IndusInd Bank

Your guide to

Fraud prevention

JAANKAAR BANO
JAGRUK RAHO

SCROLL DOWN

In
an increasingly
digital world,
safeguarding your finances
has never been more critical.
This guide provides essential
insights into preventing fraud and
securing your digital transactions.
From understanding the basics
of online scams to
implementing advanced
security measures, we've
got you covered.

Spotting Scams Before They Spot You

Explore the common types of digital fraud, including phishing, identity theft, and malware attacks. Understand the mechanisms behind each type and the impact they can have on your financial well-being.

Account Takeover

An Account Takeover – or ATO – occurs when fraudsters take ownership of an online account, often using stolen credentials. Once access is achieved, the attacker may change the password to lock out the real account owner. They may transfer money to another account, make fraudulent payments, or open new accounts (most often credit lines) in the victim's name. By the time the customer or the bank realizes that the account has been hijacked, they may have already incurred substantial losses.

Here's a closer look at some of the techniques fraudsters may use to launch an ATO attack:

Phishing Attacks

Fraudsters may obtain account credentials by sending a fake email or text message to customers that direct them to a fake bank login page. When customers enter their credentials, fraudsters steal them.

Credential Stuffing

Fraudsters leverage sophisticated bots to automatically test random credentials. Also referred to as “brute force” attacks, they leverage lists purchased on the dark web, trying different combinations until they gain access to an account.

Social Engineering

A wide variety of attacks that fraudsters use to obtain account information directly from users by tricking them, or by appealing to their emotions and fears during interactions.

Cybersecurity Issues

Fraudsters frequently exploit unpatched software and other cybersecurity weaknesses to gain access to data servers and steal customer information.

Call Centre Fraud

Call center fraud is a type of social engineering where a fraudster poses as a legitimate customer when contacting an organization's call centre. They deceive the representative into granting access to an account or performing fraudulent or malicious actions within an account.

New Account Fraud

New account fraud, also known as account creation fraud, account opening fraud, or fake account fraud, is a common type of bank fraud. It occurs when fraudsters or money mules open accounts with fraudulent intent, often using stolen or synthetic identities. They might steal legitimate customer identities through data breaches or phishing, or use sensitive information from children, deceased individuals, or even homeless people.

In some cases, mules use their own identities to create fake accounts for fraudulent purposes. Moreover, they can also create synthetic identities by combining real information with random, invented or stolen data. Once the account is established, they can accumulate charges or write checks in the victim's name.

Money Laundering

Money laundering involves disguising illegal or "dirty" money through a series of transactions involving foreign banks and/or legitimate businesses, thereby making it appear legal or "clean." This process “washes” or conceals the money's illicit origins, making it difficult to trace back to criminal activities such as drug trafficking, corruption, embezzlement, or illegal gambling.

Typically carried out by organized crime rings, money laundering consists of three stages:

Placement

Money is “**placed**” or introduced into the financial system through various methods. For instance, criminals may divide large sums of cash into smaller, less noticeable amounts, depositing them into bank accounts or using them to purchase checks or money orders. Another method, known as "**smurfing**", involves depositing money into bank accounts in small amounts that fall below anti-money laundering (AML) reporting thresholds.

Layering

In this phase, the criminal moves the funds through various transactions to obscure their origin. They may do this by buying and selling investments, using holding companies, or transferring funds between different financial entities. Transfers might be disguised as private loans or payments for goods and services.

Integration/Extraction

In the third stage, criminals blend their illicit funds into the economy, camouflaging dirty money by purchasing goods, investing in real estate or businesses, or even fabricating payrolls. Although some profits are lost in the "**washing**" process, the fraudster still walks away with a hefty sum.

Money Mules

Money mules act as intermediaries, transferring illicit funds either in person, through courier services, or digitally, all on behalf of someone else. They are transactional mercenaries, who are compensated for their role. Criminals recruit mules to help launder money obtained through online scams, fraud, or other criminal activities like drug trafficking. The mule's involvement adds additional layers of distance between the criminal and the stolen funds.

These mules move money through various channels-bank accounts, cashier's checks, cryptocurrency, prepaid debit cards, and more. While some mules knowingly assist criminals, others may be completely unaware, often misled by a sense of trust or a perceived favour for someone they believe to be honest. This makes it one of the most challenging forms of bank fraud to detect, as mules typically pass all KYC and AML checks, slipping under the radar as seemingly legitimate individuals.

Payment Fraud

Payment fraud happens when a cybercriminal carries out a fraudulent or illegal transaction. In the banking industry, various transactions occur throughout the customer account lifecycle, such as cash withdrawals, deposits, cheques, online payments, debit card transactions, wire transfers, and loan payments. Every transaction offers a chance for fraudsters to commit crime.

ACH Fraud

ACH fraud occurs when a criminal steals funds through the **Automated Clearing House (ACH)** financial transaction network, a central clearing facility. The most common type of ACH fraud involves imposter scams, where scammers use **Authorized Push Payment (APP)** schemes to deceive customers into executing fraudulent ACH transactions.

ACH fraud is alarmingly easy to commit, requiring only two pieces of stolen information: a business checking account number and a bank routing number.

Here are some common methods fraudsters use to commit ACH fraud:

ACH Kiting

Transferring funds repeatedly between accounts and financial institutions. Usually, ACH kiting happens within a company, often right before the financial year.

ACH Lapping

A payment from a bank account is diverted or falsely marked as received. Subsequent payments from other accounts are made to cover up the fraud.

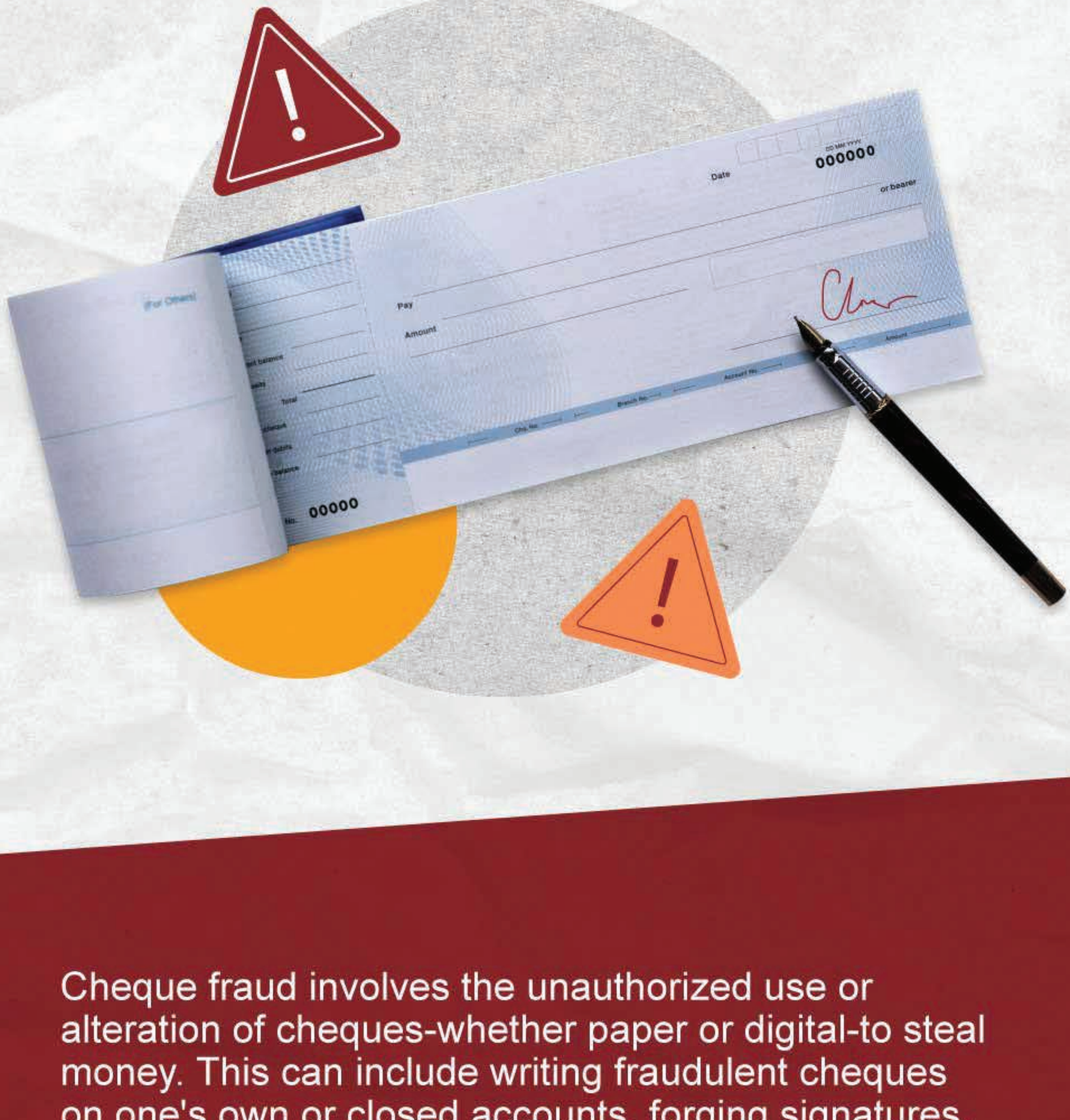
Insider Threats

A company's employee uses legitimate credentials to steal money via ACH or pass it to another fraudster.

Phishing

A fraudster deceives an employee or authorized individual into revealing their credentials, then uses them to impersonate the individual and withdraw funds.

Cheque Fraud



Cheque fraud involves the unauthorized use or alteration of cheques-whether paper or digital-to steal money. This can include writing fraudulent cheques on one's own or closed accounts, forging signatures, or creating fake cheques. It encompasses a range of deceptive practices, such as using counterfeit cheques, stolen cheques, or doctored cheques or modifying legitimate ones to divert funds from individuals or businesses.

How does cheque fraud happen?

Cheque frauds happen via one of these 3 methods

Counterfeiting

Fraudsters create fake cheques that closely mimic legitimate ones, using high-quality printers and special paper. They then use these counterfeit cheques to make purchases or withdraw money.

Cheque Washing

Criminals steal cheques from mailboxes or trash bins and use chemicals to erase the original ink. They then rewrite the cheque with a new amount and payee to commit fraud.

Stolen Cheques

Thieves steal blank cheques from individuals or businesses and use them for unauthorized purchases or withdrawals.

In each case, the fraud results from theft, manipulation of account information, or deceit against the bank.

Common Types of Cheque Fraud

Cheque fraud encompasses various methods, each exploiting different vulnerabilities inherent to cheques.

Some of the most common types include:

Forgery

Altering an existing cheque or creating a fake cheque using someone else's account information.

Paperhanging

Writing a cheque without sufficient funds and taking advantage of the “float” time between issuing and depositing the cheque.

Cheque Kiting

Writing a cheque from an account with insufficient funds but depositing funds into the account before the cheque clears to cover the shortfall.

Counterfeiting

Creating a fake cheque that closely resembles a legitimate one.

Chemical Alterations

Using chemicals to erase the original ink on a cheque, then writing new fraudulent information.

Stolen Cheques

Stealing blank cheques and altering the payee or amount before cashing or depositing them.

Cheque Washing

Erasing the ink on a cheque and rewriting it with a new payee and/or amount before cashing or depositing

Post-Dating

Writing a cheque with a future date to make it appear valid at a later time.

Closed Account Fraud

Closed account fraud occurs when someone uses another person's closed or inactive account information to carry out unauthorized transactions. This can involve using stolen debit or credit card numbers to make purchases or leveraging old account details to open new accounts without the account holder's knowledge.

In some instances, closed account fraud results from individuals failing to properly close their accounts, leaving them vulnerable to misuse. In other cases, fraudsters may obtain closed account information through data breaches or other forms of unauthorized access.

Card Fraud

Card fraud is one of the most common types of bank fraud and encompasses fraud involving any type of payment card, including credit, debit, gift, and prepaid cards.

Fraudsters may obtain card information through various methods, such as stealing physical cards, finding lost cards or card details, or using card skimming devices (for instance, at gas stations).

Card fraud can be categorized into two main types:

- Card-Present (CP) Fraud
- Card-Not-Present (CNP) Fraud.

CNP fraud is more prevalent than CP fraud.

UPI/Digital Payment Frauds

With over a billion people globally using digital payment apps like Amazon Pay and Apple Pay for **peer-to-peer (P2P)** transactions, these platforms have become prime targets for fraudsters. These apps are often vulnerable because companies may lack the data and insights needed to detect emerging fraud patterns.

Common scams include fraudsters selling goods through online marketplaces and requesting payment via these P2P apps, only to fail to deliver the items. Additionally, thieves may use stolen credit card information to set up P2P accounts and make fraudulent purchases.

How to Detect Real-Time Scams

To protect yourself from real-time payment fraud, follow these steps to identify potential scams:

Verify the Recipient

Ensure you know who you're sending money to and verify their trustworthiness. Use legitimate contact information for businesses and ask unknown individuals to prove their identity before making any transactions.

Check Website Legitimacy

Hover over links in emails (without clicking) to view the actual URL destination. Conduct a web search to confirm that the URL matches the official website of the company or organization it claims to represent.

Beware of Urgency and Pressure

Scammers often create a sense of urgency to force quick decisions. Be cautious of messages demanding immediate action or threatening negative consequences if you don't comply.

Treat Unsolicited Requests with Suspicion

Be wary of unexpected requests for payments, personal information, or login credentials. Always verify such requests through official channels before responding.

Protect Your Personal Information

Never share sensitive information like passwords, PINs, or Social Security numbers in response to unsolicited messages, emails, or phone calls.

Stay Informed

Keep up to date on the latest scamming techniques and tactics used by fraudsters. Knowledge of common scams can help you recognize and avoid them.

Use Multi-Factor Authentication

Add an extra layer of security to your accounts and transactions by enabling multi-factor authentication.

NOTE: Remember that fraudsters can be very convincing and their scams always evolve over time. When in doubt, it's always better to take a step back and verify the legitimacy of the situation before proceeding.

Wire Transfer Fraud

The term "**Wire Transfer**" originates from the era when funds were transmitted between banks via telegraph wires.

In the digital age, wire transfer fraud has evolved and typically manifests in one of two ways:

Impersonation Scams

In this type of fraud, a scammer poses as a trusted individual-such as a vendor, company executive, or family member-and urgently requests a wire transfer. The scam often exploits the victim's emotions by fabricating emergencies or high-stake situations. For example, an employee in the finance department might receive an email that appears to be from the CEO, urgently instructing them to transfer funds to secure a deal. The email may include seemingly authentic account details, but it's all a deception.

Email Hacking

In this scheme, a hacker gains access to email communications, particularly those related to an ongoing wire transfer, and subtly alters the transfer instructions. As a result, the unsuspecting victim ends up sending the funds to the fraudster"s account instead.

Common Wire Fraud Schemes

Investment Scams

Fraudsters lure victims with enticing investment opportunities via email or phone, promising high returns or guaranteed profits that never materialize.

Business Email Compromise

A fraudster gains unauthorized access to an employee's email account and uses it to steal sensitive information or funds.

Phishing Scams

Deceptive emails, disguised as legitimate communications, trick victims into revealing personal or financial details through fake forms.

Online Auction Fraud

Scammers create fake auction sites or listings, collect payments from unsuspecting buyers, and never deliver the promised goods.

Identity Theft

Fraudsters steal personal information, such as Social Security numbers or bank account details, to transfer money to their own accounts.

Application Fraud

Application fraud occurs when criminals use stolen or synthetic identities to apply for loans or lines of credit. Some of these instances are:

• A fraudster applies for a credit card and gradually builds credit over months or even years. Once they have established a good credit history, they max out the card with no intention of repaying the debt.

• Criminals may use someone else's information to apply for credit or loans. They often submit multiple applications simultaneously to different financial institutions, a tactic known as loan stacking, using automated bots and virtual machines. By the time the fraud is detected, the criminal has already obtained the funds and vanished.

First-Party Fraud
This occurs when individuals use their true identity but provide false information, such as a fake address or inflated income.

Third-Party Application Fraud
This involves creating synthetic identities by combining real and fictitious information.

Loan Fraud

Loan fraud is a subtype of application fraud and encompasses various types, including mortgage fraud, loan scams, and payday fraud. In all these cases, criminals use someone's personal information to illegally obtain a loan.

The rise of online lenders, who may not conduct thorough background checks, has contributed to an increase in loan fraud. These lenders often make their lending decisions based on basic information-such as name, address, social security number, and income-that can be easily stolen or fraudulently obtained.

How Loan Fraud Occurs

A fraudster contacts you via phone, SMS, or email, offering a loan

They pose as officers, agents, or representatives of reputable banks or financial institutions.

They claim you are eligible for unique high amount loan offers with hassle-free approval and extremely low interest rates.

If you accept, they request a range of documents such as ID, address proof, PAN number, bank account details, account statements, cancelled cheque, and income details (e.g., pay slips, tax returns) via email or WhatsApp. These documents may be misused by the fraudsters.

They then email you a loan application form to complete and return (a scanned copy), assuring you that the loan will be approved in a few days

After submitting the application, they provide a digital copy of a seemingly authentic loan acceptance letter. They may then ask you to deposit funds into a specific account, for fake reasons such as file costs, refundable security deposits, or processing fees.

How to Prevent Loan Fraud?

Research the lender to ensure it is legitimate and trustworthy.

Visit the lender's office in person if possible.

Be cautious if a lender demands processing fees or other upfront costs.

Verify the credentials of the individuals by meeting them personally and confirm the validity of their provided ID proofs, including photographs.

Avoid making payments online.

Advance Fee Fraud

Advance fee fraud is a type of scam where the fraudster persuades the victim to make a payment upfront or in advance, by promising goods, services, or opportunities they have no intention of delivering. The scam typically begins with a convincing story designed to earn the victim's trust and send an advanced payment. The fraudster may claim the payment is needed to secure a high-return investment, join an exclusive business opportunity, or unlock an inheritance or lottery winnings, for which he'll be rewarded later on.

Scammers often pose as wealthy individuals, government officials, or even distant relatives, using these identities to add credibility to their stories. To further deceive their victims, they might create elaborate fake websites, business profiles, and social media accounts to appear legitimate.

Once the victim transfers the money, the fraudster vanishes, leaving the victim with no means to recover the lost funds.

Types of Advance Fee Frauds

Lottery or Prize Scams

Victims receive notifications claiming they've won a lottery, sweepstakes, or prize, but are told they must pay fees or taxes upfront to claim their winnings. The reward never exists, and the scammers disappear once payment is received.

Inheritance Scams

Scammers pose as lawyers or representatives of a deceased individual, claiming the victim is a beneficiary of a substantial inheritance. They demand payment for fees to release the funds, which are nonexistent.

Business Opportunity Scams

Victims are offered a lucrative business opportunity requiring upfront payments for expenses like licensing, permits, or legal costs. The business never materialises, and the scammers vanish after receiving the payment.

Romance Scams

Scammers build online romantic relationships and then create crisis situations, such as a medical emergency or legal trouble. They request money to resolve the issue, often disappearing after receiving it. These scams can also evolve into money mule scams.

Job Offer Scams

Fraudulent job offers entice victims with promises of high-paying positions or work-from-home opportunities but require upfront payments for training, background checks, or other fictitious expenses. The job never materializes, and the scammer cuts off contact.

Rental Scams

Scammers pose as landlords of properties that may not exist or aren't theirs to rent. They demand deposits or advance rent payments and disappear after the victim pays.

Charity Scams

Fraudsters create fake charity organizations or impersonate legitimate ones, soliciting donations for a cause. Victims are asked to make upfront payments, but the funds never reach any charitable purpose.

Loan Scams

Scammers offer loans with attractive terms but require upfront fees or insurance payments. After the victim pays, the loan never materializes and the scammer drops all contact.

Common Tactics of Scammers

Urgency and Pressure

Scammers create a sense of urgency or pressure, compelling victims to act quickly without thoroughly evaluating the situation.

Confidentiality

They emphasize the need for secrecy and confidentiality, making the victim feel trusted and important while preventing them from seeking advice or verification from friends, family, or authorities.

Impersonation

Fraudsters impersonate trustworthy entities like government agencies, reputable businesses, or legitimate organizations. They use fake credentials, official-looking documents, or forged emails to lend credibility to their schemes.

“Too Good to Be True” Offers

Scammers often present offers that seem too good to be true, such as winning a large sum of money, receiving an inheritance, or securing a high-paying job without significant effort.

Fake Documents

Especially popular in investment scams, fraudsters provide fake contracts, certificates, or legal papers to make their claims appear legitimate and create a false sense of security.

Unsolicited Communication

Advance fee scams often begin with unsolicited contact via email, letters, or phone calls.

Payment Requests

Scammers request upfront payments for various fees like processing, taxes, legal costs, or administrative expenses.

Alternative Payments/Currencies

Victims are often asked to send money via wire transfer, prepaid cards, cryptocurrency, or other untraceable methods.

How to Prevent Frauds?

Be Skeptical of Unsolicited Communications

Show caution while approaching unexpected emails, letters, or messages from unknown individuals or organizations, especially if they promise significant financial gains or make urgent requests for assistance.

Verify Identities

Verify the identity of anyone contacting you by using official contact information, such as phone numbers from verified websites. Be particularly cautious of individuals claiming to be government officials, business executives, or heirs to large fortunes.

Research and Cross-Check Information

Conduct thorough research on any offer or proposal. Look up the individual or organization online, and cross-check details like names, addresses, and phone numbers for consistency.

Avoid Sharing Personally Identifiable Information (PII)

Do not share sensitive personal information, such as bank account details, Social Security numbers, or passport information, with unknown individuals or entities.

Question Unusual Requests

Be cautious if asked to pay upfront fees, taxes, or expenses to receive a promised benefit. Legitimate transactions rarely require such payments in advance.

Consult with Trusted Contacts

Seek advice from friends, family, or colleagues before making any financial decisions based on unsolicited offers.

Use Secure Communication Channels

Ensure that sensitive communications are conducted through secure and official channels. Avoid clicking on suspicious links or downloading attachments from unknown sources.

Report Suspicious Activity

Report any suspected fraud to relevant authorities, such as law enforcement or consumer protection agencies.

Stay Informed

Keep up to date on the latest scams and share this information with friends and family to help everyone stay vigilant.

Follow these general precautionary measures and good practices to stay protected against fraud

Avoid

- Visiting unsecured websites or using unknown browsers
- Saving passwords on public devices
- Accessing financial / confidential emails on public or free networks
- Clicking on suspicious looking pop-ups, links and emails from unknown sources
- Storing secure credentials or passwords in emails or on unknown websites
- Sharing private information with unknown users on social media
- Using the same passwords for banking and other transactions
- Installing unknown applications or softwares
- Leaving your mobile or other electronic devices or applications unlocked

Never

- Share your PIN, passwords, credit or debit card numbers, CVV, cheque book, checkbook leaves, KYC details, or KYC documents with anyone.
- Store sensitive or confidential information on untrusted or unknown devices.

Always

- Protect your phone and devices with strong passwords.
- Enable 2-Factor Authentication (2FA) whenever possible.
- Log out of internet and mobile banking sessions immediately after use.
- Use the enable/disable feature to set transaction limits on your cards or account transactions based on your usage.
- Use secure payment gateways for all online payment transactions.
- Verify the security of websites by checking for signs like "https" or a padlock icon in the address bar.
- Scan USB devices and drives before usage.
- Install anti-virus and anti-spyware on your devices and keep them updated.
- Maintain a strong password with a combination of alphanumeric and special characters and change them regularly.
- Use virtual keyboards on public devices.

Report a Suspicious or Fraudulent Transactions to

IndusInd Bank

To report an unauthorized transaction(s):

On your Debit Card / Net Banking / Mobile Banking, call our Phone Banking services at

1860 267 7777

On your Credit Card, call our Phone Banking services at

1860 267 7777

Write to us at:

reachus@indusind.com

or for disputes

Click Here

Visit any

IndusInd Bank Branch