data sutram

FINSECURE REPORT:

The Evolving Landscape of Financial Fraud

2025

Volume 2

by Data Sutram

CONTENTS

Foreword from the CEO 03

Introduction to Financial Fraud 04-05

Fraud Vs Scam 06

The Larger picture of Fraud 07

The Paradox of Financial Fraud in India 08

India’s Regulatory Framework and Institutional Landscape 09-10

The Need for Broader Investment in Anti-Fraud Technology 11

Impact of Fraud 12-13

Evolution of fraud prevention in the past and present 14

Evolving Nature of Fraud: Challenges & Solutions 15

Changing fraud trends 16

Evolved Tactics of Financial Fraud in 2025 .	17-19
Future Direction of fraud	20
Combatting Evolved Financial Fraud in Lending	21-22
Data Sutram’s Solution to Lending Fraud	23
Case Study: Profile-based Underwriting with Data Sutram	24
What Comes Next?	25
Trends for the Future of Financial Fraud	26
A Closing Word from CTO	27
Acknowledgements	28
References	28-29

Foreword

Financial transactions have always been rooted in human connection. They are anchored in trust, familiarity, and personal relationships. For centuries, whether through barter, lending, or deposits, people have transacted with those they knew and trusted, making decisions based on shared experiences and social bonds.

Today, the digital era has fundamentally altered that landscape. Gone are the days when bankers and customers interacted face-to-face; instead, engagements often occur between distant parties over the internet, sometimes without any direct human touch. As familiarity fades, financial institutions increasingly struggle to evaluate risk, personalize services, and anticipate customer needs. This loss of human connection has fuelled rising defaults, surging non-performing assets, persistent deposit crunches, and challenges in collections and insurance penetration. Ultimately, fraud has emerged as a by-product of this new environment, one in which traditional methods of customer onboarding and KYC no longer suffice.

To move forward, our industry must redefine how we get to know the customer. Leveraging new technologies and data-driven approaches, we need to reconstruct lost familiarity and restore trust in financial relationships. By integrating diverse signals—from behavioural patterns to digital footprints—we can empower institutions to make risk decisions accurately, proactively, and ethically.

The solution lies in embracing advanced onboarding methods—those that enable financial institutions to truly understand each customer, whether or not physical presence or direct connection exists. Only through this lens can we both fight fraud and unlock enduring business growth.

Rajit Bhattacharya

Founder & CEO

Data Sutram

Introduction to Financial Fraud.

What is Financial Fraud?

'Fraud' is any activity that relies on deception in order to achieve a gain. Fraud becomes a crime when it involves a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment'[1]. In other words, **if you lie in order to deprive a person or organization of their money or property, you're committing fraud.**

According to the Association of Certified Fraud Examiners (ACFE)[2], while fraud can be categorised in many ways, fundamentally, every type of fraud is either organizational or individual.

Your CEO did not ask you to buy gift cards!

Employees often receive emails from IDS that appear to be from leadership teams, requesting they purchase gift cards. This is a common scam targeting employees in large organisations.

How to detect these scams?

Check the sender's email address carefully. Scammers often use email addresses that look similar to your CEO, but with slight differences.

Like: ceo.company@gmail.com, john.smith.ceo@yahoo.com, ceo@micr0soft.com, boss@company-personalmail.com

Always verify any request with your supervisor directly, using known contact information.

Never buy gift cards based on an unexpected email.

Financial Fraud Against Individuals

When a single person is targeted by a fraudster — including identity theft, phishing scams, 'advance-fee' schemes.

Organizational Financial Fraud

Internal: Sometimes called "occupational fraud," this is when an employee, manager or executive of an organization deceives the organization itself.

External: This includes fraud committed against an organization from the outside, such as vendors who lie about the work they did, demand bribes from employees and rig costs. But customers sometimes defraud organizations, such as when they submit bad checks or try to return knock-off or stolen products. And increasingly, technology threatens organizations with theft of intellectual property or customer information.

Fraud vs Scam.

While often used interchangeably, fraud and scams represent distinct categories of financial crime with different victim profiles and impact patterns:

Fraud typically occurs **without the victim's knowledge or consent.** Criminals gain **unauthorized access to personal information** and conduct transactions or activities without the victim being aware until after the damage is done.

Scams, on the other hand, **require victim participation.** They rely on **psychological manipulation** to trick victims into voluntarily providing money, personal information, or authorization for transactions.

Fraud then is a deliberate act of deception conducted without the victim's knowledge, primarily targeting organizations and institutions through the exploitation of systems or processes. Control over fraud typically lies within robust internal protocols and risk management frameworks. In contrast, scams are deceptive schemes that manipulate individuals into voluntary participation, making consumers the key victims, and the main avenue of control rests on personal vigilance and public awareness. **The core difference is that fraud is system-oriented and often hidden from the victim, while scams are interaction-driven and require the victim's engagement**

> "As business intelligence and risk management evolve, so do fraudsters! Frauds have become more sophisticated and harder to detect with "white collar" frauds outnumbering the traditional ones. It is therefore imperative that the financial system takes a very proactive approach to fraud control. The Fraud Landscape Report helps industry participants, regulators, law enforcement agencies and the general public to increase awareness and build defence mechanisms so as to mitigate systemic risks in doing business."
>
> ***KV Srinivasan***
> *CEO, Profectus*

Consumer Financial Scam

1. **Investment Fraud:** securities fraud, Ponzi schemes, commodities fraud, cryptocurrency scams
2. **Consumer Products and Services Fraud:** Worthless products, fake services, unauthorized billing, non-delivery of products
3. **Employment Fraud:** fake business opportunities, paid-interviews for jobs
4. **Prize and Grant Fraud:** Lottery and sweepstakes scams, advance fee schemes
5. **Identity and Credit Fraud:** Account takeover, synthetic identity, credit manipulation
6. **Relationship and Trust Fraud:** Imposter schemes, emotional exploitation

Fraud against Businesses

Internal (Occupational) Fraud

- Employee misuse of company resources through asset theft, false reporting, or unauthorized payments.

External Fraud

- Asset theft or misappropriation , bribery, or vendor manipulation by customers, suppliers, or outside parties. attempts to influence employee decisions

Did you know?

Internal fraud remains a serious and rising challenge for banks: in 2022, 78% of banks surveyed by Deloitte expected insider fraud risk to grow, with many already reporting frequent incidents and identifying limited employee monitoring as a key vulnerability. Collusion, where staff cooperate to circumvent controls, amplifies the impact of these frauds

Mason Wilder, Research Director at the Association of Certified Fraud Examiners (ACFE), writes, that the top fraud trends of 2025 reflect a rapidly changing socio-economic landscape: social engineering and financial pressures continue to drive fraud, but **generative AI is now powering more sophisticated scams such as phishing and impersonation, alongside an escalation in cryptocurrency and digital asset crime due to soaring asset values.** Wilder notes the rise of risks where AI service providers themselves misrepresent technologies, and highlights intensifying regulatory obligations, especially with new laws in the UK and continued post-pandemic enforcement in the U.S. He points out that increased public awareness may begin to blunt the effectiveness of scams like 'pig butchering,' although cyber-scam losses as a whole are still growing, driven by organized crime adapting tactics. According to Wilder, synthetic identity fraud—using AI-generated personas and documents—is set to surge, threatening to overwhelm current organizational controls, and financial institutions.

According to the most recent Nasdaq Verafin reports, approximately ***$3.1 trillion in illicit funds flowed through the global financial system in 2023*** a figure that remains the current global benchmark. The same report estimated that ***global fraud losses reached $485.6 billion in 2023.*** Focusing on Europe, the 2025 report highlights that ***750 billion in illicit funds moved through the continent's financial networks, with $103.6 billion in fraud-related losses*** that year, underscoring the scale and persistence of cross-border financial crime.

Global illicit finance remains vast and deeply entrenched: the International Monetary Fund estimates that 2% to 5% of global GDP—amounting to $800 billion to $2 trillion—is laundered each year. Yet, less than 1% of these illicit proceeds are seized or frozen by

In 2025, regulatory action is intensifying, and organizations are investing heavily in advanced detection tools and holistic, data-driven risk strategies to counter increasingly adaptive threats. Despite this, digital transformation and cross-border finance continue to outpace the development of adequate controls, underscoring the need for ongoing vigilance and innovation to safeguard both consumers and institutions worldwide.

The Paradox of Financial Fraud in India.

When asked "What is the state of financial fraud in the country?" - the answer depends entirely on who is responding and which lens they choose to examine the data through. On July 21, 2025, the Indian government presented what appeared to be a positive narrative to Parliament: reported bank frauds had witnessed a dramatic **61% decline in FY 2024-25,** dropping from 3.22 lakh cases in FY 2023-24 to just 1.25 lakh cases in the next FY. This substantial reduction, backed by Reserve Bank of India data, painted a picture of success driven by enhanced digital security protocols, sophisticated monitoring systems, and strengthened coordination between financial institutions and law enforcement agencies.

However, the Reserve Bank of India's own 2024-25 annual report revealed a starkly different reality beneath these encouraging case numbers. The **total value of bank fraud losses had almost trebled from Rs. 12,230 crore in 2023-24 to Rs. 36,014 crore in 2024-25** — a threefold increase that dwarfed the positive trends in case reduction. While the RBI attributed part of this escalation to the fresh registration of 122 old fraud cases following a Supreme Court judgment from March 2023, this accounting adjustment could not fully explain away the staggering Rs. 36,014 crore that had vanished from India's banking system.

This dichotomy reveals a troubling evolution in financial crime: **Frauds are becoming larger in scale and more sophisticated in execution**. The decline in case numbers suggests that prevention measures are successfully catching smaller, more routine fraud attempts. Yet the dramatic increase in per-fraud values indicates that criminal networks are adapting, concentrating their efforts on fewer but significantly more lucrative operations.

The sectoral breakdown further illuminates this complexity. While public sector banks reported fewer individual cases than their private counterparts, they accounted for a staggering **71.3% of total monetary losses**, primarily due to loan-related frauds that typically involve much larger sums. Meanwhile, private banks logged **59.4% of all registered cases,** predominantly through digital payment frauds via credit/debit cards and internet banking, where individual transaction sizes remain smaller but volumes are high.

This evolving landscape represents the eternal cat-and-mouse game between financial criminals and regulatory authorities. **Loan-related frauds dominate the financial damage sphere, accounting for 92% of total losses across all banks,** underscoring persistent threats from fake loans, fund diversion, and willful defaults.

For businesses and ordinary citizens caught in this crossfire, the critical question becomes: **what practical steps can be taken, and what level of technological investment is the financial ecosystem willing to make?**

India’s Regulatory Framework and Institutional Landscape.

India’s cyber fraud and cybersecurity regime includes the Information Technology Act 2000 (IT Act), the Digital Personal Data Protection Act 2023, sectoral guidelines by RBI, and dedicated institutions such as the Indian Cyber Crime Coordination Centre (I4C) and CERT-In. Recent amendments to government Allocation of Business (AoB) Rules have clarified governmental responsibilities, assigning I4C a central role in financial cybercrime enforcement, while CERT-In focuses on monitoring and alerts for vulnerabilities without enforcement powers. This clearer delineation fosters better agency coordination and incident handling.

I4C operates the Cyber Fraud Mitigation Centre that integrates data from banks, telecoms, ISPs, and law enforcement. Its deployment of tools like **“Pratibimb” for tracing mobile-based fraud** and aggressive blocking of SIM cards, IMEI numbers, and non-compliant apps demonstrate strong enforcement efforts. Integration with the National Payment Corporation system further assists in proactive fraud mitigation.

Regulatory Wins

- Enforcement mechanisms under the IT Act are yielding results with penalties and prosecutions. In FY 2024-25, the Reserve Bank of India imposed 353 penalties totaling ₹54.78 crore on banks and regulated entities for contraventions including cybersecurity, KYC, fraud reporting, and statutory non-compliance.
- As of July 2025, banks using RBI’s mandated Financial Fraud Risk Indicator (FRI) system (developed by the Department of Telecom) have blocked over 1.4 lakh mobile numbers linked to financial fraud, following detection and reporting from the National Cybercrime Reporting Portal and government intelligence platforms.
- Cyber audit requirements and resilience frameworks (such as RBI’s CSITE and annual IT audit mandate) have driven widespread compliance, with all NBFCs above ₹500 crores and most commercial banks now conducting annual cybersecurity audits and reporting improvements in incident detection rates.
- In FY25, Collaborative public-private intelligence platforms such as the upcoming Digital Payment Intelligence Platform have enabled real-time sharing, helping detect and prevent fraudulent transactions at a much faster rate.

Limitations and Challenges.

Key Challenges in India’s Financial Fraud Regulation Environment

- **Regulatory Lag:** The process of drafting and enacting legislation is often slower compared to the rapid pace of technological advancements. Existing legislations are often unable to keep up with emerging threats like AI-based attacks deepfakes, and novel forms of cyber fraud, leaving critical gaps in enforcement.
- **Implementation Challenges:** The large and diverse Indian financial ecosystem leads to uneven implementation and variable enforcement of security frameworks and compliance across the sector.
- **Digital literacy & Consumer Vulnerability:** Low digital literacy and cyber hygiene, particularly in underserved communities, increase risk exposure to scams.
- **Critical Infrastructure Risks:** Upgrading digital defense systems is costly and complex on a national scale. Outdated technologies and reliance on imported hardware continue to expose vital infrastructure such as power grids, telecom, and defense networks to evolving threats.

> “India’s fraud landscape is entering a new era—where threats are no longer episodic but engineered. Over the next decade, we’ll see a sharp rise in synthetic identity fraud, deepfake-enabled impersonation, and AI-driven social engineering that exploits both digital and behavioural vulnerabilities. As BFSI leaders, we must move beyond reactive controls to build fraud resilience as a strategic capability—anchored in real-time intelligence, cross-institutional collaboration, and ethical AI. The challenge isn’t just to detect fraud faster, but to anticipate it smarter—before trust is breached.”
>
> **Rajesh Bansal**
>
> **Ex Founding CEO-Reserve Bank Innovation Hub**

The Multi-Stakeholder Strategy to Control Financial Fraud: Combatting The Mule Account Menace

One of the most persistent and devastating components of this fraud ecosystem has been the proliferation of mule accounts, which are bank accounts used by criminals to receive, transfer, or launder illicit funds, with or without the knowledge of the account holder. The scale of this problem in India had recently reached alarming proportions with India's cybercrime coordination centre (I4C) flagging around 4.5-4.6 lakh bank accounts as suspected mules in 2023-24 alone.

According to BioCatch's 2024 report on digital banking fraud trends, at one partner bank in India, nine out of every ten mule accounts went completely undetected. The data showed that every device involved in mule activity in India accessed an average of 35 accounts each, underscoring the industrial scale of these operations. Perhaps most concerning was the international dimension: while initial mule account activity originated primarily from within India, after a month, only 20% of mule account sessions originated domestically, with 16% utilizing VPNs to obscure their locations.

In the previous year’s Data Sutram report, the company had highlighted the danger of mule accounts and identified advanced data-powered fraud pattern recognition as the most promising solution for detection and prevention. Their analysis proved prescient — financial technology companies like Data Sutram, Bureau, and Clari5 are now helping banks deploy AI-based fraud detection systems that can identify mule accounts in real-time rather than waiting for defrauded customers to raise complaints. One significant breakthrough in India's fight against mule accounts has been the deployment of sophisticated AI-powered detection systems. The RBI's MuleHunter.AI represents just one example of this technological revolution. Developed by the Reserve Bank Innovation Hub, this AI system can identify 19 different suspicious patterns in mule account behavior and has proven to be three times more accurate than traditional manual detection methods while dramatically reducing the time needed to identify fraudulent accounts.

The Need for Broader Investment in Anti-Fraud Technology.

As India continues its rapid digital transformation, the lessons from 2024-25 reveal a clear pattern: the war against financial crime cannot be won through regulation alone. It requires a sophisticated combination of cutting-edge technology, institutional reform, public-private cooperation, and continuous adaptation to evolving threats.

The deployment of AI tools like MuleHunter.AI, Data Sutram's DS Trust, and similar products represents more than just defensive measures — it's a fundamental reimagining of how financial institutions approach fraud prevention. By replacing static rule-based systems with dynamic, learning algorithms, banks can stay ahead of increasingly sophisticated criminal operations that previously exploited predictable detection patterns.

The success of these initiatives demonstrates that technology and human insight can indeed tip the balance in favor of legitimate financial activity. The key lies in understanding these technologies, supporting their implementation through adequate investment, and maintaining vigilance in an environment where the next breakthrough in fraud prevention may determine the outcome of this ongoing digital battle.

In this landscape report, we will explore how this technological revolution is reshaping India's fight against financial crime, examining the tools, strategies, and investments that are creating a more secure financial ecosystem while highlighting the persistent challenges that require continued innovation and vigilance.

Impact of fraud.

The Scale of the Problem.

The overall effects of fraud in India are substantial and escalating, as highlighted in the Data Security Council of India (DSCI) Cyber Threat Report 2025. The report reveals that financial fraud and cybercrime are on a sharp rise, with total annual losses now estimated at 0.7% of India's GDP. The banking and financial services sectors bear the brunt of these losses, with retail, e-commerce, and government digital services also experiencing significant impact. Increasingly sophisticated attack methods—such as phishing, account takeovers, and digital payment fraud—have widened the pool of victims to include both large corporations and small businesses, as well as individual consumers.

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. The DSCI report further emphasizes a shift toward technology-driven scams that exploit digital payments and personal data, urging organizations across sectors to make substantial investments in advanced threat detection, robust cybersecurity frameworks, and ongoing user education to effectively mitigate the growing threat landscape.

According to official government reports, cyberfraud and related financial crime losses are projected to cost India 0.7% of GDP in 2025, exceeding ₹1.2 lakh crore (approximately $14 billion USD), with the Indian Cyber Crime Coordination Centre (I4C, Ministry of Home Affairs) citing this figure for 2024–25. About 0.7% of the Indian population is directly at risk from cyberfraud, based on I4C data. The sectors facing the highest losses include banking and financial services (projected ₹8,200 crore), retail and e-commerce (₹5,800 crore), and government services (₹3,400 crore) in 2025, with additional significant impact reported in insurance, healthcare, hospitality, and industries handling sensitive personal data, highlighting the need for robust cross-sectoral risk management and regulatory attention.

Sector	Estimated Loss (₹ Cr)
Banking and Financial Services	8,200
Retail and E-commerce	5,800
Government Services	3,400
Insurance	Significant*
Healthcare	Significant*
Hospitality	Significant*

Recent government data show that in 2024, Indian consumers reported over 7.4 lakh (740,000) cyber fraud cases with total losses of ₹22,845 crore, a dramatic increase from the previous year. For 2025, cybercrime complaints are expected to cross 25 lakh (2.5 million), including at least 5 lakh (500,000) consumer-targeted fake brand scams. For businesses, losses are estimated at ₹20,000 crore in 2025, with banking, finance, retail, and e-commerce sectors most affected. Over 36.37 lakh (3.637 million) incidents of financial fraud, including both consumer and business victims, were reported in 2024 on the National Cyber Crime Reporting Portal and Citizen Financial Cyber Fraud Reporting and Management System, both operated by the Indian Cyber Crime Coordination Centre (I4C)

Evolution of fraud prevention.

Traditional Approaches to Fraud Mitigation

People commit financial fraud when three elements—pressure, opportunity, and rationalization—align to create the "perfect storm," a concept known as the fraud triangle. According to extensive research by the Association of Certified Fraud Examiners (ACFE), acute financial or workplace pressures (like unmanageable debt or unrealistic professional targets) can drive individuals toward fraud, but only if they also have access to funds or systems (opportunity) and can justify their actions to themselves (rationalization).

This fraud triangle has long been used as the foundational framework to manage fraud schemes, especially by businesses. Traditional fraud defenses, known as rule-based monitoring systems, function by establishing static rules that flag transactions or behaviors fitting predetermined criteria. These rules might include threshold breaches—such as transactions above a certain monetary value—or identifying interactions with known suspicious accounts. Institutions apply these logic checks to monitor for anomalies within financial flows, often setting parameters around location, transaction type, frequency, or customer profiles.



Limitations of Rule-based Monitoring Systems

The main limitations of traditional rule-based fraud detection systems stem from their reliance on static, predefined parameters that are slow to adapt to new or evolving fraud schemes. Because these systems only flag activity that matches set rules—such as transaction size or known account status—they often miss novel or complex fraud tactics that don't fit established patterns. This leads to a high rate of false positives, overwhelming staff with unnecessary alerts, while allowing sophisticated criminals to bypass detection by staying just within safe thresholds or exploiting loopholes. Consequently, as fraudsters innovate and digital transactions diversify, static rule-based approaches struggle to keep pace with the speed and complexity of modern financial crime.

Therefore, as organizations strive to stay ahead of increasingly sophisticated fraud schemes, the approach to detection and prevention must evolve beyond foundational frameworks. As Vincent M. Walden writes in Improving fraud risk management with an enhanced Fraud Triangle, simply relying on the classic model of pressure, opportunity, and rationalization is no longer sufficient. Walden contends,

> **"Modern fraud risk management programs are more effective when they integrate analytics, employee monitoring, and digital behavior patterns, enabling organizations to proactively surface anomalies and potential misconduct."**

Walden highlights the need for the strategic use of real-world behavioral and technological data, stating that "the combination of analytics and continuous, practical evaluation, augmented by the right technology, provides leaders with real-time insight into the effectiveness of their anti-fraud strategies." In this context, the introduction of alternative data sources—such as device intelligence, external risk indicators, and digital footprints—becomes indispensable.

Fraudsters are increasingly sophisticated, leveraging synthetic identities and networks to evade traditional fraud detection systems. Legacy systems, which focus on individual account behavior and anomaly detection, often struggle to identify these complex fraud circles because each synthetic identity may appear legitimate in isolation. Detecting such fraud requires a shift to network-based analysis that examines relationships, patterns, and connections across multiple accounts and data sources over time.

International agencies such as the FATF and Europol, consistently highlight the shortcomings of traditional rule-based fraud detection. Their reports emphasize that static, predetermined controls are increasingly ineffective against modern, evolving fraud techniques, frequently leading to delayed responses, high false-positive rates, and persistent adaptability by fraudsters. These agencies advocate for adoption of dynamic, data-driven, and machine-assisted solutions to address the growing complexity and sophistication of today's fraud landscape.

> "Fraud is no longer merely opportunistic or transactional, confined to exploiting process gaps. It has evolved into a multi-disciplinary activity—targeting the behavioural and psychological vulnerabilities of customers while simultaneously exploiting the technological and procedural weaknesses of institutions. To win the fraud battle of the future, financial institutions must move beyond incident management and focus on building systemic resilience, agility, and trust across the ecosystem. Through shared, AI-driven fraud intelligence networks and deeper regulatory–industry collaboration."
>
> **Sachin Pillai**
>
> **CEO, Hinduja Leyland Finance**

Changing fraud trends.

Digital Forgeries & Synthetic Identities

- Digital document forgeries have overtaken physical counterfeits, rising 244% year-over-year as AI-driven and fraud-as-a-service tools become mainstream.
- Since 2022, fake identities made with real and fake data have surged by 450%. Lenders using Aadhaar e-KYC for instant loans or BNPL are at high risk. Criminals use AI to generate convincing documents, build trust with lenders, then disappear after taking large loans—leaving fintechs unable to track them down.

AI-Driven Threats Multiplying:

- Generative AI and deepfake technologies are fueling a surge in sophisticated attacks, with digital forgeries and deepfakes now responsible for 40% of all biometric fraud.
- Phishing scams are now more targeted and harder to spot because of AI-generated fake texts and videos. Even new digital banking users in smaller cities are at risk. According to a 2025 CERT-In report, phishing caused 38% of all reported fintech frauds in India, with scammers pretending to be RBI or UPI help desks, and even fake bank grievance centers.

Sophistication and Accessibility

- The rise of as-a-service models means both organized fraud rings and amateur fraudsters now have access to advanced tools, increasing the volume and sophistication of attacks while lowering barriers to entry, and even fake bank grievance centers.

Evolved Tactics of Financial Fraud in 2025.

Synthetic Identities

Fraudsters create synthetic identities by combining real and fabricated data (e.g., a stolen national ID number, a legitimate address, and a fake email). These identities mimic legitimate behavior, making them hard to flag individually.

Individual-Centric Approach

Traditional systems analyze single entities (e.g., a customer's transaction history, login patterns, or credit activity) for anomalies, such as sudden spikes in spending or unusual login locations.

Fraud Circles

Fraudsters operate in networks, where multiple synthetic identities work together to perpetrate fraud (e.g., money laundering, loan stacking, or account takeovers). Relationships between accounts—such as shared phone numbers, IP addresses, or transaction patterns—are key to uncovering these schemes.

Data Silos

Legacy systems often rely on limited, siloed data sources, missing the broader context needed to detect networked fraud.

"Fraud is a topic of industry-wide interest today. We have been tracking this data over the last three years, and the trend has continuously risen. Based on the metrics we observe, the industry is experiencing an all-time high in frauds, using quick mortality of loans as a proxy. Detecting fraud is not possible through conventional algorithms or policies. What is required now, both on the asset and liability sides, are advanced algorithms capable of detecting anomalies—customer profiles that seem too good to be true, behaviors that deviate from the norm. These algorithms need to confidently identify whether a customer or a file is likely fraudulent. We believe the industry is moving towards decisions on lending and account openings based not just on probability of default or estimated customer lifetime value, but also on the probability of fraud. This will drive significant changes in workflows and risk policies of financial institutions in India. It is a critical topic requiring new capabilities, new data, and significant investments."

Yashraj Erande

MD & Partner, BCG

From Identity Theft to Synthetic-Manipulated Identities

Identity Theft is defined as when a fraudster acquires and uses someone else's real personal information (e.g., name, ID number, address) to access financial services, open accounts, or conduct illicit transactions. Victims face financial loss, legal complications, and reputational damage. The Asia-Pacific region, including India, currently experiences the world's highest average identity-based fraud rate at 6.8% of all identity checks.

Traditional Mitigation: Static KYC/document verification, blacklists, manual monitoring, and OTP-based transaction authentication.

Evolving Identity Theft: Synthetic Identities: Current challenges in identity fraud are driven by synthetic profiles, which increasingly use a blend of real and fake information—often harvested from data breaches or the dark web—to build highly believable identities that can bypass traditional verification checks. Today's fraudsters leverage AI-assisted tools not only to manipulate digital documents but also to automate the creation of synthetic profiles at massive scale. Fraudsters now use GenAI to create deepfakes, spoof voices, generate fake text and images, scrape data for fake IDs, and deploy bots for automated scams. Digital document forgeries grew by 244% in just one year, now making up 57% of document fraud, while deepfakes account for 40% of biometric fraud.

Identity Manipulation: Authentic personal details (name, date of birth) are only slightly edited to generate new document variations, escaping basic consistency checks.

Identity Compilation: Genuine and fake data are combined, such as pairing a real unique identifier with fabricated address and photo data to create a persona that feels "real" to automated systems.

Identity Fabrication: Entirely fictitious identities can be woven from templates and generative AI, sometimes using deepfakes for face or voice, making detection especially challenging.

Increased Accessibility to Organised Financial Fraud Techniques

Organized groups have always coordinated to carry out planned financial fraud by sharing information, hacking systems, and staging multi-step attacks. They orchestrate large, sustained criminal campaigns targeting multiple institutions. The evolution of technology, particularly Artificial Intelligence (AI), however, has significantly empowered organised fraud. Fraudsters now use advanced techniques that are both more sophisticated and more accessible than ever before. Over 50% of financial institutions recover less than 25% of fraud losses, partly due to the sophisticated planning and cross-border operations of organized fraud rings that make fund tracing extremely difficult. 2

Fraud Rings: are organised groups that carry out coordinated attacks, often by reusing information such as names, document numbers, and faces across different fraudulent checks. A critical component of their operations is the use of collusion and extensive networks to launder money and obscure their tracks.

Internal Collusion: A significant threat comes from internal collusion, where external criminal operatives work with insiders who have detailed knowledge of a bank's systems, processes, and control weaknesses. This collaboration enables fraudsters to exploit vulnerabilities more effectively. Limited oversight and business pressure to meet targets can increase the risk of internal stakeholders facilitating fraudulent transactions

Money Mule Networks: Mule accounts are a cornerstone of organised financial crime, acting as intermediaries to transfer stolen funds and launder money on behalf of criminals. These networks obfuscate the criminals' identities and the source of illicit funds, making it difficult to trace the money. There are different types of money mules, ranging from unwitting victims to willing accomplices.

Fraud-as-a-Service (FaaS): and Shared Methodologies: A major development is the rise of Fraud-as-a-Service (FaaS), where experienced cybercriminals package and sell fraud tools, tutorials, playbooks, and stolen data (such as login credentials and credit card information) on the dark web. This lowers the barrier to entry, enabling amateur fraudsters to leverage sophisticated attack methods that were previously only available to professional fraud rings. These platforms share methodologies on how to manipulate documents and provide the GenAI tools to do so cheaply and at scale.

> “Fraud today touches every corner of an organization, no function, department, or process is immune. It has evolved into a borderless, tech-powered enterprise fuelled by deepfakes, synthetic identities, digital arrest scams, and other types of fraud. With geopolitics, supply chains, and consumer shifts adding to the volatility, prevention lies in foresight: combining forensic intelligence with data and tech to anticipate threats, respond with agility, and build lasting fraud resilience.”
>
> **Mukul Shrivastava**
>
> **Partner - Ernst & Young**

Future Direction of fraud.

Combatting Evolved Financial Fraud in Lending

India's lending opportunities are experiencing unprecedented expansion, driven by a convergence of macroeconomic momentum, digital innovation, and demographic transformation. The nation's credit market is witnessing a sharp rise in demand, propelled by strong GDP growth of 8.2% in FY2024 and robust financial inclusion initiatives that have brought 78% of adults into the formal banking system.

India's consumer loan market is expected to reach $1 trillion by 2029 and bankers express continued optimism about loan demand across agriculture, manufacturing, infrastructure, and services sectors.

NBFC & Private Credit Expansion

- NBFCs are playing a pivotal role in broadening credit access, particularly in MSME, consumer, and infrastructure segment
- Private lending markets registered a 53% increase in H1 2025 alone, with transactions worth $9.0 billion compared to $5.9 billion in H1 2024

MSME Sector Dominance

- MSMEs are the backbone of India's economy, contributing 29% of GDP and 45% of manufacturing output
- The sector provides employment to 110 million people, driving substantial demand for business loans
- Financial literacy and awareness are rising, especially in semi-urban and rural areas, fueling credit demand

Urbanization & Middle India Growth

- Rapid urbanization is accelerating growth, with urban population share projected to reach 37.4% by 2025
- Steady expansion of "Middle India" households is creating new credit opportunities across housing finance, consumer loans, and vehicle financing

Digital Transformation

- UPI facilitated over 16.58 billion transactions in October 2024, streamlining disbursement and repayment while lowering transaction costs
- Digital payment transaction value surged to ₹2,428.2 trillion in FY2024 from ₹1,414.6 trillion in FY2021
- Transaction volumes ballooned from 43.7 billion to 164.4 billion in just three years, reflecting rapid formalization of retail credit demand

However, lending-related financial fraud in India has reached alarming proportions, with loan frauds accounting for the overwhelming majority of financial crime by value in the banking sector. Banking fraud in India involved ₹36,013 crore in FY 2024-25. Of this total amount, loan-related frauds accounted for ₹33,148 crore, or over 92% of all fraud amounts reported. Public sector banks bore the brunt of lending fraud by value, accounting for ₹25,667 crore (71.3%) of total fraud amounts in FY 2024-25. State Bank of India alone reported ₹7,663.92 crore in fraud amounts during FY 2024-25.

A critical vulnerability in India's lending fraud landscape is the significant time lag between fraud occurrence and detection. For large frauds exceeding ₹100 crore, the average detection lag extends to 57 months, allowing fraudsters substantial time to siphon funds and evade accountability. Banks traditionally focused on books and records analysis but often lacked capability within credit monitoring teams to perform adequate background checks and gather market intelligence on borrowers.

Regulatory Push

The Reserve Bank of India has implemented comprehensive regulations to combat lending fraud. Banks must establish Early Warning Signals frameworks to identify red flags in loan accounts with exposures above ₹50 crore. The RBI's Master Direction on Fraud Risk Management issued in July 2024, mandates banks to set up dedicated Data Analytics and Market Intelligence units to facilitate collection and processing of information for early fraud detection

Data Sutram's Solution to Lending Fraud: The shift from Product to Profile-based Underwriting

Data Sutram is helping banks and NBFCs move beyond traditional siloed data to a complete, insight-driven understanding of every customer across the relationship lifecycle. The DS Platform processes signals from 250+ data sources, to create a 360° intelligence layer for proactive portfolio monitoring. DS Trust works on identifying high-risk customers like first-time defaulters and mule accounts through their proprietary "Trust Score". Using its intelligence layer, DS provides a Trust Score for every identity, which considers diverse user behaviors influenced by digital adoption levels, cultural patterns, regional differences, and age demographics.

DS Trust Score to preemptively identify mule accounts in liability journeys.

A leading financial institution partnered with Data Sutram to evaluate the DS Trust Score as part of its fraud detection and risk management strategy. The objective was clear: strengthen the ability to identify high-risk customers while minimizing false positives and ensuring that genuine customers faced as little disruption as possible.

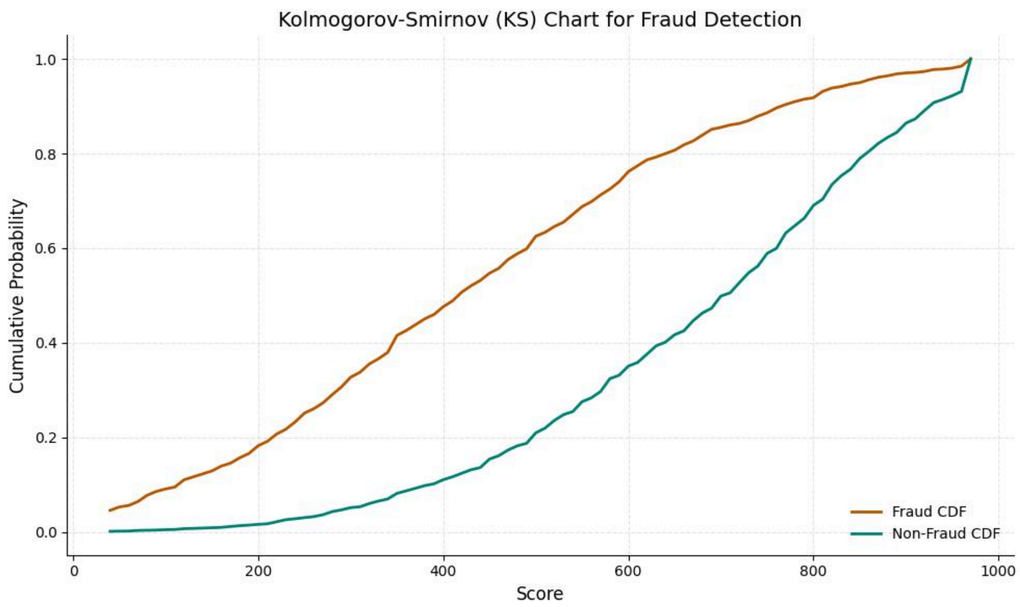


Fig : KS Chart shows how the DS Trust Score distinguishes between fraud and non-fraud customers.

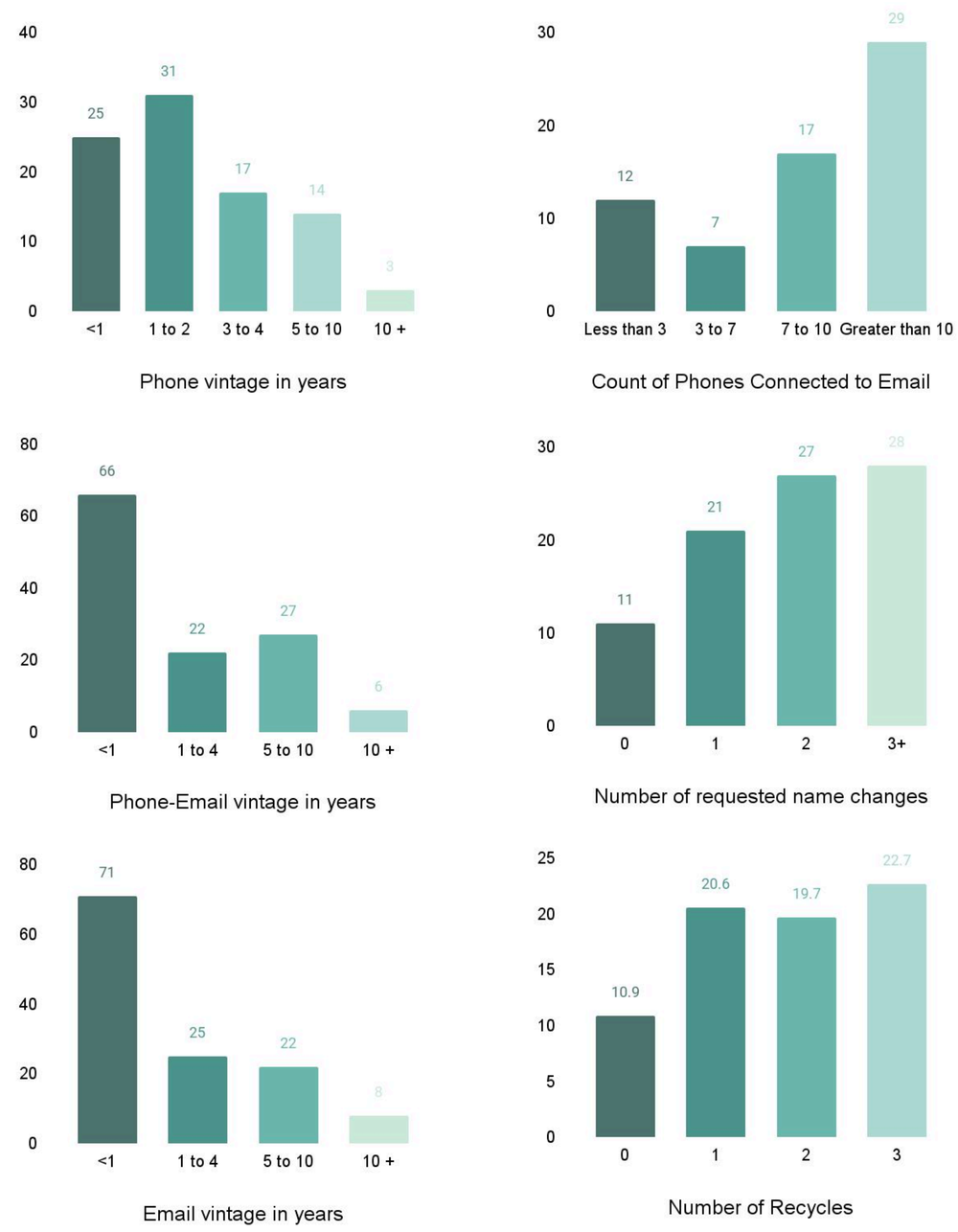
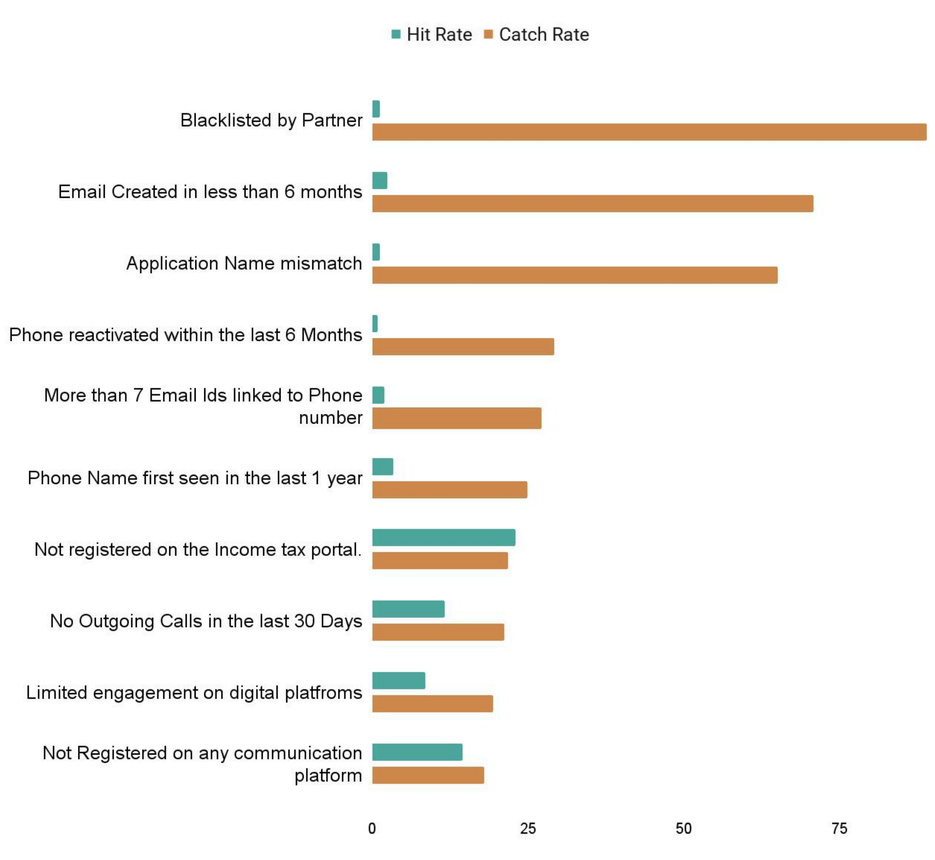


Fig : Bad Rate across some prominent features.

The evaluation demonstrated that the DS Trust Score is an effective in sharply separating the bad actors from genuine customer.The model proved its effectiveness across both controlled and real-world scenarios. Separability at low bands allowed the customer to create strong gating criteria. While the tags generated as part of score output allowed the customer to create mitigation steps and a means of remediation for the customer. The charts below showcase the performance of the different tags and performance of features.



Profile-based Underwriting with Data Sutram

Trust Score is a **behavioural** risk signal that helps assess the authenticity, intent, and reliability of a customer at the very first point of contact — using just basic inputs like phone number or email. When combined with a profile's credit score, it provides a holistic view of the customer to the bank or NBFC.

How Does the DS Trust Score Work?

- **Verifiability:** Confirms if identity details (PAN, phone, email) match across trusted external sources
- **Vintage:** Checks how long an identity (phone/email) has existed and been in active use.
- **Footprint & Spread:** Evaluates digital presence across platforms to spot genuine vs. synthetic behaviour.
- **Velocity & anomalies:** Flags unusual patterns like shared devices or rapid changes that hint at fraud.

Key Risk Signals We Detect

Identity Mismatch

- Name does not match with phone/email/PAN records
- Partial or no match across official sources

Suspicious Phone Behaviour

- Recently activated numbers
- SIM reactivation or SIM porting within 6 months
- One phone linked to many identities

Email Anomalies

- Temporary or invalid email IDs
- Storage full, domain doesn't exist
- One email ID linked to multiple phones

Blacklist Signals

- Flagged for negative activity by network partners

Lack of Digital Presence

- No or limited history across utility, e-commerce, tax, or communication platforms
- Not found on IT portal

Why it works?

- Moves beyond silo'd data
- Knows the human behind the application and their needs
- Intelligence-first methodology prevents evolved lender fraud.

What Comes Next?

According to KPMG, 59% of banks have implemented technology stacks with orchestration layers that integrate multiple data sources into a single system. Those without this capability identified it as an urgent priority, recognizing the significant benefits of a unified approach.

These trends reflect an industry-wide shift toward intelligent, adaptive, and collaborative fraud detection—necessary to combat the complexity of digital financial crime in 2025 and beyond.

Over the next decade, financial fraud in India is projected to escalate both in volume and sophistication, fueled by widespread digital adoption, increasingly advanced attack technologies, and persistent regulatory and security challenges. Losses are expected to grow annually, with criminals rapidly adapting their tactics to exploit new payment systems and digital financial products.

> The evolution of fraud has mirrored the pace of digital transformation — from opportunistic schemes to highly orchestrated, cross-border operations. As we look ahead, fraudsters will increasingly exploit AI, deepfakes, and synthetic identities, challenging traditional detection frameworks. The next decade demands a shift from reactive controls to predictive intelligence, where risk leaders must collaborate across ecosystems to build resilient, adaptive defenses. Fraud is no longer just a financial threat; it's a systemic risk to trust, governance, and societal stability."
>
> **Nitin Dharma**
> **CRO, Tata Capital**

> "As the banking ecosystem continues to evolve on digital adoption, we will experience higher sophistication of fraud risk as well (across identity, eligibility, transaction and collateral). Digital venture builders need to be one step ahead. Solving for seamless journeys will be important but we do need to over invest in protecting downside risk as well."
>
> **Abhinav Bansal**
> **MD & Partner, BCG**

Trends for the Future of Financial Fraud

- Explosion of Digital Fraud: Digital platforms, especially UPI, e-wallets, embedded finance, and BNPL products, will remain primary targets. Phishing—driven by deepfakes and AI-generated content—will account for a significant share of attacks, even as more Indians adapt to digital payments, including in rural and Tier 2/3 cities.
- Synthetic Identities & ATO Surges: Synthetic identity fraud (mixing real and artificial credentials) has already grown 450% since 2022 and is projected to become a silent crisis for instant-lending fintechs, BNPL providers, and banks unless identity and transaction intelligence are enhanced.
- Rising Professionalization and Scale: Financial fraud rings and transnational operations will broaden their reach, using automation, AI, and massive data leaks to engineer scams at scale, particularly account takeovers and credential stuffing.
- Regulatory and Compliance Shifts: While India's regulators are scaling requirements for risk-based authentication, continuous KYC, and cross-institutional data sharing, gaps in merchant verification, onboarding, and compliance will create attack surfaces that fraudsters can exploit, especially if supervisory enforcement lags behind innovation.
- Government Response & Advanced Defenses: Initiatives like the national suspect registry and AI-driven tracing tools have already led to large-scale account freezing, SIM/IMEI blocks, and mapping of fraud networks, helping curb further losses—but will need to be updated continually to counter newer, more distributed schemes.
- Proactive, Data-Driven Security: Financial institutions will increasingly shift from reactive incident response to proactive, real-time fraud modeling, using behavioral biometrics, device intelligence, tokenization, and federated learning models to detect subtle anomalies and cross-platform fraud patterns.
- Quantum and Next-Gen Tech: The emergence of quantum computing, advanced biometrics, and federated AI will transform both detection and prevention, but may also arm highly resourced fraudsters with new attack vectors—keeping the "arms race" between attackers and defenders intense throughout the decade.

A Closing Word From The CTO

Safeguarding Trust in a Digital India

Fraud is not a new phenomenon in India. It has existed in many forms over decades. What has changed is the scale, sophistication, and speed at which bad actors operate today.

This makes fraud not just a technological challenge, but a systemic one. India's growth story—its GDP, its credibility, and its global trust—depends on our ability to secure our digital ecosystem. No single institution can solve this in isolation. What we are witnessing is a necessary shift from fragmented, individual efforts to coordinated, ecosystem-wide responses. Regulators, platforms, and players like us are coming together to create shared infrastructures: mechanisms to exchange intelligence, share data on bad actors, and collectively build resilience.

Fraud is no longer confined to the financial industry. It touches gaming, retail, government subsidies, cryptocurrency, and more. The financial sector may be at the forefront because of its centrality to India's economy, but this is an all-industry problem. And as fraudsters migrate from one sector to another, the need for collaborative guardrails across industries only grows.

At our core, we see ourselves as enablers and custodians of trust. By building infrastructures powered by shared intelligence, we help safeguard not just transactions, but the confidence of an entire economy. Securing India's digital future requires collective vigilance, shared responsibility, and an unwavering commitment to protect every individual who participates in our digital ecosystem.

Because only when trust is protected can innovation truly flourish.

Aisik Paul

Co-Founder & CTO

Data Sutram

Acknowledgements

The authors would like to express their sincere gratitude to the following industry leaders and experts whose invaluable insights have shaped the perspectives presented in this report:

Rajesh Bansal
Ex Founding CEO, Reserve Bank Innovation Hub

KV Srinivasan
CEO, Profectus

Abhinav Bansal
MD & Partner, BCG

Mukul Shrivastav
Partner, EY

Sachin Pillai
CEO, Hinduja Leyland Finance

Nitin Dharma
CRO, Tata Capital

Yashraj Erande
MD & Partner BCG

Their forward-thinking perspectives on the evolving fraud landscape—from synthetic identity fraud and AI-driven social engineering to the imperative for cross-institutional collaboration and systemic resilience—have been instrumental in highlighting the critical challenges and opportunities facing India's financial services sector. Their commitment to building a more secure, intelligent, and trust-based financial ecosystem continues to inspire innovation and proactive fraud prevention strategies across the industry.

References

The Law Dictionary. https://thelawdictionary.org/fraud/

Association of Certified Fraud Examiners (ACFE) is widely recognized for its comprehensive and standardized fraud definitions and taxonomies.

Deloitte India Banking Fraud Survey Edition IV, 2022. https://www.deloitte.com/in/en/services/consulting-financial/research/india-banking-fraud-survey-edition-IV-2021.html

Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes - 31 August 2011 https://www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf

Mapping India’s Cybersecurity Administration in 2025 https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025?lang=en

Reserve Bank of India, Annual Report 2024–25 (Government of India)

References

LSVP. (2025, June 4). Our Investment in Data Sutram - Building India's financial fraud detection layer. Lightspeed Venture Partners.

Bureau. (2025, September 8). Proactive Money Mule Detection During User Onboarding. Bureau Blog.

Clari5. (2023, October 31). Clari5 Inbound Monitoring & Scam Detection Solution

Association of Certified Fraud Examiners (ACFE). Fraud definitions and taxonomies.

Bureau. (2025, September 8). Proactive Money Mule Detection During User Onboarding. Bureau Blog.

Carnegie Endowment for International Peace. (2025, September). Mapping India's Cybersecurity Administration in 2025. https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025?lang=en

Clari5. (2023, October 31). Clari5 Inbound Monitoring & Scam Detection Solution.

CRIF. (2025). Credit Landscape in India.

CRISIL. (2025). Report on Loans and Financial Services Industry in India.

Deloitte India. (2022). Banking Fraud Survey Edition IV. https://www.deloitte.com/in/en/services/consulting-financial/research/india-banking-fraud-survey-edition-IV-2021.html

EY India. (2025). Venkatasubramanian, D. Onwards and upwards: A positive outlook for private credit in India. https://www.ey.com/en_in/insights/strategy-transactions/onwards-and-upwards-a-positive-outlook-for-private-credit-in-india

KPMG. (2019). Global Banking Fraud Survey.

KPMG Australia. (2025, January). Authorised Push Payment (APP) Scam Prevention. https://kpmg.com/au/en/home/insights/2025/01/authorised-push-payment-app-scam-prevention.html

LSVP. (2025, June 4). Our Investment in Data Sutram - Building India's financial fraud detection layer. Lightspeed Venture Partners.

Reserve Bank of India. (2025). Annual Report 2024–25. Government of India.

The Law Dictionary. Fraud Definition & Meaning - Black's Law Dictionary. https://thelawdictionary.org/fraud/

United Nations Office on Drugs and Crime (UNODC). (2011, August 31). Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes. https://www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf

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