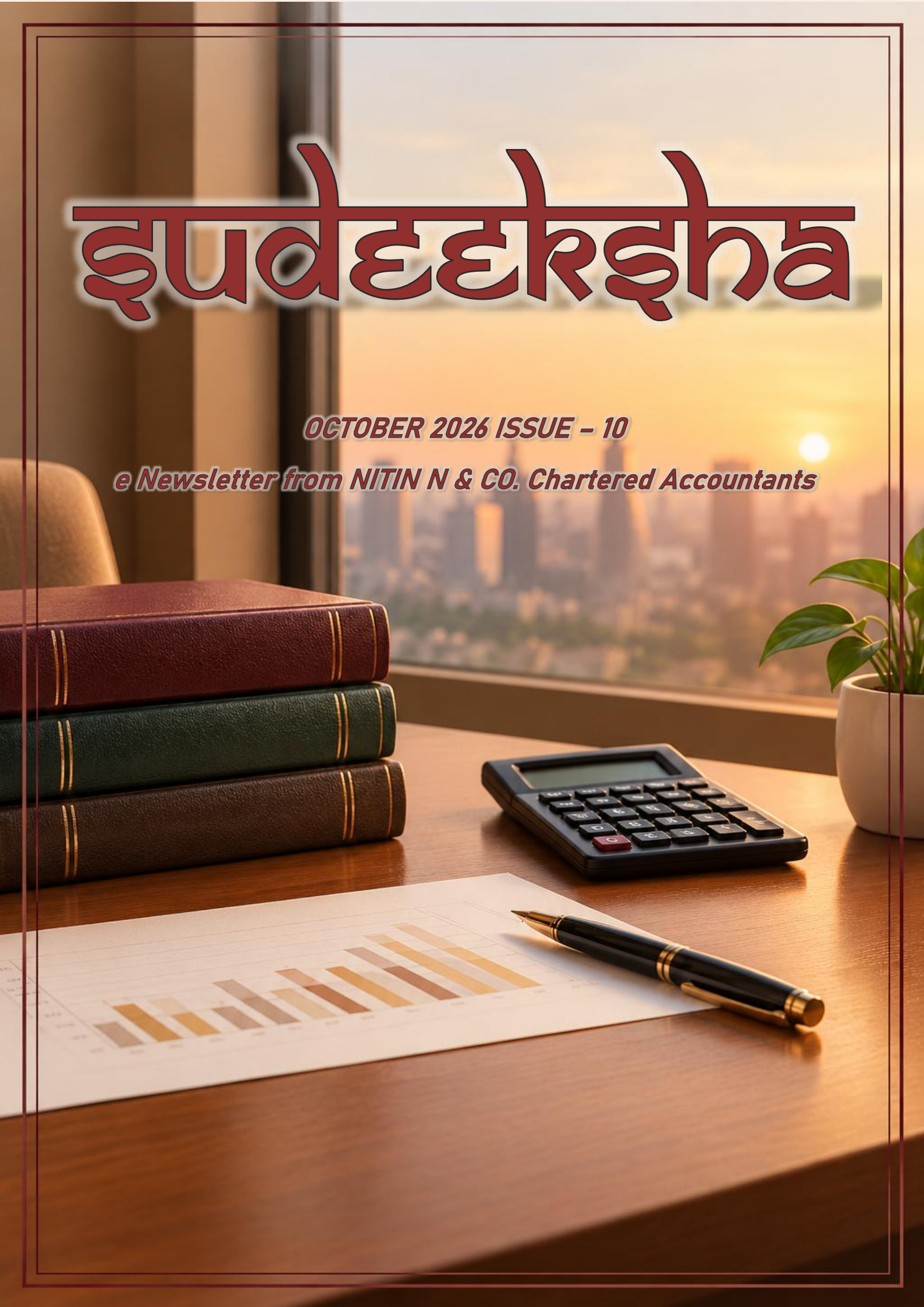
sudeeksha

OCTOBER 2026 ISSUE – 10

e Newsletter from NITIN N & CO. Chartered Accountants



INSIDE

In a world where laws evolve, businesses transform, and technology reshapes the professional landscape, staying informed is more important than ever. This edition brings together perspectives on some of the key issues shaping today's legal, financial, and business environment. From understanding foreign exchange regulations under FEMA and insolvency resolution under the IBC to exploring cyber security, forensic accounting, and trademark protection, each article offers valuable insights into contemporary professional practice. The edition also takes a closer look at how Maruti's advertising has contributed to Suzuki's brand identity. Through these diverse topics, we aim to encourage informed thinking, deepen professional understanding, and equip readers to navigate an increasingly complex and dynamic world.

FROM THE DESK

October marks the beginning of second half of the Financial Year and the month of closure as far as most annual compliances are concerned. It is the month where the focus shifts from the previous financial year to the current and is a very important phase of planning that determines the road ahead.

The *Nav Ratri* that falls in the same month signifies the victory of good over evil and invokes the spirit of *Shakti* (feminine). Let us all remember to realise that proper use of time gives the advantage, power and comfort to carry out our tasks effectively and efficiently.

For our profession, time assumes immense significance just like the *Durgashtami, Maha Navami* and *Vijaya Dashami* and we should understand that the foundation for victory is supposed to be laid out much earlier for that moment to materialise at the appropriate time.

Best Wishes for a victorious career and a life that gives the satisfaction and pride of success.

DISCLAIMER

This newsletter is prepared for general informational purposes only and contains the views, opinions, and interpretations of the author(s). The information provided herein does not constitute professional advice-legal, financial, tax, or accounting-and should not be relied upon as a substitute for consultation with a qualified professional.

While every effort has been made to ensure the accuracy and reliability of the content, the author(s) and the firm do not accept any responsibility for errors, omissions, or misstatements, whether arising from negligence or otherwise. Readers are advised to verify all information independently and exercise their own judgment and discretion before taking any action based on the content of this newsletter.

This newsletter is intended solely for the readers of this publication and may not be reproduced, redistributed, or used in any other form without the express written consent of the author(s). The firm expressly disclaims any liability for any direct, indirect, or consequential loss or damage arising from the use or interpretation of the information provided.

EDITION OVERVIEW

1	FEMA: Foreign Exchange Management Act, 1999	Page 5-7
2	When a Business Runs into Trouble: Understanding CIRP under the IBC, 2016	Page 8-10
3	Cyber security: protecting our digital world	Page 11-16
4	Forensic Accounting: Beyond the numbers	Page 17-20
5	Trademark Registration in India: From Distinctiveness to Examination Objections	Page 21-24
6	Did Maruti's Ads Build Suzuki's Brand?	Page 25-28
7	Crossword	Page 29
8	Memory Box	Page 30

Anjitha Anil
Trainee
Email ID: anjithaanil1536@gmail.com



FEMA: Foreign Exchange Management Act, 1999

The Foreign Exchange Management Act (FEMA), 1999 is a significant legislation relating to foreign exchange transactions in India. It has replaced the Foreign Exchange Regulation Act (FERA), 1973 and became effective from 1 June 2000. The introduction of FEMA was made to aid in the liberalization of foreign exchange regulations and boost India's international trade and commerce. It is of great significance to the economic development, foreign trade and foreign investment.



Objectives of FEMA

With a few important objectives, FEMA was introduced:

- To ease foreign trade and international payments.
- To facilitate orderly development of the foreign exchange market in India.
- To control foreign exchange transactions.
- To attract foreign investment in India.
- To establish clear rules for persons and enterprises engaged in international financial transactions.

The FEMA has several key features, including:

FEMA deals with different foreign currency payments and foreign currency transactions. It offers guidelines on imports and exports of goods and services, payments to foreign countries, receipts from foreign countries, and investment in foreign business ventures.

The Act makes a distinction between current account transactions and capital account transactions. Typical current account transactions are payments for travel, education, imports and services. Capital account transactions cover some investments, loans and cross-border transactions of assets. The transactions are to be conducted according to the pertinent FEMA rules and regulations.

Role of the Reserve Bank of India

The Reserve Bank of India (RBI) is given a significant role for administering the foreign exchange regulations under FEMA. It gives instructions and regulations, authorises eligible institutions to engage in foreign exchange and supervises relevant foreign exchange transactions. Authorised banks and other authorised dealers facilitate foreign exchange transactions as per the rules for the individuals and businesses.

The importance of FEMA in business is unmatched. The importance of FEMA in business can be unequalled.

For companies involved in international trade, FEMA is of particular importance. In Germany, for instance, on receipt of the machinery, an Indian company has to make foreign currency payments as per the applicable provisions. Likewise, any Indian business that is paid by a foreign customer is subject to the applicable foreign exchange regulations.

In addition to this, FEMA also lays down a system with regards to foreign investment in Indian enterprises. It facilitates specific processes for foreign financial transactions and enhances investor confidence.

The Difference Between FEMA and FERA

The introduction of FERA came into being in India when it adopted a more rigid policy to control foreign exchange. FEMA replaced FERA with more management-oriented system. FERA went rigorous in controlling foreign exchange while FEMA emphasizes on the facilitation of possible transactions and controlling the foreign exchange in a changing global economy more effectively.

Consequences of Non-Compliance with FEMA

FEMA rules mandate that people and businesses adhere to them when they are involved in foreign exchange transactions. The Act imposes monetary penalties and other penalties for violations. Thus, companies need to keep proper records, abide by reporting obligations, and consult with professionals as needed to ensure compliance, and maintain transparency in financial dealings.

Broad classification of transactions under FEMA

A. Inbound transactions

Inbound transactions refer to money, investments or other financial resources coming into India from foreign countries.

Examples:

- Foreign Direct Investment (FDI): A foreign company invests money in an Indian company.
- Foreign remittances: A person working abroad sends money to family in India.
- Export earnings: An Indian exporter receives payment from a foreign buyer.
- Foreign loans: An eligible Indian business receives a loan from a foreign lender.
- NRI investments: A non-resident Indian invests in eligible Indian assets.

B. Outbound transactions

Outbound transactions refer to money, investments or other financial resources moving from India to foreign countries.

Examples:

- Overseas investments: An Indian company invests in a business abroad.
- Import payments: An Indian business pays a foreign supplier for goods.
- Education remittances: A student sends money abroad to pay college fees.
- Medical remittances: A person sends money abroad for medical treatment.
- Foreign travel expenses: An Indian resident purchases foreign currency for permitted travel expenses.

Inbound and outbound transactions must comply with the applicable FEMA provisions, RBI regulations and government rules. Some transactions are restricted or prohibited.

Illustrations of penalties under FEMA

Under Section 13 of FEMA, 1999, a person who violates the Act, its rules or regulations may be liable to a penalty. The amount depends on the nature and value of the contravention.

Offence / contravention	Person who may be liable to pay	Penalty
Making an unauthorised foreign exchange transaction	Person who commits the contravention	Up to 3 times the amount involved, if quantifiable
Making a contravention whose amount cannot be calculated	Person who commits the contravention	Up to ₹2,00,000
Continuing the contravention after the first day	Person responsible for the contravention	Additional penalty up to ₹5,000 for each day it continues
Company violating FEMA requirements	Company and persons responsible for its business, subject to Section 42	Penalty as applicable under FEMA

Conclusion

FEMA is one of the most important laws connecting India's financial system with the international economy. It plays a significant role in facilitating international trade, foreign payments, and cross-border investments. It provides a legal framework for managing foreign exchange transactions and helps maintain stability in India's foreign exchange market. As India continues to strengthen its business relationships with other countries, it becomes essential for businesses, investors, students, and financial professionals to understand the provisions of FEMA.

By ensuring compliance with FEMA regulations, individuals and businesses can conduct international financial transactions smoothly and lawfully. The Act also encourages foreign investment, promotes transparency, and supports the growth of international business activities. Understanding FEMA helps prevent legal complications and ensures that foreign exchange transactions are carried out according to the prescribed rules.

FEMA came into effect on 1 June 2000, replacing the Foreign Exchange Regulation Act (FERA), 1973. Unlike FERA, which focused mainly on strict control of foreign exchange, FEMA adopted a more flexible and management-oriented approach to support India's changing economic environment. Even today, FEMA remains one of the key laws regulating foreign exchange transactions in India and plays an important role in promoting economic development and strengthening India's participation in the global economy.

****

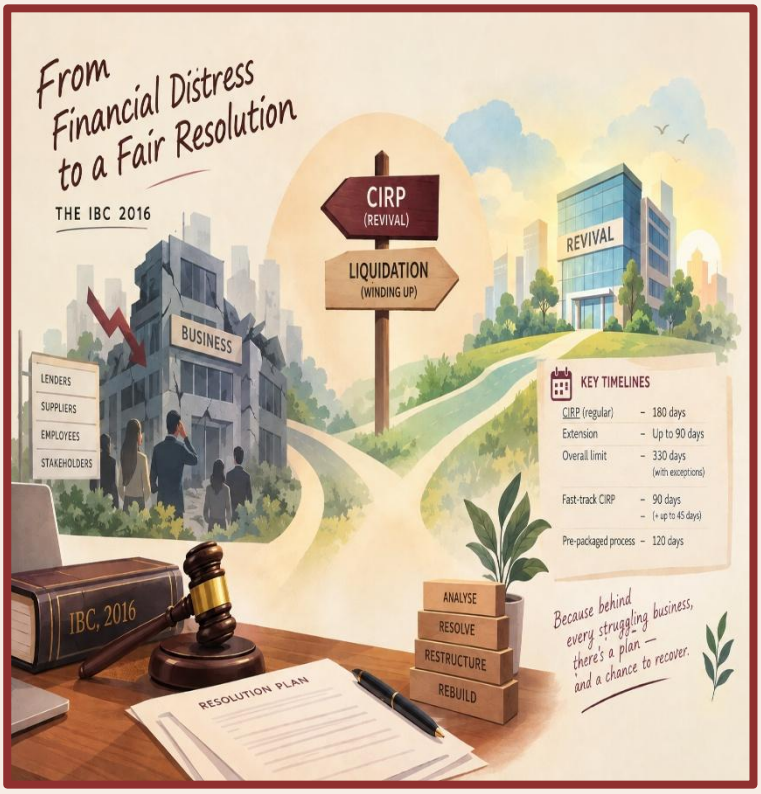
Anagha Mariya
Articled Assistant
Email ID: anaghamariya480@gmail.com



When a Business Runs into Trouble: Understanding CIRP under the IBC, 2016

Running a business is not always easy. A company may face financial difficulties due to falling sales, rising costs or unpaid dues. When it becomes difficult to repay loans and other obligations, the impact is felt not only by the company but also by its lenders, suppliers and employees. Does this mean the business has to shut down? Not necessarily.

The Insolvency and Bankruptcy Code, 2016 (IBC) provides a way to deal with such situations. It gives financially distressed companies an opportunity to recover while protecting the interests of their creditors. If the business cannot be revived, its assets can be sold and the proceeds distributed according to the law. One of the key mechanisms under the Code is the Corporate Insolvency Resolution Process (CIRP), which helps determine whether a struggling company can be saved or should move towards liquidation.



When Does the Process Begin?

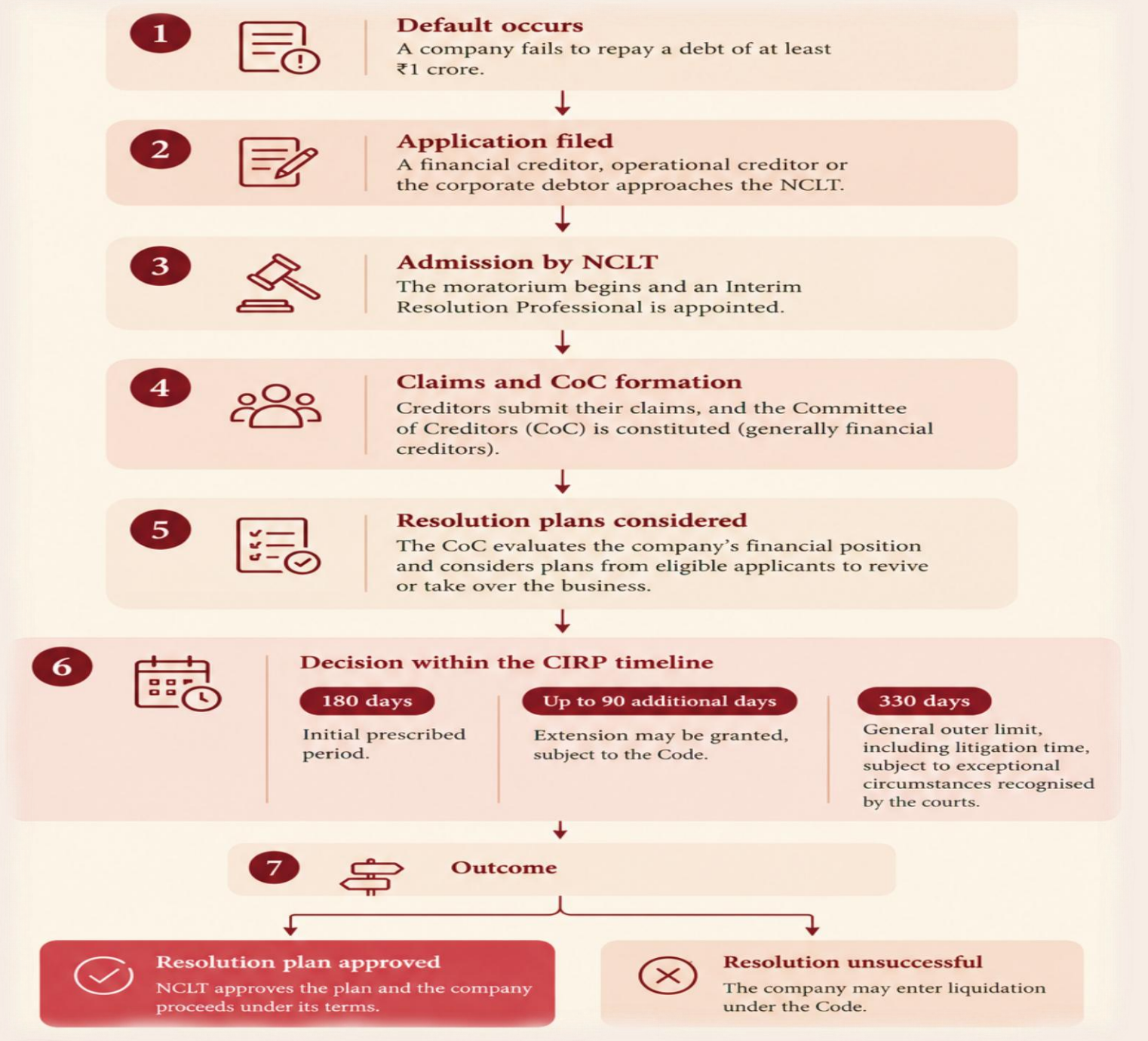
CIRP can begin when a company fails to repay a debt that has become due and payable. The minimum default amount for initiating CIRP is **₹1 crore**, following the Central Government's notification dated 24 March 2020. The process can be initiated by a financial creditor, such as a bank, under Section 7; an operational creditor, such as a supplier, under Section 9; or the company itself under Section 10. Financial debt generally arises from borrowings, while operational debt relates to goods, services, employment and statutory dues.

The courts have also helped clarify how these provisions work in practice. In *Pioneer Urban Land v. Union of India*, the Supreme Court recognised homebuyers as financial creditors. To initiate CIRP, the application must be filed jointly by at least 100 allottees or 10% of the allottees in the same project, whichever is less. In *Mobilox Innovations v. Kirusa Software*, the Court clarified that a genuine dispute existing before an operational creditor's demand notice can prevent the admission of a CIRP application.

From Financial Trouble to a Possible Revival

Once the National Company Law Tribunal (NCLT) admits an application, the Corporate Insolvency Resolution Process (CIRP) officially begins. A moratorium under Section 14 restricts certain legal proceedings, recovery actions and enforcement of security against the company. An Interim Resolution Professional is appointed to manage the process, invite claims from creditors and facilitate the formation of the Committee of Creditors (CoC), which generally consists of financial creditors. The CoC evaluates the company's financial position and considers resolution plans submitted by eligible applicants who propose to revive or take over the business. A resolution plan requires approval from at least 66% of the CoC's voting share, followed by approval from the NCLT. If the plan is approved, the company can continue its operations under the approved terms. If no viable resolution is achieved, the company may proceed to liquidation. The overall objective of CIRP is to maximise the value of the company's assets while balancing the interests of creditors and other stakeholders.

CIRP at a Glance: Major Steps and Timelines



Who Can Take Over a Company?

A resolution plan cannot be submitted by just anyone. Section 29A sets out categories of persons who are ineligible to submit a resolution plan, including certain wilful defaulters and persons connected with accounts classified as non-performing assets, subject to the conditions and exceptions under the law. These restrictions are intended to prevent the insolvency process from being used by ineligible persons to regain control of a company without meeting the prescribed requirements.

Sometimes, a settlement can provide a practical way forward for a company facing insolvency. Under Section 12A of the IBC, an admitted CIRP application may be withdrawn with the approval of 90% of the CoC's voting share, subject to the prescribed procedure. This allows the company and its creditors to reach a mutually acceptable settlement without necessarily continuing the insolvency process. Such settlements can help avoid delays and costs while providing an opportunity to resolve outstanding dues.

When Revival Is No Longer Possible

Unfortunately, not every business can be revived. If no resolution plan is received within the prescribed period, the NCLT rejects the plan, or the CoC decides to proceed with liquidation in accordance with the Code, the company may enter liquidation. In such cases, the liquidator takes charge of the company's assets, realises their value and distributes the proceeds among creditors and other stakeholders according to Section 53 of the IBC. This distribution follows a specific order of priority known as the *waterfall mechanism*, which determines who receives payment first and how the available funds are allocated.

The distribution begins with insolvency resolution and liquidation costs, followed by specified workmen's dues and secured creditors who relinquish their security. Employee dues, unsecured financial creditors, specified government dues, remaining debts and dues, preference shareholders and equity shareholders follow in the prescribed order. The liquidator is generally required to complete the process within one year, subject to applicable regulations and circumstances. Although liquidation marks the end of the business in its existing form, the process ensures that the available assets are distributed according to the law.

A Different Approach for MSMEs

For eligible micro, small and medium enterprises (MSMEs), the IBC offers another option: the **Pre-Packaged Insolvency Resolution Process (PPIRP)** under Sections 54A to 54P. Unlike regular CIRP, this process allows the company and its creditors to work towards a resolution before formally approaching the NCLT. It applies to defaults of at least ₹10 lakh and requires the prescribed approval of financial creditors. The process must be completed within 120 days, while the existing management generally continues to run the business under the supervision of the Resolution Professional, subject to the Code. This approach aims to reduce delays, costs and disruption, giving eligible smaller businesses a better opportunity to recover. This helps smaller businesses recover with minimal disruption.

The Takeaway: Saving a Business Is Worth Exploring

The IBC recognises that financial difficulties do not always have to mean the end of a business. By bringing creditors together, setting clear timelines and establishing a framework for resolution and liquidation, it provides a structured approach to managing corporate distress. For chartered accountants, understanding the provisions and procedures of the IBC is essential to advising businesses, assessing financial risks and supporting them through challenging situations. A sound understanding of the process also helps them contribute to informed decision-making and the protection of stakeholders' interests. This supports better outcomes.

****

Aswathy R Nair
Assurance and consulting staff-2
Email ID: nairaswathy1997@gmail.com



CYBER SECURITY: PROTECTING OUR DIGITAL WORLD

Stay Safe, Stay Smart, Stay Secure!



1. Introduction

In today's digital world, technology has become an essential part of our everyday lives. We use the internet for education, communication, banking, shopping, entertainment, and many other activities. Smartphones, computers, and digital platforms have made our lives easier and more convenient. However, as our dependence on technology increases, so does the risk of cyber threats. This is where cyber security plays a vital role.

Cyber security refers to the practice of protecting computers, mobile devices, networks, applications, and data from unauthorized access, cyberattacks, theft, and damage. It involves using technologies, security measures, and responsible online practices to ensure that digital information remains safe and secure.

In simple words, cyber security is the digital protection that keeps our personal information, financial details, and online activities safe from cybercriminals. It is not just the responsibility of IT professionals or large organizations; it is everyone's responsibility. Every individual who uses the internet must understand the importance of staying safe online.

2. Why Is Cyber Security Important?

The internet connects millions of people around the world and provides endless opportunities. At the same time, it creates opportunities for cybercriminals to misuse personal information and exploit security weaknesses. A single careless click on a suspicious link can sometimes lead to serious consequences.

Cyber security is important for several reasons:

Protection of Personal Information: Our names, phone numbers, addresses, photographs, passwords, and other personal details can be misused if they fall into the wrong hands. Cyber security helps protect this sensitive information.

Prevention of Financial Fraud: Online banking, digital payments, and shopping have become common. Security measures help reduce the risk of financial fraud, unauthorized transactions, and identitv theft.

Safety of Businesses and Organizations: Companies store valuable information about their customers, employees, and operations. Cyberattacks can cause financial losses, interrupt services, and damage their reputation.

Protection of Educational Institutions: Schools and colleges use digital platforms for classes, examinations, and storing student records. Cyber security helps protect these systems and maintain the privacy of students and teachers.

Maintaining Privacy and Trust: Strong security practices help people communicate, learn, and conduct transactions online with greater confidence.

Thus, cyber security is essential for building a safer and more trustworthy digital environment.

3. Common Types of Cyber Threats

Cyber threats can take many forms. Understanding the most common types is the first step towards protecting ourselves.

a) Malware

Malware, or malicious software, is designed to harm devices, steal information, or gain unauthorized access to systems. Viruses, worms, spyware, and ransomware are examples of malware.

Malware can enter a device through suspicious downloads, infected attachments, unsafe websites, or untrusted applications. It may slow down a device, damage files, or expose private information.

***Safety tip**: Install applications only from trusted sources, keep your software updated, and use reliable security tools.*

b) Phishing

Phishing is a cyberattack where criminals send fake emails, messages or links to steal sensitive information such as passwords, bank details or OTPs. These messages often appear to come from trusted organisations or banks.

For example, a fake bank message may urge you to click a link to avoid account blocking, leading to a fraudulent website.

***Safety tip**: Always verify the sender and website before sharing personal information. Never disclose an OTP or password to someone who asks for it unexpectedly*

c) Ransomware

Ransomware is a type of malware that locks or encrypts a victim's files and demands payment to restore access. It can affect individuals, businesses, hospitals, educational institutions, and government organizations.

A ransomware attack can interrupt important services and cause significant financial and operational damage.

***Safety tip**: Keep regular backups of important files and avoid opening unexpected attachments or downloading suspicious files.*

d) Password Attacks

Weak or reused passwords make online accounts more vulnerable to cyberattacks. Cybercriminals may guess common passwords or use credentials stolen from previous data breaches to gain access to multiple accounts. If the same password is used across different platforms, a single breach can put several accounts at risk.

***Safety tip**: Create strong, unique passwords for different accounts. A password manager can help you store them securely.*

e) Identity Theft

Identity theft occurs when someone uses another person's personal information without permission to commit fraud or impersonate them online. Stolen information may be used to create fake accounts, access online services or carry out unauthorised financial transactions.

***Safety tip:** Share personal information carefully. Check your accounts regularly for unknown transactions or login attempts and report anything suspicious.*

f) Social Engineering

Social engineering is a technique in which attackers manipulate people into revealing confidential information or performing unsafe actions. They may pretend to be a bank employee, technical support agent, friend, or authority figure to gain trust.

***Safety tip**: Do not trust a request simply because it sounds urgent or comes from a familiar name. Verify the person's identity through an independent and trusted channel.*

4. Recent Real-World Cyberattacks: Facts, Figures and Lessons

Cyberattacks are not just theoretical dangers. Real incidents demonstrate how cybercriminals exploit technology and human behaviour to steal money, expose confidential information, and disrupt essential services. The following examples highlight the scale of the problem.

a) Phishing and Online Fraud: FBI's 2025 Internet Crime Report

Incident: The Federal Bureau of Investigation (FBI) in the United States published its 2025 Internet Crime Report in April 2026. The report documented the scale of internet-enabled crime reported to its Internet Crime Complaint Center (IC3).

Figures involved:

- More than **1 million complaints** were received during 2025.
- Reported losses from internet-related crimes reached approximately **US$20.9 billion**.
- Phishing and spoofing were among the most frequently reported complaint categories.

These figures cover many kinds of internet crime, including investment scams and other frauds. They are not losses caused by phishing alone.

Lesson: Verify unexpected messages, avoid suspicious links, and never share banking credentials or OTPs with unknown persons.

Source: FBI, 2025 Internet Crime Report.

b) Ransomware: Change Healthcare Cyberattack (2024)

Incident: In February 2024, Change Healthcare, a US healthcare technology company, suffered a ransomware attack associated with the BlackCat/ALPHV cybercriminal group. The incident disrupted healthcare payments and affecting providers, pharmacies and patients.

Figures involved:

- Approximately **192.7 million individuals** were reported as affected by the data breach by July 2025.
- The disruption affected healthcare-related operations across the United States.

The figure represents the reported number of individuals affected by the breach, not the number of people who necessarily lost money.

Lesson: Organizations should maintain secure backups, use multi-factor authentication, restrict access to sensitive systems, and prepare emergency recovery plans.

Source: US Department of Health and Human Services, Change Healthcare incident updates.

c) Identity Theft: The Change Healthcare Data Breach

Incident: The Change Healthcare cyberattack exposed sensitive personal and healthcare information, potentially including medical records, insurance details and other identifying information. The incident highlighted how cyberattacks can compromise confidential data and expose individuals to identity theft and fraudulent activities.

Figures involved: Approximately **192.7 million individuals** were reported as affected. The exposure of personal information on such a large scale increases the risk of identity theft, financial fraud and targeted scams, as cybercriminals may misuse the stolen information to impersonate individuals or gain unauthorised access to their accounts.

Lesson: Avoid sharing unnecessary personal information online, use unique passwords, enable multi-factor authentication, and monitor accounts for unfamiliar activity. Stay alert to suspicious emails and messages to prevent phishing attacks and identity theft.

Source: US Department of Health and Human Services, Change Healthcare incident updates.

d) Social Engineering and AI-Assisted Fraud

Incident: Cybercriminals use social engineering techniques and AI-generated emails, fake profiles, voices, and videos to impersonate trusted individuals, such as company executives, bank officials, or family members. By creating urgency and exploiting trust, they trick victims into transferring money, sharing passwords, or disclosing confidential information. These scams are increasingly difficult to detect because AI-generated content can closely resemble genuine communications.

Figures involved: The FBI's 2025 Internet Crime Report recorded **22,364 complaints involving artificial intelligence**, with reported losses of approximately **US$893.3 million** in the United States.

These figures cover AI-related complaints across different types of crime and do not represent social engineering alone.

Lesson: Verify urgent financial requests through a separate, trusted communication channel. Even a familiar voice or realistic video should not automatically be treated as proof of identity.

Source: FBI, 2025 Internet Crime Report.

e) Cybercrime in India: Rising Cybersecurity Incidents

Incident: India's expanding digital economy has increased the importance of protecting online payments, personal data, government services, and business networks.

According to figures published by the Government of India, the Indian Computer Emergency Response Team (CERT-In) tracked the following numbers of cybersecurity incidents:

- **2023:** 15,92,917 incidents
- **2024:** 20,41,360 incidents
- **2025:** 29,44,248 incidents

The figures show a substantial rise in reported and tracked cybersecurity incidents. However, they do not mean that every incident involved financial fraud or a confirmed data breach.

Lesson: Individuals should secure their digital accounts, while organizations should improve monitoring, incident response, and employee awareness.

For suspected financial cyber fraud in India, call **1930** as soon as possible and report the incident through https://cybercrime.gov.in.

Source: CERT-In statistics published by the Government of India, March 2026.

What Do These Cases Teach Us?

These incidents show that cyberattacks can cause financial losses, data theft, service disruptions, and loss of trust. Reported figures must be interpreted carefully, as complaints, financial losses, and affected individuals do not always indicate confirmed harm. Individuals and organisations must remain vigilant and take proactive steps to protect sensitive information. Awareness, strong security practices, and timely reporting are essential for a safer digital world.

5. Cyber Security in the Age of Social Media

Social media platforms have become an important part of modern life. They help us connect with friends, share experiences, learn new things, and express our ideas. However, careless use of social media can expose users to privacy risks, fake profiles, cyberbullying, online scams, and identity theft.

Sharing too much personal information, accepting unknown friend requests, and clicking on suspicious links can put users at risk. Cybercriminals may use publicly available information to create convincing scams or impersonate someone.

To stay safe on social media, users should make their accounts private when appropriate, review privacy settings regularly, avoid sharing sensitive information publicly, and report suspicious accounts. Students and young internet users should also understand that online actions can have lasting consequences.

Think before you click, think before you share, and always protect your digital identity. Using strong passwords and enabling two-factor authentication can further help protect social media accounts from unauthorised access.

6. Cyber Security: A Shared Responsibility

Cyber security is a shared responsibility involving individuals, families, educational institutions, businesses, governments, and technology providers. Organizations must protect their systems and customer information, while individuals must follow safe online practices.

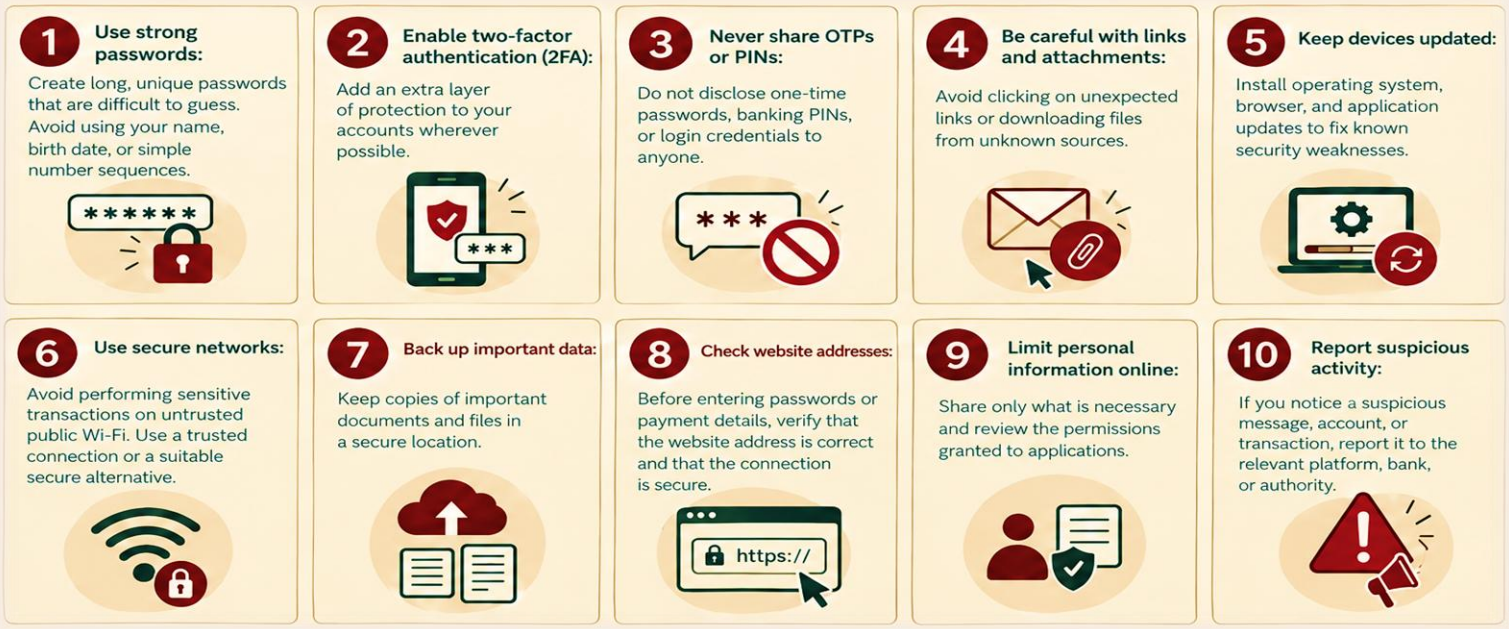
Educational institutions can play a major role by organizing cyber awareness programmes, workshops, seminars, and practical demonstrations. Students should learn how to identify online scams, protect their accounts, respect digital privacy, and report cyberbullying.

Parents and teachers can guide children in using technology responsibly. Organizations can train employees to recognize phishing attempts and follow security procedures. Governments and law enforcement agencies also help by developing cybercrime policies, investigating offences, and promoting public awareness.

A secure digital world can be built only when everyone takes cyber security seriously.

7. Essential Cyber Security Tips for Everyone

Practising a few simple habits can significantly improve online safety.



Remember, cyber security is not achieved through technology alone. Awareness, caution, and responsible behaviour are equally important.

8. What Should You Do If You Become a Victim of Cybercrime?

Even careful internet users can sometimes become victims of cybercrime. Acting quickly can help reduce the damage.



Do not feel ashamed or remain silent if you experience cybercrime. Reporting incidents helps authorities respond and may prevent others from becoming victims.

9. Conclusion

Cyber security has become one of the most important requirements of the modern digital age. As technology continues to develop, cyber threats are also becoming more sophisticated. Protecting our digital identity, personal information, and online accounts requires continuous awareness and responsible behaviour.

Real-world cyberattacks demonstrate that the consequences can extend far beyond a single device or individual. From financial scams to large-scale data breaches, the damage can affect millions of people and disrupt essential services.

Every click, download, password, and online interaction can affect our digital safety. By using strong passwords, enabling two-factor authentication, recognizing suspicious messages, keeping devices updated, and reporting cybercrime, we can reduce many common risks.

A safer internet begins with informed users. Let us make cyber security a daily habit rather than an occasional concern.

"Think Before You Click. Protect Before You Connect."

Stay alert. Stay informed. Stay cyber secure!

References and Further Reading

1. FBI — *2025 Internet Crime Report: https://www.fbi.gov/file-repository/2025_ic3report*.pdf
2. FBI — *Cryptocurrency and AI Scams Bilk Americans of Billions*: https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions
3. US Department of Health and Human Services — *Change Healthcare Cybersecurity Incident FAQs:* https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html
4. Press Information Bureau, Government of India — *Assistance to States to Tackle Cyber Incidents*: https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2244504
5. National Cyber Crime Reporting Portal, India: https://cybercrime.gov.in

Note: All statistics are based on the cited reports and their stated reporting periods. Figures may change as investigations and official reporting continue.

****

Athira Unnikrishnan
HR Manager, Head- 1 Assurance and Consulting
Email ID: unnikriishnanathira123@gmail.com



FORENSIC ACCOUNTING: BEYOND THE NUMBERS

Uncovering financial irregularities, tracing transactions, and strengthening trust in the world of business.



1. Introduction: When Numbers Tell a Different Story

Every financial transaction leaves behind a trail. An invoice, a bank transfer, a journal entry, or a change in an accounting record may appear routine when examined individually. However, when viewed collectively, these transactions can reveal inconsistencies, concealed relationships, or patterns that warrant further investigation.

In an increasingly complex business environment, financial irregularities are not always obvious. They may be concealed within seemingly legitimate transactions, supported by incomplete documentation, or spread across multiple accounts and reporting periods. Traditional accounting procedures may record these transactions without necessarily revealing the underlying circumstances.

This is where **forensic accounting** comes into play.

Forensic accounting is the application of accounting knowledge, auditing techniques, financial analysis, and investigative procedures to examine financial matters, identify potential irregularities, and establish facts supported by evidence. The term forensic refers to the use of investigative findings in contexts where they may be relevant to legal proceedings, disputes, regulatory inquiries, or internal disciplinary action.

Forensic accounting extends beyond identifying whether the figures in financial statements agree. It seeks to understand how those figures arose, whether the underlying transactions are genuine, where the money moved, and whether the available evidence supports the recorded financial information.

2. Forensic Accounting vs. Traditional Auditing

Although forensic accounting and auditing share several techniques, their objectives and scope are different.

A statutory audit is primarily intended to obtain reasonable assurance that financial statements are free from material misstatement, whether due to fraud or error, and to express an opinion on those statements. It is not designed to guarantee the detection of every instance of fraud.

Forensic accounting, on the other hand, is generally undertaken to investigate a specific suspicion, allegation, financial discrepancy, or dispute. The scope is tailored to the matter under investigation, and the work may involve detailed examination of individual transactions, tracing of funds, review of electronic records, and reconstruction of financial events.

For example, a routine audit may identify an unusual increase in expenses or a difference between inventory records and physical stock. A forensic investigation may go further by examining the underlying invoices, verifying the existence of suppliers, tracing payments to their ultimate recipients, reviewing approval records, and determining whether the available evidence indicates an error, control failure, or possible fraud.

Thus, forensic accounting does not replace statutory auditing. Rather, it serves a distinct investigative purpose and may complement an audit when specific concerns arise.

3. Areas Where Forensic Accounting Makes a Difference

Forensic accounting is relevant across businesses of different sizes and sectors. Some of its principal applications include:

a. Financial Statement Fraud

Financial statements may be deliberately manipulated to present a stronger financial position than actually exists. This could involve premature revenue recognition, recording fictitious sales, understating liabilities, overstating inventory, or capitalising expenses that should have been charged to the statement of profit and loss.

Forensic accountants examine supporting documents, transaction dates, subsequent receipts, journal entries, and related records to determine whether reported figures are adequately supported.

b. Misappropriation of Assets

Misappropriation may involve unauthorised withdrawals, diversion of collections, misuse of company funds, theft of inventory, or personal expenditure charged to the business.

Tracing bank transactions, reconciling receipts, examining expense claims, and comparing accounting records with independent evidence can help identify suspicious movements of funds or assets.

c. Procurement and Vendor Fraud

Procurement fraud may involve fictitious vendors, duplicate invoices, inflated prices, false purchase orders, and conflicts of interest. Investigations include verifying vendors, matching invoices with purchase orders and delivery records, analysing payments, and identifying employee–supplier connections.

d. Employee and Payroll Fraud

Irregularities may arise through fictitious employees, duplicate salary payments, unauthorised reimbursements, manipulated attendance records, or inflated expense claims. Examining payroll data, employee records, bank details, and approval workflows can help uncover inconsistencies.

e. Corporate Disputes and Financial Losses

Forensic accounting is useful in shareholder disputes, partnership disagreements, suspected diversion of business opportunities, contractual claims, and disputes concerning the calculation of financial losses. It can assist in reconstructing transactions and quantifying losses, as supported by the evidence and methodology used.

4. The Forensic Investigation Process

A forensic investigation requires a systematic approach to ensure that the findings are objective, traceable, and supported by reliable evidence.

Step 1: Understanding the Concern
The investigator first understands the nature of the allegation, the business environment, the relevant parties, and the period under review. The scope and objectives are defined to ensure that the investigation addresses the specific issues involved.

Step 2: Collection and Preservation of Evidence
Relevant records may include ledgers, invoices, bank statements, contracts, emails, inventory registers, payroll records, and electronic accounting data. These records must be collected and preserved appropriately. Where electronic evidence is involved, maintaining its integrity and documenting how it was obtained are particularly important.

Step 3: Financial and Data Analysis
The collected information is analysed to identify unusual patterns, inconsistencies, duplicate transactions, unexplained adjustments, and deviations from normal business activity.

Analytical techniques may include trend analysis, ratio analysis, transaction matching, bank reconciliation, examination of journal entries, and tracing funds across accounts. Digital tools can assist in analysing large volumes of transactions and identifying patterns that may not be apparent through manual review.

Step 4: Verification and Corroboration
An unusual transaction is not necessarily fraudulent. It may result from a genuine accounting error, a timing difference, an incomplete record, or an authorised business decision.

Accordingly, potential irregularities must be verified through supporting documents, independent confirmations, explanations from relevant personnel, and other available evidence. Conclusions should not extend beyond what the evidence reasonably establishes.

Step 5: Reporting the Findings
The final report generally sets out the scope of the engagement, procedures performed, evidence examined, observations, financial implications where determinable, and limitations encountered. It should distinguish established facts from suspicions, assumptions, and matters requiring further investigation.

Depending on the circumstances, the findings may assist management in taking corrective action, support dispute resolution, or be considered in legal or regulatory proceedings. A clear, well-documented report also helps ensure transparency, accountability, and informed decision-making

5. Red Flags: What Businesses Should Watch For

Financial misconduct often leaves behind warning signs, although no single indicator proves that fraud has occurred. Management and finance teams should pay attention to:

- Frequent manual journal entries, particularly near the financial year-end, without adequate supportings.
- Repeated payments to the same vendor involving similar invoice numbers or amounts.
- Significant differences between physical inventory and accounting records.
- Unusual transactions with related parties or suppliers whose ownership and relationships are unclear.
- Unexplained changes in bank reconciliations, customer balances, or vendor balances.
- Missing invoices, altered documents, or gaps in the transaction trail.
- Payments made outside established approval procedures or transactions split to avoid authorisation limits.
- Unusual accounting adjustments or changes to records without a clear audit trail.

These indicators should prompt appropriate verification rather than immediate conclusions. A sound investigative approach considers the circumstances, supporting evidence, possible explanations, and financial significance of each observation.

6. Technology and the Changing Face of Forensic Accounting

As businesses increasingly rely on digital accounting systems, online payments, cloud-based records, and automated transaction processing, forensic accounting is evolving beyond the examination of physical documents.

Data analytics can help identify duplicate payments, unusual transaction frequencies, unexpected relationships between vendors and employees, and deviations from established transaction patterns. Digital forensic techniques may also assist in examining system logs, access records, and changes made to electronic information.

However, technology is only an aid to investigation. The quality of the conclusions depends on the reliability of the underlying data, the suitability of the analytical methods, and the professional judgement applied in interpreting the results. An unusual pattern identified by software must still be examined in its business context.

7. The Role of Chartered Accountants

Chartered Accountants possess a strong foundation in accounting, auditing, taxation, financial reporting, internal controls, and regulatory compliance. These skills provide a valuable basis for forensic accounting assignments.

Depending on their expertise and the scope of engagement, Chartered Accountants may assist in tracing transactions, reviewing financial records, identifying control weaknesses, analysing suspected misstatements, quantifying financial losses, and preparing evidence-based reports.

Forensic engagements also demand professional skcepticism, objectivity, confidentiality, careful documentation, and independence of judgement. Where the matter involves specialised digital evidence, legal interpretation, or other technical issues, collaboration with appropriately qualified professionals may be necessary.

Importantly, the role of a forensic accountant is not to presume wrongdoing but to investigate impartially and report findings supported by evidence.

8. From Investigation to Prevention

Forensic accounting is valuable not only after an irregularity has occurred but also in helping organisations strengthens their preventive measures.

Businesses can reduce the risk of financial misconduct by establishing clear authorisation limits, segregating responsibilities, conducting regular bank and ledger reconciliations, verifying vendors, maintaining proper supporting documentation, and restricting access to accounting systems. Periodic internal audits and effective whistle-blower mechanisms can further help identify concerns at an early stage.

A strong internal control environment does not eliminate every risk, but it reduces opportunities for misconduct and improves the likelihood that irregularities will be detected promptly.

9. Conclusion: Trust Must Be Supported by Evidence

In business, financial information is more than a collection of figures. It reflects transactions, decisions, responsibilities, and the integrity of the systems through which an organisation operates.

Forensic accounting provides a structured way to examine that information when questions arise. By combining accounting expertise with investigative discipline, it helps organisations understand financial irregularities, evaluate evidence, assess potential losses, and address weaknesses in their control systems.

Ultimately, the significance of forensic accounting lies not merely in uncovering what went wrong, but also in helping businesses understand why it happened and how similar situations can be prevented.

When financial integrity is at stake, the objective is not simply to follow the money, but to establish the facts behind every significant transaction.

****

Theresa Nileena N.S
Articled Assistant
Email ID: rojanilin@gmail.com



Trademark Registration in India: From Distinctiveness to Examination Objections

An analysis of distinctiveness, classification, trademark symbols, examination objections and statutory timelines

1. Introduction

In a competitive business environment, a trademark is more than a name, logo or visual identity. It helps consumers identify the commercial source of goods or services and represents the goodwill associated with a business. Protecting that identity is therefore an important part of a business's intellectual-property strategy.



In India, trademark registration is principally governed by the Trade Marks Act, 1999 and the Trade Marks Rules, 2017. Filing an application does not guarantee registration. An application may face objections relating to distinctiveness, similarity with earlier marks, classification, the description of goods or services, or inconsistencies in the mark's representation. A careful filing strategy can reduce avoidable objections and help the applicant define the protection actually required.

2. What Constitutes a Trademark?

Section 2(1)(zb) of the Trade Marks Act, 1999 defines a trademark as a mark capable of graphical representation and capable of distinguishing the goods or services of one person from those of others. The definition covers, among other things, words, letters, numerals, devices, logos, shapes and combinations of colours, subject to the statutory requirements.

Common forms include a word mark (the name or word itself), a device mark (a logo or graphic), and a composite mark (a combination of wording and visual elements). These are not interchangeable. An application for a word in plain characters does not necessarily provide the same protection as an application for a particular stylised logo. Applicants should decide whether they need protection for the name, the logo, or both; separate applications may be appropriate where both are commercially important.

3. Why the Correct Class Matters

Sections 7 and 18 of the Act, read with Rule 20 of the Trademarks Rules, 2017, use the International Classification of Goods and Services, commonly known as the Nice Classification. Classes 1–34 generally cover goods, while Classes 35–45 cover services. The class is not merely an administrative label: it helps define the goods or services for which registration is sought and the practical scope of the application.

Choosing the correct class begins with the business's actual or intended activities, not simply its industry name. For example, downloadable software may fall in Class 9, while software development or software-as-a-service activities may fall in Class 42; retail or business-related services may require consideration of Class 35. A business selling solar panels and also providing installation or technical services may need to examine more than one class. The precise specification must be checked against the current Nice Classification and the actual business model.

An incorrect or overly narrow specification may leave commercially important goods or services outside the requested protection. An unnecessarily broad specification can invite objections or create difficulties if the applicant cannot justify the range of goods or services. A single application may cover multiple classes, but the prescribed fee applies class-wise. Rule 23 also allows the Registry to require a restriction or amendment where goods or services fall in additional classes.

Classification does not decide similarity by itself. Goods or services in different classes may still be considered similar or commercially related, while items in the same class are not automatically similar. In a Section 11 analysis, the nature of the goods or services, their purpose, trade channels, consumers and the overall likelihood of confusion remain important. The official class headings and descriptions should therefore be used as a starting point, not as a substitute for legal analysis.

4. The Meaning and Use of ™ and ®

The symbols ™ and ® communicate different things. The ™ symbol is commonly used to indicate that a business is claiming a word, name or logo as a trademark. It may be used even while an application is pending or where the mark is unregistered, provided the presentation is not misleading. The symbol itself does not confer registration or create the statutory rights of a registered proprietor.

The ® symbol indicates that the mark is registered. It should be used in India only when the relevant mark is actually registered and only in relation to the goods or services covered by that registration. Registration of a logo does not automatically mean that every word appearing in it is separately registered, nor does registration for one class mean that the mark is registered for all classes.

Section 107 of the Act prohibits falsely representing a mark as registered, including representing an unregistered part of a registered mark as separately registered or suggesting that registration covers goods or services outside the actual registration. Contravention may attract imprisonment of up to three years, or fine, or both. Accordingly, applicants should generally use ™ before registration and reserve ® for a valid registration covering the relevant goods or services. The status should be checked before symbols are added to packaging, websites, invoices or promotional material.

5. Trademark Registration Process

The usual process involves: (1) searching existing marks; (2) identifying the correct mark format and class or classes; (3) filing Form TM-A with the prescribed fee and specification; (4) examination by the Registry; (5) responding to objections and attending a hearing, if required; (6) acceptance and publication in the Trademarks Journal; (7) possible opposition by a third party; and (8) registration if the legal requirements are satisfied and no opposition prevents it.

The application should accurately identify the applicant, the mark, the goods or services, and whether the mark is used or proposed to be used. Evidence supporting a claim of prior use should be retained and submitted where required. The application representation is particularly important for device and composite marks because it helps determine what the applicant is asking the Registry to protect.

6. Absolute Grounds: Section 9

Section 9 deals with absolute grounds for refusal, including lack of distinctive character, descriptive indications and expressions that have become customary in trade. Section 9(1)(b), for example, concerns marks consisting exclusively of indications that may designate the kind, quality, intended purpose, geographical origin or other characteristics of goods or services.

A descriptive element does not necessarily mean that every mark containing it must be refused. The statutory test and the mark as a whole must be considered. Evidence that a mark acquired distinctiveness through use may be relevant where the statutory requirements are met. Applicants should avoid relying only on assertions that a mark is unique; arguments should explain how the mark functions as a badge of commercial origin and should be supported by appropriate evidence where necessary.

7. Relative Grounds: Section 11

Section 11 addresses conflicts with earlier trademarks and other specified earlier rights. Under Section 11(1), the Registry considers the relevant similarity or identity of the marks and goods or services and whether confusion or association is likely.

Assessment is based on the overall impression of the competing marks. Relevant considerations can include visual, phonetic and conceptual similarity; the distinctive and dominant features of each mark; the nature of the goods or services; relevant consumers; and the circumstances in which purchases are made. A difference in colour or font does not automatically eliminate confusion, and a shared descriptive element does not automatically establish it. The facts and the applicable legal test must be addressed separately from any Section 9 objection.

8. Amendments and Representation of the Mark: Section 22

Section 22 empowers the Registrar, on appropriate terms, to permit correction of an error or an amendment to an application. It is not an unrestricted right to replace the mark originally filed with a materially different mark. Where the written particulars and the uploaded representation do not match, the applicant should first identify the precise inconsistency and consider whether it can be corrected without changing the identity or scope of the mark.

Correcting a genuine clerical error is different from replacing a word mark with a new logo or changing a composite mark into a device-only mark. The original application, its representation and the objection must be examined before deciding whether a request such as Form TM-M is appropriate. Applicants should not assume that a clarification can override the original representation or expand the application beyond what was filed.

9. Responding to an Examination Report

An examination report should be answered objection by objection. First, distinguish absolute grounds, relative grounds and procedural requirements. Secondly, verify the cited marks, their status, proprietor, filing dates and specifications. Thirdly, develop evidence-based arguments on distinctiveness, confusion, prior use or acquired distinctiveness where relevant. Finally, comply with any procedural requirement relating to representation or classification using the appropriate prescribed form, where applicable.

For a Section 9 objection, explain why the mark is not exclusively descriptive or why it is capable of distinguishing the applicant's goods or services. For a Section 11 objection, compare the marks as a whole and address the relevant goods or services and likelihood of confusion. A procedural objection about the device representation or NICE specification should be dealt with separately; it should not be assumed that an argument on distinctiveness resolves a formal defect.

If the Registry is not satisfied with the written response, a hearing may be scheduled. The applicant should monitor notices and attend as directed. Rule 33(4) is particularly important: failure to respond within one month from receipt of the examination report may result in the application being treated as abandoned.

10. Statutory Timelines: A Practical Checklist

Trademark proceedings are deadline sensitive. The following are key statutory or rule-based periods under the Trademarks Act, 1999 and Trademarks Rules, 2017. The date of receipt or service specified in the relevant provision should be recorded carefully, and the current Registry notice and applicable Rules should always be checked.

Stage	Time limit	Legal reference / practical note
Reply to examination report	One month from receipt of the report	Rule 33(4), Trade Marks Rules, 2017. If no response is filed, the Registrar may treat the application as abandoned.
Notice of opposition	Within four months from publication in the Trade Marks Journal	Section 21(1). Monitor the Journal publication date; opposition is not automatic.
Counterstatement to opposition	Within two months from receipt of the opposition copy	Section 21(2). Failure to file within the prescribed period may result in the application being deemed abandoned.
Opponent's evidence / statement of reliance	Within two months from receipt of the counterstatement	Rule 45. Failure to act within the period may result in the opposition being deemed abandoned.
Applicant's evidence / statement of reliance	Within two months from receipt of the opponent's evidence or intimation	Rule 46. Check the applicable service date and procedural directions.
Opponent's reply evidence	Within one month from receipt of the applicant's evidence	Rule 47; generally limited to evidence in reply.
Renewal of registration	Every ten years; renewal can be sought within the prescribed period before expiry	Section 25. Monitor the expiry date and file the prescribed renewal request and fee in time.

11. Common Mistakes to Avoid

- Filing without searching for earlier marks and missing examination, opposition, evidence or renewal deadlines.
- Selecting classes based on industry rather than specific goods or services
- Assuming logo protection covers the word, or word protection covers all stylised versions.
- Using ® before registration or in relation to goods or services not covered by the registration.
- Assuming that marks in different classes can never conflict.
- Making unsupported claims about prior use or acquired distinctiveness.
- Treating Section 9 and Section 11 as the same objection.
- Changing the mark representation without checking the limits of Section 22 and the original filing.

12. Conclusion

The Trade Marks Act, 1999 and Trade Marks Rules, 2017 protect commercial identity while balancing the interests of applicants, proprietors and consumers. Effective protection requires selecting the right mark and classes, conducting a proper search, and using ™ and ® correctly. Examination objections must be addressed with sound legal reasoning and reliable evidence, while adhering to statutory deadlines and amendment limits. A successful trademark strategy combines commercial planning with legal compliance throughout registration.

Official references

- Trade Marks Act, 1999 — especially Sections 2(1)(zb), 7, 9, 11, 18, 21, 22, 25 and 107.
- Trade Marks Rules, 2017 — especially Rules 20, 23, 33 and 45–47.
- IP India, "Basics of Trademarks" and "Filing Process (Step-by-Step)".
- Official legislation and current forms should be checked on the IP India website.

****

Anish C Kamath
Head- 2 Assurance and Consulting, IT Manager
Email ID: anishckamath191@outlook.com



Did Maruti's Ads Build Suzuki's Brand?

Transfer Pricing Corner

When an Indian company's advertising builds a foreign parent's brand, should the parent pay for it? India's tax department said yes. The courts have said no, so far.

Every Maruti car on Indian roads carries the Suzuki "S" on its bonnet. So when Maruti spends crores on TV ads, billboards and dealer campaigns, whose brand is it really building: Maruti's in India, or Suzuki's in Japan?



For more than a decade, the Income Tax Department argued that part of that money built Suzuki's brand, and that Suzuki should have compensated Maruti for it. If Suzuki did not, the "missing" compensation was income India had lost.

The question sounds simple, but it has produced one of India's longest-running transfer pricing battles. It touches every Indian company that sells under a foreign group's name: cars, phones, appliances, cosmetics, even eyewear

The Facts

Maruti Suzuki India Ltd (MSIL) is the Indian company of Japan's Suzuki Motor Corporation (SMC). MSIL manufactures cars under a licence from SMC, using SMC's technology, and pays royalty for it. Its cars carry the co-branded trademark "Maruti-Suzuki".

Like any car maker, MSIL spends heavily on **advertisement, marketing and sales promotion (AMP)**. The Transfer Pricing Officer (TPO) looked at that spend and reasoned as follows:

1. MSIL spends proportionately more on AMP than comparable Indian companies.
2. Its ads display the Suzuki name and logo.
3. So the "extra" spend must have promoted the Suzuki brand, which SMC owns.
4. SMC never paid MSIL for this service, so an arm's length compensation should be added to MSIL's income.

For the year that reached the Delhi High Court in 2015, the adjustment on account of AMP was **₹154.12 crore**. Royalty paid by MSIL to SMC was examined separately under transfer pricing; this adjustment was purely for advertising.

The Weapon: The "Bright Line Test"

The Department's tool was the **Bright Line Test (BLT).** It compares a company's AMP spend, as a share of sales, with what comparable independent companies spend. Anything above that line is presumed to have been spent for the foreign brand owner.

The test does two jobs at once. It creates an international transaction where no agreement exists, and then it measures that transaction. That double role is exactly what the courts objected to.

A simple illustration:

Particulars	Amount
Sales of Indian company	₹10,000 crore
AMP actually spent	₹400 crore (4%)
Average AMP of comparables	2.5% of sales
"Bright line" (2.5% × ₹10,000 crore)	₹250 crore
Excess treated as brand-building for foreign AE	₹150 crore
Adjustment = excess + a mark-up for the "service"	₹150 crore + mark-up

Fifteen Years in Court

The pendulum has swung twice, and it has not stopped yet.

When	Forum	What happened
2010	Delhi High Court (Maruti, first round)	Held that AMP spend above what comparables spend could be an international transaction. The Supreme Court later disposed of the appeal, leaving the core question open.
2013	ITAT Special Bench (LG Electronics)	Inferred a tacit understanding with the foreign parent from proportionately higher AMP spend, and approved the Bright Line Test.
Mar 2015	Delhi High Court (Sony Ericsson)	Held that the law does not provide for the Bright Line Test. Overruled LG Electronics to that extent.
Dec 2015	Delhi High Court (Maruti, second round)	The decisive blow: excess AMP spend does not prove an international transaction exists.
Nov 2024	Supreme Court	Rejected the Department's petition against the Whirlpool of India ruling on the same issue.
Aug 2026	Delhi High Court (Suzuki Motorcycle India)	Dismissed the Department's appeals again, following Sony Ericsson and Maruti.

What the Delhi High Court said in Maruti (2015):

- Prove it, don't presume it. The Department must show an international transaction exists from facts, not deduce it from how much was spent.
- The Bright Line Test cannot be used even to find a transaction, let alone to price it, because the law has no machinery for it.
- Brand value has many causes. A brand's worth depends on many factors. Higher ad spend alone does not prove the foreign owner gained.
- Incidental benefit is not a transaction. That Suzuki's brand also gains from Maruti's ads does not mean Maruti rendered Suzuki a service.

Where it stands today: the Department's appeal against the Maruti and Sony Ericsson rulings is still pending in the Supreme Court, with no stay. The Delhi High Court keeps ruling for taxpayers, but its recent orders say that if the Supreme Court decides otherwise, that ruling will apply to these cases too. So the final word is still to come.

The Other Side: AMP as a Tax Planning Tool, and Where BEPS Draws the Line

The AMP dispute is not only about what the Department can tax. It also shows how multinational groups decide where brand profits sit. Who owns the brand, who pays to build it and who keeps the returns are all choices a group can make, within limits.

How groups have structured it

- **Brand in a low-tax hub.** The trademark is owned by a group company in a low-tax country. Operating companies in high-tax countries pay it royalty and also bear local marketing costs. The brand's value grows; the profit from it is booked where tax is lowest.
- **Licensed manufacturer or full-risk distributor.** The Indian company is described as an entrepreneur that bears its own AMP for its own sales. Higher AMP lowers Indian profit, while the brand-owner gains value without paying for it. This was exactly the Department's suspicion in Maruti.
- **Limited-risk distributor.** The reverse model. The parent reimburses AMP or guarantees the Indian company a fixed routine margin. India taxes a small but stable profit; the brand returns go to the parent.
- **Royalty plus AMP.** The Indian entity pays royalty for using the brand and also pays to promote it. Together these can move a large share of profit out of India.

Planning vs evasion

As our September issue put it, tax planning works within the law and tax evasion works against it. Choosing a business model is legitimate planning, if the contracts, the conduct and the profits all match. A limited-risk distributor must actually have its risks borne by the parent; an entrepreneur must actually make its own marketing decisions. Where paper says one thing and conduct shows another, the structure fails, both under Indian TP rules and under BEPS.

Where BEPS draws the line

The OECD's Base Erosion and Profit Shifting (BEPS) project, Actions 8 to 10 and the revised Transfer Pricing Guidelines (Chapter VI), changed the question. Legal ownership of a brand is no longer enough to claim its returns. Returns must follow the people who actually perform and control the DEMPE functions: Development, Enhancement, Maintenance, Protection and Exploitation of the intangible.

- **Substance over paper.** A brand-owning company with no staff making marketing decisions cannot keep the brand profit, even if it holds the trademark.
- **Marketing intangibles.** If a local company performs AMP beyond what an independent distributor would, it may be entitled to extra return or to a share of the intangible's value. This is the OECD's answer to the very question the Bright Line Test tried to answer.
- **Global minimum tax.** Under Pillar Two, large groups (consolidated revenue of €750 million or more) pay at least 15% in each country. Parking brand profit in a near-zero-tax hub gains much less than before.
- **Anti-abuse rules.** India's General Anti-Avoidance Rule and the Principal Purpose Test that India adopted through the Multilateral Instrument (MLI) can deny benefits where obtaining a tax benefit was a main purpose of an arrangement.

What It Means for You in 2026

From 1 April 2026, transfer pricing has moved from Sections 92-92F of the 1961 Act to Sections 161-173 of the Income-tax Act, 2025. From Tax Year 2026-27, Form 48 replaces Form 3CEB and asks for transactions reported for each associated enterprise (AE) separately. The section numbers have changed; the AMP question has not been settled.

Transfer pricing sections: old Act vs new Act

Provision	Income-tax Act, 1961	Income-tax Act, 2025
Arm's length price for international transactions	Section 92	Section 161
Meaning of associated enterprise	Section 92A	Section 162
Meaning of international transaction	Section 92B	Section 163
Specified domestic transactions	Section 92BA	Section 164
Computation of arm's length price	Section 92C	Section 165
Reference to Transfer Pricing Officer	Section 92CA	Section 166
Safe harbour	Section 92CB	Section 167
Advance Pricing Agreement	Section 92CC	Section 168
Modified return after APA	Section 92CD	Section 169
Secondary adjustment	Section 92CE	Section 170
TP documentation (Local File / Master File)	Section 92D	Section 171
Accountant's report	Section 92E (Form 3CEB)	Section 172 (Form 48)
Definitions	Section 92F	Section 173
Thin capitalisation (interest limit)	Section 94B	Section 177
Dispute Resolution Panel	Section 144C	Section 275
Penalty: failure to keep TP documents	Section 271AA	Section 442
Penalty: failure to furnish accountant's report	Section 271BA	Section 447
Penalty: failure to furnish documents to TPO	Section 271G	Section 457
Country-by-Country Reporting	Section 286	Section 511

Mapping as per ICAI's tabular mapping of the two Acts.

If your client sells under a foreign group's brand, these steps reduce the risk:

1. **Read the licence agreement.** Check who owns the brand, what the Indian company pays for, and who bears marketing costs. A clear clause that the Indian entity bears AMP for its own sales is the first line of defence.
2. **Keep the purpose on record.** Campaign briefs, board approvals and agency contracts should show the spend was aimed at Indian customers and Indian sales.
3. **Separate selling costs from brand-building**. Trade discounts, dealer incentives and sales commissions push sales; they are not brand-building and should not be lumped into "AMP".
4. **If the AE pays, report it**. Where the foreign parent reimburses or co-funds marketing, there is a real international transaction. Benchmark it and report it.
5. **Watch the Supreme Court**. Clients with past AMP additions should keep the issue alive in appeal and consider whether a contingent liability disclosure is needed.
6. **Auditors and TP certifiers, ask the question**. Does the client display a foreign group's brand? Is there any arrangement, written or unwritten, about marketing costs?

Key Takeaway

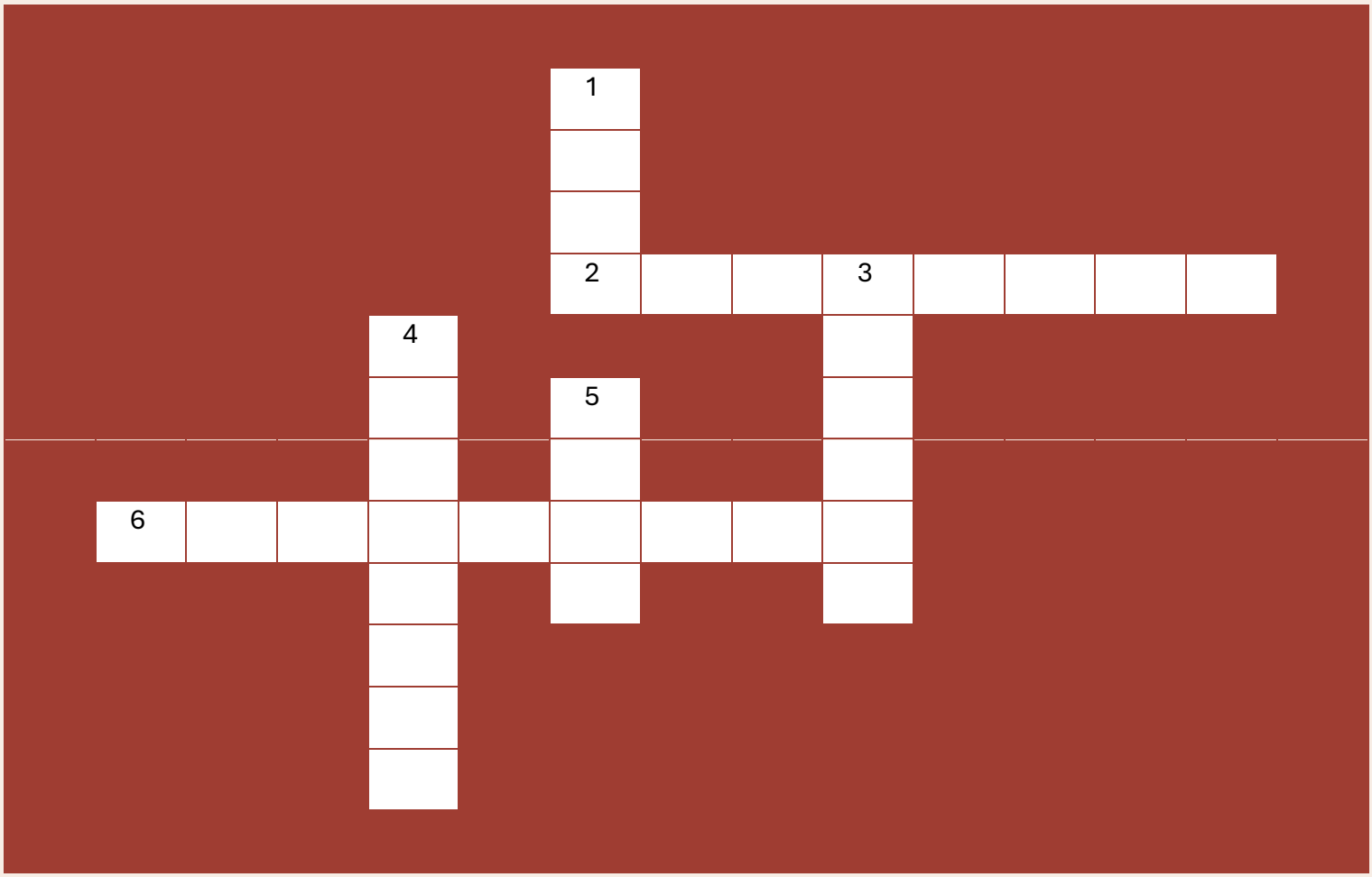
An Indian company's advertising may well make a foreign brand stronger. Under Indian law as the Delhi High Court reads it, that alone does not create a taxable international transaction. The Department must prove an arrangement; it cannot infer one from how much was spent. Until the Supreme Court speaks, good contracts and good records are the best protection.

Did you know? The same issue has been argued for brands across many industries, including mobile phones, appliances, cosmetics and two-wheelers. Suzuki's own motorcycle company won its case in the Delhi High Court as recently as August 2026.

****

Crossword

Six clues - one from each feature in this edition



CLUES

ACROSS

2. What is the name of a deceptive message or website designed to steal sensitive information?

6. What is the legal term for a sign that distinguishes one business's goods or services from another's?

DOWN

1. What is the abbreviated name of the insolvency resolution process for a distressed corporate debtor?

3. Which Japanese automotive company's brand is central to the article on Maruti's advertising and transfer pricing?

4. What must support investigative findings and help establish the facts?

5. What is the acronym of India's Foreign Exchange Management Act?

The answers from last month's crossword are also included for reference to help you revise and track your progress.

ACROSS: 2-Memorandum, 6-Taxable income, 7-TDS, 9-Output tax, 10-CIN
DOWN: 1-Input tax credit, 3-FDI, 4-Tax return, 5-Remittance, 8-Auditor

BIRTHDAY CELEBRATION



sudeeksha

OCTOBER 2026 ISSUE – 10

e Newsletter from NITIN N & CO. Chartered Accountants

Thank you for reading

Scan here

For more