st working day of April/July/October/January.

The account can be closed after expiry of 5 years from the date of opening of account.

The depositor may extend the account for further period of 3 years.

Premature closure is permissible subject to certain conditions.

Deposits in SCSS qualify for deduction u/s 80-C of Income Tax Act.

Current rate of interest is 8.2% per annum (2024)

Sukanya Samriddhi Account Scheme

Minimum deposit ₹ 250/- Maximum deposit ₹ 1.5 Lakh in a financial year.

Account can be opened in the name of a girl child till she attains the age of 10 years.

Only one account can be opened in the name of a girl child.

Account can be opened in Post offices and in authorised banks.

Withdrawal shall be allowed for the purpose of higher education of the Account holder to meet education expenses.

The account can be prematurely closed in case of marriage of girl child after her attaining the age of 18 years.

The account can be transferred anywhere in India from one Post office/Bank to another.

The account shall mature on completion of a period of 21 years from the date of opening of account.

Deposit qualifies for deduction under Sec.80-C of I.T. Act.

Interest earned in the account is free from Income Tax under Section -10 of I.T. Act.

Current interest rate is 8.2% per annum (2024)

C. Capital Markets

The capital market is a market where buyers and sellers or companies and Governments can raise long term funds. The markets work with financial security instruments like bonds and stocks. The duration of this market is for one year or longer.

Investments in Capital Markets

The capital markets consist of equity and debt markets in which companies and Governments are participants. They raise capital from public investors for the long term and thereafter such investors can trade such equity securities amongst each other.

Types of Investments in Capital Markets

Equity shares: Equity shares in day-to-day use are also referred to as stocks or shares. They represent a fractional ownership of certain companies. Equity shareholders participate in the profits and losses incurred by a company to the extent of their shareholding in the company. Such shareholders are members of the company which gives them the right to express views on the company's proposals and also to vote on the same. Dividend payments are not guaranteed for equity shares. Shareholders are deemed to be the owners of the company. Companies pay dividends to common shareholders only after repaying creditors and servicing preferred shareholders. These shareholders are deemed to be the owners of the company and they have the right to express an opinion on the matters pertaining to the company. In case the company makes a loss, they get a lower or even zero dividend. In case the company makes profits, the highest gains are made by such shareholders as well.

Equity shares represent ownership in a company by its shareholders. When one buys shares in a company, a share certificate expressing that ownership is issued to the shareholder.

Mutual Fund: Mutual funds are a kind of collective investment. On a collective basis, investors deploy funds in stocks, short term investments or other securities. There is a fund manager in a mutual fund that determines the investments to be made by the fund and also maintains the records of gains and losses of the fund. The gains or losses thus generated are distributed to the investors in the fund. The mutual fund management company collects funds from investors and also charges them a fee for the service. After deducting the fees, the remaining funds are then invested on behalf of the investors in the market. The advantage of investing in such a manner is that the investor does not have to manage buying and selling of shares since the fund manager is performing the role instead.

Although Mutual funds are a convenient way of investing money for investors, there are several risks associated with them. The amount invested in the mutual funds can increase or decrease depending on the performance of the market. It is therefore essential that investors are fully aware of the risks before committing to invest in mutual funds.

Debenture/Bond: A debenture or a bond is a contract. One party is a lender while the other party in the contract is the borrower. The contract contains details of the rate of interest, the dates on which the interest is to be paid as well as the date of repayment of the principal amount. Loan instruments issued by the Central or State Governments are called bonds while instruments issued by companies in the private corporate sector are called debentures. These are rated by credit rating agencies.

For Investors seeking a regular and steady income, debentures or bonds are ideal. Such instruments have higher rates of interest as compared to deposits in banks. Some bonds also offer tax savings.

Rights of shareholders

To receive shares on allocation or purchase

Annual reports to be made available

Timely receipt of dividends if declared by companies

Attendance at and voting on matters in general meetings

If the company is indulging in malafide activities which are not in the interests of the shareholders, shareholders have a right to complain against the same and receive a satisfactory response.

Points to be noted while investing

Employ an investing strategy suitable to your lifecycle

You can take higher risks at a younger age. As a result, that is the best time to undertake investments.

By the time you are 50 years old, risky instruments should be avoided

By the time you are 60 years old, avoid equity investments altogether because by then additional sources of income may have stopped.

Where to seek information about investing

Investing options and methods are available at www.iepf.gov.in

You can get information about companies at www.mca.gov.in

Please read offer documents carefully in case of IPOs. Do at the very least read Risk factors, litigation, promoters, company history, project, objects of the issue etc.

How To Invest

Only invest in companies with a solid foundation and which can withstand the pressures of the marketplace so that they can provide a better performance over a long time.

Beware of free information circulating on TV, print media, websites, emails, SMSs, social media etc

Only invest according to your income

Only transact with authorized intermediaries or representatives.

How Not To Invest

Don't invest based on free information without carefully considering the details

Do not be fooled by dubious advertisements

Do not be unduly taken in by impressive sounding data or numbers or claims

Do not lose your poise in sectors with rapidly climbing prices

Do not take loans in order to invest

While interest increases every day, it may not be necessary for the profit to go up every day as well

REMEMBER

Profits are only realized when they reach your bank account (not when they are mainly on paper or on an Excel sheet)

You can demand honest behaviour only when you remain honest yourselves and it is only then that you can legitimately fight for your rights.

2. Prevention & Safety from Financial & Cyber Frauds

This chapter intends to caution citizens about various schemes floated by fraudulent companies/ persons and to take preventive measures to avoid losing their hard-earned money. Investors should be aware about various fraudulent schemes floated and features through which such schemes can be identified.

A. Ponzi, Multi-Level Marketing, Pyramid Schemes & Zero Sum Game

Introduction

A Ponzi scheme is an investment fraud that pays existing investors with funds collected from new investors. We may define some "red flags" to identify a ponzi scheme:

i. High returns with little or no risk.
ii. Overly consistent returns
iii. Unregistered investments
iv. Unlicensed sellers
v. Secretive, complex strategies
vi. Informal, often brochure-like and advertorial paperwork
vii. Difficulty receiving payments after initial phases

viii. Fluctuations in rates of return after contract
ix. Unresponsive Customer Service
x. Extravagant display or emotive appeals by promoters

In the classic "pyramid" scheme, participants attempt to make money solely by recruiting new participants, usually where:

The promoter promises a high return in a short period of time;

No genuine product or service is actually sold or produced;

The primary emphasis is on recruiting new participants.

Easy money or passive income

No demonstrated revenue from retail sales

Complex commission structure

A zero-sum game on the other hand, is a system in which one person's gain is another person's loss. What all three have in common is that they don't create any value and while the zero-sum game doesn't hide this fact, the ponzi and the pyramid scheme try to pretend they do create value. Ponzi or pyramid schemes might in fact produce some revenue or have small investment returns, but the majority of the returns come from new members joining. This, however, is hidden from investors, making the returns seem much bigger than they are.

Ponzi Scheme

A Ponzi scheme is a fraudulent investing scam which generates returns for earlier investors with money taken from later investors. This is similar to a pyramid scheme in that both are based on using new investors' funds to pay the earlier depositors. Both Ponzi schemes and pyramid schemes eventually crash when the flow of new investors reduce and there isn't enough money to circulate. It should also be remembered that the upper levels of the pyramid is composed of the apex fraudster, his / her promoters, friends, family, employees, agents etc and more often than not they get their returns. As long as the carrying capacity of newer depositors allows it, the scheme will continue funding itself (though illegally) and depositors in the middle would gain some returns. Meanwhile

Ponzi schemes characteristics that should be warning signals:

i. High investment returns with little or no risk:
ii. Unregistered investments & firms: Ponzi schemes typically involve investments that have not been registered with financial regulators (like the SEBI).
iii. Non-transparent Methods: Investments cannot be understood or on which no complete information can be found or obtained. Often curious investors are satisfied by lucky draws and gifts.
iv. Difficulty receiving payments: Investors particularly newer ones don't receive a payment or have difficulty cashing out. Ponzi scheme promoters sometimes try to prevent participants from cashing out by offering even higher returns for staying put.
v. Use of Informal Channels for Publicity: Social network or religious advertisements may be used.
vi. Multiple Entities to receive money: The clients are asked to write checks with a different name than the name of the corporation (such as an individual) or to send checks to a different address than the corporate address.
vii. Even when such schemes start to crash, the promoters and partners may continue to lure customers by false promises, show of false concern, formation of informal groups and associations, making wild allegations about incompetence and likely failure against the investigating authorities and /or competent authorities, often through informal channels like social media etc.

Note: Genuine Depositors should beware of such practices and be careful to guard their personal information, documents and data so that these cannot be misused by unscrupulous agents (on their own or secretly hired by the promoters / partners / original depositors of the fraudulent enterprise)

A Ponzi scheme is an investment fraud where clients are promised a large profit in short term at little risk. Companies engaged in Ponzi schemes focus all of their energies into attracting new clients to make investments. These new investments (income) are used to pay original investors their returns, marked as a profit from a legitimate transaction. Ponzi schemes mainly rely on a constant flow of new investments to continue to provide returns to older investors.

How does a Ponzi scheme work?

i. Funds from new investors are used to pay purported returns to earlier investors.
ii. Promise of much higher return than prevailing in the market with little or no risk.
iii. Initial clients paid off.
iv. Deliberately communicated success stories through social media and advertising, display of wealth & influence
v. Unregistered investments and unlicensed sellers.
vi. Secretive, complex strategies, issues with paperwork and difficulty in receiving payments.
vii. The emphasis is on enrolment of members rather than sale of products.

Why would anyone be interested in investing such schemes?

The answer can be:

Lack of awareness about safe investing techniques, improper understanding of financial system

Greed, desire for easy money, “Keeping up with the Joneses”

Use of celebrity and fake advertisement, promotion by community leaders & important persons

Use of religious or community sentiment

Blind faith and inducement through free samples

Regulatory gaps

How to protect yourself from Ponzi schemes:

Beware of promise of higher returns:

Any scheme promising abnormally high returns should be considered with caution. Compare the rates with the methods employed by the scheme to generate the returns. Use your common sense.

Unknown Company:

You might have heard about a scheme promising higher returns, but are you also aware about the company and its credibility? If not, how can you put your hard-earned money into a company or organisation which is unknown to you? Don’t rely on reputation or word of mouth alone. One of the best ways to know about a company is doing your own research on internet or social media. If you do not find any reliable information on the net, it is better to steer clear.

Track Record of Promoters:

They should have clean image in terms of delivering promises. If you are unable to find any information, then do a search on the internet.

Registration Requirements:

If a person is planning to invest in a non-banking finance company (NBFC), then he/ she should be well aware that every NBFC is required to be registered with the Reserve Bank of India (RBI). NBFCs are not allowed to use the name of the RBI in any manner.

Ratings Assigned:

NBFCs which accept deposits should have minimum investment grade credit rating granted by an approved credit rating agency for deposit collection.

Terms & Conditions:

The charges should be considered well before taking the final call. Understand your investments; keep copies of all the investment and communications. Insist on original agreements not scans or photo-copies. Do not give the originals to anyone, never to the company.

Take Informed Decision:

One should check for the past record of the schemes, management team, corresponding regulations & financial information. **Your decision should never be guided by greed or desire for easy money.** Check registration and background of individuals selling the investment. Do not trust anyone blindly in financial matters even if he / or she is a neighbour or an old acquaintance.

Remember that even if the promoters of an NBFC are of impeccable repute and the credit rating is good, there is risk on these deposits as they are unsecured and the risk of insolvency is there.

Union Government model guidelines for states to curb Ponzi schemes:

The Union Government has issued model guidelines titled as "Direct Selling Guidelines 2016" framework for states to regulate direct selling and multi-level marketing businesses to protect consumers from Ponzi frauds. Ponzi schemes are banned under the Prize Chit and Money Circulation (Banning) Act, 1978. Though it is a Central Act, the respective State Governments are the enforcement agency of this law. These newly issued guidelines will allow states to make some change in their guidelines as per their localised requirements.

MLM and Pyramid schemes

Multi-level Marketing (MLM) is a marketing strategy designed to promote their product by through distributors, offering multiple levels of compensation.

Pyramid schemes are, however, fraudulent schemes, disguised as an MLM strategy. The difference between a pyramid scheme and a lawful MLM program is that there is no real product that is sold in a pyramid scheme, and commissions are based only on the number of new individuals one introduces into the scheme.

Setup

The main idea behind the MLM strategy is to promote maximum number of distributors for the product and exponentially increase the sales force. The promoters get commission on the sale of the product as well as compensation for sales their recruits make. Thus, the compensation plan in multi-level marketing is structured such that commission is paid to individuals at multiple levels when a single sale is made, and commission depends on the total volume of sales generated.

In the case of pyramid schemes, money is charged simply for enrolling other people into the scheme and no real product is actually sold. Only a few people (those who are involved in starting the scheme) make money, and when no new individuals can be recruited, the scheme fails and most of the promoters, except the top ones lose their money.

Difference between MLM and pyramid schemes:

Procedure	MLM	Pyramid Schemes
Sales of actual product or services to consumers	MLM offers products	Pyramid schemes do not
Commissions are paid on sale of products and not on enrolments	MLM has a hierarchical commission set up on the sales of products	Pyramid schemes are based solely on new enrolments
Termination & Buy- back	Company buys back inventory from participants at the time of termination	Pyramid schemes do not have any inventory.

Source of Profit	Even for MLM companies that are legal, the bulk of the profits (if any) come not from selling products but from recruiting other members	Pyramid schemes quickly become unsustainable because there aren't enough people to support it

MLM Compensation Plans

MLM strategy has different compensation plans which differ slightly based on how the commission is distributed among promoters. The plans include Unilevel, Stairstep Breakaway, Matrix, Binary and Hybrid plans.

The Unilevel model is the simplest one. The design is such that a person can recruit unlimited "frontline" distributors for the product. The frontline distributors are encouraged to recruit more distributors, and thus the cycle continues. Commissions are paid up to seven levels deep.

The Stairstep Breakaway model is designed to encourage individuals as well as group sales. In this model, a group leader is assigned with multiple recruits under them. The goal is to achieve as set of volume of sales in a set time. Once that it achieved, the distributors move to a higher commission level. This pattern continues up to a certain limit, after which the distributor breaks away and this pattern of commission ceases. From this point onwards, other commissions and incentives are provided to the representative.

Matrix models are similar to the first type, except that a limited number of distributors can be sponsored at any level, and once that pre-set number is reached, another matrix can be started.

Binary models allow only two distributors to be sponsor in the frontline, and if there are more sponsors, they spill over to the next level. So, at any level, only two distributors are required to complete the compensation plan. Also, the compensation has to be balanced between the two distributors at any level, such that the volume of sales does not exceed a certain percentage of the distributor's total sales.

Hybrid models, as the name suggests, combine any of the above-mentioned compensation plans.

Pyramid Scheme compensation models

The models include in the Pyramid Scheme include 8-ball model and Matrix scheme. In The 8-ball model each person has to recruit two people into the scheme. These people have to pay a sum to enter the scheme called a "gift sum". The captain or the person at the top receives the gift money from 8 people before exiting the scheme. The remaining people move up the scheme, and this pattern continues as more people are recruited into the scheme.

Matrix scheme is also a pyramid scheme except that people are required to pay for a product in advance and wait in a queue in order to enter the scheme. When the recruited person further recruits a certain number of people, he or she receives a product like a camcorder or television that is worth much less than the money paid, and exits the scheme. This scheme collapses when no more people are willing to pay and join.

Examples

Pyramid scheme: Malaysian SwissCash, Speak Asia, City Limouzines,

MLM companies: Amway, Mary Kay, Max International, Herbalife, Modicare, Avon, DXN India, 4Life, Forever Living,

RBI on MLM & Pyramid Schemes

The Reserve Bank of India has cautioned the public against Multi-level Marketing (MLM) activities. The Reserve Bank stated that MLM/ Chain Marketing/ Pyramid Structure schemes promise easy or quick money upon enrolment of members. Income under such schemes majorly comes from enrolling more and more members from whom hefty subscription fees are taken rather than from the sale of products they offer. It is incumbent upon all members to enrol more members, as a portion of the subscription amounts so collected is distributed among the members at the top of the pyramid. Any break in the chain leads to the collapse of the pyramid, and the members lower down in the pyramid are the ones that are affected the most.

The Reserve Bank has advised that members of public should not be tempted by promises of high returns offered by entities running Multi-level Marketing/ Chain Marketing/ Pyramid Structure Schemes.

The Reserve Bank has also said that acceptance of money under Money Circulation/ Multi-level Marketing/ Pyramid structures is a cognizable offence under the Prize Chit and Money Circulation (Banning) Act 1978. Members of public coming across such offers should immediately lodge a complaint with the State Police.

DIRECT SELLING

	Direct Selling Vs Pyramid	
Parameter	**Direct Selling**	**Pyramid Scheme**
Meaning/ Definition	Direct Selling" means marketing, distribution and sale of goods or providing of services as a part of network of Direct Selling, other than under a pyramid scheme, to the consumers, generally in their houses or at their workplace or through explanation and demonstration of such goods and services at a particular place.	A Pyramid Scheme is a business model that recruits members via a promise of payments or services for enrolling others into the scheme, rather than supplying investments or sale of products. As recruiting multiplies, recruiting becomes quickly impossible, and most members are unable to profit; as such, pyramid schemes are unsustainable and often illegal.
Driving Object	Sale of products and services to the ultimate consumer.	Little or no effort is made to market the product. All the focus is on enrolment on new people and collecting money from them.
Cost of Entry	No or only a reasonable entry fee.	Charge steep start-up costs for joining, including mandatory training, a starter kit and a non-refundable membership fee.
Plan/ Scheme	Plans are primarily based on the value of sale of products.	Plans are primarily based on money paid by new recruits, and not on product sales
Mandatory Enrollment	Enrolment of recruits is not compulsory for doing business.	Enrolment of recruits is compulsory for doing business.
Underlying Product	Involves marketing of products under established brand names	Either no products are involved, or else the products are a cover and are not really sold to consumers
Quality of Products	High quality	Camouflage or sham products, inferior quality
Buy-back/ guarantee of product(s)	Product come with buy-back option	No right to return, buy-back or cooling off scheme required.
Exit Policy	Sellers can exit at any time by returning the inventory.	No refund or exit policy exists.
Returns	Depends upon the value of products sold and not the number of people recruited.	Money from new participants is used to pay recruiting commissions to earlier participants.
Sales Incentive	Primarily derived from sale of goods and are paid directly through banking channels.	Based on recruiting new people rather than on sales. The payments are made usually through members.

B. New Age Frauds – Cyber Scams & Online frauds

Lottery email from foreign countries

Fake email from financial regulators

Employment emails using the name of reputed companies.

Credit Card Limit updation calls posing as bank officials

Hacking of internet banking password

Prize winning pop-up while working on Internet

COMMON ONLINE FRAUDS: FAKE EMAILS

Email fraud is the intentional deception made for personal gain or to damage another individual through email. Confidence tricks tend to exploit the inherent greed and dishonesty of their victims. The prospect of a 'bargain' or 'something for nothing' can be very tempting. Email fraud, as with other 'bunco schemes' usually targets naive individuals who put their confidence in get-rich-quick schemes such as 'too good to be true' investments or offers to sell popular items at 'impossibly low' prices.

419 FRAUDS

Section 419 in The Indian Penal Code: Punishment for cheating by personation — Whoever cheats by personation shall be punished with imprisonment of either de-scription for a term which may extend to three years, or with fine, or with both.

The Nigerian '419' Scam

The Nigerian '419' scam, also known as the Nigerian Prince scam, the Spanish Prisoner scam, or the Black Money scam is actually a series of scams involving a person overseas offering a share in a large sum of money (hereinafter referred to as the scammer) to someone (hereinafter referred to as the victim) or a payment on the condition that the victim will help them, i.e., the scammer to transfer money out of their country. These scams are often known as 'Nigerian 419' scams because the first wave of the scam started from Nigeria. The '419' part of the name comes from the section of Nigeria's Criminal Code which outlaws this practice.

The scammer usually contacts the victim at random by means of an email, letter, and text message or through any other form of social media. The scammer then tells an elaborate story about large amounts of money belonging to him/her trapped in banks or other investments during events such as civil wars or coups, and are in countries that are currently in the limelight due to one reason or another. Another line of the plot may be that the scammer has or is about to acquire a large inheritance that is 'difficult to access' because of government restrictions or taxes in his/her country. The scammer then offers the victim a large sum of money to help him/her transfer his/her personal fortune out of the country.

Scammers may also ask for the victim's bank account details to 'help him/her transfer the money' and use this information to later steal their funds. Or the scammer may ask the victim to pay fees, charges or taxes to 'help release or transfer the money out of the country' through the victim's bank. These fees usually start out as quite small amounts of money and if they are paid, the scammer might make up new fees that require payment before the victim can receive his/her 'reward'. The demand for money keeps increasing as long as the victims are willing to be a part of it. Nevertheless, the victim is never sent the money that was promised.

The Nigerian '419' scam is an advance fee scheme which occurs when the victim pays money to someone in anticipation of receiving something of greater value, such as a loan, contract, investment, or gift and then receives little or nothing in return. **An advance-fee scam is a form of fraud and one of the most common types of confidence trick.**

There are a variety of advance fee schemes which may involve the sale of products or services, the offering of investments, lottery winnings, 'found' money, or many other opportunities. Some scammers offer to find financing arrangements for their clients who pay a 'finder's fee' in advance. They require their clients to sign contracts in which they agree to pay the fee when they are introduced to the financing source. Victims often learn that the scammer is ineligible for financing and does not have or can arrange the money only after they have paid the 'finder' i.e., the scammer according to the contract. Such agreements may be legally enforced unless it can be shown that the 'finder' never had the intention or the ability to provide financing for the victims.

The following elements of the offence can be identified-

That there was a pretence;

That the pretence emanated from the accused person i.e., the scammer

That the pretence was false;

That the accused knew of the falsity of the pretence, i.e., he did not believe it to be true

That there was an intention to defraud

That the property or thing is capable of being stolen

That the accused induced the owner to transfer his/her whole interest in the property.

'Pretence' is this context refers to the misstatement or misrepresentation of facts with the intent to defraud the complainant, the accused person must have made a statement (either orally or in writing) which was false and he must have known it to be false. A conviction for this offence cannot be sustained if the complainant is not shown to have been 'induced' to part with his property based on the pretence of the accused person. The elements of the offence must be fully established before a court of law would convict a person of obtaining by false pretences.

ATM Card 419 Scam: The ATM Card Payment Scam is used in conjunction with other scams, such as a fake Lottery Scam, Unpaid Contractor Scam or similar exploits. The victim is promised an ATM card with which the victim can withdraw millions dollars (up to a large limit per day) at any location that accepts ATM cards. However, like all Advance Fee Frauds, the victim must pay a fee to receive the card. If it ever is received, it will not work. A "Replacement card" will be offered, again for a fee.

Auction 419 Scam: The scammer "wins" an auction on eBay or another auction site, then "overpays" for the item with a tuque or money order. The scammer then asks the target to send him the overage.

Black Currency 419 Scam: The scammer has a large amount of currency available to share with the target, but the currency has been defaced. However, the currency can be cleaned if the target will purchase enough of the correct cleaning solution (this type of 419 is also called "wash wash"). Black Currency 419 "tales" and techniques are commonly used in many other types of 419 operations.

Cashier's Cheque 419 Scam: The scammer has Cashier's Cheques or money orders he/she needs cashed, and the target can keep a percentage of the cheque for cashing it and forwarding the proceeds net his commission to the scammer. Then the original cheque or money order sent to the target eventually bounces, and the target is out the money advanced to the scammer. The target also is cash out to his bank for any problems with his account caused by the bouncing of the original cheque as he must make up any overdrafts and pay any relevant fees etc.

Charitable Organization 419 Scam: The scammer approaches a charitable organization with a request for help, usually about getting a large sum of money transferred out of a country in which the charitable organization's brethren can claim to be persecuted. A percentage of the proceeds is often offered to the charitable organization for their assistance. The scammer needs monies for fees in order to get the monies freed up.

Chat Room 419 Scam: The scammer meets the target online in a chat room etc. or through a dating or instant messenger online service, befriends the target, and gets the target to advance him/her monies for various reasons. Often leads into Romance 419 scam.

Classic 419 Scam: The scammer has or can gain access to a large sum of money by some means and he/she needs the financial and personal help of the target, in return for a percentage of the funds, to get the necessary transactions processed and get monies out of the country. Many other types of 419 are in actuality variants of Classic 419.

Disaster 419 Scam: The scammer says someone has been killed in a plane crash, earthquake, tsunami, or other disaster, leaving a large sum of money behind which can be claimed by the target or split between the target and the scammer if the scammer can be advanced the monies necessary to process the transaction.

Employment 419 Scam: The scammer "employs" the target to process financial transactions for a commission and has the target advance the net proceeds of these transactions to the scammer before the cherubs sent to the target bounce. Also, another form, where the scammer offers a lucrative job to the target but certain fees must be paid up front by the target to get the job.

Extortion 419 Scam: The scammer says that if the target does not send him money the scammer will hurt or kill the target and/or his family.

Inheritance 419 Scam: The scammer informs the target that someone has died with no relatives to claim the large cash bequest left by the deceased. Often, the scammer says that if someone does not claim the money it will revert to the Government and no-one will get it. The target is asked to "stand in" as a relative to claim the money, with the scammer taking care of all the details, and then split the proceeds with the scammer. The scammer needs monies for fees to get the target declared the rightful inheritor.

Lottery 419 Scam: The scammer says the target has won a lottery, but fees and taxes etc. must be paid before the proceeds can be released.

Oil Scam 419 Scam: The scammer has secured a large amount of oil at below market prices, and the target can get in on the deal for a fee.

Real Estate 419 Scam: The scammer wants to buy real estate, but cannot free up his monies just now to do it, so he asks the target to advance him/her all or some of the funds for the purchase in return for partial ownership of the real estate or a large future fee to be paid to the target.

Recovery 419 Scam: The scammer claims he/she can recover monies lost by the target in a previous 419 operation, but fees must be paid in advance to accomplish this.

Reload 419 Scam: The scammer approaches a target who has already been 419ed and offers the target another type of 419 deal to enable the target to "replace" his/her lost monies or the scammer claims has can bring the previous deal to fruition, if necessary, fees are paid by the target.

Re-shipper 419 Scam: The scammer will attempt to obtain stolen merchandise for personal use or to sell. Because many companies will not send merchandise to Nigeria or Eastern Europe due to warnings about stolen credit card purchases, the scammer must find an in-country person to receive then reship the goods. Click the link for a complete description.

Unpaid Contractor 419 Scam: In this variant of the Classic 419 Scam Advance Fee Fraud, the scammer will claim to be with the Central Bank of Nigeria (CBN), the Nigerian National Petroleum Company (NNPC) or some government ministry. The name of CBN president Charles Soludo is often used in this scam. The victim is told to pose as a contractor who has not yet been paid by the Nigerian government from a "completed project". The money is to be split between victim and the scammer. Payments from the victim will be required to participate in this crime.

War Booty 419 Scam: The scammer says he is a trooper who has stumbled across a large sum of war booty and will pay the target a percentage if the target helps him/her personally and financially to get it out of the country. Often leads into Black Currency 419.

Scam 419 Scam: The scammer informs the target that a distant relative has died leaving a large sum of money which the target can inherit if the proper fees are paid.

Tips to Avoid 419 Advance Fee Fraud

The best tip is to DELETE any mail from a stranger which resembles the mails we described above. Same mail may be forwarded to the service provider's mail ID like abuse[dot]yahoo.com, abuse[dot]hotmail.com depending on the sender’s mail ID. Similarly, you can forward the mail before you junk it to local police email ID.

CREDIT & DEBIT CARD FRAUD

Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of payment in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an add-on to identity theft. Card account information is stored in a number of formats. Account numbers are often embossed or imprinted on the card, and a magnetic stripe on the back contains the data in machine readable format.

Debit card fraud - duplicating one or more of your bank cards, makes up the most regularly seen types of fraud.

Types of Credit Card Fraud

Mail/Internet order fraud: The mail and the Internet are major routes for fraud against merchants who sell and ship products, as well Internet merchants who provide online services. In this, fraudster presents stolen card information by indirect means, whether by mail, telephone or over the Internet to merchant site and orders the delivery of goods of lower value to avoid suspicion

Account takeover:

There are two types of fraud within the identity theft category, application fraud and account takeover.

Application fraud occurs when criminals use stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may create counterfeit documents.

Similarly, you can forward the mail before you junk it to local police email ID if they have any

The scammer "wins" an auction on eBay or another auction site, then "overpays" for the item with a tuque or money order. The scammer then asks the target to send him the overage.

Some merchants added a new practice to protect consumers and self-reputation, where they ask the buyer to send a copy of the physical card and statement to ensure the legitimate usage of a card.

Skimming:

Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant, and can be as simple as photocopying of receipts. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The skimmer will typically use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip.

Instances of skimming have been reported where the perpetrator has put a device over the card slot of a public cash machine (automated teller machine), which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pinhole camera to read the user's PIN at the same time.

Carding:

Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant, and can be as simple as photocopying of receipts. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The skimmer will typically use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip.

Safety tips to avoid Credit Card Fraud

1. There is a critical 3-digit number on the back of the card called CVV (card verification value). Always erase and memorise it.

2. Better hang around when your card is being swiped.

3. A card's magnetic strip has the basic details of the cardholder. But the card also comes with a blank space for you to sign in. You must sign on the card to avoid unauthorized use.

4. Always sign up for SMS/EMAIL alerts for all transactions.

5. Always check your monthly bank statements for any suspicious transactions

6. Disable your credit card account if you are not using it.

7. Shred the financial documents with care

8. Do not store your personal and credit card information on the computer

9. Do not write the PIN number down.

10. During the online transactions, check if the web address starts with HTTPS, which ensures the encryption of all important data.

11. Never delay to report a lost credit card as the consequences can be highly disastrous.

12. Close the account that you suspect is being hit by the fraud.

13. Thoroughly check the authenticity of the firm, the website, or any other transactional society where your money would be flowing through.

14. Never give away your personal information over the phone unless you are sure of the person the other end.

15. Take a pause before venturing into any kind of online transaction and decide upon the authenticity of the transaction.

Safety tips to avoid Debit or ATM Card fraud

1. When you type your PIN number at an ATM, make sure that you sufficiently obscure the keypad from being viewed by an onlooker.

2. NEVER let the shopkeeper take your debit card out of your sight. There is no need for him/her to do so, unless he/she intends to do something unlawful.

3. Secure your debit card physically by storing it at a safe place.

4. NEVER write your PIN number at a place where it can be seen by someone who you do not intend to show it to.

5. ALWAYS destroy the receipts from merchants that you no longer require, especially when you have paid for using your debit card.

6. If you do not receive your debit card or PIN number from the bank within a reasonable amount of time after requesting one, check with the bank when it was sent and when you should expect to receive it. It may have been picked up by someone else in transit.

7. When at an ATM, make sure that no external devices are attached to the ATM machine and no wires are hanging around.

8. Check your account statements carefully for transactions that you may not have made

Using ATM machine

1. Safeguard your credit cards and ATM cards at all times.

2. If you notice something suspicious about the card slot on an ATM (like an attached device), do not use it and report it to the responsible authorities.

3. Never disclose your ATM card and credit card PIN numbers to strangers.

4. Beware of your surroundings while withdrawing money at ATM centers. Do not crumple and throw away the transaction slips or debt card memos: read them, make a mental note of the details and then, either tear them or shred them to trash.

5. Periodically check your account balances on Internet or by requesting your bank or credit card company to send you statements to ensure that no transactions are happening behind your back.

6. While entering any personal identification numbers, use your discretion to shield the keypad so that your hand movements are not very visible and you enter your passwords secretly.

7. Be careful while withdrawing money from ATM Machine the attacker can shoulder surf to see your PIN.

8. In case any one behind you while withdrawing money just tell the ATM Security guard to ask him to wait out.

JOB FRAUD

We often see that several unemployed youth paying huge cash to fraudsters for securing jobs in Government Services or Corporate Sector. Taking advantage of the innocence of these unemployed youth, fraudsters float fictitious companies and give attractive advertisements to the press and attract the unemployed youth towards them and after collecting money as 'caution deposit/security deposit' and dupe them. Here are some of the frauds committed by such criminals.

Fake JOB VISA for employment abroad

Training and employment in the same company and Employment abroad

Data warehousing works.

Employment fraud in Railways Recruitment

Employment in reputed PSU s and Private Companies.

HOW TO SUSPECT A FRAUD?

If you find any of the following signs in your transactions, you have strong reason to SUSPECT it...

Transactions being carried in cash

Originals are missing and certified copies are shown to you.

Documents in colour Xerox and laminated

Signatures are varied in all places

Documents are only notarized

Seller himself is missing during deal materialization

Sale deed signed in blue ink / stamps in blue ink. It is mandatory to use black ink in Sub Registrar office

Seller is forcing you to finalize the deal in undue haste in the guise of owner leaving abroad etc.,

Turn impatient and embarrassed when you ask them certain questions

C. DO'S & DON'TS OF INTERNET USE

Do not enter your account details on fake web-sites

If you receive any email asking you to ‘update your account details’ or ‘verify your information because your account details were stolen’, exercise caution and call the bank first.

Be careful when you download

We’re often tempted by attractive offers or schemes – be careful when downloading or opening attachments as files can trigger a virus and your information can get stolen.

Type in the URL in the address bar

Instead of using links, type the bank or company URL in the address bar, as sometimes clicking on links will redirect you to a fake address. Make a practice of always typing in the URLs so you will memorize the accurate web address and not rely on links.

Regularly check your accounts

Maintain an awareness of the financial activity in your bank accounts and make a habit of regularly checking them. Report any suspicious or uncertain transactions to your bank account or credit card firm.

Always verify the web address

For any financial website that enables you to log in, ensure the URLs always start with “https://” as the ‘s’ stands for security. If you make purchases online, again ensure the web address of the online retailer starts with https:// and has a ‘lock’ icon on the status bar to ensure your details remain encrypted.

Set online transaction limit

It is also a good idea to set a ‘transaction limit’ with your credit card provider for every purchase online as this limits your exposure as it prohibits transactions beyond the limit. Check with them to see if they offer this service.

Enable SMS notifications

If your bank or credit card provider offers SMS notifications for every transaction, enable it as you can keep tabs if your card has been stolen or misused. If you notice any suspicious transactions, call your bank immediately to block the card.

General precautions:

Never write down your PIN codes anywhere they can be easily found

Do not give your PIN codes to anyone

Do not use the same online password for all your bank accounts. Create unique passwords

Change your bank account passwords frequently to ensure the safety of your account.

Do not let strangers access your computer and ensure it remains in a safe place at all times.

Do not ‘save’ passwords on your browser as much as possible.

Install anti-virus software to ensure your computer stays up to date on the security front.

Protect your identity and accounts

Credit cards: If you used credit card information in a fraudulent transaction, contact your card issuers immediately to make a fraud report. As part of the process, you may be required to get a new account number.

Log-ins and passwords. If you registered for access to a fraudster’s website using usernames or passwords that you use elsewhere, be sure to update accounts with new log-ins as soon as possible.

Do’s:

Do verify the registration and disciplinary history of any broker, adviser, or trading platform with the SEBI.

Get a second opinion from a trusted adviser, family member, or friend before making an investment.

Delete—don't open—unsolicited email. Often, opening an email will signal a spammer that the email account is active and more spam will follow.

Verify business addresses by doing an online map search and looking at the location using the street-level view. Many fraudulent websites will use fake addresses, which can be easily spotted with a virtual visit.

Review privacy settings on social media platforms and conceal or delete information that pinpoints where you live, where you went to college, what you do for a living, where you trade or bank, how often you invest, etc.

Check email addresses carefully to avoid phishing attacks.

Learn about the common persuasion tactics fraudsters use.

Don't:

Don't respond to unsolicited sales calls or email.

Don't give credit card, payment information, or personal information over the phone, in an email, or to a website that is sent as a link in an email.

Don't fund trades or investments by wiring money, sending prepaid credit or gift cards, using digital assets such as Bitcoin, or making other unusual forms of payment.

Don't communicate using encrypted messaging apps with "brokers" or others promising to make you money. These apps provide global access and hide the true location of the person on the other end.

Don't trade or invest in schemes you don't fully understand.

Don't engage with people promoting investments or trading schemes on social media.

Don't trade or invest with unregistered entities or individuals that operate outside the country.

Don't engage with people you are introduced to through third parties or organizations. Affinity fraud targets people through social groups and use those connections to build credibility. Places of worship, professional organizations, service organizations, and others are common targets for affinity fraudsters.

3. Regulatory Framework & Enforcement

A. Economic Offences, Legislations & Enforcement Agencies

Economic Offences are a broad category ranging from Tax evasion to smuggling to theft of antiquities, land grabbing, etc. These are covered under a variety of legislations from IT Act to COFEPOSA, FERA, FEMA, IPC NDPS, IPC etc. and have own designated investigation authorities.

Sl. No.	Economic crimes	Acts / Legislation	Enforcement authorities
1	Tax evasion	Income Tax Act	Central Board of Direct Taxes
2	Illicit trafficking in contraband goods (smuggling)	Customs Act 1962 COFEPOSA, 1974	Collectors of Customs
3	Evasion of Excise Duty	Central Excise Act, 1944	Collectors of Central Excise
4	Cultural object's theft	Antiquity and Art Treasures Act, 1972	Police/State CB-CID/CBI
5	Money laundering	Foreign Exchange Regulations Act, 1973; Money Laundering Act, 2002	Directorate of Enforcement

6	Foreign contribution manipulations	Foreign Contribution (Regulation) Act, 1976;	Police/CBI
7	Land grabbing/Real estate frauds	IPC	Police/State CB-CID/CBI
8	Trade in human body parts	Transplantation of Human Organs Act, 1994	Police/State CB-CID/CBI
9	Illicit drug trafficking	Narcotic Drugs and Psychotropic Substances Act 1985 & NDPS Act, 1988	NCB/ Police/State CB-CID/CBI
10	Fraudulent bankruptcy	Banking Regulation Act, 1949	Police, CBI
11	Corruption and bribery of public servants	Prevention of Corruption Act, 1988	State/Anti-Corruption Bureau/ Vigilance Bureau/ CBI
12	Bank frauds	IPC	Police/State Vigilance/CB-CID/CBI
13	Insurance frauds	IPC	Police/State Vigilance/CB-CID/CBI
14	Racketeering in employment	IPC	Police/State CB-CID/CBI
15	Illegal foreign trade	Import & Export (Control) Act,1947	Directorate General of Foreign Trade/CBI
16	Racketeering in false travel documents	Passport Act, 1920/IPC	Police/State CB-CID/CBI
17	Credit cards fraud	IPC	Police/State CB-CID/CBI
18	Terrorist activities	IPC & related Acts	Police/State CB-CID/CBI
19	Illicit trafficking in arms	Arms Act,1959	Police/State CB-CID/CBI
20	Illicit trafficking in explosives	Explosives Act, 1884 & Explosive Substances Act, 1908	Police/State CB-CID/CBI
21	Theft of intellectual property	Copyright Act, 1957 (Amendments 1984 & 1994)	Police/State CB-CID/CBI
22	Computer crime/software piracy	Copyright Act, 1957/I.T.Act, 2000	Police/State CB-CID/CBI
23	Stock market manipulations	IPC	Police/State CB-CID/CBI
24	Company frauds	Companies Act, 1956/IPC MRTP Act, 1968 Police/CBI/SFIO	

Record of Economic Offences & Investigations

The record of investigations and prosecutions of major economic offences and financial frauds as culled from Crime In India Volume II are short listed below with respect to Karnataka's neighbours and other comparable major states.

	Major Economic Offences in Key States								
SL	**State/UT**	**Year**			**Mid-Year Projected Population in Lakhs**	**Rate of Economic Offences**	**Charge sheeting Rate**	**Conviction Rate**	**Pendency %**
		2019	**2020**	**2021**	**2021**	**2021**	**2021**	**2021**	**2021**
1	Karnataka	6795	5107	6447	669.9	9.6	52.9	7	94
2	Kerala	6584	9136	5421	355.4	15.3	39	13.6	97.3
3	Maharashtra	15686	12453	15550	1247.6	12.5	57.2	13.1	98.6
4	Tamil Nadu	3517	2898	3574	764.8	4.7	69.5	8.2	95.3
5	Telengana	11465	12985	20759	377.7	55	60.1	31.8	89.2
6	Andhra Pradesh	8806	7467	9273	528.5	17.5	73.5	17.2	87.6
7	West Bengal	9593	8709	10750	982.9	10.9	77.5	9.1	99.3
8	Goa	165	153	131	15.6	8.4	55.3	35	97.6

Major Economic Offences in Key Cities										
City	Year			Of Which Criminal Breach of Trust & Forgery, Fraud / Cheating	Mid-Year Projected Population in Lakhs	Rate of Economic Offences	Charge sheeting Rate	Loss of Property from Breach of Trust & Forgery, Fraud / Cheating	Conviction Rate	Pendency %
	2019	2020	2021	2021	2021	2021	2021	2021	2021	2021
Bengaluru	2850	2085	2715	2695	85	31.9	52.4	2116	4	96.6
Kochi	469	481	434	432	21.2	20.5	38.5	357	5.8	98.6
Mumbai	5556	3927	5671	5656	184.1	30.8	43.8	2756	21.3	98.3
Chennai	811	696	840	834	87	9.7	66.4	797	24.6	95.9
Hyderabad	1895	3427	4870	4854	77.5	62.7	50.7	202	42.6	94.9
Kolkata	2327	1817	2077	2074	141.1	14.7	81.1	1879	100	99.8

	Economic Offences Disposal by Courts															
SL	Crime Head	Cases Pending Trial from the Previous Year	Cases Sent for Trial during year	Total Trial Cases	Cases Abated by Court	Cases Withdrawn from Prosecution	Compounded	Plea bargain	Quashed	Disposed of Without Trial	Stayed	Convicted	Discharged	Acquitted	Conviction Rate	Pendency Percent
1	Criminal Breach of Trust	126238	13085	139323	45	10	460	5	9	529	59	882	258	1709	31	97.6
2	Counterfeiting	8877	537	9414	4	1	2	0	2	9	11	72	4	80	46.2	98.2
3	Forgery, Cheating & Fraud	479921	73932	553853	277	32	3573	218	183	4283	675	4577	800	10457	28.9	96.4
	Karnataka	23668	3591	27259	41	0	330	0	32	403	86	87	11	1146	7	94

The bulk of these cases comprise Breach of Trust and Fraud, Forgery & Cheating. The cases involving loss of property are among the highest in Mumbai, Bengaluru and Kolkata.

Often, Breach of Trust, Fraud, Forgery & Cheating, Cyber Crimes like Online fraud, OTP fraud, social media Fake News / Publicity, Fake Profiling etc. have areas of overlap with Deposit related financial frauds covered under KPID as do Banking & Credit Card / ATM frauds. Further, in many cases of the Karnataka Protection of Interest of Depositors in Financial Establishments Act (KPID) frauds, there are financial and property relations with Cooperatives, Ponzi Schemes, Multi-level Marketing & Direct Selling and Land Registration.

The data on a selection of major KPID cases (39) are analysed and indicate that at least 16 (41%) start as Cooperatives (particularly Souharda Cooperatives) and about 10 (26%) use MLM, 10 (26%) use Direct Selling, 12 (31%) use Land Development, 5% use Tours & Travels, 5% use Bullion Trading, 6 (15%) use various online trading in Bit Coin / Shares and offline methods like Plantations and 21 (52%) use various combinations for making sharable profits.

In terms of payment to investors & depositors, 37(94%) use interest / profit from their alleged activities while 1 exclusively uses Plantation returns and 2 combine it with Gifts / Services (Medical & Pharmaceutical). Thus, multiple routes for both scheme operation and / or investment which may be MLM / Ponzi / Direct Selling / Gold Loans are seen. Almost all the schemes have significant investments in real estate and recoveries hinge on the ability to weed out these investments. Thus, depositors and investors must realize that such fraudulent schemes are based on a web of money transfer and deceit and hence once money is invested, it would be difficult to recover.

B. Regulatory Proviso

India has a number of legislations that attempt to tackle the problem of Ponzi schemes and financial frauds.

1. The Chit Funds Act, 1982

Under this Act, only schemes registered and regulated by the state governments are permitted to function. They are then regulated by the Registrar of Chits as appointed under section 61 of the Chit Funds Act. The Act further mandates an arbitration procedure before the Registrar with powers similar to a civil court under the Code of Civil Procedure, 1908. The Registrar is empowered to attach properties of any party to the dispute, and he may further wind up a registered chit if contravening with the Act. Per the Act, all chit companies are banned from appropriation of the chit collections as well as accepting any deposits.

2. Prize Chits and Money Circulation Schemes (Banning) Act, 1978

Section 2(a) of the PCMCS Act explains 'conventional chit' as a transaction by any name under which a person responsible for the operation of the chit enters into an agreement with a number of persons that each of them would subscribe a certain sum of money (or grain) by periodical instalments through a definite period and each subscriber would receive by way of tender, lot or auction a prize amount. This is not prohibited under the PCMCS Act. What is however banned are 'Prize Chit' and 'Money Circulation Schemes'.

Section 2(c) of the PCMCS Act explains money circulation schemes as those for making quick or easy money, or receipt of any money or valuable thing as consideration for a promise to pay money on any contingency relative or applicable to enrolment of members into the scheme. Section 2(e) of the Act explains prize chits as any transaction under which a foreman collects money and utilizes the same or any income arising from it for the purposes of awarding periodically to a specific number of subscribers determined by lot or otherwise, whether or not the prize recipient is liable to make further payments in the scheme. Alternatively, for the purpose of refunding the same to those who haven't won the prize on the termination of scheme or after expiry of any stipulated period.

Section 3 of the Act bans prize chits and MCS and enrolment to these schemes. Sections 4 and 5 are penal provisions. Section 6 entails offences committed by companies. Section 7 empowers a police officer, not below the rank of officer in charge of a police station, to exercise power to enter and search premises and to seize things used for such scheme. Section 8 provides for forfeiture of newspaper and publication containing money circulation scheme. Section 13 of the PCMCS Act empowers the State governments to make rules on consultation with the RBI.

3. The Companies Act, 2013 & Companies (Acceptance of Deposits) Rules, 2014

The primary focus under the Companies Act, 2013 is from the perspective of corporate frauds. Section 447 defines a corporate fraud including any omission, concealment of any fact or abuse of position submitted by any individual with the aim to deceive, to acquire benefit from, or to harm the interests of the company or its investors or its shareholders, regardless of whether or not there is any wrongful gain or wrongful loss.

The provision further stipulates that the misrepresenting individual is liable for detainment for a period between 6 months and 10 years in addition to a fine. If the fraud relates to public interest, the minimum imprisonment is 3 years.

Serious Fraud Investigation Office

Section 211 of the Act empowers the Central Government to establish a Serious Fraud Investigation Office for the purpose of investigation into company related frauds. For the duration of the SFIO's investigation beginning from assignment of case to the officer, no other parallel investigation may subsist. **The SFIO may arrest individuals if it has reason to believe that he is guilty based on the material in possession. SFIO shall submit a report to the Central**

Government on conclusion of investigation. Central Government may direct SFIO to initiate prosecution against the company. SFIO shall share information they possess regarding a case being investigated by the latter and vice versa.

4. Companies (Acceptance of Deposits) Rules, 2014

Section 73 and 76 of the Companies Act, 2013 concern deposits and are read with the Companies (Acceptance of Deposits) Rules, 2014.

Per the 2014 Rules, fund raised by an entity with a promise to refund with or without interest at the end of a specified period will be treated as deposits. With the detailed and stringent definition of deposits, operators raising funds through surrogates have been largely suffocated.

Per the definition clause, eligible companies that do intend to raise public deposits would need to have a minimum net worth of INR 100 crore or a turnover of at least INR 500 crore rupees. Further, the rules include a definition of "deemed deposit" where any scheme that provides returns to investors, whether in cash or kind, is deemed to be a deposit, a gap earlier misused.

5. Securities and Exchange Board of India Act, 1992 & Securities and Exchange Board of India (Collective Investment Scheme) Regulations, 1999

The Securities and Exchange Board of India has so far initiated as many as 567 cases against illegal investment schemes collecting public money. These Collective Investment Schemes are defined under Section 11AA of the SEBI Act, 1992. They have been regulated by the Act and the SEBI (CIS) Regulations, 1999.

6. The Banning of Unregulated Deposit Schemes Act, 2019

The Banning of Unregulated Deposit Schemes Act, 2019 or the BUDS Act, was purposed at curbing all fraudulent, unregulated, deposit schemes. In so doing, it lists certain deposit schemes valid and regulated by MCA, SEBI, RBI, etc., such as certain collective investment schemes, alternative investment funds, portfolio management services, employee benefit schemes, mutual fund schemes, etc. regulated by SEBI; deposits accepted by NBFCs, etc. as regulated by RBI, insurance contracts regulated by IRDAI; schemes or arrangements made or offered by co-operative societies, chit funds, etc. regulated by the relevant State Government or Union Territory Government; housing finance companies regulated by the NHB; pension funds regulated by the PFRDA; pension schemes or insurance schemes framed under the Employees' Provident Fund Miscellaneous Provisions Act, 1952; Deposits accepted or permitted under the provisions of Chapter V of the Companies Act, 2013 regulated by MCA.

Section 2(4) of the Act explains, deposits are the amount of money received by way of an advance or loan or in any other form, by any deposit taker with the promise to return whether after a specific period or otherwise, either in cash or in-kind or in the form of the specific service, with or without any benefit in the form of interest, bonus, profit or in any form.

This Act forbids and penalizes the acceptance of deposits under any course of action which is not regulated or under ordinary course of business. Penalty is further stipulated on failure to return monies are accepted by way of regulated deposit schemes on maturity of any promised service in lieu of the deposits.

Offences:

Soliciting deposits under the unregulated deposit schemes,

Acknowledgement of deposits under the unregulated deposit schemes,

Fraudulent default in registered deposit schemes and

Unfair instigation in relation to unregulated deposit schemes

Trial: Designated Courts

7. The Banning of Unregulated Deposit Schemes Rules, 2020

The BUDS Rules define the term 'competent authority' as an authority appointed by the appropriate government under Section 7 of the BUDS Act, according to which the Authority has the same powers as vested in a civil court under the Code of Civil Procedure, 1908 (CPC) while conducting investigation or inquiry in respect of offences under the Act.

Major Highlights

a) Provisional Attachment of the Property

b) Central Database and Intimation to Repository Authority

c) Restrictions to Advertising

8. THE KARNATAKA PROTECTION OF INTEREST OF DEPOSITORS IN FINANCIAL ESTABLISHMENTS ACT, 2004

"Deposit" includes and shall be deemed always to have included any receipt of money or acceptance of any valuable commodity by any Financial Establishment to be returned after a specified period or otherwise, either in cash or in kind or in the form of a specified service with or without any benefit in the form of interest, bonus, profit or in any other form,

"Financial Establishment" means **any person or a group of individuals accepting deposit under any scheme or arrangement or in any other manner** but does not include a corporation or a co-operative society owned or controlled by any State Government or the Central Government or a banking company;

Attachment of properties on default of return of deposits -

(1) The Government or the District Magistrates in their respective jurisdiction, suo moto or based on the market intelligence reports or Police Authority on receipt of any complaint may cause investigation of a complaint or fraudulent transaction referred to in this section through its functionaries, collect the information regarding the properties and money believed to have been acquired by any financial establishment, from public or organizations or other institutions as deemed appropriate.

Section 7. Assessment of assets and deposit liabilities -

The Competent Authority under this Act has to assess the deposit liabilities and the assets of the Financial Establishment and submit a report thereof to the Special Court. The Competent Authority thereafter **shall issue notice either individually or by means of effective media publication**, inviting the claims by secured creditors, if any, and **also the depositors of the Financial Establishments to submit their claims with proper proof** to establish the same

Section 8. Report by the Competent Authority –

After making a report under section 7, the Competent Authority shall make an application to the Special Court seeking permission to make payment to the depositors from out of the money realized.

1. Calling of claim is a process given in the law wherein **"proper proof"** is to be provided to establish the claim.
2. The notice is issued **"individually or by means of effective media publication"** i.e., it should come to the notice of the individual and not merely to the notice of some agent
3. All such processes prefer the application to be made in person and bulk applications are not allowed so as to avoid falsification and influence
4. Verification is done at the time of submission of form itself and only those who don't have a necessary document, need to return for re-verification. Hence if documents are correct there is no need for multiple visits
5. These precautions are also necessary because there are cases received of middlemen submitting claims in bulk and as such agents have ulterior motives, possibly commercial interests and are untrained in procedures, they may make serious or deliberate errors and mix ups.
6. A few non-depositors have disguised themselves as claimants and made applications in the past leading to rejections and unnecessary problems

7. Many persons particularly early investors in pyramid style frauds who have got almost all their money back, try to get some extra, undeserved claims registered by applying. Such persons could forge documents and take away legitimate claims of genuine depositors at loss particularly in situations where the attachment is less than the total claim.
8. Many persons have been again cajoled by the Directors/ Partners / Promoters of Kanva and some other Financial Enterprises to submit their original Bonds/ Agreements in return for promised future benefits. Such persons may try to forcefully submit their claims or use bulk claims submitted through third party to slip in false claims
9. Some middlemen are allegedly collecting money from gullible people, pretending to be their sympathizers filing a few complaints and holding a few demonstrations, uploading videos with baseless allegations just so that they can further exploit these people to possibly

   i) Pay additional money for "services"

   ii) Divert their claims to some other person

   iii) Include claimants who have already received their entire deposit and also some profit

   iv) Surreptitiously slip in those Directors, Partners and Promoters of the FE who are also depositors

   v) Introduce an agency business with a paid package to prepare, process and submit claims

Keeping the above possibilities in mind, and given that any statutorily given procedure must have non - replicable forms which are numbered, traceable and accountable, the claims system has been designed.

SPLOCA Guidelines on Filing of Claims

i. All those cases where ONLINE claims are called would have the **option for offline also** for those who do not have access to internet. In the cases where, due to lack of database, software for online claims cannot be prepared and claim can only be called OFFLINE/ MANUALLY.

ii. The system of claims is not a harassment but a necessity given the directions in the law and the necessity to correctly obtain depositor information and contact details as well as protect the privacy and financial information of the depositor.

iii. No person incapable of appearing in person need come and may for reasons set down in writing, with proof of identity as depositor, authorize another person to collect form, submit claim, documents in original as required and even represent during verification. If the instructions are followed and proper documents of proof collected in advance, the concerned persons may if they wish come only once - for Submission & Verification which, all documents being in order could be done simultaneously. iv. Persons who are unwell, outside Bangalore, elderly etc. may send a nominee or any authorized agent through a Power of Attorney, to obtain and also submit forms.

v. A key part of providing "proper proof to establish claim" includes the following: (a) Proof of Identity as Depositor (b) Proof of Nomination & Identity of Nominee in case of death / incapacitation of Depositor (c) Proof of the investment (d) Proof of Returns (e) Proof of the account to which claims are to be deposited.

It may also be noted that some persons are trying to convince Depositors, many of whom are aged and infirm to come in large numbers to the offices of Competent Authorities for agitations and demonstrations. Already a few such persons have come three or four times and been made to stand for hours doing demonstrations in the open. It is strange that such persons are considered fit enough to hold protests in sun and rain multiple times, but should find it difficult to come to file their claims.

vi. The Competent Authorities are accountable to the law, the courts and to **all the Genuine Depositors.** When **a public authority designs a system, it has to serve the majority of the claimants and cannot be partial to a few or to any self-proclaimed agent or middleman. Hence any action taken or modification of the system within the limits of the law and orders of the court must be sought by the majority of the Genuine Depositors.**

General Instructions on Filing Claims

1. FORM: Every person obtaining a Form in case of MANUAL submission, must show Depositor ID (Copy of Aadhaar / PAN/ Driving License), Bond / Agreement with Financial Enterprise and PoA in case of Authorized Agent. The Depositor's/ Nominee's / PoA holder's Mobile Number and Mailing Address with Pin Code shall be entered in Form Issue Register along with Form Sl Number and Unique Form Number.
2. TOKEN: While submitting claims, obtain a Token with Counter Number & Serial Number, Timing, sign on Token Register. The Token shall carry Unique Form Number which shall be used as the unique identity number for digitization, tracking, queries and communication etc.
3. SUBMISSION: The Token Counterfoil shall be presented when called for by the Counter concerned and handed over along with documents of claims. Tokens cannot be carried over to later date unless signed thereon by the Counter Clerk and returned. They will be examined and a receipt along with copy of accepting / rejecting / document required shall be issued. The Claimant shall sign in the Acknowledgement of the Form and retain carbon copy.
4. SIGNATURE: Where required, documents shall be signed by depositor only (unless minor or deceased in which case parent / guardian / PoA holder shall sign)
5. PRODUCING DOCUMENTS: Bonds / Agreements / Notarized Affidavits and statutory documents shall be produced in original. Where copies are allowed as support documents, either ink signed attested clear xerox copy of every page shall be provided or original shall be provided alongside xerox copy for attestation by concerned CA only. No scans / WhatsApp copies are acceptable.
6. NUMBER OF CLAIMS: A single claim for every can be produced at a time for every Customer / Client ID (as given in MoU / Bond with Financial Enterprise). Multiple claims, bunched papers, multiple or family or group claims cannot be produced in one instance and each claim shall have a token.

Procedure

NOTE 1: Special Procedure

1. The receipt on Claims Applications shall be on first come, first served basis with following exceptions in the order mentioned:

i. Senior Citizens above 60 years of age
ii. Women with child in arm
iii. Physically challenged/ Infirm
iv. Women
v. Medically unfit with recent medical certificate

2. The claims shall be accepted from the depositor only except for the following:

i. Nominee or Legal Heir or Members of the immediate family - Parents / Spouse / Children, due to illness or disability or death of the depositor.

ii. Members of the extended family due to illness or disability or death of the depositor and absence or disability or death of Nominee or Legal Heir or Members of the immediate family, provided Depositor/ Nominee / Legal Heir has provided signed authorization or death certificate is available

iii. Parents of minor children

iv. Power of Attorney Holder duly authorized for the specific purposes with reasons

1. ***Fill the above statement for each of the deposits made Separately. One Statement for One Customer ID.***
2. ***FE means the Financial Establishment in which the investment is made.***
3. ***It is mandatory to attach certified copy of Bank Statement issued by the concerned Bank from the date of investment till date as Proof of Deposit made and profit received.***

i. Aadhaar Card shall be verified online

ii. Mobile Number shall be called or SMS sent for confirmation

iii. Depositors living in other states / countries shall have to make a WhatsApp call / return mail from their confirmed email address within 1 hour for confirmation. A Test mail with an authorization document shall be sent to them which shall be filled in and digitally signed, printed and scanned and mailed back with a picture of their face. Alternatively, the claimant shall make a WhatsApp video call to confirm identity.

NOTE 2: Documents to be filed

i. Adhaar/ Valid Driving License
ii. PAN
iii. MOU / Investment / Loan / Lease Agreement
iv. Bank Passbook Face Sheet
v. Family / Genealogy Tree by Competent Authority (Jurisdictional Tahsildar)
vi. Nomination Proof
vii. Death Certificate / Hospitalization/ Illness Certificate / Disability/ Infirmity Certificate/ VISA Certificate duly certified by Issuing Authority
viii. Attested copies should be of original documents and not PDF or photo images and must be ink signed by Attestor.
ix. In case any original document is lost, FIR filed in jurisdictional police station shall be enclosed to that effect.
x. Certified copy of the Bank Statement from the date of investment till date duly certified by the respective bank.
xi. Self-attested copy of Pass Book updated till date. Original Pass Book shall be produced for verification.

9. Regulatory Proviso for MLM, Pyramid Schemes, Direct Selling etc.

A. Consumer Protection (E-Commerce) Rules 2020

KEY FEATURES

▪ Definition of e-commerce entities: E-commerce entity includes any person who owns, operates, or manages a digital or electronic facility or platform for e-commerce. It will also include: (i) any entity engaged by an e-commerce entity for the fulfilment of orders, (ii) any related party (as defined under the Companies Act, 2013) of an e-commerce entity.

▪ Fallback liability: In case of non-delivery of goods or services by a seller on a marketplace platform, which causes loss to the consumer, the marketplace will be subject to a fallback liability.

▪ Regulation of associated enterprises: Marketplace e-commerce entities are prohibited from: (i) listing associated enterprises as sellers on its platform, and (ii) sharing information for the unfair advantage of its associated enterprises. Associated enterprises include enterprises: (i) related through a common chain of managing directors, partners or shareholders, (ii) having 10% of more common ultimate beneficial ownership, or (iii) having a relationship of mutual interest, as may be prescribed.

▪ Use of name or brand associated with marketplace entity: Marketplaces may not use its name or brand for promotion or offer for sale of goods or services, to suggest that these offerings are from the marketplace itself.

▪ Abuse of dominant position in a market: An e-commerce entity is not allowed to abuse its dominant position in any market.

▪ Requirement to appoint certain personnel: All e-commerce entities are required to appoint: (i) a Grievance Officer to address consumer grievances, (ii) a nodal person for coordination with law enforcement agencies, and (iii) a Chief Compliance Officer for ensuring compliance with the Consumer Protection Act and Rules thereunder. These persons should be residents in India.

▪ Information requests by law enforcement: The Draft Rules require e-commerce entities to provide information under their control or possession upon request by a government agency. The government agency which is lawfully authorized for investigative, protective or cybersecurity activities may place such a request in writing.

▪ Country of origin of goods: The 2020 Rules require e-commerce entities to disclose the country of origin of goods. (i) Provide a filter mechanism on their website based on country of origin, (ii) display notification regarding origin of goods at pre-purchase stage, and (iii) display suggestions of alternatives to ensure a fair opportunity for domestic goods.

▪ Flash sale: The Draft Rules prohibit e-commerce entities from organizing flash sales. Flash sale is defined as a sale organized by fraudulently intercepting the ordinary course of business using technology means, to allow only a specified seller or group of sellers managed by the e-commerce entity to sell highly-discounted goods and services. Further, the sale would be termed a flash sale only if it is operational for a pre-determined period, on selective goods or services or otherwise, to draw a large number of consumers.

▪ Cross-selling: The Draft Rules define cross-selling as sale of goods or services which are related, adjacent, or complementary to a purchase made by a consumer at a time from any e-commerce entity, with intent to maximize the revenue of such an e-commerce entity. The e-commerce entity engaging in cross-selling has to provide adequate disclosure to users about: (i) name of the entity providing data for cross-selling, (ii) data of such entity used for cross-selling.

▪ Mis-selling: The Draft Rules prohibit mis-selling of goods or services by e-commerce entities. Mis-selling is defined as a deliberate misrepresentation of information (by e-commerce entities) about such goods or services as suitable for the user who is purchasing them.

▪ Misleading advertisements: An e-commerce entity should not allow misleading advertisements on its platform. Under the Act, misleading advertisement is defined to include: (i) falsely describing product or service, (ii) falsely guaranteeing or misleading about nature, substance, quantity, or quality of product or service, (iii) representation which may be considered unfair trade practice, and (iv) deliberately concealing important information.

B. CONSUMER PROTECTION DIRECT SELLING RULES 2021

3. Definitions:

(c) "direct seller" means a person authorized by a direct selling entity through a legally enforceable written contract to undertake direct selling business on principal-to-principal basis;

(d) "direct selling entity" means the principal entity which sells or offers to sell goods or services through direct sellers, but does not include an entity which is engaged in a Pyramid Scheme or money circulation scheme;

(f) "money circulation scheme" means the schemes defined in clause (c) of section 2 of the Prize Chits and Money Circulation Schemes (Banning) Act, 1978 (43 of 1978);

(g) "mis-selling" means selling a product or service by misrepresenting in order to successfully complete a sale and includes providing consumers with misleading information about a product or service or omitting key information about a product or providing information that makes the product appear to be something it is not;

(i) "Pyramid Scheme" means a multi layered network of subscribers to a scheme formed by subscribers enrolling one or more subscribers in order to receive any benefit, directly or indirectly, as a result of enrolment or action or performance of additional subscribers to the scheme, in which the subscribers enrolling further subscribers occupy a higher position and the enrolled subscribers a lower position, resulting in a multi-layered network of subscribers with successive enrolments:

4. Mandatory maintenance of records – Every direct selling entity shall maintain at its registered office, either manually or electronically, all such documents as are required under any law for the time being in force, including the following documents or records, as may be applicable, namely:

(a) Certificate of Incorporation;

(b) Memorandum of Association and Articles of Association;

(c) Permanent Account Number and Tax Deduction and Collection Account Number;

(d) Goods and Services Tax registration; (e) Goods and Services Tax Returns;

(f) Income Tax Returns;

(g) Balance Sheet, Audit Report and such other relevant reports; (h) Register of direct sellers;

(i) Certificate of Importer-Exporter code (in case of imported goods)

(j) License issued under the Food Safety and Standards Authority of India Act, 2006 (34 of 2006) for the purposes of manufacture or sale of food items;

(k) License and Registration Certificate issued under the Drugs and Cosmetics Act, 1940 (23 of 1940) for the purposes of manufacture or sale of drugs, including Ayurvedic, Siddha and Unani drugs and Homoeopathic Medicines;

(l) Certificate of Registration of Trademark.

9. Application of e-commerce rules – The direct sellers as well as the direct selling entities using e-commerce platforms for sale shall comply with the requirements of the Consumer Protection (e- Commerce) Rules, 2020.

10. Prohibition of Pyramid Scheme and money circulation scheme: No direct selling entity or direct seller shall–

(a) promote a Pyramid Scheme or enrol any person to such scheme or participate in such arrangement in any manner whatsoever in the garb of doing direct selling business;

(b) participate in money circulation scheme in the garb of doing direct selling business.

C. Karnataka Direct Selling Rules 2019

The Karnataka Rules have the proviso in Rules 8 & 9 to appoint a Nodal Officer and / or designate officers of other regulatory departments to assist the Nodal Department in the implementation of these Rules and to set up a mechanism to monitor the activities of Direct Sellers & MLMs and prohibition of Money Circulation & Pyramid Schemes.

4. International Fraud Prevention Information

A. USA

Avoid Fraud

According to the Willie Sutton principle, fraudsters tend to go "where the money is"—and that means targeting older people who are nearing or already in retirement. Financial fraudsters tend to go after people who are college-educated, optimistic and self-reliant. They also target those with higher incomes and financial knowledge, and have had a recent health or financial change.

To entice you to invest, fraudsters use high pressure and a number of "tricks of the trade." Here are some common tactics:

The "Phantom Riches" Tactic—dangling the prospect of wealth, enticing you with something you want but can't have.

The "Source Credibility" Tactic—trying to build credibility by claiming to be with a reputable firm or to have a special credential or experience.

The "Social Consensus" Tactic—leading you to believe that other savvy investors have already invested.

The "Reciprocity" Tactic—offering to do a small favour for you in return for a big favour.

The "Scarcity" Tactic—creating a false sense of urgency by claiming limited supply.

Protect yourself with these strategies:

End the conversation. Let them know you'll think about it and get back to them. Have an exit strategy so you can leave the conversation if the pressure rises.

Turn the tables and ask questions. Before you give out information about yourself, ask and check.

Talk to someone before investing. Even if the seller and the investment are registered, discuss your decision first with a family member, investment professional, lawyer or accountant.

Red Flags of Fraud

To stay on guard and avoid becoming drawn into a scam, look for the warning signs of investment fraud:

Guarantees: Be suspect of anyone who guarantees that an investment will perform a certain way. All investments carry some degree of risk.

Unregistered products: Many investment scams involve unlicensed individuals selling unregistered securities—ranging from stocks, bonds, notes, hedge funds, oil or gas deals, or fictitious instruments, such as prime bank investments.

Overly consistent returns: Any investment that consistently goes up month after month—or that provides remarkably steady returns regardless of market conditions—should raise suspicions, especially during turbulent times. Even the most stable investments can experience hiccups once in a while.

Complex strategies: Avoid anyone who credits a highly complex investing technique for unusual success. It is critical that you fully understand any investment you're seriously considering—including what it is, what the risks are and how the investment makes money.

Missing documentation: If someone tries to sell you a security with no documentation—that is, no prospectus in the case of a stock or mutual fund, and no offering circular in the case of a bond—he or she may be selling unregistered securities. The same is true of stocks without stock symbols.

Account discrepancies: Unauthorized trades, missing funds or other problems with your account statements could be the result of a genuine error—or they could indicate churning or fraud.

A pushy salesperson: No reputable investment professional should push you to make an immediate decision about an investment. If someone pressures you to decide on a stock sale or purchase, steer clear.

Banking Scams

Banking scams involve attempts to access your bank account. The most common banking scams include:

Overpayment scams - Someone sends you a check, instructs you to deposit it in your bank account, and wire part of the money back to them. But the check was fake, so you'll have to pay your bank the amount of the check, plus you'll lose any money you sent him.

Unsolicited check fraud - A scammer sends you a check for no reason. If you cash it, you may be authorizing the purchase of items or signing up for a loan you didn't ask for.

Automatic withdrawals - A scam company sets up automatic withdrawals from your bank account to qualify for a free trial or to collect a prize.

Phishing - You receive an email message that asks you to verify your bank account or debit card number.

How to Protect Yourself

Do’s

Be suspicious if you are told to wire a portion of funds from a check you received back to a company.

Be wary of lotteries or free trials that ask for your bank account number.

Verify the authenticity of a cashier’s check with the bank that it is drawn on before depositing it.

When verifying a check or the issuer, use contact information on a bank’s website.

Don’ts

Don’t trust the appearance of checks or money orders. Scammers can make them look legitimate and official.

Don’t deposit checks or money orders from strangers or companies you don’t have a relationship with.

Don’t wire money to people or companies you don’t know.

Don’t give your bank account number to someone who calls you, even for verification purposes.

Don’t click on links in an email to verify your bank account.

Don’t accept a check that includes an overpayment.

Telephone Scams

Telephone scammers try to steal your money or personal information. Scams may come through phone calls from real people, robocalls, or text messages. Callers often make false promises, such as opportunities to buy products, invest your money, or receive free product trials. They may also offer you money through free grants and lotteries. Some scammers may call with threats of jail or lawsuits if you don’t pay them.

Protect Yourself From Telephone Scams

Remember these tips to avoid being a victim of a telephone scam:

Do’s:

Register your phone number with the Spam Registry offered by your service provider.

Be wary of callers claiming that you’ve won a prize or vacation package.

Hang up on suspicious phone calls.

Be cautious of caller ID. Scammers can change the phone number that shows up on your caller ID screen. This is called “spoofing.”

Don’ts:

Don’t give in to pressure to take immediate action.

Don’t say anything if a caller starts the call asking, “Can you hear me?” This is a common tactic for scammers to record you saying “yes.” Scammers record your “yes” response and use it as proof that you agreed to a purchase or credit card charge.

Don’t provide your credit card number, bank account information, or other personal information to a caller.

Don’t send money if a caller tells you to wire money or pay with a prepaid debit card.

Investment Scams

Investment scams promise high returns, without financial risk. Use this information to report and protect your investments.

How to Protect Yourself

Do's

Research investment opportunities and investment professionals. Check for registration with SEBI / RBI.

Learn where the investment and the investment professional have registered. It may be in your state or with other regulators.

Get all the details of an investment in writing, but still do your own research.

Ask questions about costs, timing, risks, and other issues.

Don'ts

Don't give in to pressure to invest immediately.

Don't be influenced by promises that seem too good to be true. These promises may include "guaranteed earnings" or "risk-free" investments.

Don't invest just because the investment professional seems nice, trustworthy, or has professional titles.

Don't invest based on claims that other people, have invested.

Don't feel obligated to invest, even if the professional gave you a gift, lunch, or reduced their fees.

Lottery and Sweepstakes Scams

Prize scammers try to get your money or personal information through fake lotteries, sweepstakes, or other contests. Many claim that you've won a prize but must pay a fee to collect it. Others require you to provide personal information to enter a "contest." These scams may reach you by postal mail, email, phone call, robocall, or text message.

Signs of a Prize Scam

Scammers still use the promise of a prize to get your money or personal information.

Three signs of a prize scam:

You have to pay to get your prize. So, if someone tells you to pay a fee for "taxes," "shipping and handling charges," or "processing fees" to get your prize, you're dealing with a scammer. And if they ask you to pay by sending cash, or paying with gift cards or cryptocurrency to get your prize, don't do it. Scammers use these payments because it's hard to track who the money went to. And it's almost impossible to get your money back.

They say paying increases your odds of winning. But real sweepstakes are free and winning is by chance. It's illegal for someone to ask you to pay to increase your odds of winning.

You have to give your financial information. There's absolutely no reason to ever give your bank account or credit card number to claim any prize or sweepstakes. If they ask for this information, don't give it. It's a scam.

Scammers Tricks

Scammers try to look official. They want you to think you've won a government-supervised lottery or sweepstakes. Scammers use names of organizations you might recognize. Scammers might pretend to be from well-known government sweepstakes.

Scammers send you a message (via text, email, or social media) to get your personal information. You might be told that you won a gift card or a discount code to a local store. Or the message may say you won something expensive, like an iPad or a new car from your local dealership. Scammers hope you'll respond with your personal information or click on links that can take your personal information or download malware onto your device. Don't respond.

Scammers make it seem like you're the only person who won a prize. But the same text, email, or letter went to lots of people. If your message came by mail, check the postmark on the envelope or postcard. If your "notice" was mailed by bulk rate, it means many other people got the same notice, too.

Scammers say you've won a foreign lottery, or that you can buy tickets for one. Messages about a foreign lottery are almost certainly from a scammer. First, it's illegal to play a foreign lottery, second, if you buy a foreign lottery ticket, expect many more offers for fake lotteries or scam investment "opportunities." Finally, there are no secret systems for winning foreign lotteries, so don't believe someone who tells you they can help you win.

Scammers pressure you to act now to get a prize. Scammers want you to hurry up and pay or give them information. They tell you it's a limited time offer or you have to "act now" to claim your prize. They don't want you to have time to evaluate what's really happening. Don't be rushed — especially if they want you to do something to get your prize.

Scammers send you a check and ask you to send some of the money back. This is a fake check scam. If you deposit the check, it can take the bank weeks to figure out that it's fake. In the meantime, the bank has to make the funds available, so it can look like the money is in your account. But once the bank finds out the check is fake, they'll want you to pay back the funds.

Protect Yourself From Lottery and Sweepstakes Scams

Do's

Ask yourself if you entered a particular contest. If you didn't enter it, the prize notice is likely a fake.

Some scammers use the names of organizations that run real sweepstakes. Research the company's contact information. Contact them to verify if the prize is legitimate.

Register your phone number with the Spam Registry offered by your service provider. Report spam text messages to your mobile carrier, then delete them.

Hang up on suspicious calls.

Don'ts

Don't pay a fee, taxes, or shipping charges to receive a prize.

Don't wire money to, or deposit a check from, any organization claiming to run a sweepstakes or lottery.

Don't provide your credit card number or bank account information to receive a prize.

Don't believe someone just because they say they're from the government or an official-sounding organization.

Don't reply to, or click on any links in, a spam text message.

Don't give in to pressure to take immediate action.

Don't believe anyone claiming to be from a foreign lottery or sweepstakes. It's illegal to enter foreign contests like these.

Charity Scams

Some scammers take advantage of the public's generosity. They especially take advantage of tragedies and disasters.

How to Protect Yourself from Charity Scams

Follow these tips to detect common charity scam tactics:

Do's

Check out the charity if it is registered with Income Tax Department.

Verify the name. Fake charities often choose names that are close to well established charities.

Don'ts

Don't give in to high pressure tactics such as urging you to donate immediately.

Don't send cash. Pay with a check or credit card. Pay to a bank account only if at all.

Don't pay online for charities.

Pyramid Schemes

Pyramid schemes are scams that need a constant flow of new participants to keep them going. They are marketed as multi-level marketing programs or other types of legitimate businesses. They use new recruits' "investments" to pay "profits" to those participating longer. Pyramid schemes collapse when they can't recruit enough new participants to pay earlier investors. These scams always fail—it's mathematically guaranteed.

Pyramid Schemes

In the classic "pyramid" scheme, participants attempt to make money solely by recruiting new participants, usually where:

The promoter promises a high return in a short period of time;

No genuine product or service is actually sold; and

The primary emphasis is on recruiting new participants.

All pyramid schemes eventually collapse, and most investors lose their money.

Fraudsters frequently promote pyramid schemes through social media, Internet advertising, company websites, group presentations, conference calls, YouTube videos, and other means. Pyramid scheme promoters may go to great lengths to make the program look like a business, such as a legitimate multi-level marketing (MLM) program. But the fraudsters use money paid by new recruits to pay off earlier stage investors (usually recruits as well). At some point, the schemes get too big, the promoter cannot raise enough money from new investors to pay earlier investors, and people lose their money.

Hallmarks of a pyramid scheme:

Emphasis on recruiting. If a program focuses solely on recruiting others to join the program for a fee, it is likely a pyramid scheme. Be sceptical if you will receive more compensation for recruiting others than for product sales.

No genuine product or service is sold. Exercise caution if what is being sold as part of the business is hard to value, like so-called "tech" services or products such as mass-licensed e-books or online advertising on little-used websites. Some fraudsters choose fancy-sounding "products" to make it harder to prove the company is a bogus pyramid scheme.

Promises of high returns in a short time period. Be sceptical of promises of fast cash – it could mean that commissions are being paid out of money from new recruits rather than revenue generated by product sales.

Easy money or passive income. There is no such thing as a free lunch. If you are offered compensation in exchange for doing little work such as making payments, recruiting others, or placing online advertisements on obscure websites, you may be part of an illegal pyramid scheme.

No demonstrated revenue from retail sales. Ask to see documents, such as financial statements audited by a certified public accountant (CPA), showing that the company generates revenue from selling its products or services to people outside the program. As a general rule, legitimate MLM companies derive revenue primarily from selling products, not from recruiting members.

Complex commission structure. Be concerned unless commissions are based on products or services that you or your recruits sell to people outside the program. If you do not understand how you will be compensated, be cautious.

All Pyramid Schemes Collapse

When fraudsters attempt to make money solely by recruiting new participants into a program, that is a pyramid scheme, and there is only one possible mathematical result – collapse. Imagine if one participant must find six other participants, who, in turn, must find six new recruits each. In only 11 layers of the "downline," you would need more participants than the entire population of the United States to maintain the scheme. This infographic shows how all pyramid schemes are destined to collapse.

Pyramid Schemes Posing as Multi-Level Marketing Programs

Advertisements or offers to make "easy money" or "online income" out of your own home are typical of MLM (Multi-level Marketing) programs that are promoted through Internet advertising, company websites, social media, presentations, group meetings, conference calls, and brochures. In an MLM program, you typically get paid for products or services that you and the distributors in your "downline" (i.e., participants you recruit and their recruits) sell to others. However, some MLM programs are actually pyramid schemes -- a type of fraud in which participants profit almost exclusively through recruiting other people to participate in the program.

Pyramid schemes masquerading as MLM programs often violate the laws prohibiting fraud and laws requiring the registration of securities offerings and broker-dealers. In a pyramid scheme, money from new participants is used to pay recruiting commissions (that may take any form, including the form of securities) to earlier participants just like how, in classic Ponzi schemes, money from new investors is used to pay fake "profits" to earlier investors. Recently, the SEC has sued the alleged operators of large-scale pyramid schemes for violating the federal securities laws through the guise of MLM programs.

Beware of these hallmarks of a pyramid scheme:

No genuine product or service. MLM programs involve selling a genuine product or service to people who are not in the program. Exercise caution if there is no underlying product or service being sold to others, or if what is being sold is speculative or appears inappropriately priced.

Promises of high returns in a short time period. Be leery of pitches for exponential returns and "get rich quick" claims. High returns and fast cash in an MLM program may suggest that commissions are being paid out of money from new recruits rather than revenue generated by product sales.

Easy money or passive income. Be wary if you are offered compensation in exchange for little work such as making payments, recruiting others, and placing advertisements.

No demonstrated revenue from retail sales. Ask to see documents, such as financial statements audited by a certified public accountant (CPA), showing that the MLM company generates revenue from selling its products or services to people outside the program.

Buy-in required. The goal of an MLM program is to sell products. Be careful if you are required to pay a buy-in to participate in the program, even if the buy-in is a nominal one-time or recurring fee (e.g., $10 or $10/month).

Complex commission structure. Be concerned unless commissions are based on products or services that you or your recruits sell to people outside the program. If you do not understand how you will be compensated, be cautious.

Emphasis on recruiting. If a program primarily focuses on recruiting others to join the program for a fee, it is likely a pyramid scheme. Be sceptical if you will receive more compensation for recruiting others than for product sales.

How to Protect Yourself

Do's

Be wary if you have to recruit more participants to increase your profit, or get your investment back.

Ask if the company sells non-tangible products and services rather than physical products.

Check out the business with the Better Business Bureau, your state attorney general, or state licensing agencies.

Ask to see financial statements audited by a certified accountant. Find out if the company earns income from selling its products or services to customers, not to its sales team.

Be sceptical of success stories and testimonials of fantastic earnings.

Don’ts

Don’t invest until you’ve verified that the business is legitimate.

Don’t get involved in businesses that make you recruit new participants.

Don’t buy into franchises that promise big or quick profits.

Don’t invest in any “opportunity” bearing warning signs of a pyramid scheme.

Ponzi Schemes

A Ponzi scheme is a type of investment fraud. Use this information to identify, report, and protect yourself against this type of scam.

How Ponzi Schemes Work

Ponzi schemes rely on money from new investors to pay “returns” to current investors. To keep the scheme going, the scammers must continually recruit new investors and discourage current investors from cashing out. Otherwise, they will not bring in enough cash to pay current investors, and the scheme will collapse.

Ponzi Scheme

A Ponzi scheme is an investment fraud that pays existing investors with funds collected from new investors. Ponzi scheme organizers often promise to invest your money and generate high returns with little or no risk. But in many Ponzi schemes, the fraudsters do not invest the money. Instead, they use it to pay those who invested earlier and may keep some for themselves.

With little or no legitimate earnings, Ponzi schemes require a constant flow of new money to survive. When it becomes hard to recruit new investors, or when large numbers of existing investors cash out, these schemes tend to collapse.

Ponzi schemes are named after Charles Ponzi, who duped investors in the 1920s with a postage stamp speculation scheme.

Ponzi scheme “red flags”

Many Ponzi schemes share common characteristics. Look for these warning signs:

High returns with little or no risk. Every investment carries some degree of risk, and investments yielding higher returns typically involve more risk. Be highly suspicious of any “guaranteed” investment opportunity.

Overly consistent returns. Investments tend to go up and down over time. Be sceptical about an investment that regularly generates positive returns regardless of overall market conditions.

Unregistered investments. Ponzi schemes typically involve investments that are not registered with the SEC or with state regulators. Registration is important because it provides investors with access to information about the company’s management, products, services, and finances.

Unlicensed sellers. Federal and state securities laws require investment professionals and firms to be licensed or registered. Most Ponzi schemes involve unlicensed individuals or unregistered firms.

Secretive, complex strategies. Avoid investments if you don't understand them or can't get complete information about them.

Issues with paperwork. Account statement errors may be a sign that funds are not being invested as promised.

Difficulty receiving payments. Be suspicious if you don't receive a payment or have difficulty cashing out. Ponzi scheme promoters sometimes try to prevent participants from cashing out by offering even higher returns for staying put.

Tips to Help Avoid Investment Fraud Online

The key to avoiding investment scams on the Internet is to be an educated investor.

1. Look out for "Red Flags"

Wherever you come across a recommendation for an investment on the Internet, the following "red flags" should cause you to use caution in making an investment decision:

It sounds too good to be true. Any investment that sounds too good to be true probably is. Be extremely wary of claims on the Internet that an investment will make "INCREDIBLE GAINS" or is a "BREAKOUT STOCK PICK." Claims like these are hallmarks of extreme risk or outright fraud.

The promise of "guaranteed" returns with little or no risk. Every investment entails some level of risk, which is reflected in the rate of return you can expect to receive. Most fraudsters spend a lot of time trying to convince investors that extremely high returns are "guaranteed" or that the investment "can't miss." Don't believe it.

Offers to invest outside the United States. You should carefully examine any unsolicited offer to invest outside of the United States. Many fraudsters set up operations outside the United States to make it more difficult for regulators to stop their fraudulent activity and recover their victims' money.

Pressure to buy RIGHT NOW. Don't be pressured or rushed into buying an investment before you have a chance to think about – and investigate – the "opportunity." Be especially sceptical of investments that are pitched as "once-in-a-lifetime" opportunities.

2. Be Wary of Unsolicited Offers

Investment fraud criminals look for victims, including seniors, on the Internet. If you see a new post on your wall, a tweet mentioning you, a direct message, an e-mail, or any other unsolicited – meaning you didn't ask for it and don't know the sender – communication regarding a so-called investment opportunity, you should exercise extreme caution. An unsolicited sales pitch may be part of a fraudulent investment scheme

3. Look out for "Affinity Fraud"

An investment pitch made through an online group of which you are a member, or on a chat room or bulletin board catering to an interest you have, may be an affinity fraud. Affinity fraud refers to investment scams that prey upon members of identifiable groups, often seniors, religious or ethnic communities, professional groups, or combinations of those groups. Even if you know the person making the investment offer, be sure to check out everything – no matter how trustworthy the person seems who brings the investment to your attention. Remember, the person making you the offer may not know that the investment is a scam.

4. Be Thoughtful About Privacy and Security Settings

Seniors who use social media as a tool for investing should be mindful of the various features on these websites that can help protect privacy. Understand that unless you guard personal information, it may be available not only to your friends, but for anyone with access to the Internet – including fraudsters.

5. Ask Questions and Check Out the Answers

Be sceptical. Investigate the investment thoroughly and check the truth of every statement you are told about the investment.

Common Investment Scams Using Social Media and the Internet

While fraudsters are constantly changing the way they approach victims on the Internet, there are a number of common scams of which you should be aware:

“Pump-and-Dumps” and Market Manipulations

“Pump-and-dump” schemes involve the promoting of a company’s stock (typically small, so-called “microcap” companies) through false and misleading statements to the marketplace, in order to sell the cheaply purchased stock at a higher price. These false claims could be made on social media such as Facebook and Twitter, as well as on bulletin boards and chat rooms.

Fraud Using “Research Opinions,” Online Investment Newsletters, and Spam Blasts

While legitimate online newsletters may contain useful information about investing, others are merely tools for fraud. Some companies pay online newsletters to “tout” or recommend their stocks. Touting isn’t illegal as long as the newsletters disclose who paid them, how much they’re getting paid, and the form of the payment, usually cash or stock. But fraudsters often lie about the payments they receive and their track records in recommending stocks. To learn more, read our tips for checking out newsletters.

High Yield Investment Programs

The Internet is awash in so-called “high-yield investment programs” or “HYIPs.” These are unregistered investments typically run by unlicensed individuals – and they are often frauds. The hallmark of an HYIP scam is the promise of incredible returns (30 or 40 percent – or more) at little or no risk to the investor.

Internet-Based Offerings

Offering frauds come in many different forms. Generally speaking, an offering fraud involves a security of some sort that is offered to the public, where the terms of the offer, such as the likelihood of a return, are materially misrepresented.

How to Protect Yourself From Ponzi Schemes

Do’s

Be wary of any investment that regularly pays positive returns regardless of what the overall market is doing.

Avoid investments if you do not understand them or cannot get complete information about them.

Be alert to account statement errors, which may be a sign of investment fraud.

Be suspicious if you do not receive a payment or have difficulty cashing out.

Do Not

Do not put your money in investments that promise big returns with little to no risk.

Do not contribute to any investment that is not registered with the SEBI or with state regulators.

Do not get financially involved with any unlicensed investment professional or unregistered firm.

MLM Schemes

MLM companies sell their products or services through person-to-person sales. That means you’re selling directly to other people, maybe from your home, a customer’s home, or online.

If you join an MLM program, the company may refer to you as an independent “distributor,” “participant,” or “contractor.” Most MLMs say you can make money two ways:

by selling the MLM’s products yourself to “retail” customers who are not involved in the MLM by recruiting new distributors and earning commissions based on what they buy and their sales to retail customers

Your recruits, the people they recruit, and so on, become your sales network, or "downline." If the MLM is not a pyramid scheme, it will pay you based on your sales to retail customers, without having to recruit new distributors.

Most people who join legitimate MLMs make little or no money. Some of them lose money. In some cases, people believe they've joined a legitimate MLM, but it turns out to be an illegal pyramid scheme that steals everything they invest and leaves them deeply in debt.

What's a Pyramid Scheme, and How Do You Spot One?

Pyramid schemes are scams. They can look remarkably like legitimate MLM business opportunities and often sell actual products, maybe even ones you've heard of. But if you become a distributor for a pyramid scheme, it can cost you and your recruits — often your family and friends — a lot of time and money that you won't get back.

The promoters of a pyramid scheme may try to recruit you with pitches about what you'll earn. They may say you can change your life — quit your job and even get rich — by selling the company's products. That's a lie. Your income would be based mostly on how many people you recruit, not how much product you sell. Pyramid schemes are set up to encourage everyone to keep recruiting people to keep a constant stream of new distributors — and their money — flowing into the business.

Often in a pyramid scheme, you'll be encouraged or even required to buy a certain amount of product at regular intervals, even if you already have more inventory than you can use or sell.

You may even have to buy products before you're eligible to be paid or get certain bonuses. You also may have to pay repeated fees for other items, like training sessions or expensive marketing materials. In addition, the company may say you can earn lavish rewards, like prizes, bonuses, exotic vacations, and luxury cars. However, it often turns out that you have to meet certain product purchase, recruitment, training, or other goals to qualify for the rewards, and only a handful of distributors ever qualify.

Eventually, most distributors find that no matter how hard they work, they can't sell enough inventory or recruit enough people to make money. They also can't keep up with required fees or the inventory purchases they need to make to qualify for rewards, and they can't earn enough money to cover their expenses. In the end, most people run out of money, have to quit, and lose everything they invested.

Warning signs of a pyramid scheme:

Promoters make extravagant promises about your earning potential. Stop. These promises are false.

Promoters emphasize recruiting new distributors for your sales network as the real way to make money. Walk away. In a legitimate MLM program, you should be able to make money just by selling the product.

Promoters play on your emotions or use high-pressure sales tactics, maybe saying you'll lose the opportunity if you don't act now and discouraging you from taking time to study the company. Leave by the nearest exit. Any company that tries to pressure you to join is one to avoid.

Distributors buy more products than they want to use or can resell, just to stay active in the company or to qualify for bonuses or other rewards. If you see this happening, keep your money.

Ticket Scams

Ticket selling scams happen when a scammer uses tickets as bait to steal your money. The scammer usually sells fake tickets, or you pay for a ticket, but never receive it. They are common when tickets for popular concerts, plays, and sporting events sell out.

Ways That Ticket Scammers Go After Your Money

Scammers, including individuals and fake resale companies, take advantage of ticket shortages by:

Charging prices much higher than the face value of a ticket

Creating counterfeit tickets with forged barcodes and logos of real ticket companies

Selling duplicates of a legitimate ticket and emailing it to several buyers

Pretending to sell tickets online to steal your credit card information

How to Protect Yourself

Do’s

Buy tickets at the venue box office.

Buy tickets from authorized brokers and third party sellers, with verified contact information.

Look for red flags in the ticket offer. If the offer has imperfect English or unusual phrases, the offer could be a scam.

Verify that the seller has a real physical addresses and phone numbers. Scammers often post fake addresses, PO Box, or no address on their websites.

Check the actual web address of the resale ticket seller. Some scammers create phony websites that look like real ticket sellers' websites.

Search online for negative reviews about the seller. Use the seller’s name, email address, and phone number, along with the words “fraud,” “scams,” and “fake tickets”.

Verify the details on the ticket. Check the date and the time printed on the tickets. Make sure the section and seat numbers actually exist at the venue.

Have the seller meet you in person in a public place for the ticket exchange.

Ask the seller for proof that they bought the tickets, if you are buying from an individual.

Use a credit card to pay third party sellers. Your credit card offers protections, if you need to dispute a charge.

Check for complaints against a ticket seller with your state’s consumer protection agency.

Don’ts

Don’t transfer money to pay for tickets.

Don’t trust sellers who want you to pay with a prepaid money card.

Don’t meet an individual ticket seller alone or in a low-traffic area.

Don’t automatically trust online search results for ticket sellers. Search results can include paid ads, sellers that charge high fees, and scams.

Internet and Social Media Fraud

Many investors use the Internet and social media to help them with investment decisions. While these online tools can provide many benefits for investors, these same tools can make attractive targets for criminals. Criminals are quick to adapt to new technologies – and the Internet is no exception.

The Internet is a useful way to reach a mass audience without spending a lot of time or money. A website, online message, or social media site can reach large numbers with minimum effort. It's easy for fraudsters to make their messages look real and credible and sometimes hard for investors to tell the difference between fact and fiction. If an investment promotion grabs your interest, research the “opportunity” even before providing your phone number and email address. Otherwise, you may be setting yourself up to be targeted for investment fraud.

The key to avoiding investment fraud on social media sites or elsewhere on the Internet is to be an educated investor. To learn specific steps you can take, see What You Can Do to Avoid Investment Fraud. Below, we tell you where various types of fraud may show up online such as Social media, Online investment newsletters, Online bulletin boards and chat rooms and Spam.

Social media

Social media, such as Facebook, YouTube, Twitter, and LinkedIn, have become key tools for investors. Whether they are seeking research on particular stocks, background information on a broker-dealer or investment adviser, guidance on an overall investment strategy, up to date news or to simply want to discuss the markets with others, investors turn to social media. Social media also offers a number of features that criminals may find attractive. Fraudsters can use social media in their efforts to appear legitimate, to hide behind anonymity, and to reach many people at low cost. For additional information, see these Investor Alerts and Bulletins:

Always be wary of unsolicited offers to invest. Unsolicited sales pitches may be part of a fraudulent investment scheme. If you receive an unsolicited message from someone you don't know containing a "can't miss" investment, your best move maybe to pass up the "opportunity" and report it to the SEC Complaint Centre.

Online investment newsletters

While legitimate online newsletters contain valuable information, others are tools for fraud. Some companies pay online newsletters to "tout" or recommend their stocks. Touting isn't illegal as long as the newsletters disclose who paid them, how much they're getting paid, and the form of the payment, usually cash or stock. But fraudsters often lie about the payments they receive and their track records.

Fraudulent promoters may claim to offer independent, unbiased recommendations in newsletters when they stand to profit from convincing others to buy or sell certain stocks. They may spread false information to promote worthless stocks.

The fact that these so-called "newsletters" may be advertised on legitimate websites, including on the online financial pages of news organizations, does not mean that they are not fraudulent. To learn more, read our tips for checking out newsletters.

Online bulletin boards and chat rooms

Online bulletin boards, chat rooms and social media sites are a way for investors to share information. While some messages may be true, many turn out to be bogus – or even scams. Fraudsters may use online discussions to pump up a company or pretend to reveal "inside" information about upcoming announcements, new products, or lucrative contracts.

You never know for certain who you're dealing with, or whether they're credible, because many sites allow users to hide their identity behind multiple aliases. People claiming to be unbiased observers may actually be insiders, large shareholders, or paid promoters. One person can easily create the illusion of widespread interest in a small, thinly traded stock by posting numerous messages under various aliases.

Other online offerings may not be fraudulent per se, but may nonetheless fail to comply with the applicable registration provisions of the federal securities laws. While the federal securities laws require the registration of solicitations or "offerings," some offerings are exempt. Always determine if a securities offering is registered with the SEC or a state, or is otherwise exempt from registration, before investing.

Spam

"Spam" – junk e-mail – often is used to promote bogus investment schemes or to spread false information about a company. With a bulk e-mail program, spammers can send personalized messages to millions of people at once for much less than the cost of cold calling or traditional mail. Many scams, including advance fee frauds, use spam to reach potential victims.

B. UK

Spot the warning signs

If you've been contacted unexpectedly, or are suspicious about a call or text message, make sure you stop and check the warnings signs.

Is it unexpected? Scammers often call out of the blue. They may also try and contact you via email, text, post, social media, or even in person.

Do you feel pressured to act quickly? Scammers might offer you a bonus or discount if you invest quickly, or they may say the opportunity is only available for a short time.

Does the offer sound too good to be true? Fraudsters often promise tempting rewards, such as high returns on an investment.

Is the offer exclusively for you? Scammers might claim that you've been specially chosen for an investment opportunity, and it should be kept a secret.

Are they trying to flatter you? Scammers often try to build a friendship with you to put you at ease.

Are you feeling worried or excited? Fraudsters may try to influence your emotions to get you to act.

Are they speaking with authority? Scammers might claim that they're authorised and often appear knowledgeable about financial products.

If you answered 'yes' to any of these questions, or you're unsure if a contact is genuine, follow the steps below to protect yourself.

1. Check the firm or individual
2. Check if the firm or individual is authorised by a Government Regulatory Authority
3. Never click on links in emails or on company websites. It could be part of the scam.
4. Check that the Company / firm Registration number is genuine (you may check on RoC website if it is a company) and contact details you've been given match the details on the website. Merely checking the website of the company is not helpful.

Do's:

Treat all unexpected calls, emails and text messages with caution. Don't assume they're genuine, even if the person knows some basic information about you

Hang up on calls and ignore messages if you feel pressured to act quickly. A genuine bank or business won't mind waiting if you want time to think

Check your bank account and credit card statements regularly

Consider getting independent financial advice or guidance before a big financial decision

Check overseas regulators if you're dealing with an overseas firm (you should also check the list of scam warnings from overseas regulators)

Don't:

Give out your bank account or credit card details unless you're certain who you're dealing with

Share your passwords with anyone (including your social media passwords)

Give access to your device by downloading software or an app from a source you don't trust. Scammers may be able to take control of your device and access your bank account

What to do if you've been scammed

Report it

If you're worried about a potential scam or you think you may have been contacted by a fraudster, report it to us. This could help prevent others falling victim to the same criminal.

Call us on 0800 111 6768 or use our contact form to get in touch.

For anything we don't regulate, or if you've lost money to a scam, contact Action Fraud on 0300 123 2040 or via their website.

Be wary of future scams

It's important to be extra careful if you've already been scammed. Fraudsters could try and target you again, or they may sell your details to other criminals.

The new scam might be completely different, or it could be related to the previous scam. For example, you could be contacted with an offer to get your money back or to buy back an investment after you pay a fee. These are known as recovery room scams.

If you have any concerns at all about a potential financial scam, contact us immediately.

List of Acronyms and Website Resources for Anti-fraud Messaging

Acronym	C8Member	Website Resource
Australia ASIC	Australian Securities and Investments Commission	https://www.moneysmart.gov.au/scams
Belgium FSMA	Financial Services and Markets Authority	http://www.fsma.be/en/Consumers.aspx
Germany BaFin	Bundesanstalt fürFinanzdienstleistungsaufsicht	http://www.bafin.de/DE/Verbraucher/Verbraucherthemen/Marktmanipulation/marktmanipulation_node.html
Hong Kong SFC	Securities and Futures Commission	http://www.sfc.hk/web/EN/investor-corner.htmlhttp://www.sfc.hk/web/EN/alert-list/
Hong Kong IEC	Investor Education Centre	http://www.hkiec.hk/web/en/investment/misconduct-and-scams/index.htmlhttp://www.hkiec.hk/web/en/investment/stock-trading/choosing-broker/finding-a-broker.html
Japan FSA	Financial Services Agency	http://www.fsa.go.jp/en/http://www.fsa.go.jp/en/refer/cold/index.html
Japan JSDA	Japan Securities Dealers Association	http://www.jsda.or.jp/sonaeru/inv_alerts/index.htmlhttp://www.jsda.or.jp/en/newsroom/investor-alerts/index.html
Malaysia SC	Securities Commission	http://www.sc.com.my/enforcement/investor-alerts/sc-investor-alerts/ http://www.investsmartsc.my
Nigeria SEC	Securities and Exchange Commission	http://www.sec.gov.ng
Portugal CMVM	Comissão do Mercado de Valores Mobiliários	http://www.cmvm.pt/EN/Apoio%20Ao%20Investidor/Warning%20Notices/Pages/ifs_alerta.aspx?nrmode=unpublished
Singapore MAS	Monetary Authority of Singapore	http://www.moneysense.gov.sg/Understanding-Financial-Products/Investments/Consumer-Alerts.aspx
South Africa FSB	Financial Services Board	www.mylifemymoney.co.za
UK FCA	Financial Conduct Authority	http://www.fca.org.uk/consumers/scams

US CFTC	Commodity Futures and Trading Commission	http://www.smartcheck.gov http://www.cftc.gov/consumerprotection
US FINRA	Financial Industry Regulatory Authority	http://www.SaveAndInvest.org/FraudCenter/ http://www.ConEmIfYouCan.org
US SEC	Securities and Exchange Commission	http://www.investor.gov http://www.sec.gov/investor

C. FREQUENTLY ASKED QUESTIONS

i. I have been offered a loan from an organisation at very low interest rates but I have to first deposit some money in bank account of that organization. Do I need to suspect?

Always check details of the organization offering loans first and never transfer anything or give out your bank account details to any stranger.

ii. I have been offered to work from home and earn after I pay an advance fee for training. Should I Go ahead?

You should always be sure regarding the credibility about the company offering such jobs. Many of the work from home schemes turn out to be 'Get rich quick scams' and are only means of luring people for getting high amount of money by doing simple tasks sitting at home. No money can be earned without hard work and never fall prey to such temptations.

iii. Recently I received an email informing me that I have won a lottery and to claim the award I have to transfer some money first. Should I accept the offer?

The temptation to win a 'jackpot' is always high but a lot of it can be fraudulent. Here, you may get a notice or receive information that you've won something but need to send funds to pay for charges or other fees to release goods or enable the huge prize money to be transferred to your account. Do not fall prey to such offers as they are not genuine. You will only end up losing your funds.

iv. There is wonderful Investment opportunity assuring guaranteed profits with free holiday package. I just have to invest some money and convince my friends also to invest and join. I will get high commission also. What should I do? Is it a genuine offer?

Guaranteed profits can generally be myths and are frequently used as tactics to trap gullible investors to invest in an exciting products or scheme that sounds highly attractive. These can be bogus schemes, generally known as Ponzi/Pyramid schemes. The offers like free holidays, travel etc. are only means to attract innocent investors.

v. I want to report a fraud. What should I do?

You can report the details under "Report a suspicious scheme" screen of this portal. Alternately, you can file a complaint with the local police office/Economic Offence Wing Office.

vi. What are phishing scams? How can I keep my hard-earned money safe in Net banking/Mobile banking methods?

If you're an Internet user, please be aware of phishing scams that arrive in your inbox requesting money to be transferred. These scams are often under the disguise of 'Help' from someone you may know, a lottery 'win' that needs your bank details or even ideas to 'double or triple your money in months.'

Scammers often use several clever tactics to send convincing and well-disguised emails to convince receivers to send money by threats or even invoking sympathy for a charitable cause. Some of the most common phishing methods include the following:

Using fake URLS that look accurate – pay attention to spelling errors

Emails that are fear-based or 'urgent'

Using names of real companies and copying their logo and signature

Using names of friends and colleagues in help-related emails for charitable causes or to get them out of tricky situations.

If the email is personal in nature and is from someone you know, always confirm with the person first before taking any further action. If the email seems to be from your bank or any financial institution you deal with, call them to validate it before sending anything. Often scammers mimic or disguise the email id so it seems like it is from the bank so it's best to be safe and pay attention.

vii. Signs of Elder Investment Fraud

Many investment professionals choose to prey on elderly victims because, especially in a poor economy. That's where the money is: in retirement accounts and life-long savings. Due to deteriorating health, cognitive impairment, isolation and other challenges of aging, elderly investors are often vulnerable to elder abuse, even from financial advisors they have relationships with.

Parents often find it taboo to discuss financial issues, so take the initiative to speak to your parents about their finances and investments and share your concerns about the potential for misconduct. Ask questions about how and where they are investing their money.

Additionally, be on the lookout for these signs that elder financial fraud is occurring:

Your parents talk about a new financial advisor or broker who "guarantees" high returns fast.

Your parents have given control of or access to their financial accounts to another person.

Your parents have recently changed their Power of Attorney or Beneficiary.

Your parents put their money in a new investment opportunity, but they have not received statements or documentation about the investment in writing.

Your parents make their checks out directly to an investment adviser.

Your parents have been instructed by someone not to discuss their investment.

Your parents don't review their statements or don't ask questions about suspicious transactions.

Your parents have trouble contacting their advisor or the advisor fails to return their calls.

viii. Fraudsters Target the Aged

Investment scams target your parents because that's where the money is—and because fraudsters see seniors as an easy sell. Additionally, senior investors are vulnerable because of:

Cognitive impairments. Not only do elderly investors make their own financial mistakes as cognitive ability declines, but others are more than happy to take advantage of those who seem confused and have memory trouble.

Loss of a spouse. If your Dad has always handled the budget and has passed away or become very ill, Mom may suddenly be in charge of the finances. This can be very intimidating, especially if there are additional cognitive impairments.

Isolation. Without regular interactions, it is easy to fall prey to investment schemes and even harder for others to uncover misconduct.

Financial Taboos. Seniors are often hesitant to discuss their finances with friends and family and often internalize investment losses.

More time. Your parents may have more time to take calls or attend "free lunch" investment seminars, giving fraudsters a much better chance to charm your parents into their scams.

Tips to Help Seniors Avoid Investment Fraud

Here are tips for protecting yourself or your elderly parents from senior investment fraud:

Carefully examine all of your statements and documents, checking for large losses in value, changes in asset allocation and unrecognized withdrawals.

Do your research. Make sure you understand how the investment works.

Ask a lot of questions. And, be concerned if the salesperson avoids answering them.

Verify the information. After you ask your questions, confirm what you were told. Don't simply rely on the salesperson's answers.

Ignore unsolicited calls and emails.

Don't be pressured to "act now." High pressure sales tactics are used by scammers. It is very rare for any legitimate investment to require you to act right away. Always take time to research and consider a potential investment.

Keep control of your cash. No matter how well you know your advisor, make sure you maintain control over your assets and know what's happening with your portfolio.

Don't get fooled twice. If you have already been the victim of misconduct, and now you're getting offers to help you recover your cash or invest in something that's twice as good as the last thing, be suspicious. Fraudsters are increasingly using this tactic to hit victims of investment fraud.

ix. Earliest Signs of Investment Fraud

The promoter is very aggressive or harassing

You are asked to pay in cash

The investment is only available in a very limited time window

The promoter "guarantees" very high returns on the investment

The promoter reaches you through unsolicited email, phone calls, or mail

5. Steps to Take after Discovering Fraud

If you realized you were scammed or the deposit you made was a fraud, the sooner you take action, the better you can protect yourself and help others. Getting all of your stolen money back may prove difficult, but the more you delay, the dimmer the chances. Most people waste valuable time trying to contact others, the scam company or to form associations. Others often believe the scam company agents and allow more time to recover. These are standard "recovery room" techniques all scammers use which operate on your helplessness, emotions and hope. Hence, ACT IMMEDIATELY.

The Revenue Department, Government of Karnataka, under the directions of the Honourable CM Shri Siddaramaiah and Revenue Minister Shri Krishna Byre Gowda, have set up an elaborate mechanism to assist you in recovering and compensating the maximum amount you have deposited, legally possible. This system is designed to assist every individual, provided you are willing to be transparent and quick in sharing information or filing a complaint. Please contact the Economic Offences Cell of your jurisdictional Deputy Commissioner Office (A list of such offices and contact numbers are attached) and report the matter in due detail with document copies. (See Annexure for a list of such offices and contact numbers and the procedure). You may also file a complaint directly with your police station.

Your first steps should focus on stopping further losses and gathering the information you have about the scheme and the perpetrators while it is still fresh. Then, report the crime as soon as possible. Next, look into how you can repair the damage and avoid fraud in the future.

1. Don’t pay any more money

This may sound obvious, but some schemes use the promise of large returns to persuade victims to send one fee after another, even when the victims suspect something is wrong.

Also, be on the lookout for recovery frauds and middle-men operating these. These frauds target recent victims and claim to be able to get the stolen money back if the victims first pay an upfront fee, “donation,” retainer, or back taxes. The perpetrators of these advance-fee frauds often pose as government officials, attorneys, or recovery companies. Often they are “sleeping agents” of the main scam company who use associations or groups of scam victims to engineer a recovery scam.

2. Collect all the pertinent information and documents

While the events are still fresh in your memory, develop a timeline and collect documents and information that could help when it comes time to report or investigate the fraud. Write down conversations you had with the fraudsters or their agents with the approximate dates and times they took place. Documents and information to collect and keep include:

i. Investment Certificate and Payment Receipts (if any)
ii. Names, titles, or positions used by the fraudsters.
iii. Social media profiles, group posts, chats, or other online interactions.
iv. Website addresses and screen shots.
v. Emails and email addresses. Save these electronically, or print them out with the full header information. (Your email provider or a web search can describe how to capture header information.)
vi. Phone numbers you used to contact them.
vii. Account information, statements, trade confirmations, disclosures, and sales materials.
viii. If credit cards were used, include the receipts or statements.
ix. Exchanges of digital currencies, such as bitcoin.
x. Records of other forms of payment including cancelled checks or receipts for transfers, money orders, or prepaid cards.
xi. Any correspondence received, including envelopes.
xii. Offices, godowns, properties etc of the scam company you know of or visited including addresses
xiii. Employees / Agents / Staff of the scam company that you interacted with or know
xiv. Any promoters / key personalities who encouraged you directly or through media to invest
xv. If you have paid or received amounts in cash, you need to ensure you have proof of crediting / debiting the exact amount to your account and proof of having reported the transaction in your IT Return for that fiscal year.

3. File a complaint with jurisdictional police station or Economic Offences Cell of your jurisdictional Deputy Commissioner Office with as much of the above information as you have and necessary identity documents (See Annexure). You will be provided with a unique Complaint Number which you should use to update yourself about the progress of the enquiry. DO NOT SHARE YOUR DOCUMENTS / COMPLAINT NUMBER WITH ANY RECOVERY AGENT OR THE FRAUD COMPANY.

4. You may agree to participate in a survey (through a structured questionnaire) conducted by the Special Officer & Competent Authority, IMA & Other Financial Frauds, Revenue Department, Government of Karnataka. This will assist us to better regulate and eliminate scams while your data and identity will be kept confidential.

5. For additional information, you may visit us at: https://sploca.karnataka.gov.in/MIS/public/login

ANNEXURE

Economic Offences Cell, Deputy Commissioner Office

A. Complaint Monitoring

i. Admit preliminary complaints regarding deposit frauds involving KPIDFE / BUDS

   a. Reduce oral complaints to writing after confirming identity of complainant by Adhaar / EPIC / Passport / PAN and after ensuring complainant is affected party and not an interlocutor (Note: An Advocate duly appointed or a PoA holder shall be treated on par as an affected party)

   b. Email complaints may also be taken and an official Email ID may be given wide publicity for this purpose

   c. Guidelines regarding complaint submission may be published on the official website

   d. The complaint should provide the name, address, and agent names & contacts of the Financial Establishment, its Schemes, any promotional material (in soft or hard copy) or communication channels used by the FE, details of deposit made and returns received (with specific dates), exact nature of the fraud.

   e. A socio-economic profile of the complainant may be prepared based on the questionnaire given to ascertain the profile of investors in the fraud complained against. A list of de-frauded persons known to the complainant may also be compiled to arrive at the extent and incidence of the scam

ii. Carry out preliminary enquiries and gather “market intelligence” and submit to DC for reporting to Government

iii. Formal assistance of other investigative and regulatory authorities may be taken like – Police, Income Tax, District Registrar, Registrar of Companies, Lead Bank Officer etc.

B. Grievance Redressal & Guidance for Fraud Investigations & Claims

i. Grievances and / or queries regarding the following may be admitted and answered after confirmation that the information is sought by an affected depositor or complainant:

a. Stage of investigation by police: If by local police, the details shall be updated every month in a format and updated on the website of DC. If by CID / Central Agencies, quarterly updation may be sought from SPLOCA

b. Status of Claim: The various statutory stages of claim application and validation are provided in this SOP. If Competent Authority is a local officer, (eg. Assistant Commissioner) the details should be updated in a format attached and uploaded on website.

c. Guidance on Claim Application: May be provided based on the procedures and draft Claim Application Form attached herewith.

d. Specific or complex queries: Clarification may be sought from SPLOCA through DC

C. List of DC Offices, Economic Offence Cells & Contact Information