data sutram

FinSecure India

Demystifying Fraud to Empower Growth

AUGUST 2024

Contents

1

Foreword

We must approach fraud as we would approach viruses, diseases, or crimes—comprehensively and collaboratively. We need to accept that the problem of fraud is here to stay. It will only evolve with time, and technology alone will not be enough to stop it.

There is currently a gap in how quickly we react to fraud, and a lack of empathy in dealing with the problem. To solve for fraud then, there has to be a social movement combining AI, tech, the community, law, infrastructure, and more. Data Sutram's call to action is clear: Fraud is not an issue that any single entity can tackle alone. Organisations must invest in the latest technologies, like AI and machine learning, to stay ahead of fraudsters. At the same time, they should commit to industry collaboration, sharing intelligence and adopting best practices. Individuals must stay informed and vigilant, understanding that their role in fraud prevention is crucial. Together, we can create a resilient ecosystem.

This report aims to serve as both a wake-up call and a roadmap for businesses and consumers. It highlights the current landscape of fraud, the potential vulnerabilities in existing systems, and the economic impact of unchecked fraudulent activities. Additionally, the report shares the nature of the problem today, its magnitude, how it will evolve, and why a collaborative approach is essential to solving it. Key insights include the importance of adopting AI-driven fraud detection tools, the need for cross-industry data sharing, and the role of consumer awareness in fraud prevention.

Engage with our solutions, participate in the community, and be part of the movement that secures our financial future. The time to act is now.

Rajit Bhattacharya
Founder & CEO
Data Sutram

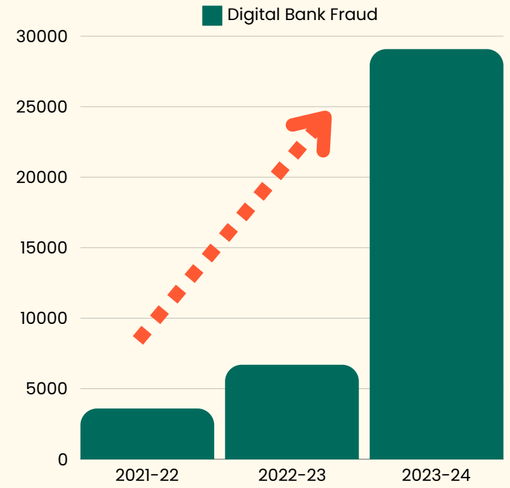
> India reports nearly 800 digital payment fraud cases daily.[1]

[1]

2

About the Report

With nearly 800 online fraud cases reported daily, the impact of financial fraud in India extends beyond monetary losses, eroding consumer trust in digital payment systems. At the juncture where India is fast-embracing digitalisation, addressing the challenges posed by digital fraud has become increasingly urgent for both consumers and financial institutions in India.



In 2023-24, the Reserve Bank of India reported nearly a 5-times increase in digital fraud cases seen in a fiscal year.[5]

According to RBI's Annual Report, card and digital payment fraud cases worth INR 1,457 Cr. were reported in 2023-24. For reference, in the years prior, the fraud reported amounted to INR 155Cr and INR 277 Cr. respectively. That is just calculating internet-based fraud above INR 1.00 Lakh. When we further consider frauds reported below INR 1 Lakh, one RTI response by RBI revealed that the total number of cases increases by 2.70 Lakh, amounting to transactions worth INR 653 Cr.

4.6% of all digital transactions globally are fraudulent, Estimated global losses from digital payment fraud in 2023 is $20 billion.[2]

51% of organisations have experienced fraud in the last two years, with 76% organizations experiencing an increase in financial crime activity in 2023.[3]

The global fraud detection and prevention market size was valued at USD 43.97 billion in 2023 and is projected to grow from USD 52.82 billion in 2024 to USD 255.39 billion by 2032.[4]

2.1 Scope of the Report

Hand in hand with the increase in digital transactions in India, which rose by 24% in value and 53% in volume, fraud incidents have surged, with a 65% increase in payment fraud cases in 2023, leading to financial losses exceeding Rs 1,200 crore. UPI frauds alone constituted around 40% of these incidents, highlighting vulnerabilities in popular digital payment methods. The rise in digital fraud results in substantial financial losses and undermines consumer trust, with 60% of consumers expressing hesitance to engage in online transactions following high-profile fraud cases. The imperative for banks and financial institutions is not just monetary but also about maintaining public trust in digital financial systems. Therefore, this report proposes viewing digital financial fraud as a social problem. By shifting our perspective from financial loss to social impact, we can consider more bottom-up solutions effective for both top financial institutions and the disenfranchised individual struggling to recover the INR 2000 lost in a phishing scheme.[7]

1 Reframing Financial Fraud as a Social Problem

- Shifting the focus of fraud from financial to social impact
- Consider the entire ecosystem while building a solution
- Radically re-imaginating how to combat fraud

2 Understanding Small-Scale Fraud Trends

- Providing insights into drivers of small-scale bank fraud
- Understanding the recent upsurge in fraudulent activities
- Identifying the "why" behind the growing problem

3 Adopting a Multi-Stakeholder Approach

- Identifying key stakeholders in combating financial fraud
- A case for breaking down silos between stakeholders
- Developing comprehensive, collaborative solutions

2.2 Methodology

The report employs a qualitative dominant mixed-methods approach to paint a holistic picture of small-scale financial fraud as a social problem.

- **Internal Insights:** The report utilizes insights from Data Sutram's AI-driven platform to detect fraudulent accounts, enhancing understanding of customer behavior and fraud patterns in the Indian financial landscape.
- **Literature Review of Secondary Quantitative Data:** A comprehensive review of industry reports, academic studies, and regulatory directives provides context on the scale and trends of financial fraud, highlighting key areas of concern across various sectors.
- **Qualitative Insights:** In-depth interviews with representatives from financial institutions and regulatory bodies reveal challenges and strategies in combating fraud, as well as the social implications of financial crime on consumers.

By employing this approach, the report aims to provide a comprehensive and nuanced understanding of small-scale financial fraud as a social problem, while also offering actionable insights and recommendations for stakeholders to develop effective, collaborative solutions.

3

Understanding Bank Fraud

3.1 What is bank fraud?

To understand digital fraud with relation to banks, we must take a step back to understand how banks have historically been perceiving financial fraud and their mitigation.

Financial Bank Fraud can be categorised into two types:

1. High Value Fraud: Refers to fraudulent activities that result in substantial financial losses, often involving large sums of money. This type of fraud can occur in various contexts, including investment scams, Ponzi schemes, and other sophisticated financial crimes.

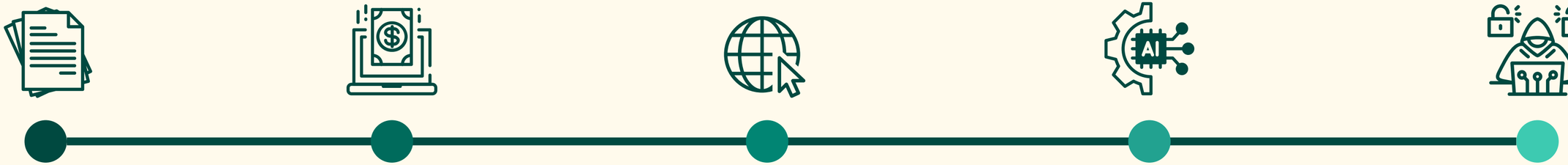
2. Small Value Fraud: Refers to fraudulent activities that involve relatively small amounts of money compared to high-value fraud. These types of fraud are often more frequent and can affect a larger number of victims, but each individual incident results in minimal financial loss.

	1. Size	2. Frequency	3. Nature
High Value Fraud	High-value fraud involves significant financial losses, often amounting to thousands or millions of dollars per incident, with examples including investment scams and corporate fraud.	High-value fraud generally occurs less frequently due to the complexity and planning involved, targeting larger institutions or high-net-worth individuals.	High-value fraud has impacts that can extend to shareholders and employees due to reputational damage and operational challenges.
Small Value Fraud	Small-value fraud typically results in smaller financial losses, usually ranging from a few dollars to several hundred dollars per incident, with common examples such as petty theft and minor credit card fraud.	Conversely, small-value fraud occurs much more frequently, with many incidents happening daily, often in an opportunistic manner, affecting a wide range of individuals and small businesses.	The cumulative effect of small-value fraud leads to substantial impacts on many individuals and increased costs for businesses in fraud prevention and management.

High Value Fraud has been existing for as long as financial institutions exist. However, the financial fraud landscape has undergone significant changes in the past decade, driven by advancements in technology, evolving fraud tactics, and increased regulatory scrutiny. Increased digitalisation has resulted in a drastic increase in small value fraud. This exponential increase, largely due to technological advancements, is of immediate interest.

3.2 The Changing Nature of Bank Fraud

To understand what has enabled bank fraud to increase so exponentially in the past few years, it is important to understand the modus operandi of bank fraud in the past few decades. Following is an overview of banking fraud over time, mapped to the changing technological landscape.



Before 1970s

Paper-Based Transactions

Fraud involved paper-based transactions, primarily through falsifying authentication and forgery.

1970s-1990s

Emergence of Digital Transactions

Emergence of digital transactions led to physical theft of credit cards and basic identity theft.

1990s -2000s

Rise of the Internet and E-Commerce

The rise of the internet saw phishing and fake websites tricking consumers into revealing sensitive information.

2000s-2010s

Automation and Advanced Technology

Fraudsters employed automated tools for credential stuffing and exploited cryptocurrencies for anonymous transactions.

2010-2020s

Increased Digitalisation & Creation of DPIs

Increased digitalization led to cyber-enabled fraud, with organized crime exploiting digital technologies and weak KYC policies.

3.3 Bank Fraud in 2024

Financial fraud is an overlapping concept, with blurred lines on intent, medium, jurisdiction, scale and nature of crime. Therefore, having narrowed down to ‘small-value’ bank fraud, and considering the changing nature of fraud due to evolving technology, we finally land at an intersection of financial fraud that has led to the current media panic, trust deficit and meteoric rise in financial fraud cases.

Digital Bank Fraud in 2024 can be broadly defined as any or all fraudulent activities perpetrated by external parties through digital means (eg. emails, websites, malicious software, etc.) with the aim of stealing banking assets or credentials of bank customers.

4 Key Aspects of Bank Fraud Today

Personalisation of Attack

Fraudsters increasingly use personalisation and social engineering, often involving publicly available information about victims to manipulate them.

Deception or falsification

Relying heavily on fake personas, elaborate ruses and schemes, the root is some form of high-stake social deception and falsification of identities.

Remote-Virtual Access

By its nature, bank fraud is committed remotely and/or virtually, relying on the difficulty in authentication over digital media.

Internal Collusion

Either consciously, or inadvertently, internal stakeholders end up facilitating or enabling fraudulent transactions.

Newspapers are constantly peppered with terms like phishing, ATOs, romantic scams. We get warnings about fake calls, suspicious links and virus that will steal our data, but to be able to solve for the various types of bank fraud, we need to be able to understand the source and nature of the problems itself. To further understand the nature of bank fraud on the basis of the four qualifiers mentioned previously, we can further categorise the major types of bank fraud prevalent today.

Online unauthorised payment transactions	Manipulation of the payer to issue a payment order online	Piggybacking on authentic brands or financial products	Manipulation of existing financial information/infrastructure
Phishing	Vishing	Fake Website Scams	Identity Theft
Malware	Social Engineering Techniques	Authorized Push Payment (APP) Fraud	Application Fraud
e-Transfer Interception Fraud	Imposter Scams	Digital Payment Fraud	Database Leak
Account Takeover	Business Email Compromise	Deep Fakes	False Promises

4

Understanding Fraud Solutions

4.1 Profiling Fraudsters

As the nature of fraud continues to evolve, a robust KYC process allows for ongoing monitoring and adaptation to new threats. This proactive approach not only safeguards the financial institution but also builds trust with customers, ensuring a safer and more secure financial environment. The Reserve Bank of India (RBI) has established key KYC rules to mitigate fraud risks, and as of 2023, has added additional amendments to the Master Directions on Fraud.[8]

As per the rules, banks must move beyond basic KYC to

1. Do customer due diligence at various intervals, and not just during account creation.
2. Verify customer identities using reliable independent sources.
3. Conduct ongoing due diligence to understand user behaviour and nature of transactions.
4. Proactively report suspicious activity.

Effective fraud profiling then requires more data points on top of the existing authentication layers, as well as a triangulation of the personal identifiers to be able to build a whole persona of a particular customer. By stockpiling digital footprints, then different fraud-prevention solutions aim to actually build an entire digital profile, thereby identifying their authenticity and behaviour.

Data Sutram's Trust Score today categorises and filters the authenticity of a particular application on the basis of numerous secondary identifiers, which help further understand the customer.

> Who are you onboarding? How well do you know the customer? This largely revolves around capturing the profile. Is it a person drawing a salary and doing a job, or a businessman running a shop? When you digitally authenticate documents, it doesn't give you the power to understand what lies beneath those numbers in terms of authenticity. Building a profile during onboarding is crucial. The RBI emphasizes Customer Due Diligence (CDD). In today's world, with aggressive business targets, many of these aspects get compromised, often resulting in not knowing the customer at all. This is the starting point, as failing to build a good profile can lead to significant issues.
>
> ***- Himadri Chatterjee***
> ***Former President, Axis Bank***

4.2 Combining Technology & Social Behaviour: Mule Accounts

The Indian banking sector, like many around the world, has been grappling with the issue of mule accounts used for money laundering. Mule accounts are essentially bank accounts that receive funds from illegal activities and then transfer them elsewhere, acting as a bridge in the laundering process.

These types of accounts constitute up to 55% of all fraud cases in India. Moreover, industry research suggests, bankers are unaware of 9 out of 10 of the mule accounts in their system.

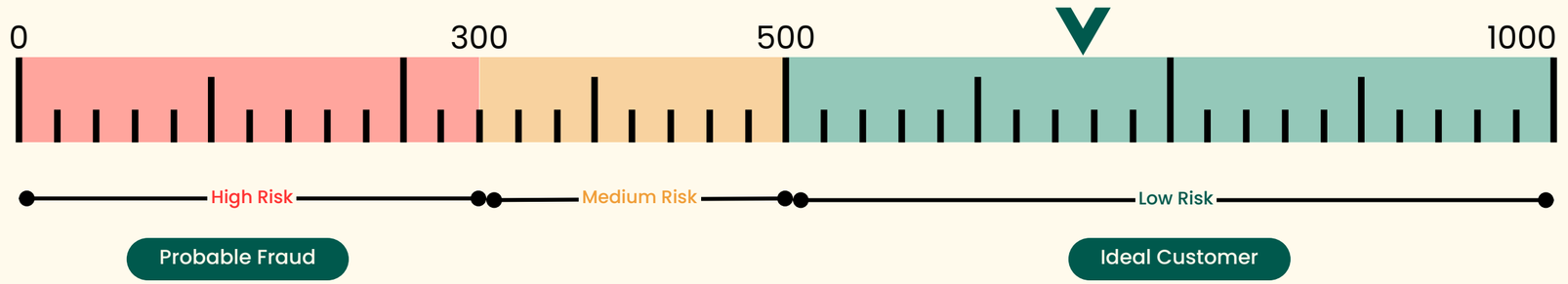
Mule accounts are a critical tool used by fraudsters to launder money and facilitate various financial crimes. These accounts are opened by individuals, either knowingly or unknowingly, and are used to transfer and obscure the origins of illicit funds. Sophisticated fraud networks often use stolen or synthetic identities to open mule accounts, making them difficult to trace back to the actual perpetrators. There are several types of mule accounts, including those opened intentionally by deceivers using stolen identities, accounts sold by peddlers to criminals, accounts used by accomplices who knowingly or unknowingly participate in the scheme, accounts of misled victims who believe they are engaging in legitimate business transactions, and accounts of victims whose accounts are compromised by fraudsters without their knowledge. Addressing mule account fraud requires targeted detection strategies and public awareness to prevent individuals from unknowingly participating in these schemes.

> Because of the emergence of this large pool of mule accounts and the ability of the fraudsters to devise newer methods in terms of defrauding, the banks and financial institutions need to stay a step ahead. As we get more into this data-rich world and everything happens digitally, the ability to build profiles and monitor transactions is the only way that financial institutions can probably have a better ability in terms of detecting and then clearly doing something about the prevention of mule accounts.
>
> *- Himadri Chatterjee,*
> *Former President, Axis Bank*

Case Study: DS Authenticate for Detecting Mule Accounts

Profiling mule accounts, and fraudsters requires multiple layers of data insights and intelligence, and also needs different approaches of combating, alerting and mitigating a possible fraud.

Data Sutram has developed a DS Trust Score as part of its product, DS Authenticate. The DS Trust Score runs from 0 to 1000, lower the score, higher the chances of the identity being a fraudulent one. On receiving an Identity (Name, Phone, Email & Other PII), DS Authenticate scrubs it across multiple open source data sources like Telco, digital platforms, logistics players, government sources, etc. and tries to create a complete view of the individual's persona. The score depends on the number of connections it can find across these platforms, building confidence against the identity.



While developing this scoring system to weed out mule accounts in banking systems, Data Sutram has gained insights into how different types of mule accounts have different levels of difficulty in detection at the application stage. Following is a case study of the telltale signs that can help red-flag a mule account, based on this scoring system.

Deceiver Mule Accounts

This type of mule intentionally opens accounts using stolen or synthetic identities to commit fraud. It is likely to operate a network with hundreds or thousands of mule accounts as part of a larger scam network.

What are the challenges in detecting this type of account?

Synthetic Identity Fraud:
Synthetic identities are challenging to detect because they blend real and fake information, making traditional verification processes less effective. Fraudsters exploit gaps in KYC procedures to pass as legitimate customers.

High Volume, Low-Value Transactions:
These Mule accounts often engage in high-frequency transactions involving small amounts. These transactions can easily bypass the radar of traditional fraud detection systems, which may focus on large, suspicious transfers.

Fraud Mitigation: dsTrustScore

Financial institutions can employ models like the DS Trust Score to assess the risk of mule accounts. This model leverages alternative data sources, including digital footprints, social media activity, and cross-referencing identity elements across a closed user group association, to detect anomalies that may indicate synthetic identities or coordinated fraudulent activities.

Telltale Signs of a Deceiver Profile

Unusual or Inconsistent Identity Information:

- **Mismatched Personal Data:** Discrepancies in personal information, such as mismatched names, dates of birth, and addresses, can indicate the use of synthetic identities.
- **Unverified or Suspicious Documents:** Use of low-quality, digitally altered, or unverifiable identification documents during the account opening process.
- **Multiple Accounts with Similar Information:** The same address, phone number, or email address is used to open multiple accounts under different names.

High Volume of Account Openings:

- **Multiple Accounts at One Institution:** The deceiver might open several accounts at the same bank in a short period, often using different identities.
- **Accounts Across Multiple Institutions:** Opening accounts at different banks or financial institutions simultaneously or within a brief period to diversify the risk.

Digital Footprint Discrepancies:

- **Inconsistent Digital Behavior:** Differences between the digital footprint of the individual (e.g., social media activity, online presence) and the information provided to the bank.
- **Use of Anonymous or Untraceable Communication Channels:** The individual may use VoIP numbers, disposable email addresses, or proxy servers to obscure their true identity.

Case Study:

The Fraud Case

Name: Rohit Mehta	
Phone: 89X XXXX32	
Email: rockXXXXXXXX@gmail.com	
PAN: DCKPMXXXXW	
dsTrustScore	**150**

Negative Flags:

- **Name Mismatch as per Banking Records.**

The name provided at the application stage does not match the name connected to the phone number on the UPI Network.

- **Low Digital Vintage**

The provided phone number has been recycled multiple times in the past. Also, the same phone number is seen with multiple other names.

- **High Bank relation count**

Multiple bank accounts connected to the same Identity.

Discovery:

- The phone number was a temporary one picked up for the sole purpose of defrauding FIs.
- Identity created through fragments of stolen personal information.

Conclusion: Probable Mule Account

Peddler Mule Account

This individual sells their genuine bank account to a fraudster, allowing the account to be used for receiving and transferring stolen funds.

Challenges in Detecting Peddler Mule Accounts

1. Legitimate Account Appearance:

Genuine Account Ownership:
Since the peddler is the legitimate owner of the account, it often passes initial KYC (Know Your Customer) checks without raising any red flags. The account appears legitimate because it is opened with authentic identification documents and personal information.

Normal Activity History:
The account may have a history of normal, legitimate transactions before it is sold or rented out. This history makes it difficult to distinguish the account from those of genuine customers, especially if the fraudulent activities are delayed or sporadic.

Delayed Suspicious Activity:
Fraudulent activities might not begin immediately after the account is sold or rented. The peddler may wait for a period before engaging in suspicious activities, making it difficult for banks to link the account to the sale or rental.

Exploitation of Vulnerable Populations:
Peddlers may come from vulnerable populations who are difficult to detect due to socio-economic factors. They might be motivated by financial desperation or coerced into renting their accounts, making them less likely to raise suspicions.

Telltale Signs of a Pedler Profile

Geographical Discrepancies:

- **Transactions from Unusual Locations:** The account shows transactions or logins from locations that are inconsistent with the account holder's known residence or usual activity. For example, the account holder is based in one city or country, but transactions are occurring from another.
- **Use of ATMs in High-Risk Areas:** Frequent ATM withdrawals in areas known for high levels of fraud or criminal activity, which might indicate the account is being used by someone other than the legitimate owner.

Multiple Accounts or Cards:

- **Opening Additional Accounts:** The account holder may suddenly open multiple accounts or request additional debit/credit cards, which are then used in ways that are inconsistent with their usual behaviour.
- **Linked Accounts Showing Similar Patterns:** Other accounts linked to the same account holder or under their name begin to show similar suspicious activity, such as rapid fund transfers or high transaction volumes.

Case Study:

The Fraud Case

Name: Sarla Agarwal	
Phone: 673X XXXX33	
Email: sarXXXXX@gmail.com	
PAN: AKKPAXXXXP	
dsTrustScore	**340**

Negative Flags:

- **High Location Volatility**

Multiple bank accounts in regional Banks and cooperative banks are connected to the phone number.

- **No Professional History**

No Employment history found against pan (no connected UAN). Also, no GST/Udhyam was discovered.

- **Multiple IFSC**

Multiple Bank branches IFSC from multiple districts from a nearby region.

Discovery:

- Thousands of low-value transactions at cyclic periodic intervals
- Common repeated receiver bank accounts.

Conclusion: Suspected Mule Account

Accomplice Mule Account

Accomplices knowingly participate in the scheme, using their own accounts to send and receive money at the direction of a fraudster.

Challenges in Detecting Accomplice Mule Accounts

1. Legitimate Account History:

Established Account History:
Accomplices typically use accounts with a legitimate history of normal activity, making it difficult for banks to distinguish between routine transactions and those that are fraudulent. The account may have a long-standing relationship with the bank, which can delay the detection of suspicious behaviour.

2. Use of Multiple Accounts:

Account Diversification:
Accomplices may open or use multiple accounts to distribute their activities, making it difficult for any single bank to detect the full scope of their fraudulent activities. This strategy can also involve using accounts at different financial institutions to further obscure their actions.

3. Trust-Based Exploitation:

Exploitation of Trusted Status:
Accomplices who have established trust with the bank—such as long-term customers or those with high balances—can exploit this status to avoid scrutiny. Banks may be less likely to question the activities of trusted customers, giving accomplices more leeway to conduct fraudulent transactions.

Use of Professional or Business Accounts:
Accomplices might use professional or business accounts, which naturally have higher transaction volumes and more complex activities, to mask fraudulent transactions. These accounts are often subject to less scrutiny due to their nature.

Telltale Signs of an Accomplice Profile

Geographical Discrepancies:

- **Multiple IP Addresses:** The account is accessed from various IP addresses, particularly those from different regions or countries, indicating that someone other than the legitimate account holder may be controlling it.

Multiple Accounts with Similar Activity:

- **Opening Additional Accounts:** The accomplice might open several accounts in different banks or even within the same bank to spread out the illicit activities, reducing the chance of detection.
- **Linked Accounts:** Other accounts linked to the same person or address may exhibit similar suspicious behaviours, indicating that the accomplice is managing or has access to multiple mule accounts.

Case Study:

The Fraud Case

Name: Siddhart Agarwal	
Phone: 699X XXXX43	
Email: siddXXXXXXXX@gmail.com	
PAN: ANSPAXXXXU	
dsTrustScore	**50**

Negative Flags:

- **High Location Volatility**

Multiple login I.Ps. found from multiple locations.

- **Reported by CUG member**

The Identity was blocked by a CUG member. Reported as fraud.

Discovery:

- Thousands of low-value transactions at cyclic periodic intervals.
- Common repeated receiver bank accounts. Also, the communication details were changed soon after opening the account. Lastly, The account showed minimal personal or routine financial activity, such as no regular bill payments, salary deposits, or everyday spending.

Conclusion: Probable Mule Account

Misled Mule Account

Customers believe they are engaging in legitimate business transactions. They are often misled into thinking they are helping someone in need, unaware that they are facilitating fraud.

Challenges in Detecting misled Mule Accounts

1. Genuine Belief in Legitimacy:

Authentic Intentions:
The Misled genuinely believe they are participating in a legitimate activity, such as a job, investment, or romantic relationship. Their transactions might appear normal because they think they are helping someone or fulfilling a job requirement.

Lack of Deceptive Behaviour:
Unlike fraudsters or willing accomplices, the Misled does not intentionally deceive the bank or try to hide their activities, making it harder to detect fraud based on behavioural red flags alone.

Gradual Introduction of Suspicious Activity:
Fraudulent activity may start small and increase gradually, blending in with the account's normal activity. This slow buildup can make it difficult for automated systems to detect anomalies early on.

Routine Communication:
The Misled continues to engage with the bank in routine ways, such as responding to emails, checking balances, or asking for transaction support. This normal engagement makes it harder for bank staff to suspect anything unusual.

Telltale Signs of an Misled Profile

Suspicious Job Offers or Investment Opportunities:

- **Employment in Payment Processing:** The account holder may claim to be working in a job that involves receiving and transferring money as part of "payment processing" or "financial management," which are common covers for mule account activities.
- **Too-Good-To-Be-True Investments:** The Mislead might mention being involved in an investment opportunity that promises unusually high returns with minimal effort, a common tactic used by fraudsters to lure victims.

Case Study:

The False Case- False Positive

Name: Anshul Sharma	
Phone: 869X XXXX32	
Email: an.kXXXXXXXX@gmail.com	
PAN: CHKPKXXXXS	
dsTrustScore	**720**

Negative Flags:

- -

Discovery:

- An account that has been relatively inactive or used for typical personal transactions suddenly experiences a surge in activity, particularly involving large deposits and withdrawals post joining a new firm.

Note: Employment history was later checked, the provided Employer did not exist (not registered)

Conclusion: Fraudulent Customer

4.3 Digital Fraud VS Digital Growth, How to Strike a Balance?

Basel Committee on Banking Supervision draws up a graphical illustration of how digital growth and financial fraud share an intrinsic relationship. As illustrated in Figure 1 there is a positive relationship between the diffusion of digitalisation in banking – and its benefits – and the risk of bank fraud.[10]

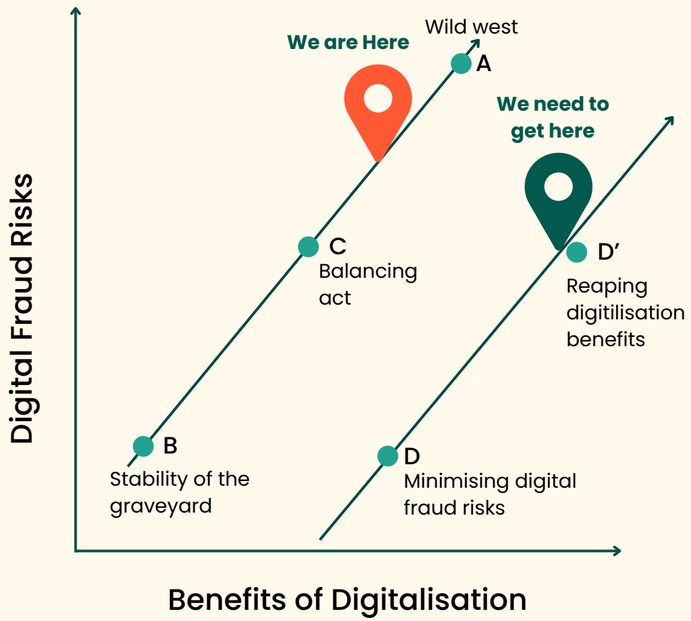


Figure 1: *Benefits and fraud risks from the digitalisation of finance*

The challenge for policymakers lies in striking the right balance between the benefits of digitalization in banking and the risks of digital fraud. Pursuing an unconstrained "maximalist" approach to digitalization (point A) can yield greater advantages from online banking services but may also significantly increase material digital fraud risks. This wild-west is absolutely out of the question.

Conversely, reverting to a predominantly "analogue" banking system (point B) would eliminate or substantially reduce digital fraud risks but at the cost of forfeiting the financial growth & stability driven by digital banking.

At present, the Indian financial ecosystem is at a middle-ground between points A and C. The key is to first move the industry to the optimal equilibrium point (point C) that maximizes the advantages of digitalization while minimizing fraud risks.

Once at point C, we can further explore ways to further reduce fraud risks for a given level of digitalization (shifting from point C to point D) or to reap even greater benefits from digitalization for a given fraud risk level (shifting from point C to point D'), truly harnessing the potential of a Digital India for All.

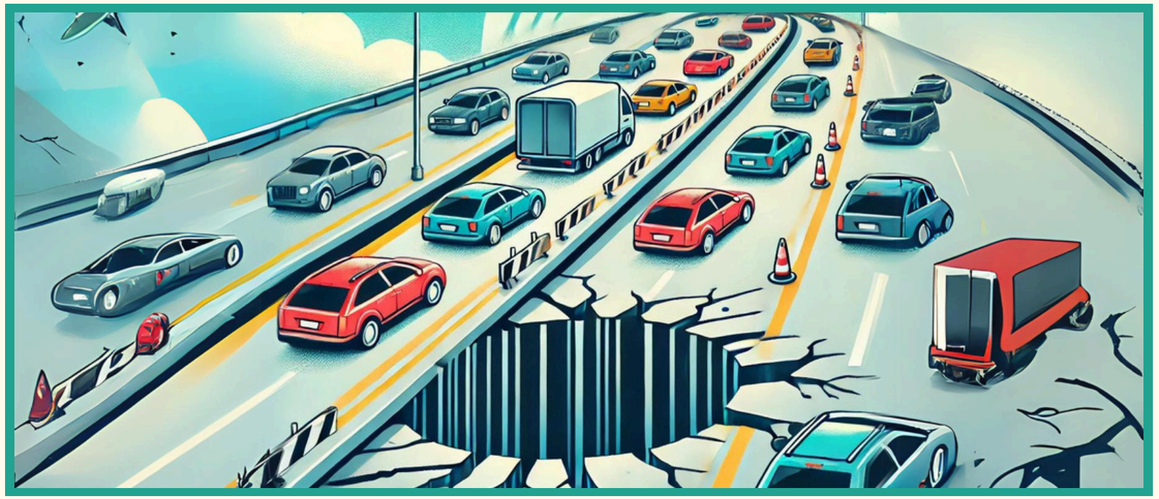
> We need to build a community around solving fraud. The tech guy needs to understand the business, and the business guys need to understand the tech in a sense that the guys who are managing fraud cannot just say that I don't understand tech.
> We cannot simply go around saying let somebody else take care of it, it is somebody else's problem, it’s not my problem.
>
> ***-Abhishek Bose***
> ***Head of Data Science, TATA Capital***

While fraud can be a consequence of digitalisation, to stop India’s journey towards becoming Digital First because of it would be as senseless as stopping any development project because of its aligned risks. Any public infrastructure comes with its downsides, it is up to us as a society to solve for it.

Fraud today is like a pothole on a highway.

We could ignore it, drive over it, absorb the damage to our car and forget about it. Over time, the passing on of the problem leads it to becoming bigger, starting to up the consequence of driving over it. Eventually, it crumbles the entire infrastructure.

Or, as individuals, we always have the choice of warning the driver behind us of the pothole. Bringing public awareness to a problem is always the first step to prevent individual harm, as well as work towards a solution together.

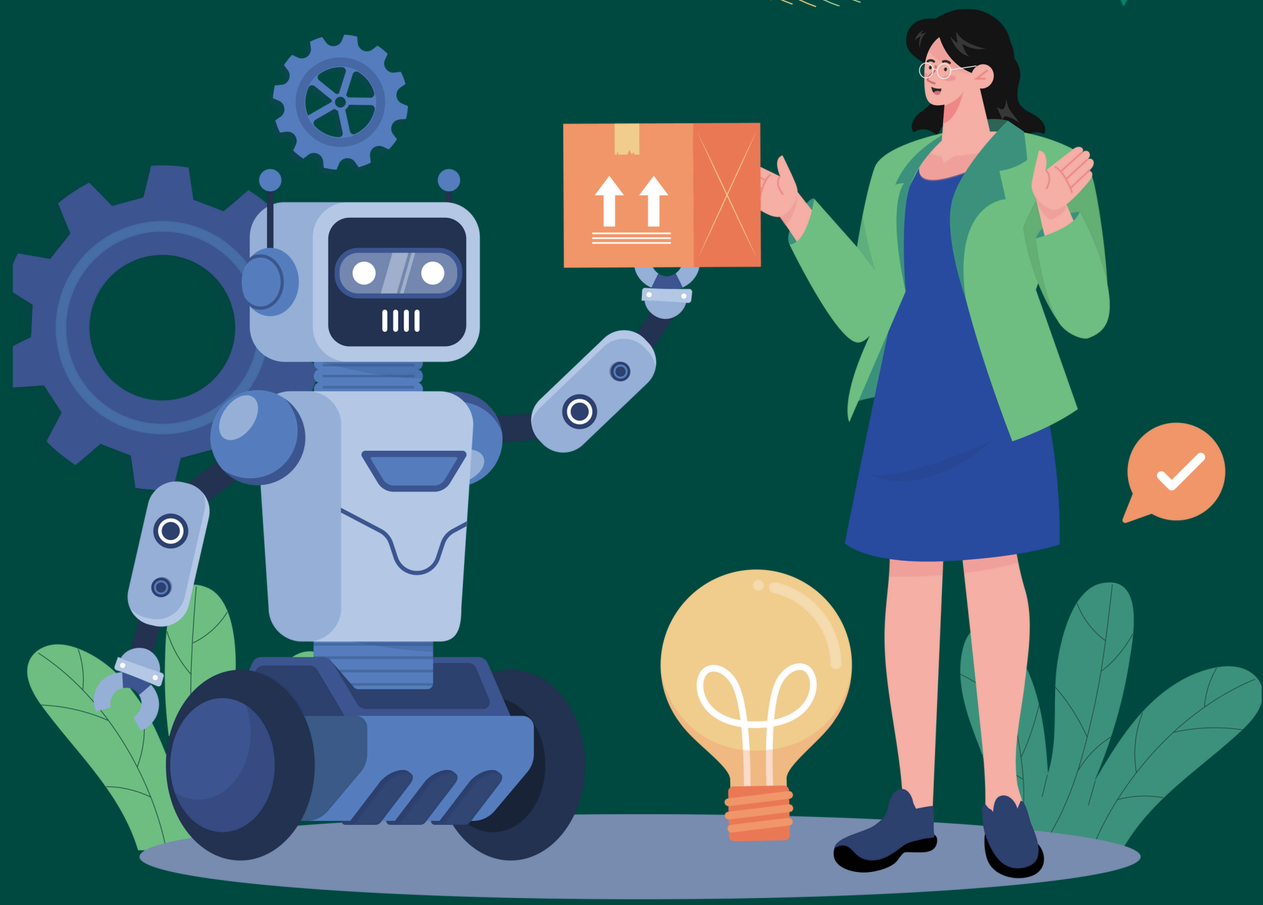


5

How can we Solve for Fraud?

5.1 The Technological Angle

> The data available today is significantly more extensive than what we relied on in the past. Previously, a PAN card, voter ID, or passport, along with a Bureau score, sufficed. Now, we can connect to diverse data sources to uncover deeper insights, such as discrepancies like a different pizza delivery address and a normal mailing address. By analysing various data points, we can reveal surprising information, especially in cases of dual identities where one persona is responsible and the other engages in questionable activities. Such detailed analytics were simply not feasible in our earlier environment.
>
> ***- Abhishek Bose***
> ***Head of Data Science, TATA Capital***



In today's social and technological landscape, fraudsters are constantly evolving, making profiling, red flagging and catching frauds harder everyday. Just as the industry is learning fraud trends and solving for it, so are the fraudsters themselves, innovating to bypass solutions being built in.

Fraud-solving technology leverages three key elements: Digital Public Infrastructure (DPI), Artificial Intelligence (AI), and scalable affordability.

1. Digital Public Infrastructure (DPI) serves as a significant blessing by digitizing and making data accessible, enabling seamless communication and service delivery across various sectors. This digitization allows for the aggregation of vast amounts of data, which can be leveraged for fraud detection and prevention.

2. Artificial Intelligence (AI) plays a crucial role in processing millions of transactions accurately and identifying patterns indicative of fraudulent behaviour. AI systems continuously learn from new data, enhancing their predictive capabilities over time, leading to more effective fraud detection.

3. Scalable affordability ensures that fraud detection solutions can operate efficiently at scale with very low turnaround times (TAT), allowing businesses to maintain operational efficiency without compromising security. This scalability is achieved through cost-effective technologies, making fraud prevention accessible to organizations of all sizes.

> Today, there is a multitude of data sources for alternate checks, but tomorrow, there may be a few more relevant data sets, while some others become obsolete. This continuous evolution of data within the ecosystem necessitates a unified scoring system controlled by a community model. This model should determine the likelihood of fraudulent activity on a scale, as one cannot declare someone fraudulent until further investigation. The analytics should provide this suspicious activity scale and make it available as a service, enabling institutions to consume it quickly. Based on our experience with the fraud sandbox in India, we believe that a sandbox environment allows for faster innovation and enables other players with innovative solutions to participate.
>
> ***- Manish Jain***
> ***Country Managing Director, Experian***

5.2 The Regulatory Imperative

Regulation plays a crucial role in combating fraud by establishing frameworks that promote accountability, transparency, and compliance among financial institutions. The Reserve Bank of India (RBI) has issued comprehensive directives to enhance fraud risk management, ensuring that banks implement robust internal controls and reporting mechanisms. These regulations facilitate early detection and reporting of fraudulent activities, allowing for timely action against fraudsters while reducing overall risk to the financial system.

Regulatory Directives for Banks

The RBI has issued comprehensive Master Directions on Fraud Risk Management for various financial sectors, including commercial banks, cooperative banks, and non-banking financial companies. These directives aim to enhance the framework for early detection and reporting of fraud, requiring banks to implement robust internal audit systems and ensure compliance with principles of natural justice before classifying entities as fraudulent. Additionally, banks must establish dedicated frameworks for customer reporting of fraud and maintain accountability through oversight by senior management.

Establishing Digital Payments Intelligence Platform

To bolster security in the digital payments landscape, the RBI is establishing a Digital Payments Intelligence Platform that leverages advanced technologies like AI and machine learning. This platform will facilitate real-time data sharing and enhance network-level intelligence, enabling stakeholders to identify and address fraud threats effectively. By improving the security and reliability of digital payment systems, the RBI aims to boost consumer confidence and promote the adoption of digital financial services.

Central Directory for Fraud

The RBI has also established a Central Fraud Registry, a searchable database designed to help banks identify, control, and mitigate fraud risks. This registry allows for the efficient sharing of information about fraudulent activities and unscrupulous borrowers, enabling banks to implement necessary safeguards and preventive measures. Furthermore, banks are required to conduct periodic reviews of their internal controls and credit sanction processes to detect early warning signals of potential fraud, thereby enhancing overall fraud management efforts.

Currently, we lack a comprehensive fraud reporting system that not only addresses fraud holistically but also classifies it according to its nature and causes. Understanding what led to a particular fraud incident, as well as identifying which issues are solvable and which are more challenging, is essential for creating a clearer prevention strategy. Unfortunately, this critical industry-wide information is not readily available today.

- Parijat Garg
Ex-Senior Vice President, CRIF India

5.3 Financial Literacy

Financial literacy is essential in mitigating fraud, especially as digital transactions become more prevalent. By equipping individuals with the knowledge and skills to navigate financial products and risks, financial literacy empowers consumers to make informed decisions and recognize potential fraud. Initiatives aimed at enhancing financial education are crucial for reducing vulnerability to scams and fostering a more secure financial environment.

Empowering the Underserved

Tailored educational programs are necessary for vulnerable populations, such as women and rural communities, ensuring they have access to essential financial knowledge and resources to protect themselves against fraud.

Shaping Future Finances

Integrating financial education into school curricula prepares future generations for sound financial decision-making, equipping them with the skills to manage money effectively and recognize fraudulent schemes from an early age.

Infotainment for Financial Inclusion

Leveraging technology and engaging content, such as infotainment, can significantly enhance financial literacy among the general public. Public interest campaigns can raise awareness about fraud risks and promote responsible financial behaviours, ultimately fostering a more informed society.

5.4 Profit Motivations: Why are VCs looking at fraud as a big market?

The NASDAQ Report notes:

> *Financial institutions have been at the forefront of fraud prevention for decades and continue to be actively engaged and invested in this fight: our survey of anti-financial crime professionals found that 75% of respondents reported an increased investment in headcount in 2023 compared to the previous year. Financial institutions are responding to the intense pressure to effectively prevent fraud, uncover money laundering, and ultimately safeguard the financial system — all while ensuring they fulfil regulatory expectations despite facing inefficient processes, rapidly-evolving technology, and ever-increasing operational costs. Today, they are working to incorporate cutting-edge techniques and technology, including artificial intelligence to improve the efficiency of their processes and better detect threats.*[11]

The fraud detection and prevention market is experiencing significant growth, projected to expand from USD 28.8 billion in 2024 to USD 63.2 billion by 2029, at a compound annual growth rate (CAGR) of 17.0%[12]. This surge is driven by the increasing sophistication of cyber threats, with businesses and financial institutions compelled to implement robust fraud prevention systems to safeguard sensitive data. Additionally, the market is expected to reach USD 90.07 billion by 2028, highlighting the urgent need for effective solutions as online fraud incidents continue to rise . As the financial services sector remains particularly vulnerable, the imperative for startups is clear: they must focus on developing innovative, scalable solutions that enhance user experience while effectively mitigating fraud risks.

Venture capitalists (VCs) and investors play a pivotal role in addressing fraud within the fintech landscape, especially as financial inclusion and digital infrastructure expand. Recognizing that fraud can significantly impact business models, VCs are increasingly focused on backing startups that prioritize robust fraud prevention strategies. This involves implementing solutions that minimize the impact on customer experience while effectively managing risk.

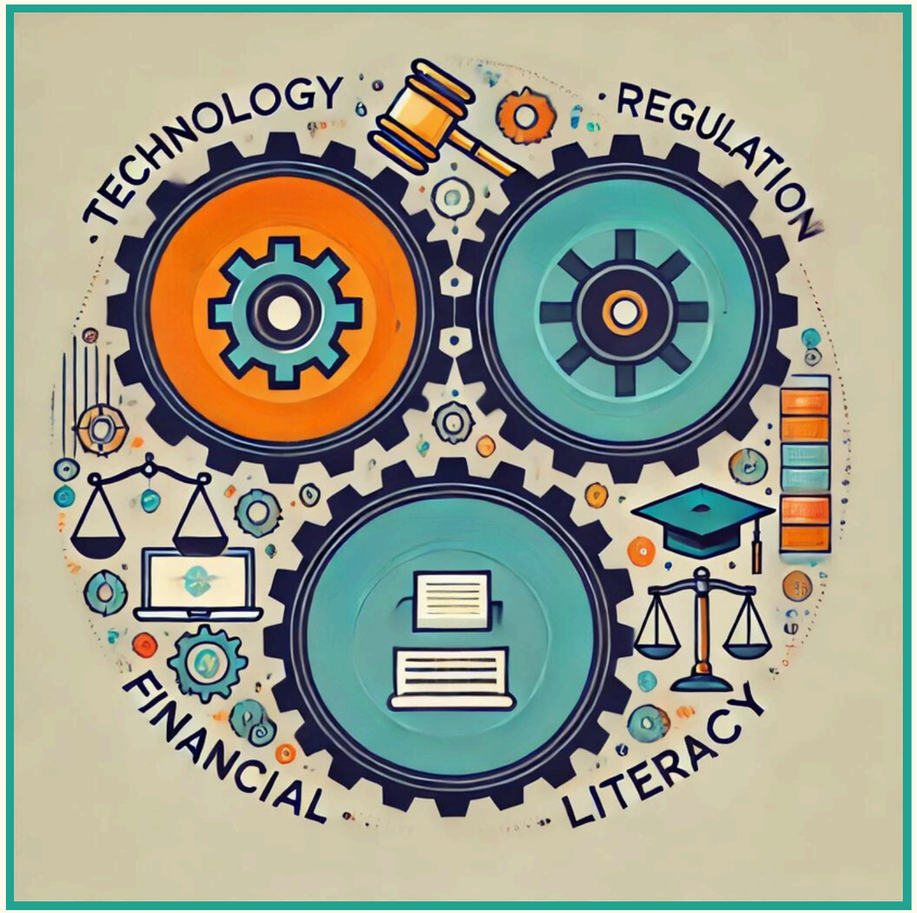
Many portfolio companies are adopting third-party fraud risk management (FRM) solutions or developing their own systems to validate high-value transactions, ensuring a seamless user experience while maintaining operational efficiency. When evaluating companies that tackle fraud, VCs prioritize a deep understanding of the problem combined with top-notch technology, as both elements are essential for creating scalable solutions. Additionally, the evolution of the market for fraud solutions indicates a growing need for regional approaches that cater to localized fraud patterns and regulatory requirements, while also fostering collaboration between global and local solutions to address cross-border fraud effectively. By investing in innovative fraud prevention technologies and supporting companies that prioritize security, VCs not only protect their investments but also contribute to building a more resilient financial ecosystem.

> Regional solutions are essential for addressing localized needs and regulatory requirements, as they are better equipped to tackle specific fraud patterns, cultural nuances, and language features. Access to region-specific data enhances fraud detection. However, as the fintech landscape matures, a hybrid approach will emerge, where global and local solutions collaborate to tackle cross-border fraud more effectively.
>
> ***- Sweta Rau***
> ***Founder & GP, White Venture Capital***

6

Roadmap to Building a Financially Inclusive and Safe Future for All

It’s clear that no single entity—be it a company, industry, technology provider, or government—can tackle the intricate issue of financial crime in isolation. This presents a unique opportunity for collaboration in developing a comprehensive framework and establishing shared benchmarks for successful anti-financial crime initiatives. We all share a collective responsibility—to ourselves and to society—to contribute to the solution.



> From my perspective, we need a group of ethical hackers who can provide insights on a regular basis—whether monthly or quarterly. These individuals could be compensated by a consortium of companies, creating a fund to pay them for sharing the top ten trends they observe in the industry. This approach could significantly benefit the sector, and I am genuinely excited about the potential for collaboration between old solutions and new innovative insights.
>
> *- Abhishek Bose*
> *Head of Data Science, TATA Capital*

I envision an environment where multiple data assets can be brought together to innovate both analytics and technology capabilities. In this environment, participating financial institutions can experiment with new innovative offerings and collaboratively solve problems. APIs would be readily available for the community to consume solutions, allowing participants — whether they are data providers, technology providers, or experts who have successfully addressed specific types of fraud — to contribute their solutions. This setup would enable financial institutions to choose from various options without the hassle of shortlisting from a vast array of solutions. They could easily test, select, and switch between solutions as needed. I believe this approach will not only address fraud, but also extend to other areas, as the landscape is continually evolving.

-Manish Jain
Country Managing Director, Experian

However, beyond these components, a social movement is needed—one led by the finance and tech sectors but involving society at large. Financial literacy must be pushed into every school, every village in the country, educating individuals on what to do and, crucially, what not to do when interacting with digital public infrastructure. By empowering people with the knowledge to protect themselves and deploying AI and machine learning to detect fraud in real time, we can create a resilient ecosystem where fraud is not just managed but actively prevented. Collaboration between financial institutions, regulators, law enforcement, and consumers will be key to making this vision a reality.

7

References

Endnotes

1 "Beware: 800 Online Financial Frauds a Day." The Times of India, 2024, https://timesofindia.indiatimes.com/business/india-business/beware-800-online-financial-frauds-a-day/articleshow/111241765.cms.

2 TransUnion. "TransUnion Report Finds Digital Fraud Attempts Spike 80% Globally From Pre-Pandemic Levels." TransUnion Newsroom, 2023, https://newsroom.transunion.com/transunion-report-finds-digital-fraud-attempts-spike-80-globally-from-pre-pandemic/.

3 PricewaterhouseCoopers. Platform fraud: the new frontier of economic crime. PwC, 2023. https://www.pwc.com/gx/en/services/forensics/gecs/global-economic-crime-fraud-report-snapshot-2.pdf.

4 Mordor Intelligence. "Global Fraud Detection and Prevention Market Size & Trends." Mordor Intelligence, 2024, https://www.mordorintelligence.com/industry-reports/global-fraud-detection-and-prevention-fdp-market-industry.

5 "Bank Frauds Up Almost 300% in Last Two Years, Digital Frauds Up 708%: RBI." Hindustan Times, 2024, https://www.hindustantimes.com/business/bank-frauds-up-almost-300-in-last-two-years-digital-frauds-up-708-rbi-101717060171280.html.

6 ibid.

7 Digital Payments in India: What's Driving the Big Growth." The Times of India, 2023, https://timesofindia.indiatimes.com/technology/tech-news/digital-payments-in-india-whats-driving-the-big-growth/articleshow/109102923.cms.

8 Master Direction - Know Your Customer (KYC) Direction, 2016." RBI, 25 Feb. 2016, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10292

9 "Mule Account Detection." *BioCatch*, 2024, https://www.biocatch.com/mule-account-detection.

10 Basel Committee on Banking Supervision. *Digital Fraud and Banking: Supervisory and Financial Stability Implications*. Bank for International Settlements, 2022, https://www.bis.org/bcbs/publ/d558.pdf.

11 Nasdaq. 2024 Global Financial Crime Report. 2024, https://nd.nasdaq.com/rs/303-QKM-463/images/2024-Global-Financial-Crime-Report-Nasdaq-Verafin-20240115.pdf

12 Fraud Detection and Prevention Market Worth $63.2 Billion by 2029." PR Newswire, 12 June 2024, https://www.prnewswire.com/news-releases/fraud-detection-and-prevention-market-worth-63-2-billion-by-2029---exclusive-report-by-marketsandmarkets-302170571.html.

References

Newspaper Articles

1. "Bank Frauds Up Nearly 300% in Last Two Years, Digital Frauds Up 708%: RBI." *The Economic Times*, 2024, https://economictimes.indiatimes.com/industry/banking/finance/banking/bank-frauds-up-nearly-300-in-last-two-years-digital-frauds-up-708-rbi/articleshow/110555108.cms.

2. "Beware: 800 Online Financial Frauds a Day." *The Times of India*, 2024, https://timesofindia.indiatimes.com/business/india-business/beware-800-online-financial-frauds-a-day/articleshow/111241765.cms.

3. "RBI Data Suggests Rise in Online Payment Frauds in India: Reasons and What Users Should Do." *The Times of India*, 2024, https://timesofindia.indiatimes.com/technology/tech-news/rbi-data-suggests-rise-in-online-payment-frauds-in-india-reasons-and-what-users-should-do/articleshow/110627011.cms.

4. "Corporate Fraud: Just How Prevalent Is It?" Rotman, David. *Forbes India*, 2024, https://www.forbesindia.com/article/rotman/corpo-rate-fraud-just-how-prevalent-is-it/91971/1.

Industry Reports

1. Deloitte. *Banking Fraud Survey Report 2024*. 2024, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-banking-fraud-survey-noexp.pdf.

2. Grant Thornton. *Financial and Cyber Fraud Report 2024*. 2024, https://www.grantthornton.in/insights/financial-and-cyber-fraud-report-2024/.

3. KPMG. *Pulse of Fintech H2 2023*. Feb. 2024, https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2024/02/pulse-of-fintech-h2-2023.pdf.

4. PricewaterhouseCoopers. *Combating Fraud in the Era of Digital Payments*. 2024, https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments.pdf.

5. PricewaterhouseCoopers. *PwC's Global Economic Crime and Fraud Survey 2024*. 2024, https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html.

6. "Digital Payment and Online Security Measures for Data Protection." *PRS Legislative Research*, 2024, https://prsindia.org/policy/report-summaries/digital-payment-and-online-security-measures-for-data-protection.

7. Reserve Bank of India. "Statement on Developmental and Regulatory Policies." *RBI Bulletin*, 7 June 2024, https://rbi.org.in/scripts/BS_ViewBulletin.aspx?Id=22648.

8. Reserve Bank of India. "KYC Norms." 2024, https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=750.

9. Reserve Bank of India. "KYC Norms." 2024, https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=866.

10. Reserve Bank of India. "KYC Norms." 2024, https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1233.

11. Reserve Bank of India. "KYC Norms." 2024, https://www.rbi.org.in/commonperson/english/Scripts/Notification.aspx?Id=752.

12. Reserve Bank of India. "KYC Norms." 2024, https://daynrlmbl.aajeevika.gov.in/Circulars/RBI%20Circular%20on%20KYC%20norm.pdf.

13. Reserve Bank of India. "Report of the Working Group on Digital Lending Including Lending through Online Platforms and Mobile Apps." 7 Nov. 2023, https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF.

14. "Identify the Total Cost of Fraud and Optimise Prevention Strategy." *TransUnion*, 2024, https://www.transunion.co.uk/blog/identify-total-cost-of-fraud-and-optimise-prevention-strategy.

15. "Mule Account Detection." *BioCatch*, 2024, https://www.biocatch.com/mule-account-detection.

16. "What Is Financial Literacy and Why Is It Important?" *Experian*, 2024, https://www.experian.com/blogs/ask-experian/what-is-financial-literacy-and-why-is-it-important/.

17. "Financial Literacy." *Corporate Finance Institute*, 2024, https://corporatefinanceinstitute.com/resources/management/financial-literacy/.

18. "Fraud Detection and Prevention Market." *Allied Market Research*, 2024, https://www.alliedmarketresearch.com/fraud-detection-and-prevention-market.

19. "Global Fraud Detection and Prevention (FDP) Market." *Mordor Intelligence*, 2024, https://www.mordorintelligence.com/industry-reports/global-fraud-detection-and-prevention-fdp-market-industry.

20. "TransUnion Report Finds Suspected Digital Fraud Rate in Hong Kong Significantly Higher Than Other Global Markets." *TransUnion Newsroom*, 2024, https://newsroom.transunion.hk/transunion-report-finds-suspected-digital-fraud-rate-in-hong-kong-significantly-higher-than-other-global-markets/.

21. Nasdaq. 2024 Global Financial Crime Report. 2024, https://nd.nasdaq.com/rs/303-QKM-463/images/2024-Global-Financial-Crime-Report-Nasdaq-Verafin-20240115.pdf.

Others

1. "Net Banking Frauds." *Delhi Police Cyber Cell*, 2024, https://cyber.delhipolice.gov.in/netbanking.html.

2. "Fraud and Scams." *Barclays Corporate*, 2024, https://www.barclayscorporate.com/insights/fraud-protection/fraud-and-scams/

3. "What Is First, Second and Third Party Fraud?" *Experian*, 2024, https://www.experian.co.uk/blogs/latest-thinking/fraud-prevention/what-is-first-second-and-third-party-fraud/.

4. "Financial Frauds in India: How to Stay Ahead in Securing the Future." *IDfy*, 2024, https://www.idfy.com/blog/financial-frauds-in-india-how-to-stay-ahead-in-securing-the-future/.

5. "RBI to Launch Digital Payments Intelligence Platform for Fraud Prevention." *Business Today*, 7 June 2024, https://www.businesstoday.in/technology/news/story/rbi-to-launch-digital-payments-intelligence-platform-for-fraud-prevention-432489-2024-06-07.

6. Basel Committee on Banking Supervision. *Digital Fraud and Banking: Supervisory and Financial Stability Implications*. Bank for International Settlements, 2022, https://www.bis.org/bcbs/publ/d558.pdf.

7. Fintech Council. *The Winds of Change - Edition II*. 2024, https://www.fintechcouncil.in/pdf/The%20Winds%20of%20Change-%20Edition%20II.pdf.

8. "Cybersecurity and Fraud Prevention." *JPMorgan Chase & Co.*, 2024, https://www.jpmorgan.com/content/dam/jpm/commercial-banking/insights/cybersecurity/download-payments-fraud-Survey-key-highlights-ada.pdf.

8

Acknowledgements

We would like to express our sincere gratitude to the industry experts who provided invaluable insights and guidance throughout the development of this report. Their expertise in the field of digital fraud has greatly enriched our understanding and analysis.

Himadri Chatterjee - EX-President, Axis Bank
Parijat Garg - Ex-Senior Vice President, CRIF India
Manish Jain - Country Managing Director, Experian India
Abhishek Bose - Head of Data Science - TATA Captial
Neeraj Sinha - Partner & Leader, Financial Services, BDO India
Vraj Gokhlay - KPMG Partner, India Lighthouse
Sweta Rau - Founder & GP, White Venture Capital

Credits:

Special thanks to the Data Sutram Team for their support.

With inputs from
Kumar Ayush Sinha
Aishwarya Pattabiraman
Dipayan Basu

Research: Sreemoyee Mukherjee
Design: Roshni Balagopal

data sutram

Unlock Disruptive Growth with Actionable Intelligence Powered by External Data

At Data Sutram, we enable enterprises for growth by providing the infrastructure to derive actionable insights on the external world from over 250 sources. We solve the challenge of inefficient decision-making across the customer lifecycle, from fraud detection and customer acquisition to cross-selling and collections, ultimately reducing risk and helping businesses grow faster.

Reach out to us!

www.datasutram.com

hello@datasutram.com

Scan to Schedule a Demo