"AN ANALYSIS OF FINANCIAL FRAUD IN BELAGAVI CITY"

[1]Dr. R. N. Mangoli, Professor, Department of Criminology and Forensic Science, Rani Channamma University, Belagavi, Karnataka, India. Email-drmangoli.rn@rcub.ac.in

[2]Sharada S Busari, Postgraduate, Rani Channamma University, Belagavi, Karnataka, India.

[3]Vinayak Nidasosi, Research scholar, Rani Channamma University, Belagavi, Karnataka, India. Email-vinayaknid93@gmail.com

Abstract

In the current digital and globally interconnected economy, financial fraud has become an increasing risk to economic stability, institutional integrity, and public confidence. This research offers a thorough examination of financial fraud incidents reported in Belagavi city over a five-year span (2021–2025), intending to pinpoint common fraud categories, evaluate their occurrence, and track yearly patterns. Utilising secondary data from official police and financial complaint records, the study employs a quantitative analytical method to analyse 355 reported fraud cases.

The results indicate a changing landscape of fraud trends, showing a significant increase in both scale and intricacy from 2022 to 2024, culminating in technology-fuelled frauds such as investment scams, social media exploitation, and cyber-related crimes including hacking, QR code schemes, and digital arrest frauds. Although there was a significant reduction in both the quantity and diversity of fraud cases in 2025, ongoing vulnerabilities persist—especially concerning mobile transaction issues and digital identity theft.

The research combines criminological and forensic viewpoints to frame fraud as a tactical exploitation of systems influenced by psychological, technological, and regulatory gaps. It further examines the shortcomings of conventional detection techniques and emphasises the promise of AI-driven tools and multi-factor authentication for preventing fraud. Ending with important discoveries and policy recommendations, the study highlights the necessity for ongoing surveillance, regulatory adjustments, and improvements in cyber

security, and public awareness to address the continuously changing risks of financial fraud at both local and national levels.

Key words: *Technology-Fuelled, Cyber Security, Digital Arrest*

INTRODUCTION

In a progressively interconnected and digital global economy, financial fraud has become a widespread danger to economic stability, corporate image, investor trust, and societal confidence. Financial fraud includes a wide range of deceptive activities, such as embezzlement, manipulation of accounts, insider trading, Ponzi schemes, and cyber-related financial offenses. Such deceptive actions are frequently carried out to secure illegal financial benefits, deceive stakeholders, or distort markets.

In today's financial landscape, where capital moves rapidly through worldwide markets and organizations depend significantly on digital systems, financial fraud has transformed into a complicated and varied issue. Financial fraud involves intentional deception aimed at achieving financial benefits, covering a broad array of illegal actions such as the falsification of financial documents, asset misappropriation, money laundering, insider trading, identity theft, cyber-enabled fraud, and more recently, scams related to cryptocurrency, along with significant financial scandals including investment fraud, job fraud, and marriage fraud, highlighting the increasing complexity and scale of fraudulent activities. As technology advances, the methods for perpetrating fraud have evolved to be more intricate, leading to greater difficulties in detection and prevention.

In spite of the establishment of strong regulatory frameworks, technological progress, and internal control systems, financial fraud continues to be a recurring issue in both private and public sectors. Significant financial scandals, including investment fraud, employment fraud, and marriage fraud, highlight the increasing complexity and scope of fraudulent schemes. These events underscore systemic weaknesses and the pressing requirement for ongoing alertness, advanced detection methods, and analytical resources to avert and address such offenses.

Financial fraud represents a significant danger to the integrity of worldwide economic systems. It damages trust, disrupts markets, and causes significant financial and social damage. Financial fraud affects not just individual investors and companies but also

erodes public trust in institutions, highlighting the importance of grasping its mechanisms, effects, and prevention strategies. Through this investigation, the research aims to analyze the complex characteristics of financial fraud, examine its historical development, and suggest effective measures to reduce its occurrence in contemporary economies. Analyzing historical and current fraud tactics will aid in developing strong systems for detection, prevention, and policy changes, thus improving financial security. These historical and modern examples highlight the enduring and flexible characteristics of financial fraud, which flourishes by taking advantage of trust, information imbalances, and gaps in regulation. Through the examination of these patterns. In the digital era, financial fraud has taken on new forms, leveraging technological vulnerabilities via cybercrimes like phishing, ransomware incidents, and cryptocurrency scams.

The 2021 downfall of the cryptocurrency exchange FTX, due to the misuse of client funds, reflects past frauds and highlights the regulatory difficulties that new financial technologies present. Financial fraud is growing more complex, as criminals utilize sophisticated tools and methods to infiltrate systems. These deceptive actions—such as identity theft, credit card fraud, money laundering, and insider trading—have increased in both scale and intricacy, presenting major risks to the stability of worldwide financial systems. The financial consequences of this type of fraud are significant, burdening organizations, customers, and whole economies.

Definition of financial fraud:

Financial fraud entails dishonest actions related to public money, carried out by an individual, their representative, or with their consent, during transactions with banks, financial organizations, or comparable entities. It consists of:

1. False Statements – Presenting something as true while knowing it is false.

2. Concealment of Facts – Hiding facts knowingly.

3. Deceptive fraud – Any act designed to mislead.

4. Legally Defined Fraud – Acts or omissions specifically declared fraudulent by law.

Section on financial deception:

Bhartiya Nyaya Sanhita (BNS) 2023 tackles financial fraud, especially within the banking industry, via multiple sections.

Section 318 – Deception:

This part explains what cheating is and details the consequences for persuading someone to transfer property or agree to keep it through misleading tactics. It encompasses a wide variety of fraudulent actions, such as those related to online transactions and other misleading tactics that result in economic harm.

Section 320-Disgraceful or Deceptive Elimination or Hiding of property:

This part deals with the deceitful elimination or hiding of property to obstruct its allocation to creditors, which may apply in instances of bank fraud where assets are concealed to evade repayment.

Fraud: Is a conscious act of trickery aimed at obtaining illegal benefits for the offender or to strip a victim of their legitimate property these misleading actions can be performed by a person, a collective of individuals, or even a whole organisation. Fraud often entails distorting the truth, either by deliberately omitting essential details or by delivering misleading information to trick another party for individual or corporate benefit. Fraudsters frequently take advantage of their access to information that the victim does not possess, allowing them to deceive or confuse the victim successfully. Essentially, fraud exploits the imbalance of information and the significant expense or challenge associated with confirming the correctness of that information, which hinders comprehensive fraud deterrence initiatives. Financial fraud isn't just an economic problem; it's a complicated criminal occurrence that combines trickery, planning, and chance. In criminology, financial fraud is examined as a tactical exploitation of systems by people who take advantage of trust, power, and loopholes in regulations.

It contests conventional ideas of crime by redirecting attention from bodily harm to mental coercion and online fraud. Forensic science plays a crucial role here, since financial crimes typically produce digital or paper trails that need specialised knowledge for detection and interpretation. Whether it's tracking illegal money transfers, examining counterfeit documents, or interpreting blockchain transactions, forensic science offers the crucial

evidence needed for legal actions against financial criminals. The convergence of criminology and forensic science allows for a thorough comprehension and strategy in addressing fraud through both preventive and responsive measures. From a forensic science viewpoint, financial fraud entails the organised gathering, safeguarding, and examination of digital, transactional, and documentary evidence to identify and establish fraudulent intent. The intersection of criminology and forensic science offers a robust framework for comprehending, identifying, and thwarting financial fraud, highlighting the sociological drivers of fraudulent actions alongside the technical methods employed to carry out and hide these activities

RESEARCH METHODS

Regarding the research: The objective of the research is to quantitatively examine financial fraud cases reported in Belagavi city to recognize various types of fraud, ascertain the most commonly occurring type, and perform a year-wise comparative analysis of financial fraud incidents from 2021 to 2025.

Objectives:

1. To identify various types of financial frauds reported in Belagavi city

2. To know most frequently occurring type of financial fraud

3. To conduct a year-wise comparative analysis of financial fraud cases from 2021-2025 (up to June 2025).

Universe of the study

The universe of the study encompasses all officially reported financial fraud cases occurring within the geographical boundaries of **Belagavi city** from 2021 to 2025, including data sourced from police reports and financial complaint registries.

Types of Research

The Present study utilised the exploratory type of Research, under exploratory the researcher used comparative research method with a Quantitative research approach. It is quantitative because it relies on numerical data collected from 355 officially reported financial fraud cases in Belagavi city from 2021-2025 (up to June 2025).

Population

The sample population includes all documented financial fraud incidents within the study period that form part of the compiled 355 cases, representing the total number of reported fraud cases selected for analysis.

Data collection method

The study uses **secondary data collection**, relying on documented sources such as police records, financial complaint registries, and other official reports of financial frauds, which are systematically compiled for quantitative analysis.
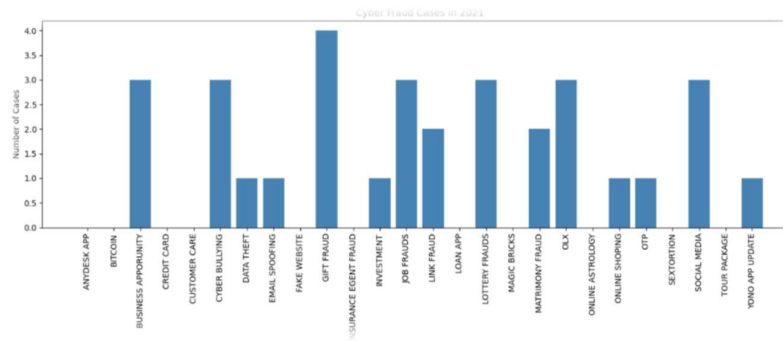
Limitation of study

I. Geographical Limitation

II. The study is restricted to Belagavi city and does not cover financial fraud cases in other regions, limiting the generalizability of findings.

III. Data Dependency: The study relies solely on secondary data from official records

IV. Unreported or unregistered financial frauds are not included, which may lead to underestimation of the actual number of cases.

V. Time Frame Limitation: The study covers only five years data from the year 2021-2025 (with up to month of June).

RESULT AND DISCUSSION

Table No. 1: Types of Financial Fraud that occurred in 2021

Sl no	Types of fraud	No of cases
1	Any Desk app	-
2	Bitcoin	-
3	Business opportunity	3
4	Credit card	-
5	Customer care	-
6	Cyber bullying	-
7	Data theft	1
8	Email spoofing	-
9	Fake website	-
10	Gift fraud	4
11	Insurance agent fraud	1
12	Investment	1
13	Job fraud	3
14	Link fraud	2
15	Loan app	-
16	Lottery frauds	-
17	Magic bricks	-
18	Matrimony fraud	2
19	OLX	3
20	Online astrology	-
21	Online shopping	-
22	OTP	1
23	Sextortion	-
24	Social media	3
25	Tour package	-
26	Yono app update	1
Total		25

Source- CEN Police Station Belagavi

In 2021, the number of financial fraud incidents was quite minimal, with merely 25 cases documented across 12 different categories of fraud. The fraud landscape was not as varied and not as dynamic as in later years. Major fraud categories comprised gift fraud (4 instances), business opportunity fraud (3 instances), and data theft (1 instance). Numerous prevalent categories like credit card fraud, online shopping, and loan app scams were missing, indicating restricted exposure to or reporting of digital fraud during that year.
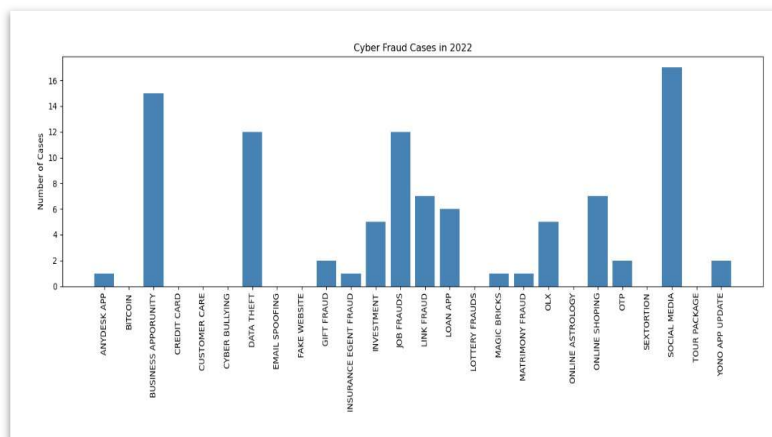
Table No. 2: Types of Financial Fraud occurred in 2022

Sl no	Types of fraud	No of cases
1	Any Desk app	-
2	Bitcoin	2
3	Business opportunity	15
4	Credit card	5
5	Customer care	-
6	Cyber bullying	3
7	Data theft	12
8	Email spoofing	-
9	Fake website	-
10	Gift fraud	2
11	Insurance agent fraud	1
12	Investment	5
13	Job fraud	12
14	Link fraud	7
15	Loan app	6
16	Lottery frauds	3

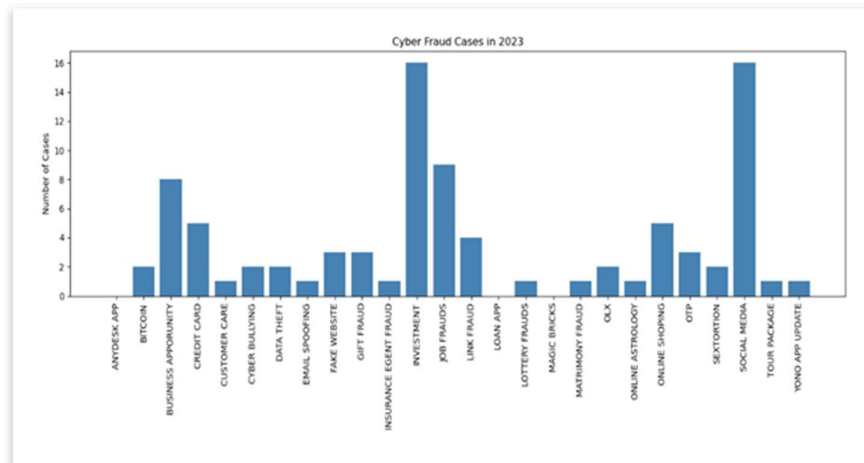| 17	Magic bricks	1
18	Matrimony fraud	1
19	OLX	5
20	Online astrology	1
21	Online shopping	7
22	OTP	2
23	Sextortion	-
24	Social media	17
25	Tour package	-
26	Yono app update	2
Total		109

Source-CEN Police Station Belagavi

In 2022, financial fraud occurrences rose significantly, totalling 109 cases across 20 different types of fraud—nearly twice the diversity observed in 2021. The major frauds Consisted of social media fraud (17 incidents), business opportunity scams (15 incidents), and data theft (12 incidents). Emerging categories such as credit card (5), online shopping (7), and Bitcoin (2) fraud highlight the increasing complexity of cybercrime and digitisation. This year saw a notable increase and variety in financial fraud activities.

Table No. 3: Types of Financial Fraud occurred in 2023

Sl no	Types of fraud	No of cases
1	Any Desk app	1
2	Bitcoin	-
3	Business opportunity	8
4	Credit card	-
5	Customer care	1
6	Cyber bullying	2
7	Data theft	2
8	Email spoofing	1
9	Fake website	3
10	Gift fraud	3
11	Insurance agent fraud	-
12	Investment	16
13	Job fraud	9
14	Link fraud	4
15	Loan app	1
16	Lottery frauds	-
17	Magic bricks	-
18	Matrimony fraud	-
19	OLX	2
20	Online astrology	-
21	Online shopping	5
22	OTP	3
23	Sextortion	2
24	Social media	16
25	Tour package	1
26	YONO app update	1
Total		81

Source: CEN Police Station Belagavi
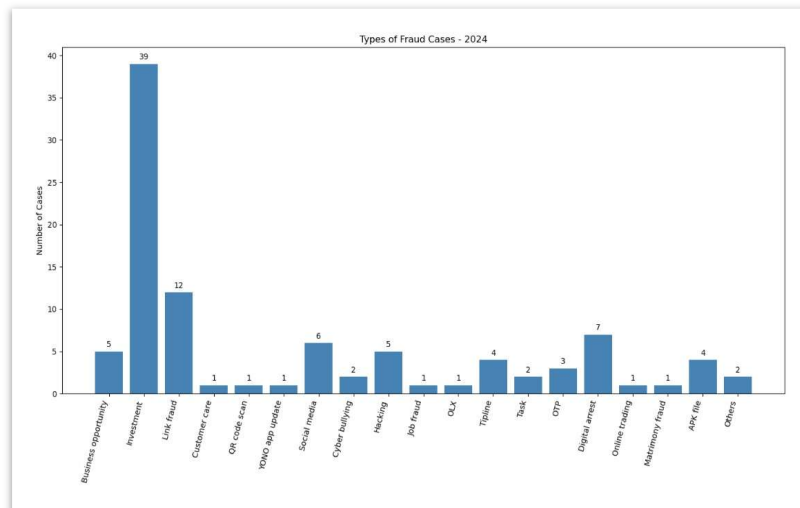
Cyber Fraud Cases in 2023

In 2023, financial fraud persisted at elevated levels, with 81 incidents across 19 categories. Investment fraud emerged as the most frequently reported type with 16 instances, closely trailed by social media fraud (16 instances) and job fraud (9 instances). New categories like counterfeit websites (3 instances) and sextortion (2 instances) showcased the changing strategies employed by scammers. Although the overall number of fraud types stayed elevated, the transition to digital and advanced fraud schemes was clear.

Table No. 4: Types of Financial Fraud occurred in 2024

Sl no	Types of fraud	No of cases
1	Business opportunity	5
2	Investment	39
3	Link fraud	12
4	Customer care	1
5	QR code scan	1
6	YONO app update	1
7	Social media	6
8	Cyber bullying	2
9	Hacking	5
10	Job fraud	1
11	OLX	1
12	Tipline	4
13	Task	2
14	OTP	3

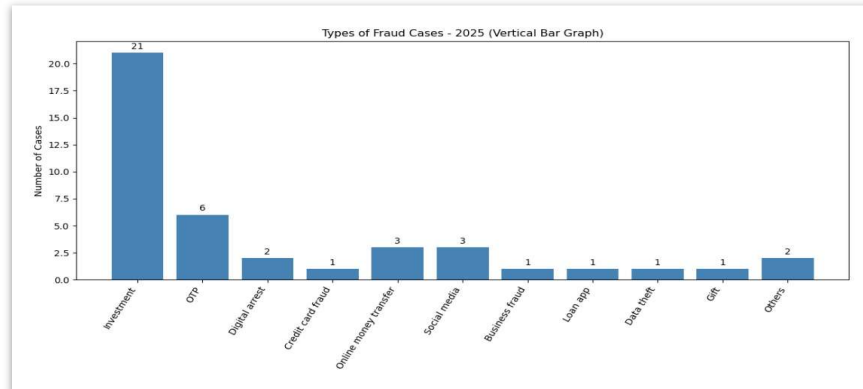| 15	Digital arrest	7
16	Online trading	1
17	Matrimony fraud	1
18	APK file	4
19	Others	2
Total		98

Source - CEN Police Station Belagavi

In 2024, there were 98 reported instances of fraud spanning 17 various categories. Investment fraud skyrocketed to 39 cases—the largest number noted for any fraud category in the past five years, signalling an increasing pattern in financial schemes. Hacking (5 instances), QR code scams, and digital arrest schemes also surfaced, underscoring a rise in technology-fuelled fraud. Social media-related fraud cases dropped from 16 to 6, potentially indicating a shift in user awareness or the focus of fraudsters.

Table No. 5: Types of Financial Fraud occurred in 2025.

Sl No	Types of fraud	No of cases
1	Investment	21
2	OTP	6
3	Digital arrest	2
4	Credit card fraud	1
5	Online money transfer	3
6	Social media	3

7	Business fraud	1
8	Loan app	1
9	Data theft	1
10	Gift	1
11	Others	2
Total		**42**

Source - CEN Police Station Belagavi

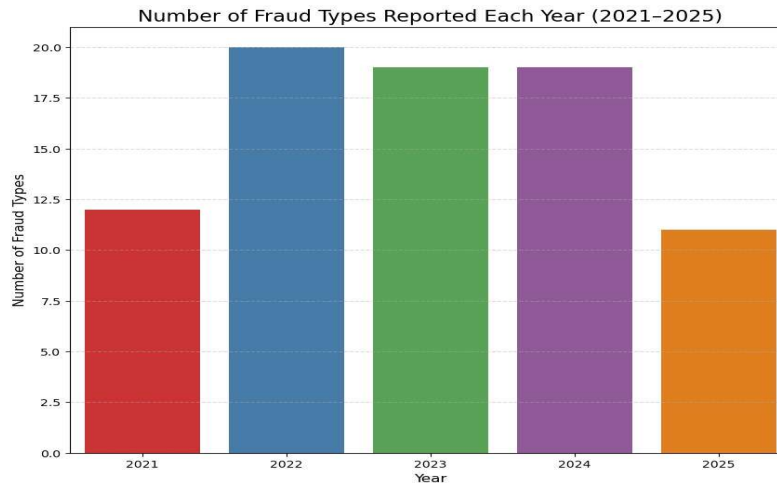Types of Fraud Cases - 2025 (Vertical Bar Graph)

By 2025, the total cases (42) and the number of fraud types (11) experienced a decrease, representing the smallest variety since 2021. Even with the decline, investment fraud stayed Substantial, totalling 21 incidents, while OTP-related scams increased to 6, reflecting ongoing weaknesses in digital verification systems. Although new fraud types, including online money transfer (3 cases), were identified, the overall decline could indicate enhanced preventive strategies or potential underreporting for the year.

Year wise Comparison:

Table No. 6: Total number of Financial Fraud occurred in 2021-2025

Sl no	Year	Total number of cases	Percentage (%)
1	2021	25	7.04
2	2022	109	30.70
3	2023	81	22.81
4	2024	98	27.60
5	2025	42	11.83
Total		**355**	**100**

Source - CEN Police Station Belagavi

Number of Fraud Types Reported Each Year (2021–2025)

The examination of fraud incidents in Belagavi city from 2021to 2025 shows a significant Change in the quantity and variety of financial offenses. In 2021, the fraud count was at its Lowest with 25 cases (7.1%), showing restricted diversity and minor effect. By 2022, there was a significant Increase in both the number of cases and the variety of fraud, indicating the start of a new Trend in financial crime.

This shift illustrates the way fraud has progressively transformed from traditional scams into increasingly intricate and technology-based plots over time. The year 2022 stood out as a pivotal moment, with 109 cases (30.97%), the peak during the five-year span. This surge was matched by a rise in the variety of fraud types, totaling 20 unique methods. The significant percentage shows that this year was marked by rampant fraudulent behavior, probably driven by a rise in online financial transactions and weaknesses related to mobile platforms. The significant jump from 25 cases in 2021 to 109 in 2022 indicates a 30.70% rise, emphasizing a swift surge in the intensity of fraud.

After the 2022 increase, the city maintained elevated fraud levels in 2023 and 2024, documenting 95 cases (26.99%) and 102 cases (28.98%), respectively. Investment fraud was prevalent during these years, reaching a high of 39 cases in 2024, establishing it as the most enduring and troubling fraud type. Moreover, social media fraud continued to fluctuate, reaching highs in 2022 and 2023 before decreasing. The information shows that fraudsters exploited expanding digital platforms and user susceptibility, keeping a persistently elevated fraud environment.

Rise of New Fraud Categories:

Fraud schemes grew more complex with the emergence of new techniques annually. In 2023, reports emerged of fake websites, sextortion incidents, and scam loan

applications, Highlighting the manipulation of online user behaviour. The year 2024 brought forth sophisticated cyber fraud methods, encompassing QR code scams, APK file frauds, hacking attempts, and digital arrest scams. These tactics illustrate how offenders swiftly adjusted to technological advances, preying on unaware victims via creative digital methods. Drop in 2025:

By 2025, the overall number of fraud cases plummeted to 21 (5.97%), aligning with the minimal figures of 2021. Even with the decline, new types Such as online money transfer scams and business fraud have appeared, indicating that fraud trends continue to evolve. The significant drop could indicate better fraud detection methods, increased oversight by financial institutions, awareness initiatives, or potentially the underreporting of incidents. The year's percentage share of the total five-year fraud tally is the least, indicating a brief pause or enhanced prevention strategies.

General Insights and Consequences:

The five-year examination reveals that financial fraud has advanced considerably in both magnitude and intricacy. The high point in 2022 and the ongoing activity into 2024 emphasise the ongoing risk of investment-related and technology-focused fraud. The slow decrease in 2025 provides some hope but also highlights the necessity of being alert to new types of fraud. As fraudsters continually evolve, law enforcement and financial organisations must keep adjusting through awareness initiatives, enhancements in digital security, and systems for real-time monitoring to avert future increases.

MAJOR FINDINGS

1. From 2021 to 2025, the trend of reported fraud cases displays a dynamic pattern of increase, variation, and subsequent decrease. In 2021, just 12 unique fraud categories were documented with a total of 25 incidents, mainly related to low-frequency scams such as gift fraud, business opportunities, and data breaches. This indicates a relatively straightforward fraud landscape, featuring fewer types and restricted effects.

2. In 2022, cases of fraud escalated to 109 incidents spanning 20 categories, almost doubling the variety observed in the prior year. Significantly, business opportunity scams increased to 15 instances, social media fraud surged to 17, and data theft elevated to 12 incidents. Recent additions like credit card fraud, bitcoin scams, and online shopping

deceit suggest a move towards greater digital and financial manipulation, Highlighting the growth of deceptive practices in online environments.

3. In 2023, there was a minor decrease in total cases to 81, yet the variety of fraud types stayed high at 19 different categories. Investment fraud surged to 16 cases, while social media fraud stayed elevated at 16, reflecting a rising fascination among Fraudsters with financial deceit and social engineering tactics. New categories such as fraudulent websites and sextortion showcased the growing intricacy and developing character of cybercrimes.

4. In 2024, the overall case count rose once more to 98, yet the variety of fraud types diminished to 17. A significant surge in investment fraud (39 cases) represented a high point over the five-year period. Emerging categories like hacking, QR code fraud, and digital arrests indicate a heightened emphasis on significant financial and cyber-related scams. Concurrently, types of fraud such as social media scams decreased, likely because of enhanced awareness or counteractions.

5. By 2025, the count of documented fraud categories decreased markedly to merely 11, and the overall cases declined to 42. Although investment fraud continued to be prevalent (21 cases), its frequency decreased by almost 50% compared to 2024. Frauds linked to OTPs (6 instances) remained a worry, emphasizing weaknesses in mobile authentication systems. Emerging fraud types, such as online money transfer scams, have appeared, but the overall reduction in both case numbers and type variety may indicate a result of enhanced control measures or underreporting.

6. In conclusion, the information indicates an evolution from a fairly simple fraud environment in 2021 to a height in intricacy and quantity from 2022 to 2024, and then a significant decrease in 2025. The evolving character of fraud—from simple scams to advanced financial and cybercrimes—highlights the necessity for ongoing vigilance, enhanced cybersecurity practices, and public awareness to combat emerging threats.

CONCLUDING REMARKS:

This study highlights the increasing complexity and variety of fraud, reaching its highest point between 2022 and 2024, especially in sectors such as investment scams and social engineering frauds. The abrupt decline in the volume and variety of fraud in 2025 indicates either enhanced law enforcement and public awareness or possible underreporting, emphasizing the persistent difficulty of accurately recording fraud data.

Financial fraud is not just a legal or technical concern; it is a socio-economic danger that damages public confidence and diminishes financial systems. In the current hyper-connected realm, where transactions occur in milliseconds and trust serves as the currency, safeguarding individuals and institutions against deception is essential, not optional. This

research not only records the patterns of fraud in Belagavi city but also advocates for a proactive, informed, and cooperative method for detecting and preventing financial fraud. The battle against fraud continues, and its effectiveness depends on alertness, adaptability, and ongoing enhancement.

RECOMMENDATIONS

1. Implement Multi-Factor authentication (MFA): Require multi forms of verification (example -password, biometrics, OTP) for account access.
2. Monitor Accounts Regularly: Check bank and credit card statements frequently for suspicious transaction.
3. Enable Transaction Alerts: Set up real time notifications for account activities via email or SMS.
4. Limited sharing of personal information: Avoid disclosing sensitive details on social media or unsecured platforms.
5. Secure Mobile Banking Apps: Ensure app have robust security features like encryption data and security code.
6. Educate Customers: Provide resources on recognizing phishing emails and scam calls.
7. Continuous Monitoring and Risk Assessment.
8. Real Time Alerts: Banks and companies should deploy fraud alert systems for unusual withdrawal or transfers.
9. Strict Regulatory Compliance: Follow anti-money laundering (AML) and Know Your Customer (KYC) norms.
10. Comply with Financial Intelligence Unit (FIU) reporting guidelines.
11. Technology-Based Measures:
    1) Encryption of Sensitive Data: Protects financial and customer data from breaches.
    2) Real-Time Transaction Monitoring.
    3) AI/ML systems to detect anomalies in spending patterns.
    4) Alerts for unusual activity.
    5) Firewalls and Antivirus: Protect systems from malware and phishing attacks.
12. Cybersecurity strengthening: Deploy firewalls, intrusion detection system (IDS), Implement end to end encryption for online transaction.

References

1. Albrecht, W. S., Albrecht, C. O., & Zimbelman, M. F. (2011). Fraud examination (4th ed.). Cengage Learning.

2. Association of Certified Fraud Examiners. (2022). Report to the nations: Global study on occupational fraud and abuse.

3. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255. https://doi.org/10.1214/ss/1042727940

4. Chakraborty, A., & Sharma, P. (2020). Forensic accounting and fraud prevention in Indian banking sector. International Journal of Management (IJM), 11(4), 52–63.

5. Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement.

6. Data Security Council of India. (2023). Cybersecurity trends report. NASSCOM. https://www.dsci.in

7. Economic and Political Weekly. (2021). Cyber frauds and the Indian banking sector. EPW, 56(34), 19–22. https://www.epw.in

8. Indian Society of Criminology. (2021). Digital financial fraud in India: A growing menace. Indian Journal of Criminology, 49(2), 45–56.

9. Joshi, M. (2022). Emerging patterns of financial fraud in digital India. Journal of Indian Law and Society, 13(1), 77–89.

10. McGuire, M. (2018). Into the web of profit: The cybercrime economy. University of Surrey, Centre for Cybercrime & Security Innovation.

11. Ministry of Home Affairs. (2023). Cyber crime statistics 2022. Government of India.

12. Mohd, S., & Nur, R. (2022). Social engineering attacks and frauds in digital financial systems. Journal of Financial Crime, 29(2), 370–384.

13. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569.

14. Reserve Bank of India. (2024). Annual report 2023–24. https://rbi.org.in.