

## SAFEGUARDING Your Money



### From The Editor's Desk

India is fast moving towards a cashless economy and hence the digital footprint is ever increasing. In this lightning-quick environment of transactions, it is extremely important to become financially adept. This edition of our newsletter will help you to take measures to safeguard your hard earned money.

There is no doubt that the Indian banking and investment ecosystem have evolved to a great extent in the last couple of decades, particularly for small and retail consumers. The advent of technology in the sector has enabled traditional services to be digitized, giving rise to a new generation of internet-based banking solutions. Additionally, it has also seen the emergence of FinTech companies that offer mobile and app-based banking, investment and e-wallet services that did not exist earlier.

While this has made financial services more accessible, it has also enabled fraudsters to use the same technology to defraud unsuspecting users. Low awareness among customers and sometimes loopholes in the system have resulted in an increase in financial crimes. Today, most of us know someone among our

friends or families who has been a victim of a financial scam of some kind.

Financial fraud is a fairly broad area. For the ease of understanding, we have penned down the sources and mediums used for few such frauds. We have also covered ways to keep your hard-earned money safe from traditional and new age frauds, as well as shared some real-life examples that explain how such scams are perpetrated. As the famous quote says 'Prevention is better than cure', we hope you find this issue of newsletter useful.

We are happy to mention that from this issue, your favorite newsletter is available in Hindi. The Hindi version can be accessed at <https://nsdl.co.in/publications/nest.php>.

As always, if you have any comments or feedback about this newsletter, please write to us at [info@nsdl.co.in](mailto:info@nsdl.co.in).

Regards,

Team NSDL

## Risks related to banking system

For most investors, bank deposit is one of the most common ways to park their savings. The convenience and perceived safety are what makes various instruments such as Fixed Deposits, Recurring Deposits etc. a go-to financial instrument. However, like all other investment avenues banking system too involves some risks.

Bank failures happen when it is unable to meet to its payment obligations, or is forced to close by RBI. If the bank fails, people lose their savings/deposits kept with the bank. They may get amount upto ₹ 1 lakh only which is covered by deposit insurance taken by banks from Deposit Insurance and Credit Guarantee Corporation. (This limit is going to be increased to ₹ 5 lakh in near future). In India, although no scheduled commercial bank has been allowed to go under since liberalization, there have been such cases among co-operative banks.

Just a few months back, many customers of a co-op bank faced problem in getting their deposits back due to restrictions imposed by RBI on the amount that can be withdrawn. Unfortunately, such kinds of instances are not unheard of, and therefore depositors need to be vigilant about the possible risks.

## WHAT YOU SHOULD REMEMBER

- To minimize your risk in case of crisis with one bank, spread your savings and deposits across multiple banks.
- While choosing a bank to open a new account, check the financial health of the institution. Do not fall for just better interest rate.
- During crisis, look out for RBI's directives including those for cash withdrawal limits as well as hardship circulars<sup>#</sup>, if you need to withdraw additional funds in case of an emergency. You can visit <https://www.rbi.org.in> in such instances.

<sup>#</sup>RBI has a special provision that allows withdrawals in excess of the limit for depositors facing hardships. Account-holders can use this provision for medical expenses or expenses related to marriage or payment of school fees. These provisions are also applicable to senior citizens, widows and people with disabilities. The additional withdrawal varies among the different groups and could change over time. In all such situations, the details, conditions and updates, if any, are published by RBI as a circular.

## Illegal schemes

### Ponzi schemes

A Ponzi scheme is a scam that lures investors by promising exceptionally high returns. A ploy that scamsters deploy is to make huge payouts upfront against a small investment. A Ponzi scheme is a fraud that pays existing investors with funds collected from new investors pocketing a big chunk out of it. At some point, the returns become notional before the scheme collapses eventually, wiping out all the wealth of investors. Ponzi scheme is named after Charles Ponzi, who duped investors in the 1920s in the United States of America with a postage stamp speculation scheme.

### Unregistered Collective Investment Schemes (CIS)

Many would have come across shady investment schemes that allow you to invest in a property or a land for which you need to pay a relatively small amount as installment every month. Some of these schemes also allow you to co-own an orchard or a holiday home at some exotic location by investing a small monthly sum. While they sound lucrative, these are all unregistered CIS which have been outlawed by SEBI. Before deciding on investing in any such scheme just check whether the scheme is registered with SEBI or not. List of SEBI registered Collective Investment Management Companies is available at

<https://www.sebi.gov.in/sebiweb/other/OtherActiondo?doRecognised=yes>



## WHAT YOU SHOULD REMEMBER

- Before investing, thoroughly understand the proposition including entry and exit rules, charges, timelines and the points in the fine print.
- Never make investments based on tips, rumours, hearsay or word-of-mouth.
- Always conduct your own research and verify the details of the party you are dealing with before investing your hard earned money with them.
- If you are new to investing or unsure about where or how to invest, consult a registered investment advisor / expert.

It is better to pay a consulting fee as against losing all your money in bad investments.

- Always deal with registered entities.
- While dealing with brokers or other intermediaries, maintain a written record (email or messages) of all instructions / orders placed.
- Always look out for information from authentic sources before making any investments.

## Understanding various frauds

It is important to know and understand various kinds of frauds or tricks usually employed by fraudsters to dupe the victims. If we know their modus operandi, there are better chances to safeguard ourselves.

### Identity theft

Identity theft is when someone obtains and uses your personal information for fraudulent purposes. Personal details such as date of birth, PAN, bank account number, credit/ debit card number can be misused in a number of ways. From issuing credit cards and diverting funds to themselves, opening accounts in your name to commit serious crimes etc. identity theft can cost you dearly.

### Phishing or Tele calling Scams

This is a very common kind of fraud that involves cybercriminals sending emails or calling on behalf of seemingly legitimate sources (regulators, banks, insurance companies, financial institutions, lawyers etc.) or even your acquaintances. The objective of these criminals is to bait unsuspecting users into sharing their personal information under false pretenses. The emails or calls are made to seem like a routine procedure or a lucrative sounding offer or in some cases a plea for help.

In one of the widely reported case involving a senior Judge, the honorable Judge received an email purportedly from one of his good friend seeking money for a medical emergency. He was given details of a bank account in which his friend wanted the money to be transferred urgently. Since the two were well acquainted, Judge transferred the amount. The matter came to surface after Judge received another email, this time actually from his friend stating that his email account had been hacked.



## WHAT YOU SHOULD REMEMBER

- If an email or a message looks suspicious, verify the source before acting on it. Sometimes, it may be better to call up the sender and check the message.
- Do not use obvious or known elements like date of birth, mobile number, house number or pet's names as your password or PIN.
- Change your password and PIN regularly, say once in a month.
- Always check all your statements such as those for your bank accounts, demat accounts, e-Wallets, credit and debit cards etc. without fail.
- In case of any discrepancy or unknown/unauthorized transaction, notify your bank or card issuer immediately.
- Subscribe to mobile SMS alerts for all major transactions.
- Check for URLs that may seem legitimate but are spelt differently or with additional characters or words - for example [iciicibank.com](http://iciicibank.com) or [statesbankofindia-online.net.in](http://statesbankofindia-online.net.in)
- Do not download any attachments or install apps from unknown sources.
- Register your mobile number for Do Not Disturb (DND) service to avoid getting spam calls.

## Fake payment links and QR codes

E-wallets like Paytm, PhonePe and digital payment options like UPI and Google Pay have become fairly common platforms for individuals to make and receive payments for online transactions. Sometimes, criminals pretend to be potential buyers and under the pretext of transferring the money using an e-wallet or UPI, send the seller a 'pay request' link or a fake QR code disguised as a receipt or confirmation message. Sellers often look at the "payer's" name and authorize the transaction only to realize later that the money was debited from instead of being credited to their account.

## KYC fraud

In order to crack down on financial frauds, regulators like RBI and SEBI have made Know Your Customer (KYC) procedure mandatory. It involves sharing a number of personal and financial details with the bank or financial institution. However, fraudsters pretending to be employees seek the customers' details either over a call or by sending a fake link. These details are then used to transfer funds to their own accounts or conduct online transactions paid for by the user. In one such case, a senior government officer was defrauded of ₹ 6 lakh after sharing account details and OTP on a fraudulent link which was sent for updating KYC.

"According to an RBI report  
Indian banking system  
detected ₹ 71,500 crore  
worth of frauds in financial  
year 2018-19"

## WHAT YOU SHOULD REMEMBER

- Understand standard procedures before using new financial services or facilities. Take out some time to familiarize yourself with features offered.
- Always check the link or QR code shared by strangers before pressing the OK or Submit button on your computer or mobile.
- Conduct all transactions including KYC procedures either on the official website or the app or in-person through an authorized agent (after verifying its credentials).
- Report all suspicious activities to your e-Wallet or digital payment operator as soon as you realize it.
- Even if you have not lost money, report any doubtful communication to concerned authority. It helps them to prevent frauds and alert other users.
- Remember, no government department, regulator like SEBI or RBI, insurance company or bank or credit card issuer etc. will ever call you to ask your PAN or bank account number or things like that.

## Skimming or card cloning

This is a technique used by scamsters to obtain your card details to create a copy of the card with the intention of misusing it. One of the most common ways this is done is by attaching a small device to the card reader or by swiping the card through a pocket-sized device which reads the data off your card. This is common at crowded places like restaurants, bars and malls where criminals can disguise themselves as staff.

## Credit card transactions over phone

Many of us have become used to making a majority of our payments using a debit or a credit card. While it provides the convenience of not having to carry cash, using cards in an insecure manner also exposes you to financial fraud. A man in Mumbai was duped while ordering home delivery for wine from a local liquor shop. The person searched for local wine shop using internet and called on a number which he found online. The person who received the order convinced the victim to give his credit card details which were used to make three payments totaling up to ₹ 1.25 lakh.



## WHAT YOU SHOULD REMEMBER

- Never give your card number, CVV number or PIN to anyone.
- Never share card details over a phone call, SMS or email.
- If a wireless card machine is not available, make the payment yourself at the payment counter. Do not give the card and PIN to anyone. Idea is that your debit or credit card should never be out of your sight.
- If you use an old card, upgrade to a card with a smart chip that offers additional security to the data on your card.
- If you lose the card or notice unknown transactions, inform your bank and block the card immediately. To ensure this, always keep the hot line numbers of your bank / card issuer handy.
- Keep a tab of all card transactions (either through charge receipts or SMS alerts) and tally it every month with the transaction statement.
- Do not share your card number on telephone where others can hear.
- While at ATM, cover the keypad with your hand while entering the PIN. This would prevent someone recording the PIN using a hidden camera.
- It is always better to use those ATMs which are guarded or located close to a bank branch. There are lesser chances of someone manipulating the machine by inserting a secret card cloning device / hidden camera at such places.
- Set the amount limits for different types of spends on your credit card carefully as per your needs. This will prevent unwarranted transactions beyond a desired limit.
- If you do not need to travel out of country, it would be good to disable international transactions on your debit and credit cards.
- It is better to request your bank to issue a new debit or credit card, after you have used it while travelling to some high risk countries.

## Securing your computer and laptops

Security flaws or loopholes caused by outdated operating systems or old version of internet browser are often used by criminals to gain access into your desktop computers or laptops. Be aware of malware and tracking software that can leak or transmit sensitive information from your system. Such malicious softwares are usually disguised as attachments and in some cases are programmed to auto install if clicked or downloaded.

## Securing your mobile/tab device

In addition to problems similar to computers as outlined above, mobile devices present a peculiar and a much bigger challenge - privacy and access to personal data. Every time you install a new app, it requests for permission to access a variety of services and data on the phone. Depending on what permissions you give, the app could get access to all your data on the phone and in all accounts connected to your mobile.

## WHAT YOU CAN DO

- Install reliable anti-virus and anti-spyware on your devices (laptop, desktop and mobiles) to protect them from malware.
- Remember one time installation is not enough. Update these software regularly and apply security patches as soon as they are released.
- Be aware of app permissions you give consent to.
- While using a computer for a financial transaction, ensure that the website has data encryption. An encrypted website has https in its URL and a lock icon next to it.
- Before selling your computer or mobile device, erase all personal information from the device, and reset it to factory settings.
- Do not use public WiFi or any open networks for financial transactions.

Remember, financial frauds are possible in many ways. Fraudsters are always looking for newer ways to exploit the vulnerable. They keep on changing their ways and so it is important to keep ourselves updated and prepared. Ultimately, we need to be responsible for safeguarding our hard earned money.



### Training Programmes for Participants:

#### CPE Training Programme for Participants

NSDL, a NISM accredited Continuing Professional Education (CPE) Provider offers CPE training programmes in different modules for eligible associated persons. In January 2020, NSDL conducted five such training programmes at Ahmedabad, Mumbai and New Delhi.

#### Investor Education initiatives undertaken by NSDL

NSDL conducts Investor Awareness Programmes (IAPs) throughout the country to ensure investors are aware of different aspects of investing. Till date, NSDL has conducted over 3900 programmes which have been attended by more than 3.79 Lakh investors. Feedback received from investors during these IAPs is extremely encouraging. The schedule of these programs is published online at <https://nsdl.co.in/Investor-Awareness-Programmes.php>. We shall be happy to conduct IAPs for your organization / institute / society. Help us in driving the investor education initiative further by writing to us at [info@nsdl.co.in](mailto:info@nsdl.co.in) about such programmes to be conducted.

**More the education, more the prudence.**

#### Forthcoming Training Programmes for Participants on Continuing Professional Education (CPE) \*

Sr. No.	Date of Training	Location of Training	Type of Training Programme
1	March 20, 2020	Mumbai	Continuing Professional Education – Depository Operations Module
2	March 21, 2020	Kolkata	Continuing Professional Education – Depository Operations Module
3	March 28, 2020	New Delhi	Continuing Professional Education – Depository Operations Module

- Schedule is subject to change.

#### Forthcoming Investor Awareness Programmes

1	02-Mar-20	Hotel Lemon Tree, M.G.B., Shanti Kunj, Malviya Nagar, Alwar - 301001, Rajasthan	Alwar	Rajasthan	06.00 p.m. - 08.00 p.m.
2	02-Mar-20	Shri Venkateshwara University, Rajabpur, N.H.-24, Venkateshwara Nagar, Amroha, Amroha - 244236, Uttar Pradesh	Amroha	Uttar Pradesh	01.00 p.m. - 03.00 p.m.

3	03-Mar-20	Arya Mahila T.T. College, Rundhia Nagar, Bharatpur - 321001, Rajasthan	Bharatpur	Rajasthan	03.00 p.m. - 05.30 p.m.
4	04-Mar-20	The International Hotel, Veekshanam Road, Mahatma Gandhi Road, Opp. Chennai Silks, Kacheripady, Kochi - 682035, Kerala	Kochi	Kerala	05.00 p.m. - 07.00 p.m.
5	06-Mar-20	Hotel Mourya Inn, 4-356, Kurnool Road, Ongole - 523002, Andhra Pradesh	Ongole	Andhra Pradesh	05.00 p.m. - 08.00 p.m.
6	06-Mar-20	54-15, 18/4, Kdgo Colony, Road Number 1, Guru Nanak Colony, Vijayawada - 520008, Andhra Pradesh	Vijayawada	Andhra Pradesh	10.00 a.m. - 01.00 p.m.
7	08-Mar-20	Hotel K K Palace, Sagar Road, Near Bypass Road, Khurai - 470117, Madhya Pradesh	Khurai	Madhya Pradesh	11.00 a.m. - 02.30 p.m.
8	13-Mar-20	Maa Ambe Hotel, Near Ajanta Steel, Samastipur - 848101, Bihar	Samastipur	Bihar	12.00 p.m. - 03.00 p.m.
9	14-Mar-20	Clark Inn, P N M Mall, Patlipitra, Patna - 800013, Bihar	Patna	Bihar	12.00 p.m. - 03.00 p.m.
10	15-Mar-20	Park Hotel, Dumraon - Buxar, Near Railway Station, Dumraon - 802119, Bihar	Dumraon	Bihar	05.00 p.m. - 08.00 p.m.
11	15-Mar-20	Super 60 Classes, Kudra - Kaimur, Near Kudra Railway Station, Rohtas - 821101, Bihar	Rohtas	Bihar	10.00 a.m. - 01.00 p.m.
13	27-Mar-20	K.L.E. Lingaraj College Of Business Administration, College Road, Belagavi - 590001, Karnataka	Belagavi	Karnataka	10.00 a.m. - 03.00 p.m.
14	28-Mar-20	Hotel Sayaji, Near Bhimnath Bridge, Opp. Parsi Agyari, Sayajigunj, Vadodara - 390006, Gujarat	Vadodara	Gujarat	06.00 p.m. - 09.00 p.m.

- Schedule is subject to change. Please visit <https://nsdl.co.in/Investor-Awareness-Programmes.php> for updated schedule.

# Knowledge Wins Contest

## What is the Bank Deposit Amount Covered Under Insurance?

To send your replies: visit/click [www.nsdl.co.in/knowledge-win-contest.php](http://www.nsdl.co.in/knowledge-win-contest.php)  
or  
Scan this QR code



# 25 Lucky Winners

get  
FREE GIFTS



## Previous Month's Winners

A. Arjun – Bangalore  
Aakash Joshi – Bhavnagar  
Abhinaba Pal – Burdwan  
Abhishek K. Gairola – Dehradun  
Abhishek Saha – Kolkata  
Akhilesh Kumar – Bareilly  
Anand Dave – Bangalore  
Ashwani Goyal – Ambala  
Ch. Suryanarayana – Anantapur

Chandresh Jain – Mumbai  
Chetali Keni – Pune  
Dharmik Shah – Mumbai  
Dr. Moses Rajamani – Kancheepuram  
Gaurav Gupta – Patna  
Gururaj Rao – Mumbai  
Hardeep Saini – Chohal  
Hari Kumar B. – Bengaluru  
Jagadeesh Rayala – Bangalore

Jithin Ram A. S. – Palakkad  
Kamlesh Tarkhala – Porbandar  
M. S. Vaidyanathan – Chennai  
Manish Maru – Jamnagar  
Mir Arif – Anantnag  
Prasad S. Yelgodkar – Pune  
Purnima D. Nath – Bangalore

Winners will soon receive their gifts on the address they have provided

### Head Office

📍 **Mumbai** : 4<sup>th</sup> Floor, 'A' Wing, Trade World, Kamala Mills Compound, Senapati Bapat Marg, Lower Parel, Mumbai - 400013 Tel.: (022) 24994200

### Branch Offices

📍 **Ahmedabad** 📍 **Bengaluru** 📍 **Chennai** 📍 **Hyderabad** 📍 **Kochi** 📍 **Kolkata** 📍 **New Delhi**

For any grievance related to Demat account, you can email us at [relations@nsdl.co.in](mailto:relations@nsdl.co.in)

For any other information related to Demat account, you can email us at [info@nsdl.co.in](mailto:info@nsdl.co.in)

**Terms & Conditions** : 1) NSDL shall be solely responsible for the execution of this Contest. 2) This Contest is open to Indian Citizens only. 3) NSDL employees are not allowed to participate in this contest. 4) All personal details submitted must be accurate and complete and are subject to proof upon request by NSDL. 5) NSDL reserves the right to discontinue the contest at any given point of time without prior intimation. 6) All winners shall be selected by NSDL and the decision taken will be final.