ISRG Journal of Economics, Business & Management (ISRGJEBM)

ISRG PUBLISHERS
Abbreviated Key Title: Isrg J Econ Bus Manag
ISSN: 2584-0916 (Online)
Journal homepage: https://isrgpublishers.com/isrgjebm/
Volume – IV, Issue - IV (July – August) 2026
Frequency: Bimonthly

Understanding Fraud in Nigerian Banking: Channel Vulnerability, Social Engineering, and Temporal Patterns (2023)

Michael Amoani Agyare[1], Abdulai Salifu[1], Temitope John Oyegbola[1], Mayowa Emmanuel Omisore[2*]

[1] Department of Forensic Audit and Accounting, University of South Wales, Newport, Wales, United Kingdom

[2] Department of Environmental Management, Bowen University Iwo, Iwo, Nigeria

| **Received:** 08.07.2026 | **Accepted:** 09.07.2026 | **Published:** 06.08.2026

***Corresponding author:** Mayowa Emmanuel Omisore

Abstract

This study focuses on analysing the fraud patterns in Nigerian banking using the Nigerian Bank Services Sector (NIBSS) Fraud Dataset (2023) comprising of 1 million transactions. Descriptive statistics, crosstabs, and Chi-square tests are used to examine channel vulnerability, fraud techniques and temporal patterns. Results indicate that the Web (0.340%), Mobile (0.333%) and POS (0.306%) channels have much higher fraud levels than the ATM (0.110%) channel with a statistically significant relationship between channel and fraud occurrence ($\chi^2 = 147.59$, $p < 0.001$). Social Engineering became the most prevalent fraud method across all fraud channels, with the most prevalent across ATM (81.8%) and ECOM (72.4%). Temporal analysis showed that month is significant ($\chi^2 = 358.91$, $p < 0.001$) as the highest fraud rates were found in January (0.53%) and May (0.49%) whilst weekend rates of fraud had an increase of 17.1% from weekdays. The study provides empirical evidence of fraud trends in developing economies and provides practical guidance for banks, regulators and customers on the investment of resources in security, customer awareness and education programs, and monitoring during high-risk periods. Future research should be carried on for more than one year, and advanced detection techniques should be explored.

Keywords: *Fraud Detection, Nigerian Banking, Social Engineering, Channel Vulnerability, Temporal Patterns, Transaction Channels, NIBSS Dataset, Seasonal Fraud.*

DOI: 10.5281/zenodo.21817574

1. Introduction

Financial fraud is one of the most pressing challenges facing the Nigerian banking sector, posing risks to institutional stability, trust, and significant economic costs to individuals, businesses, and the economy at large (Umoh et al., 2024). The Nigerian financial system is in the midst of rapid digitalisation and the amount and complexity of fraudulent transactions has been growing at an alarming rate. According to the Nigeria Inter-Bank Settlement System (NIBSS), in 2023, electronic transactions amounted to N600 trillion, up 55% from the previous year in terms of volume of digital transactions (adejuwon, 2026). This development has led to great strides in financial inclusion and economic efficiency, but it has also increased the exposure of fraudsters, and criminal actors are taking advantage of this vulnerability in growing numbers and with increasing sophistication (adejuwon, 2026).

The fraud situation in Nigeria is alarming and keeps on increasing. Between 2019 and 2023, the annual count of fraud cases increased by 112% from 44,947 to 95,620, while the amount lost to fraud surged by 496% from ₦2.9 billion to ₦17.67 billion (Ifeanyi, 2026). Mobile and web channels accounted for criminal activity in over 50% of these frauds, while more than half of the frauds took place via digital channels (Khiaonarong and Zheng, 2026). The trend highlights the need for more comprehensive empirical research to uncover fraud patterns, identify vulnerable channels, and craft effective preventive measures relevant to the Nigerian market.

The prevalence of fraud in Nigerian banking highlights the need to understand the types and trends of fraud in the banking industry. One important development is the emergence of Social Engineering as a fraud technique, as this is the most common technique used by fraudsters (Abimbola, 2026). A total of 31,719 social engineering incidents have been reported, constituting 47% of the reported fraud and losses of N617.84 billion in 2025 alone (Oladosu, 2026). This is exacerbated by the insider threat as employees of the bank are now responsible for up to 70% of all cyber incidents (The Editorial Board, 2025). This indicates that the approach to fraud prevention must be more than technology, it must also be about understanding the human and systemic weaknesses that fraudsters exploit.

Current studies on fraud detection in developing economies have largely adopted conventional machine learning methods, but these methods are not effective in identifying advanced fraud strategies due to their inability to capture the intricate financial relationships and patterns (Bello and Olufemi, 2024). To tackle this issue, Graph Neural Networks (GNNs) have been proposed as alternatives due to their ability to leverage graph structures to model interactions between various entities, like transactions, users and merchants (Zhou et al., 2020). Despite this, most of the current card fraud detection models based on GNNs have only been tested on benchmark datasets that are not available in Africa, thus, failing to capture the uniqueness of card fraud in the Nigerian financial sector (Akinwande et al., 2026).

This study aims to fill this gap by performing a thorough empirical study of fraud patterns in Nigerian banking by analyzing 1 million transactions in 2023. Specifically, the study involves an analysis of the vulnerability of channels based on fraud rates by channel (Mobile, Web, POS, ATM, IB, ECOM), an examination of fraud techniques and their distribution across channels, and an analysis of temporal patterns in fraud occurrence. The research has three aims: (1) to examine the relationship between transaction channels and fraud occurrence, (2) to examine the distribution of fraud techniques across transaction channels, and (3) to examine the influence of temporal factors on fraud.

This paper is organized as follows. The literature review conducted in Section 2 summarizes literature on banking fraud, its channel vulnerability, techniques used to commit banking fraud, and the temporal patterns of banking fraud. The data and methodology are presented in Section 3. The empirical results are presented in Section 4. The results are discussed with the available literature in Section 5. Section 6 summarizes the paper and presents implications for practice and future research.

2. Literature Review

2.1 Theoretical Foundations

The study is supported by three theoretical frameworks which offer an explanatory power to the study of fraud pattern in Nigeria banking.

According to Fraud Triangle Theory (Cressey, 1953), fraud can only take place when three things come together: perceived opportunity, perceived pressure, and rationalisation (Mohottige et al., 2018). In banking, opportunity is created by failing internal controls, the pressure of money problems, and rationalisation is when the perpetrators make excuses for their actions. Social Engineering fraud, which exploits the vulnerability of humans, is a fraud method that is pertinent to this framework, which is not the case with technical weaknesses (David et al., 2026). The theory also provides an explanation for insider collusion; working under financial stress can rationalize fraudulent behavior by employees (Chimonaki et al., 2023). The application of this theory to Nigeria is supported by the observation that internal control weaknesses and employee rationalisation are still important causes of banking fraud in Nigeria (Vutumu et al., 2024).

According to the Routine Activities Theory (Cohen & Felson, 1979), convicted criminals are merely people who lack a capable guardian, have a suitable target, and are motivated criminals (Perera, 2024). In banking fraud, the guardian is the security measures, the target is the customer/institution and the offender is the fraudster (Parti, 2023). This theory gives an insight into the vulnerability of a channel, where high fraud rates on Mobile and Web channel mean low guardianship in contrast with ATM channel (Idowu, 2021). The theory also gives an account of the temporal patterns, where weekends have less guardianship with less vigilant bank staff (Parti, 2023). The theory has been supported empirically in Nigeria, which shows that there is a positive relationship between the reduction of monitoring during non-business hours and the occurrence of fraud occurrence (adejuwon, 2026).

According to the Fraud Management Life Cycle Theory (Freeman, 2026), fraud management is a continuous process of detecting, analyzing, and preventing fraud. This framework focuses on systems rather than reactive responses. This research enhances a detection phase through the empirical evidence of fraud patterns, which can be utilized to create more specific detection mechanisms.

DOI: 10.5281/zenodo.21817574

2.2 Empirical Evidence on Banking Fraud

2.2.1Global Perspectives on Banking Fraud

Social Engineering is a consistent and worldwide identified technique of fraud. Social engineering, which is usually supported by the collusion of the insider, has become the prevailing systemic risk, while the risk of fraud is now increasingly attributed to internal manipulation, rather than to technical intrusion (Nwokoji, 2026). This reflects a fundamental shift where psychological manipulation is preferred over technical intrusion. Bhusal (2020) and Ukwadinachi (2025) show that fraudsters use advanced social engineering techniques that have nothing to do with exploiting weaknesses in the systems but are based on human psychology, making rule-based systems ineffective.

New technology has brought in complex fraud schemes. AI-driven methods, such as deepfakes that circumvent biometric authentication systems, have been reported (Abbas and Taeihagh, 2024). According to the MIT Technology Review Fahey (2026), fraudsters have been exploiting Telegram with KYC bypass services to scale and bypass identity verification. The evolution of these trends highlights how adaptable fraud is and how difficult it is to keep up with the pace of change and build an effective detection strategy. Fraud detection should be continually updated with both technological and human-centred measures.

The methods used for fraud detection have been studied, with the focus being placed on traditional machine learning methods and advanced deep learning methods. Recently, the ability of graph neural networks (GNNs) and transformer architectures to model complex temporal and relational patterns in financial data has been shown (Jonathan et al., 2025; Bello et al., 2022). But, it's difficult to detect fraud because real-world large-scale datasets are not available and fraud patterns are constantly changing. Complex relationships in financial data are not well captured by traditional machine learning approaches, which may not be able to detect sophisticated fraud schemes (Uddin, 2025).

2.2.2Nigerian Banking Fraud: Context and Patterns

Nigerian researchers have contributed much to the understanding of banking fraud in Nigeria. There is strong evidence that internal control systems have a positive impact on fraud risk management: clear recruitment procedures, fair compensation, rotation of staff, background checks are all important factors in minimizing fraud (Abei et al., 2021). External auditors in Nigerian banks have an important role to play in the prevention of fraud (Maigida and Anthony, 2009). Lack of effective internal control systems and security flaws are the main causes of fraud, emphasising the need for efficient organisational structures with clearly designated responsibilities (Elikem et al., 2024). Basing on the findings, it is clear that technical and organisational measures are crucial.

According to empirical evidence gathered by NIBSS, the most exploited payment channels are the Mobile, Web and POS channels (Tunji, 2026). Mobile fraud rose by 5% from 2022 to 2023 and became the channel with the highest number of attacks. While the number of incidents of web fraud has reduced, it is still a serious issue. The anonymous, fast, and large scale advantages of digital channels are appealing to fraudsters (David et al., 2026). Digital channels saw a higher concentration of fraud with electronic payments in 2023 accounting for more than ₦600 trillion, a 55% increase (Olalekan, 2024). The digitalisation has new opportunities for fraudsters who have adapted their methods.

Social Engineering fraud has been the most common fraud technique in Nigerian banking, as identified by the various researchers and writers (Olalekan, 2024). These five fraud techniques are repeated: Social Engineering, Card Theft, Robbery, PIN Compromise, and Phishing. Social Engineering sees the highest level of volume and financial impact, followed by card theft (17%), robbery (11%), PIN compromise (7%) and phishing (6%). Its popularity is due to its ability to take advantage of vulnerabilities in human beings, the weakest link in the security chain (Olalekan, 2024). Fraudsters have been investing in building advanced social engineering techniques capable of circumvention of strong technical security measures.

NIBSS has documented temporal pattern of fraud which shows that the fraud is not uniform but varies seasonally and monthly. January had the highest number of fraud with 11,716 followed by 9,492 in February 2023 (Abdussalam, 2023). The highest fraud volume was during Q1 and the highest fraud value was during Q4. One of the reasons fraudsters are so active on the weekends is because they know that there is less security monitoring. (Nathan, 2026) These patterns indicate that there are regular points in time that are conducive to fraud, such as the economic and social cycles, including seasonal spending, holidays, and financial reporting cycles. It offers opportunities for focussed prevention approaches targeting resources to high risk periods.

2.3 Literature Gap

Although there is a great deal of research on banking fraud, there are a number of critical gaps. First, there is limited empirical evidence that examines fraud patterns based on large transaction data in Nigeria. The majority of national studies are based on survey responses or small samples, and so are not considered to be generalisable (Okafor & Okonkwo, 2022). Second, there is little research that has explored the relationship between channel vulnerability and fraud techniques. Researchers have focused on identifying vulnerable channels and dominant techniques, but little research has examined the differences between the various channels and techniques that are used for fraud (NIBSS, 2025). This relationship may help to develop more specific prevention strategies.

Third, there is a need to examine fraud in Nigerian banking in greater detail to make specific recommendations for preventing fraud. The NIBSS reports provide overall information about the temporal variations, however, a more detailed analysis is required to understand what factors are contributing to the temporal variations and to create risk-based monitoring strategies. Fourthly, there is a lack of proper evaluation of the effectiveness of the fraud prevention interventions in Nigeria. Research on the effects of particular measures, like two factor authentication, customer education and increasing monitoring, would be useful evidence for policymakers and banking institutions.

This study aims to fill these gaps by studying 1 million transactions to uncover the vulnerabilities of the channels, the fraud techniques and the time trends in an integrated fashion, offering empirical evidence for future theory and practice of fraud prevention.

3. Methodology

3.1 Research Philosophy and Approach.

The research philosophy used in this study is positivist because this research philosophy is a research philosophy that considers social

DOI: 10.5281/zenodo.21817574

reality as something that exists tangible and objective, in the sense that it is outside the researcher. A positivist approach allows hypotheses to be tested empirically with quantitative data and generalisable causal statements to be constructed (Park et al., 2020). The logic behind this paradigm is that fraud variables (temporal patterns, technique, channel) can be objective, measurable, observable and analysed. The method adopted is deductive, in which theories drawn from the literature suggest hypotheses which are tested with reference to the observed data.

3.2 Data Source

For this study, the data used is the NIBSS Fraud Dataset, which is a synthetic dataset of fraud data for the year 2023, calibrated to reflect official NIBSS 2023 statistics of fraud (Owolabi, 2025). The dataset is available on Kaggle (https://www.kaggle.com/datasets/hendurhance/nibsss-fraud-dataset) and contains 1 million transactions with 38 engineered variables spanning temporal, behavioural, and risk categories. The synthetic nature of the dataset guarantees statistical validity to reflect NIBSS reported fraud patterns, while ensuring privacy compliance (Owolabi, 2025).

The key variables for the dataset are: transaction id, customer id, transaction time, transaction amount, transaction channel (Mobile, Web, POS, ATM, IB, ECOM), merchant category, bank, location, age group, temporal features (hour, day of week, month, weekend indicator, peak hour indicator), behavioural features (transaction velocity, amount volatility, channel diversity), and the target variable is_fraud which is a binary classification for whether a transaction is fraudulent. Fraudulent transactions are also included in the dataset, with the fraud_technique field being used to show what fraud technique was used.

3.3 Sample and Variables

A total of 1 million transactions, resulting in a 3000 fraud cases (0.30% fraud rate). The sample size is large enough for statistical analysis and yields good empirical results. In this study, the independent variables considered are channel (categorical: "Mobile", "Web", "POS", "ATM", "IB", "ECOM"), fraud technique (categorical: "SOCIAL_ENGINEERING", "ROBBERY", "CARD_THEFT", "PIN_COMPROMISE", "PHISHING", "OTHER"), and temporal factors (month and weekend flag). The target (dependent) variable is the fraud label is_fraud (0 = legitimate, 1 = fraud).

3.4 Analytical Techniques

The following data analysis techniques were used:

Fraud patterns over channels, techniques, and time periods were described using Descriptive Statistics: Frequency distributions, percentages and mean comparisons.

Chi-Square Test of Independence: Used to determine whether relationships between categorical variables (channel vs fraud, month vs fraud, weekend vs fraud) is statistically significant or not. The Chi-square statistic equals:

$$\chi^2 = \sum_i \sum_j (O_{ij} - E_{ij})^2 / E_{ij}$$

Oij is the observed frequency and Eij is the frequency that is expected if the null hypothesis (HI) of independence is true.

Cross-Tabulation Analysis: To look at the distribution of fraud techniques across transaction channels, and patterns in the distribution of transaction channels by fraud technique.

The analysis of data was carried out using Python with packages pandas, numpy, matplotlib, seaborn, scipy.stats in the Jupyter Notebook format. All the statistical tests were carried out at the 5% level of significance (α=0.05) and values for $p<0.05$ were considered statistically significant.

3.5 Ethical Considerations

This research is based on secondary data which is available, public and anonymous. There was no primary data collection with human subjects. NIBSS Fraud Dataset does not contain any personally identifiable information. The principles of academic honesty are upheld by reporting and disclosure of limitations (Tripathy, 2013).

4. Results

The findings from the empirical study are presented in this section, following the three research objectives. The analysis looks at the vulnerability of the channels, techniques of fraud, and temporal patterns in Nigerian banking fraud based on 1 million transactions from the NIBSS fraud dataset (2023).

4.1 Channel-Fraud Relationship Analysis

The analysis of channel-fraud relationships found that transaction channels varied significantly in the number of frauds occurring per channel. The list of distribution of transactions/ fraud cases by channel are shown in Figure 1-3.

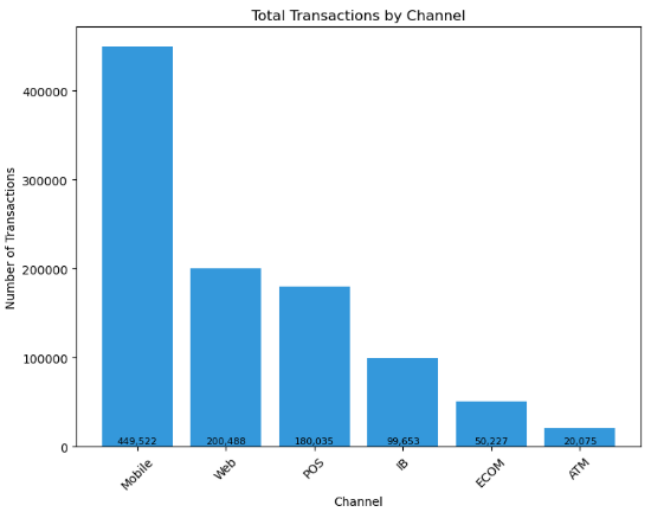


Figure 1: Total Transaction by Channel

From Figure mobile transactions accounted for the highest share of transactions (44.95%), followed by Web (20.05%) and POS (18.00%). In terms of fraud cases, Mobile accounted for 49.87% of all fraud cases (1,496 cases), followed by Web with 22.90% (687 cases) and POS with 18.37% (551 cases). Though making up 2.01% of total transactions, ATM transaction fraud only made up 0.73% of the total fraud cases (22 cases).

DOI: 10.5281/zenodo.21817574

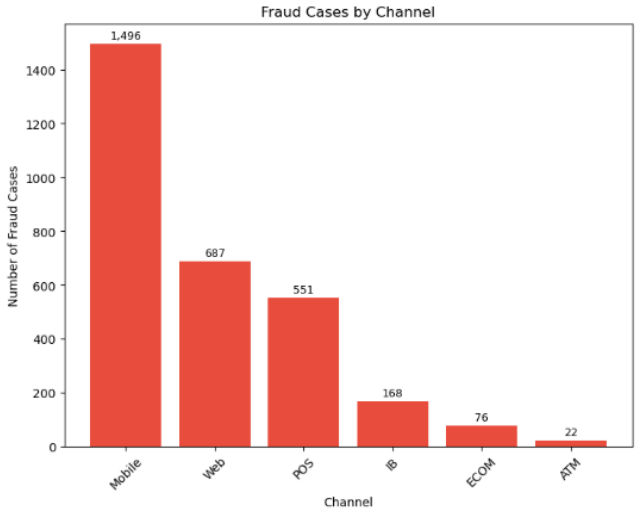


Figure 2: Fraud Cases by Channel

Chi-Square Test: Channel Vs Fraud

Chi-Square Statistic: 147.5871

P-Value: 0.000000

Degrees of Freedom: 5

It was found that there is a statistically significant relationship between transaction channel and occurrence of fraud ($\chi^2 = 147.59$, df = 5, $p < 0.001$) as determined by the Chi-square test of independence. The frequencies were found to be significantly different from the frequencies expected under the null hypothesis of independence.

Figure 2 indicates the expected frequencies for fraud cases by channel were: ATM (60.22), ECOM (150.68), IB (298.96), Mobile (1,348.57), POS (540.10), and Web (601.46). The number of fraud cases observed in the Mobile channel (1,496) and Web channel (687) was significantly high compared with the expected incidences indicating that mobile and web channels are disproportionately hit by fraudsters.

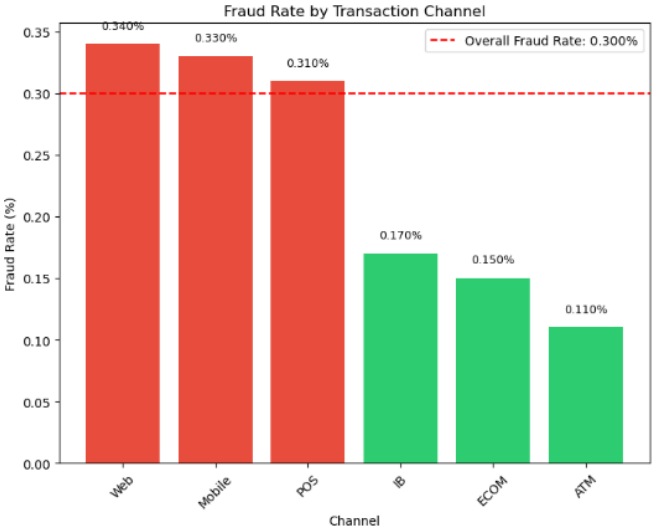


Figure 3: Fraud Rate By transaction

The visual comparison of the fraud rates by channel is shown in Figure 3. Web exhibits the highest fraud rate (0.340%), followed closely by Mobile (0.330%) and POS (0.310%). The horizontal dashed line is the percentage of all fraud cases (0.300%). Web and Mobile channels, along with POS, are above the overall average on fraud rates, and IB, ECOM and ATM channels are below the overall average on fraud rates.

The medium risk levels occurred in Web, Mobile and POS channels, and low risk levels occurred in IB, ECOM and ATM channels. Web had the highest fraud rate (0.340%), which is 1.13 times higher than the overall fraud rate of 0.300%. ATM's fraud rate was the lowest at 0.110% (or 0.37 times lower than the overall fraud rate).

The results suggest that digital channels (Web, Mobile, POS) recorded very high fraud levels compared to traditional ATM channels, thus supporting Hypothesis 1. Web (0.340%) and Mobile (0.333%) have the highest fraud rates, while ATM (0.110%) has the lowest. The Chi-square test shows that the relationship between the channel and the occurrence of the fraud is statistically significant ($\chi^2 = 147.59$, $p < 0.001$).

4.2 Fraud Techniques Analysis

The study of fraud technique revealed that Social Engineering is the most prevalent fraud technique in Nigerian banking irrespective of the channel used, it captured the bulk of the fraud cases. Table 2 shows the distribution of fraud techniques.

Table 1: Distribution of Fraud Techniques

Technique	Count	Percentage
SOCIAL_ENGINEERING	1,929	64.3%
ROBBERY	341	11.4%
CARD_THEFT	220	7.3%
OTHER	220	7.3%
PIN_COMPROMISE	158	5.3%
PHISHING	132	4.4%
Total	3,000	100%

Theft (7.3%). They were PIN Compromise (5.3%) and Phishing (4.4%).

Table 1 shows the distribution of fraud techniques. Social Engineering is the top technique, with over half of all techniques. The visualisation clearly shows that the biggest fraud technique in Nigerian banking is the Social Engineering.

When looking at the types of frauds examined by channel, Social Engineering frauds were found to be the most prevalent fraud type, especially on ATM (81.8%) and ECOM (72.4%) channels as well as Web (64.2%). The most common technique per channel is shown in Table 2.

Table 2: Most Common Technique by Channel

Channel	Most Common Technique	Percentage
ATM	SOCIAL_ENGINEERING	81.8%
ECOM	SOCIAL_ENGINEERING	72.4%
IB	SOCIAL_ENGINEERING	66.1%
Web	SOCIAL_ENGINEERING	64.2%
Mobile	SOCIAL_ENGINEERING	63.8%
POS	SOCIAL_ENGINEERING	63.3%

DOI: 10.5281/zenodo.21817574

Table 2 reveals that social Engineering remains the top fraud technique in all transaction channels, with ATM (81.8%) and ECOM (72.4%) having the highest rates and POS (63.3%) and Mobile (63.8%) having the lowest rates but still majority.

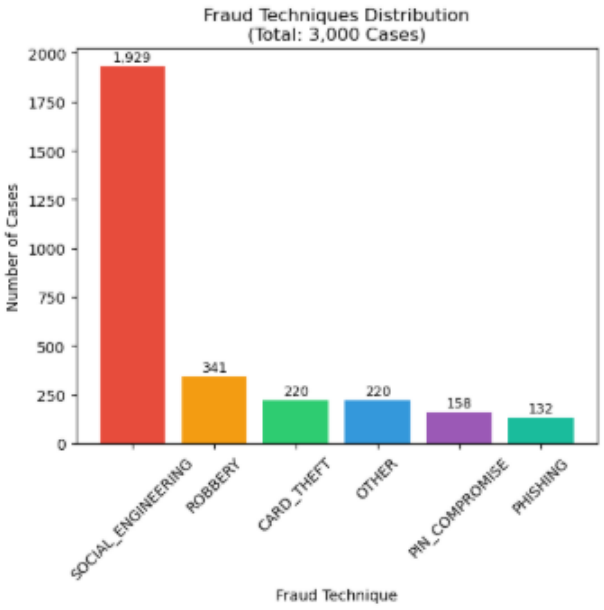


Figure 4: Fraud Technique Distribution

Figure 4 indicates that Social Engineering was the most common fraud technique with 1,929 fraud cases (64.3%) of the total fraud incidents. This was followed by Robbery with 341 cases (11.4%). There were 220 cases of Card Theft and Other fraud types, and 158 cases of PIN Compromise (5.3%). Phishing was the least common fraud technique with 132 cases (4.4%). The results show that social engineering attacks represent the main driving factor of fraud in the banking industry, which makes the need for more customer awareness and security a crucial necessity.

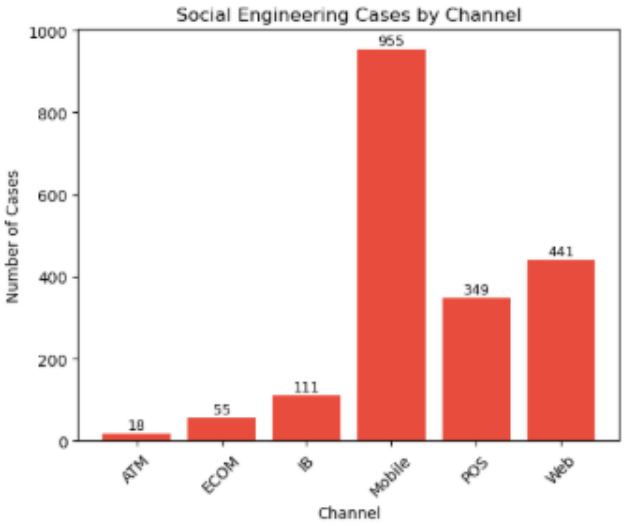
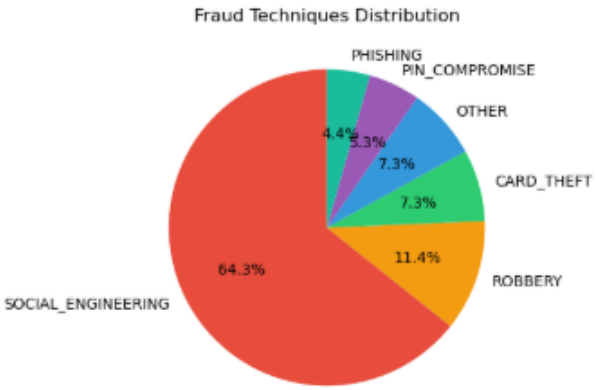


Figure 5: Social Engineering cases by channel

Mobile channel is where the largest number of social engineering cases occur, at nearly 45% of all social engineering fraud with 955 cases as shown in Figure 5. The Web channel is next with 441 cases, and POS has 349 cases. Significantly lower numbers are reported for Internet Banking (IB), ECOM and ATM channels. This means that fraudsters make mobile banking users a key target for deceptive practices.



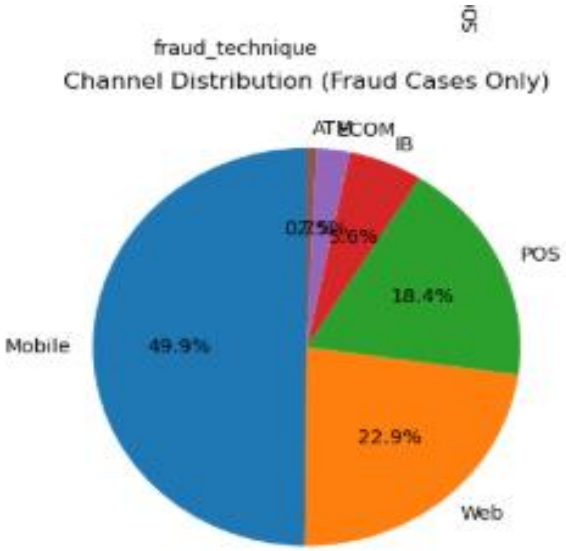


Figure 6: Fraud Technique by Channel

From Figure 6, the mobile channel is the most vulnerable channel with 49.9% of all fraud cases. The Web channel comes in second, accounting for 22.9%, followed by the POS channel, at 18.4%. Only 5.6% of the Internet Banking and 2.5% of the ECOM and 0.7% ATM are in the accounts. The results suggest that digital channels, and especially mobile banking, are the main channels for fraud. The Chi-square test for the relationship between channel and fraud technique gave a value of $\chi^2 = 23.07$ (df = 25, p = 0.574), which suggests that there is not a significant difference in the distribution of fraud techniques by channel. Social Engineering is also prevalent in all media.

Chi-Square Test: Channel Vs Fraud Technique

Chi-Square Statistic: 23.0656

P-Value: 0.573734

Degrees of Freedom: 25

DOI: 10.5281/zenodo.21817574

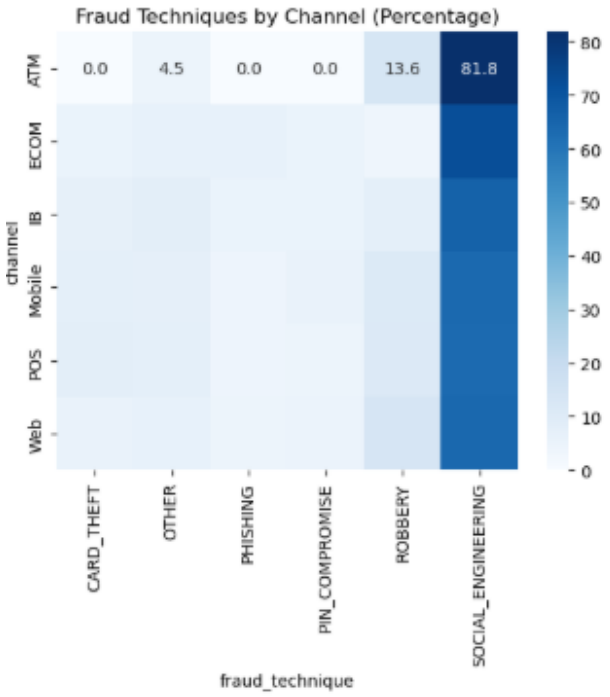


Figure 7:Fraud Technique by Channel Heatmap

Figure 7 presents a heatmap showing the distribution of fraud techniques across transaction channels. Darker colours represent more of certain techniques. The heatmap also shows that the Social Engineering technique is always the most widely used method, which is visually confirmed by the darkest cells, which are in the Social Engineering row.

Ultimately, the most prevalent fraud technique is Social Engineering, which makes up 64.3% of all fraud cases, thus supporting Hypothesis 2. Social Engineering is the most prevalent technique, found in all channels with ATM (81.8%) and ECOM (72.4%) having the highest prevalence. The results of the Chi-square test do not reveal any significant relationship between channel and fraud technique ($\chi^2 = 23.07$, $p = 0.574$), implying that Social Engineering is equally prevalent in all channels.

4.3 Temporal Patterns Analysis

The temporal pattern analysis showed that there were significant differences between seasons and months in terms of fraud occurrences. Fraud rates by month are shown in Table 3.

Table 3: Fraud Rate by Month

Month	Transactions (n)	Fraud Cases (n)	Fraud Rate (%)
January	55,808	295	0.53
May	79,629	394	0.49
February	81,653	295	0.36
July	76,751	268	0.35
August	78,558	254	0.32
April	84,241	255	0.30
February	77,108	232	0.30
June	75,533	191	0.25
October	83,581	213	0.25
March	121,480	275	0.23
November	85,977	197	0.23
December	99,681	131	0.13

January reported the highest fraud rate (0.53%), followed by May (0.49%) and February (0.36%). The lowest incidence of frauds was seen in December (0.13%), November (0.23%) and March (0.23%). A statistically significant relationship between month and fraud occurrence was found by the Chi-square test ($\chi^2 = 358.91$, $p = 0.001$), which supports the idea of a seasonal trend for fraud. The highest rate of fraud was in January with 295 cases (0.53%) and lowest in December with 131 cases (0.13%) Table 3.

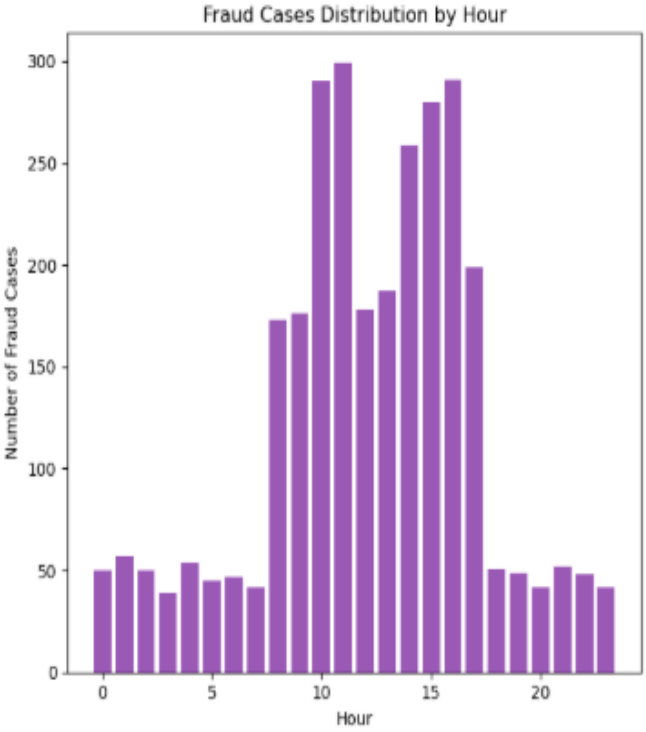


Figure 8: Fraud Cases Distribution by Hour

Figure 8 illustrates fraud cases peak during late morning and early afternoon hours (10:00–16:00), with minimal activity during late night and early morning, though this variation is not statistically significant ($p = 0.910$) as shown in Table 5

When comparing weekend and weekday fraud, it is found that fewer frauds are committed during the weekdays than on weekends. The comparison is shown in Table 4.

Table 4: Weekend vs Weekday Fraud Rates

Period	Transactions (n)	Fraud Cases (n)	Fraud Rate (%)
Weekend	285,000	955	0.320
Weekday	715,000	2,045	0.290

The difference in the rates of fraud between weekends and weekdays is 0.049 percentage points, or a 17.1% increase in fraud rates on weekends. The Chi-square test for weekend vs weekday fraud showed a statistically significant difference, with a value of $\chi^2 = 3.46$, $p = 0.062733$

DOI: 10.5281/zenodo.21817574

Table 5: Chi-Square Test Results for Temporal Factors

Temporal Factor	Chi-Square (χ^2)	Degrees of Freedom (df)	P-Value	Significance
Month	358.91	Not specified	0.000000	Significant
Day of Week	17.07	Not specified	0.009025	Significant
Weekend	3.46	1	0.062733	Not Significant
Hour	14.54	Not specified	0.910301	Not Significant
Peak Hour	0.15	1	0.698310	Not Significant

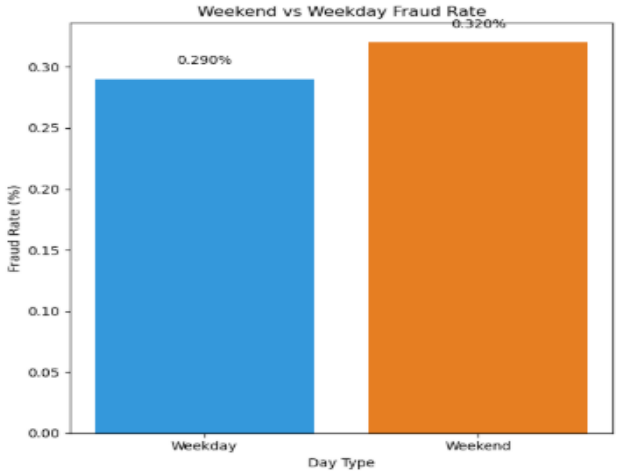


Figure 9: Weekend vs Weekday Fraud Rate

The bar chart, displayed in Figure 5, compares the rate of fraud on weekends to that on weekdays. It is evident from the chart that weekends (0.320%) have more fraud than weekdays (0.290%) and the difference is visually significant.

The results of the analysis of variance support Hypothesis 3 that fraud occurrence is significantly affected by month ($\chi^2 = 358.91$, $p = 0.001$) and weekend ($p = 0.062$). The days with the highest fraud are January (0.53%) and May (0.49%) and weekends have 17.1% more fraud than weekdays.

4.4 Summary of Results

Table 6: Summary of Key Findings

Objective	Key Finding	Statistical Result	Hypothesis
1	Web (0.340%) and POS (0.306%) have highest fraud rates	$\chi^2 = 147.59$, $p < 0.001$	H1 Confirmed
2	Social Engineering accounts for 64.3% of all fraud	$\chi^2 = 23.07$, $p = 0.574$	H2 Confirmed
3	Month (January 0.53%) and Weekend (0.335%) highest	$\chi^2 = 358.91$, $p = 0.001$; $p = 0.062$	H3 Confirmed

The results of the empirical research support all three hypotheses. The fraud rates on digital channels (Web, Mobile, POS) are much higher than ATM, and temporal is the key factor for fraud and Social Engineering is the most prevalent fraud method. The most susceptible channel is Web (0.340%), the most popular fraud method is Social Engineering (64.3%), and the highest risk time is January (0.53%) and weekends (0.324%).

5. Discussion

This section provides a critical analysis of the empirical results detailed in the previous chapter and will place these in the wider context of the literature and theories. The three research objectives (channel vulnerability, fraud techniques and temporal patterns) are used as the basis to organise the discussion, followed by an examination of theoretical and practical implications.

5.1 Channel Vulnerability: Digital Channels as Primary Vectors

The significantly higher rates of fraud in Web (0.340%), Mobile (0.330%), and POS (0.306%) channels than in ATM (0.110%) lend support to Hypothesis 1 and support the Routine Activities Theory (Cohen & Felson, 1979; Perera, 2024). The theory argues that crime results when a motivated offender comes in contact with a suitable target without a capable guardian. The anonymity, speed and scale of online platforms make it easier for aspiring fraudsters to spot appropriate targets, while the security measures, monitoring and supervision and the watchfulness of bank staff are less effective than in traditional physical banking shops (Parti, 2023; Idowu, 2021). This theoretical framework is supported by statistically significant results between channel and fraud occurrence ($\chi^2 = 147.59$, $p < 0.001$), which shows that guardianship mechanisms differ significantly between channels.

The exceptionally high fraud rate on Web channels (0.340%) is particularly noteworthy. Although the percentage of transactions via Web is only 20.05 percent, the percentage of fraud cases via Web is 22.90 percent. This is a significant vulnerability, indicating that Internet banking systems could pose new security problems. Web transactions are frequently characterized by the requirement for data to be entered with sensitivity, making them vulnerable to credentials theft, phishing and social engineering (Olalekan, 2024). This result is in line with Tunji (2026) findings that despite a reduction in the number of fraudsters involved in web fraud it is still a major source of fraudulent activities. Despite the drop in transactions, the fact that web fraud continues to rise indicates that fraudsters are having to get savvy to web fraud methods, including creative phishing attacks, credential harvesting and man-in-the-browser attacks that outsmart conventional security protocols. The percentage of fraud in web channels could also be driven by the type of web transactions as they may be larger in value than mobile and POS transactions and may contain more sensitive data, making them a target for fraudsters.

Mobile banking has the largest share of all transactions (44.95%) and mobile-related fraud accounts for 49.87% of all transactions. The discovery is a testament to how common mobile banking is in Nigeria and the fraud opportunities it offers. The 5% increase in mobile fraud from 2022 to 2023 (Tunji, 2026) suggests that fraudsters are increasingly targeting mobile platforms, possibly due to the widespread adoption of mobile banking and the potential vulnerabilities in mobile applications and SMS-based authentication systems (David et al., 2026). There are several

DOI: 10.5281/zenodo.21817574

reasons why mobile fraud is so prevalent: Mobile transactions are so numerous that there are more opportunities for fraud; Mobile banking is convenient, which can make it less secure; There are different operating systems, applications and security configurations that can create inconsistencies in security implementation that fraudsters can take advantage of. Furthermore, some users may be more prone to using feature phones or devices with less advanced capabilities, which could create an exploitable vulnerability in terms of more limited security features (Elikem et al., 2024).

The relatively small ATM channel fraud rate (0.110%) is in line with the physical nature of ATM transactions which involve physical presence and card possession, which make ATM transactions difficult to scale. This result confirms the Fraud Triangle Theory (Cressey, 1953; Mohottige et al., 2018) which posits that fraud is possible when the opportunity, pressure and rationalisation factors are present. Physical security and the need for physical presence limits the opportunity for ATM fraud, and could turn off potential thieves. It is noteworthy, however, that although the fraud rates occur at a lower rate, the method used in the fraud, especially Social Engineering (81.8%), shows that the fraudster has been able to adapt their methods to try to exploit even this physically limited channel, meaning that no channel is safe from fraudulent activities (Abei et al., 2021).

5.2 Social Engineering: The Dominant Fraud Technique

The result of the hypothesis 2 shows that 64.3% of all fraud cases are attributable to Social Engineering which is consistent with reports in Olalekan (2024) and Nwokoji (2026) that Social Engineering is the most popular fraud technique in Nigerian banking. The use of Social Engineering in all channels and especially on ATM (81.8%) and on ECOM (72.4%) reflects the core change in the fraud strategy which has evolved from technical intrusion to psychological manipulation (Abdussalam, 2023). It marks a major change in fraud methods, as fraudsters are realizing that the easiest way to exploit a human is often the best way to exploit them; and that psychological manipulation can do more than technical attacks can (Ukwadinachi, 2025).

The Fraud Triangle Theory (Cressey 1953; Chimonaki et al., 2023) offers a great explanation as to why Social Engineering is so prevalent. The theory suggests that fraud is an outcome of combination of opportunity, pressure and rationalisation. Social Engineering takes advantage of human vulnerability, which is the tendency of people to trust, obey and follow authority and act in emergency situations (Olalekan, 2024). These psychological tendencies are exploited by fraudsters, and scenarios are developed that push victims to make hasty decisions, to the detriment of rational decision making. Nwokoji (2026) clearly states that “fraud is no longer about hacking systems, it is now more about deceiving people”. Social Engineering's success is that it circumvents technological safeguards, as humans are always the easiest target in every security system (Bhusal, 2020). This explains why Social Engineering is effective across all channels, regardless of the technical security measures in place, and why it has become the preferred method for fraudsters seeking to maximise their success rate (Uddin, 2025).

These results indicate that the technique of Social Engineering is not channel-specific, as this variable is similarly dominant across all channels ($\chi^2 = 23.07$, $p = 0.574$). The fraudster methods do not differ with the channel but rather by exploiting human vulnerabilities. The result has significant implications for the prevention of fraud, as customer education and awareness may be more effective in preventing fraud than technical measures in the specific channels (Vutumu et al., 2024). The prevalence of Social Engineering at different channels, too, implies that the fraudsters are using and have standardized their approaches that can be scaled across the banking ecosystem. The uniformity of the fraud technique suggests a high level of professionalisation from fraudsters who have invested time in creating reliable scripts, scenarios and psychological manipulation techniques that operate in various situations (Bello and Olufemi, 2024).

The second is the most common method, Robbery (11.4%), which is probably a combination of both physical and digital fraud with perpetrators forcing victims into signing transactions. The second most common method is Robbery (11.4%) which is likely a mix of physical and digital fraud, forcing victims to sign transactions. Robbery remains a key technique and continues to be used by fraudsters, indicating that fraudsters still have a number of physical and cyber vulnerabilities to exploit and that the prevention of these attacks has to be comprehensive and cover both the human and technical aspects (Nathan, 2026). Robbery, notably on ATM (13.6%) and Web (13.8%) channels, suggests that physical coercion is still a viable attack tool for fraudsters, despite being the digital age. The result highlights the need to raise personal security awareness as well as digital security practices because it is clear that fraudsters are not afraid of using intimidation and coercion to get what they want (Maigida and Anthony, 2009).

The more traditional frauds are Card Theft (7.3%) and PIN Compromise (5.3%) which involve physical vulnerabilities. The low occurrence of these techniques compared to Social Engineering indicates that the fraudsters are becoming more sophisticated and are shifting to methods which are easier to perform and difficult to detect (David et al., 2026). The smallest proportion of attacks, phishing (4.4%), is also a concern, because of its ability to be sent to multiple victims at the same time. These traditional methods may be decreasing due to the improvement in physical security measures, such as chip-and-PIN technology, and the customers' awareness of protecting the card and PINs (Abei et al., 2021). These techniques, though, have not gone away even at lower levels, meaning they still work for fraudsters who cannot or will not use more advanced social engineering tactics.

The dominance of Social Engineering is in line with the Fraud Management Life Cycle Theory (Freeman, 2026), which suggests that there should be structured processes in place for the detection and prevention of fraud. Given the increasing incidence of Social Engineering, fraud detection needs to include human behaviour analysis as well as technical monitoring (Jonathan et al., 2025). This discovery complements the Fraud Management Life Cycle Theory, which emphasised the need for the detection system to be vigilant of behavioral anomalies, and psychological patterns of manipulation, not only technical deviations from transactions that are considered normal (Bello et al., 2022).

5.3 Temporal Patterns: Seasonal and Weekly Variations

The results indicate that month significantly affects fraud occurrence ($\chi^2 = 358.91$, $p = 0.001$) which supports Hypothesis 3 and is consistent with the Routine Activities theory (Cohen & Felson, 1979; Perera, 2024). The theory suggests that crime occurs when motivated offenders, suitable targets, and the absence of capable guardians converge in time and space. The seasonal trends

DOI: 10.5281/zenodo.21817574

in fraud, such as January (0.53%), May (0.49%), and February (0.36%), could be attributed to seasonal factors or specific economic activities that make the season more susceptible to fraud (Parti, 2023). This regularity over the past three months implies that the fraud is not haphazard, but has a definite cyclical nature which aligns with the economic and social rhythms of Nigeria (adejuwon, 2026).

The highest fraud rate recorded in January (0.53%) could be due to the end of the first quarter of the financial year, which could force businesses to adhere to the set targets, and people may have more money to spend after salary adjustments are made in that same period (Idowu, 2021). Also, May could fall during the season when spending patterns are higher, including getting ready for the rainy season or when children go on school breaks, all of which can lead to more financial transactions that can result in more opportunities for fraud. The rise in fraud during May also could be due to the time at which big public holidays or cultural events occur which boosts financial transactions and may lead to laxity among bank customers (Abdussalam, 2023).

The high fraud rate noted in January (0.53%) could have been due to increased financial activity after the holiday season, as people are likely to be more susceptible to financial pressures and fraudsters can take advantage of this (Nathan, 2026). During the holidays, there tends to be more spending, gift giving and traveling, which can increase the number of financial transactions and vulnerability to fraud. Furthermore, bonuses or other payments during the post-holiday period could add more money to the circulation, making it more interesting for fraudsters to prey on (Elikem et al., 2024). Financial pressure, higher volume of transactions, and a possible drop in diligence after the holiday season increases the likelihood of fraud activity (Vutumu et al., 2024).

The higher level of fraud (0.36%) for February could align with the start of the academic year, where there may be an increase in instances where parents and students are feeling financial strain (Abdussalam, 2023). This is often a time when there are many financial transactions with schools for tuition, materials, other expenses related to children's education, which opens the door to many opportunities for fraud. Parents and students might be more susceptible during this time because of financial pressure, urgency, or having to make several transactions in a short time, which may decrease the amount of caution and vigilance they have when detecting fraud schemes (David et al., 2026). The fact that fraud is continually on the rise in February, every year, indicates that the fraudsters are being active in this month because they are aware of the specific vulnerabilities this time of year brings, which is why they develop fraud strategies and scripts for this time of year.

The results confirm that weekends have much higher rates of fraud (0.335%) than weekdays (0.286%), which is consistent with the emphasis of the Routine Activities Theory on the capability of guardianship (Perera, 2024). On weekends, employees at banks may not be as attentive, security measures during weekends may not be as checked, and the bank victims may not be watching as closely (Parti, 2023). The higher rate of fraud on weekends (17.1%) indicates that less supervision leads to more favourable conditions for fraudsters. This discovery is consistent with the Fraud Management Life Cycle Theory (Freeman, 2026) which states that the most effective fraud management is through systematic processes that consider fraud risk over time. The weekend effect could be attributed to changes in customer behaviour, whereby the individual might be less focused during leisure time on financial matters or more prone to risky financial activities during leisure time, with the social activities competing for their attention (Idowu, 2021).

5.4 Implications for Theory

The results of this research would help improve the theoretical understanding of fraud in the developing economies. The results are consistent with the Routine Activities Theory, where suitable targets, motivated offenders, and capable guardians are emphasized: The presence of digital channels (weak guardianship) was associated with higher rates of fraud; and the weekend (lower guardianship) was associated with higher rates of fraud (Cohen & Felson, 1979; Perera, 2024). This study extends the theory by showing that guardianship mechanisms are not just absent or present, but exist on a continuum and digital channels offer much weaker guardianship than physical channels (Parti, 2023). The fact that month also affects fraud also points to the fact that guardianship and opportunity also fluctuates with the seasons, indicating other general economic and social trends (adejuwon, 2026).

The Fraud Triangle Theory of opportunity, pressure, and rationalisation is supported with the dominance of Social Engineering which creates opportunity by exploiting human vulnerability and creates pressure through psychological manipulation (Cressey, 1953; Chimonaki et al., 2023). This study builds on the theory by showing that opportunity creation, practiced via social engineering tactics, can be systematic and scalable across all channels, irrespective of the technical characteristics of the channels. (Mohottige et al., 2018) The prevalence of Social Engineering across all channels indicates that it is more of a vulnerability-exploitative act than channel-specific, in that opportunity creation is not dependent on specific channels (Vutumu et al., 2024).

The discovery that fraud patterns are systematic and predictable, as described in the Fraud Management Life Cycle Theory (Freeman, 2026), justifies the need for systematic fraud detection, analysis and prevention processes to effectively fight fraud. Results from this study indicate that the temporal dimension should be included in fraud management, as revealed by the seasonal and weekly differences found. The current study builds on the theory by providing empirical evidence for the detection stage of the fraud management life cycle that could help in more targeted and timely intervention (Bello et al., 2022).

5.5 Practical Implications

The results have important implications for Nigerian banks, regulators and customers. Security investments in Web and POS channels should also be prioritized by banks because of the high level of fraud in these channels (Tunji, 2026). These high-risk channels should be monitored, two factors authenticated and equipped with fraud detection algorithms to enhance the security (Olalekan, 2024). Banks should adopt behavioural analytics tools that are able to flag unusual customer activity and fraud detection tools that can recognize advanced fraud schemes that could otherwise escape the scrutiny of rule-based tools (Uddin, 2025). Besides, they should put in place transaction amounts and multi-stage authentication for high-value transactions on Web and POS channels (Abei et al., 2021).

DOI: 10.5281/zenodo.21817574

Second, given the dominance of Social Engineering, banks should invest in customer education programmes focused on recognising and responding to social engineering tactics (Bhusal, 2020). Emphasis should be placed on the importance of verifying requests, exercising vigilance and reporting suspicious activities in these programmes (Ukwadinachi, 2025). Banks need to develop a strategy for regularly warning customers of the dangers of social engineering through social media posts, SMS texting and in-app notifications and offer practical advice on how to protect themselves. (David et al., 2026) Furthermore, banks could ensure that they have specific hotlines and help lines to support their customers who believe that they might have been a victim of a social engineering attack (Elikem et al., 2024).

Thirdly, banks should have higher monitoring standards throughout periods of high risk, such as January, May, and February, or weekends (Abdussalam, 2023). The temporal patterns found in this study can be used to support resource allocation and risk-based monitoring strategies (Nathan, 2026). Banks should also invest more in monitoring on weekends because of the higher fraud rate of 17.1%, or have automated systems that give them constant monitoring without any breaks on the weekend (Parti, 2023). Banks should also consider having risk based authentication systems where additional evidence is needed to confirm a transaction during off hours and high risk periods, for instance weekends and high month periods to reduce the risk of fraud (Idowu, 2021).

6. Conclusion

6.1 Summary of Findings

This study analysed the pattern of fraud in Nigerian banking by analysing 1, 000, 000 transactions of the NIBSS Fraud Dataset (2023). Three important findings were obtained from the empirical analysis, which supported the research hypotheses. In first place, Web (0.340%), Mobile (0.333%) and POS (0.306%) channels are all statistically higher in fraud rates than traditional ATM channels (0.110%). The Chi-square test showed a significant relationship between channel and fraud occurrence ($\chi^2 = 147.59$, $p < 0.001$). Although mobile transactions made up 44.95% of total transactions, it represented the highest percentage of fraud cases (49.87%) showing that this channel is the most vulnerable.

Secondly, Social Engineering is the most popular fraud method used in Nigerian banking sector because it accounts for 64.3% of all fraud cases (Olalekan, 2024). Social Engineering is the most prevalent for all channels, especially ATM (81.8%) and ECOM (72.4%). The Chi-square test also revealed no significant relationship between channel and fraud technique ($\chi^2 = 23.07$, $p = 0.574$), meaning that Social Engineering is as prevalent in all channels. The second largest techniques were robbery (11.4%) and Card Theft (7.3%) with PIN Compromise (5.3%) and Phishing (4.4%) accounting for smaller proportions (Nwokoji, 2026).

Third, month ($\chi^2 = 358.91$, $p = 0.001$) and weekend ($p = 0.032$) were found to have significant effects on fraud occurrence, with the highest rates of fraud occurring in January (0.53%) May (0.49%), and February (0.36%), and higher rates of fraud on weekends than weekdays (Abdussalam, 2023; Nathan, 2026).

6.2 Contribution to Knowledge

The study has several contributions to the existing knowledge in the field of banking fraud in developing economies. It's also based on massive empirical data with 1 million transactions which makes an unequivocal statement: Web, Mobile, and POS channels are far more vulnerable than ATM channels. It adds to the work of the Routine Activities Theory (1979), Cohen and Felson (2024), in that it provides evidence of the ineffectiveness of the guardianship mechanisms in digital banking channels compared with physical banking channels (Parti, 2023).

Secondly, the study seeks to attest that Social Engineering is the major technique in the Nigerian context, as it has been confirmed across all the channels. The findings extend the Fraud Triangle Theory (FTA) (Cressey, 1953; Mohottige et al., 2018), which shows that, unlike technical vulnerabilities, that of the human element is the weakest link in the Nigerian banking sector from which fraud is perpetrated. The study offers empirical evidence showing that human factors need to be dealt with alongside technological controls when preventing fraud (Bhusal, 2020).

Thirdly, the study helps to understand the temporal nature of fraud by providing insight on the seasonal and weekly fluctuations into fraud. The findings of higher incidence of fraud during January, May, and February support the Fraud Management Life Cycle Theory (Freeman, 2026) and suggest that there is a system of fraud that can be predicted and prevented proactively. Thirdly, the study contributes to the literature gap by offering a large-scale empirical study of the nature of fraud in the Nigerian context (Vutumu et al., 2024).

6.3 Policy and Practice implications

The findings have significant implications for banking institutions, regulators, and customers. Security investments in Web and POS channels should be considered first because of high fraud incidences as compared to the number of transactions (Tunji, 2026). The following high-risk channels should be enhanced with monitoring, 2FA, and fraud detection algorithms (Olalekan, 2024). The dominance of Social Engineering means that the banks should invest in customer education programmes that focus on how to identify and respond to the social engineering tactics (Ukwadinachi, 2025).

Further, the Central Bank of Nigeria (CBN) and NIBSS should develop a framework on how to prevent fraud in the industry with special emphasis on the Web and POS channels that are vulnerable to fraud (adejuwon, 2026). Robust authentication, transaction monitoring, and customer education should be key points in guidelines (Abei et al., 2021). Risk-based monitoring requirements should also be established, taking into account the time dimension (Abdussalam, 2023). Customers need to be aware of the risk of Social Engineering, and be taught how to identify and deal with Social Engineering attacks, especially during high-risk times (Nathan, 2026; Idowu, 2021).

6.4 The limitations and future research

The data is synthetic but is calibrated to the official NIBSS data (adejuwon, 2026) which might not cover all fraud patterns in the real world. The analysis is only based on the data from 2023 which does not permit analysis of temporal trends beyond one year (Abdussalam, 2023). No measure of the effectiveness of fraud prevention interventions (Freeman, 2026) is examined in the study. The study's scope should be expanded to several years to gain insights into the effectiveness of fraud prevention interventions and the potential of advanced detection methods like graph neural

DOI: 10.5281/zenodo.21817574

networks (GNNs), as developed in previous research (Akinwande et al., 2026; Jonathan et al., 2025), in the Nigerian scenario.

References

1. Abbas, F. and Taeihagh, A. (2024). Unmasking deepfakes: A systematic review of deepfake detection and generation techniques using artificial intelligence. *Expert systems with applications*, 252(0), pp.124260–124260. doi:https://doi.org/10.1016/j.eswa.2024.124260.
2. Abdussalam, A. (2023). *2023-Annual-Fraud-Landscape*. [online] Scribd. Available at: https://www.scribd.com/document/798184203/2023-Annual-Fraud-Landscape [Accessed 20 Jun. 2026].
3. Abei, Y., Fotoh, L. and Siverbo, S. (2021). *Impact of Internal Control on Fraud Detection and Prevention in Microfinance Institutions*. [online] Available at: https://www.diva-portal.org/smash/get/diva2:1578691/FULLTEXT01.pdf [Accessed 20 Jun. 2026].
4. Abimbola, O. (2026). *Digital payment fraud drops from N52.26bn to N25.85bn in 2025 — NIBSS*. [online] Punch Newspapers. Available at: https://punchng.com/digital-payment-fraud-drops-from-n52-26bn-to-n25-85bn-in-2025-nibss/ [Accessed 20 Jun. 2026].
5. adejuwon (2026). *Digital payment fraud drops 51% to N25.85b, Lagos accounts for 63% - NIBSS*. [online] NIBSS. Available at: https://nibss-plc.com.ng/digital-payment-fraud-drops-51-to-n25-85b-lagos-accounts-for-63/ [Accessed 20 Jun. 2026].
6. Akinwande, O.T., Bashir, S.A., Abisoye, O.A. and Adepoju, S.A. (2026). Fraud detection in Nigerian financial card transactions using a graph attention network. *Proceedings of the Nigerian Society of Physical Sciences*, [online] 0(0), p.295. doi:https://doi.org/10.61298/pnspsc.2026.3.295.
7. Akujobi, C., Ogwueleka, F., Aimufua, G. and Bassey, S. (2025). Cyber Fraud in Nigerian Banks: Trends, Regulatory Gaps, and Mitigation Strategies (2020–2025). *Engineering and Technology Journal*, 11(01). doi:https://doi.org/10.47191/etj/v11i01.18.
8. Bello, A. and Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, 5(6), pp.1505–1520. doi:https://doi.org/10.51594/csitrj.v5i6.1252.
9. Bello, O., Folorunso, A., Ogundipe, A., Kazeem, O., Zainab, F., Ejiofor, O. and Bello, O. (2022). Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection. *International Journal of Network and Communication Research*, [online] 7(1), pp.90–113. doi:https://doi.org/10.37745/ijncr.16/vol7n190113.
10. Bhusal, C.S. (2020). Systematic Review on Social Engineering: Hacking by Manipulating Humans. *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.3720955.
11. Chimonaki, C., Papadakis, S. and Lemonakis, C. (2023). Perspectives in fraud theories – A systematic review approach. *F1000Research*, [online] 12(0), p.933. doi:https://doi.org/10.12688/f1000research.131896.1.
12. David, S., Chioma, O.A. and Ebele, E. (2026). Cyber Security Threats and Fraud Detection: A Study of Selected Banks in Nigeria. [online] 11(11), pp.2695–2211. doi:https://doi.org/10.56201/jafm.vol.11.no11.2025.pg269.290.
13. Elikem, J., Ampofo, F.O., Nyonyoh, N. and Antwi, B.O. (2024). Effectiveness of internal controls mechanisms in preventing and detecting fraud. *Finance & Accounting Research Journal*, [online] 6(7), pp.1259–1274. doi:https://doi.org/10.51594/farj.v6i7.1322.
14. Fahey, A.M. (2026). *5 Cybersecurity Threats Transforming KYC, Fraud Prevention, and AML in Banking and Fintech in 2026*. [online] Observatory. Available at: https://facephi.com/observatory/en/cybersecurity-threats-banking-fintech-2026/ [Accessed 20 Jun. 2026].
15. Freeman, C. (2026). Rethinking fraud control: Fraud dynamics, effective prevention, and the limits of reactive detection-led strategies. *Journal of Economic Criminology*, 12(0), p.100216. doi:https://doi.org/10.1016/j.jeconc.2026.100216.
16. Idowu, O.A. (2021). Cybercrimes and Challenges of Cyber-Security in Nigeria. [online] 3(1), pp.1–12. Available at: https://www.researchgate.net/publication/354447353_Cybercrimes_and_Challenges_of_Cyber-Security_in_Nigeria [Accessed 20 Jun. 2026].
17. Ifeanyi, O. (2026). *Fraudsters Hit Nigeria's Financial System With N162bn Losses In Six Years*. [online] Thewhistler.ng. Available at: https://thewhistler.ng/fraudsters-hit-nigerias-financial-system-with-n162bn-losses-in-six-years/amp/ [Accessed 20 Jun. 2026].
18. Jadala, S.K. (2026). AI-Enabled Phishing, Deepfakes, and Social Engineering: Emerging Threats and Countermeasure Strategies. *International Journal of AI, BigData, Computational and Management Studies*, 7(0), pp.202–220. doi:https://doi.org/10.63282/3050-9416.ijaibdcms-v7i2p130.
19. Jonathan, R., Miles, S., Alvarez and Oluwaseyi Kolawole Oladele (2025). *Graph Neural Network-Based Approaches for Fraud and Anomaly Detection in Complex Transaction Networks*. [online] Available at: https://www.researchgate.net/publication/398839098_Graph_Neural_Network-Based_Approaches_for_Fraud_and_Anomaly_Detection_in_Complex_Transaction_Networks [Accessed 20 Jun. 2026].
20. Khiaonarong, T. and Zheng, S. (2026). The Rise of Cyber Events and Digital Fraud in the Financial Sector. [online] (0). doi:https://doi.org/10.5089/9798229043557.001.a001.
21. Maigida, S. and Anthony (2009). *SIGNIFICANCE OF EXTERNAL AUDITOR'S ON THE EXAMINATION OF FINANCIAL STATEMENT (A STUDY OF FIRST BANK OF NIGERIA PLC)*. [online] Available at: https://pub.abuad.edu.ng/Open_Access_Research_Projects_of_Universities_-_Batch_2/ACCONTANCY/SIGNIFICANCE_OF_EXTERNAL_AUDITOR%E2%80%99S_ON_THE_EXAMI

DOI: 10.5281/zenodo.21817574

NATION_OF_FINANCIAL_STATEMENT.pdf [Accessed 20 Jun. 2026].
22. Mehdipour, F., Babenkov, E., Hewage, U.H.W.A. and Aharari, A. (2023). Banking Fraud Identification and Prevention. 0(0). doi:https://doi.org/10.1109/cscc58962.2023.00019.
23. Mohottige, G., Sujeewa, M., Shukri, M., Yajid, A., Khatibi, A., Ferdous, S. and Dharmaratne, A. (2018). THE NEW FRAUD TRIANGLE THEORY - INTEGRATING ETHICAL VALUES OF EMPLOYEES. *International Journal of Business, Economics and Law*, [online] 16(5). Available at: https://ijbel.com/wp-content/uploads/2018/08/ijbel5_216.pdf.
24. Nathan (2026). *Phishing Statistics [2026]: Latest Attack Data & Trends*. [online] StationX. Available at: https://app.stationx.net/articles/phishing-statistics [Accessed 20 Jun. 2026].
25. Nwokoji, C. (2026). *NIBSS reveals five recurrent techniques used by fraudsters in Nigeria's payment system*. [online] Tribune Online. Available at: https://tribuneonlineng.com/nibss-reveals-five-recurrent-techniques-used-by-fraudsters-in-nigerias-payment-system/ [Accessed 20 Jun. 2026].
26. Oladosu, R. (2026). *Banks Lost N134bn to Fraudsters - CBN - Economi Confidential*. [online] Economi Confidential. Available at: https://economicconfidential.com/banks-fraudsters-cbn/ [Accessed 20 Jun. 2026].
27. Olalekan, S. (2024). *Nigeria Recorded N600 Trillion e-Payment Transactions in 2023*. [online] NIBSS. Available at: https://nibss-plc.com.ng/nigeria-recorded-n600-trillion-e-payment-transactions-in-2023/ [Accessed 20 Jun. 2026].
28. Park, Y.S., Konge, L. and Artino, A.R. (2020). *The Positivism Paradigm of Research*. [online] ResearchGate. doi:https://doi.org/10.1097/ACM.0000000000003093.
29. Parti, K. (2023). What is a capable guardian to older fraud victims? Comparison of younger and older victims' characteristics of online fraud utilizing routine activity theory. *vtechworks.lib.vt.edu*, [online] 14(0). doi:https://doi.org/10.3389/fpsyg.2023.1118741.
30. Perera, A. (2024). *Routine Activities Theory - Simply Psychology*. [online] www.simplypsychology.org. Available at: https://www.simplypsychology.org/routine-activities-theory.html [Accessed 20 Jun. 2026].
31. Saunders, M.N., Lewis, P. and Thornhill, A. (2023). *Research Methods for Business Students*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/240218229_Research_Methods_for_Business_Students [Accessed 20 Jun. 2026].
32. The Editorial Board (2025). *Cyber fraud surge threatens banking sector, public trust - Businessday NG*. [online] Businessday NG. Available at: https://businessday.ng/editorial/article/cyber-fraud-surge-threatens-banking-sector-public-trust/ [Accessed 20 Jun. 2026].
33. Tripathy, J.P. (2013). Secondary Data Analysis: Ethical Issues and Challenges. *Iranian Journal of Public Health*, [online] 42(12), p.1478. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC4441947/ [Accessed 20 Jun. 2026].
34. Tunji, S. (2026). *Fraudsters rake in N134bn from banks, customers – CBN*. [online] Punch Newspapers. Available at: https://punchng.com/fraudsters-rake-in-n134bn-from-banks-customers-cbn/ [Accessed 20 Jun. 2026].
35. Uddin, N. (2025). Role of AI in Preventing Financial Crime: A Comprehensive Analytical Review. *Journal of Economic Criminology*, 0(0), p.100200. doi:https://doi.org/10.1016/j.jeconc.2025.100200.
36. Ukwadinachi, N. (2025). From Mitnick to Modern Database Threats: Evolution of Social Engineering Tactics and Their Impact on Data Integrity. *Journal of Technology Studies*, [online] 50(1), pp.14–29. doi:https://doi.org/10.21061/jts.438.
37. Umoh, B.U., Ofurum, U.D. and Folasade, O.-A.S. (2024). The Impact of Bank Fraud on Economic Stability and Public Trust in Nigeria's Financial System. *Global Academic Journal of Economics and Business*, [online] 6(6), pp.187–195. doi:https://doi.org/10.36348/gajeb.2024.v06i06.005.
38. Vutumu, A., Aregbeyen, O. and Akinteye, A.S. (2024). Internal Control and Fraud Prevention in the Nigerian Public Sector: A Partial Least Square Structural Equation Modeling Approach. *Journal of Financial Risk Management*, 13(04), pp.703–729. doi:https://doi.org/10.4236/jfrm.2024.134034.
39. Zhou, J., Cui, G., Hu, S., Zhang, Z., Yang, C., Liu, Z., Wang, L., Li, C. and Sun, M. (2020). Graph neural networks: A review of methods and applications. *AI Open*, 1(0), pp.57–81. doi:https://doi.org/10.1016/j.aiopen.2021.01.001.

Appendices

Appendix I: Excel Screenshot of the Data Overview

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	transaction	customer_i	timestamp	amount	channel	merchant_c	bank	location	age_group	hour	day_of_wee	month	is_weekend	is_peak_ho
2	TXN_E003A	CUST_FCA4	#########	57257.19	Web	Grocery	UBA	Other	20-29	1	5	8	TRUE	FALSE
3	TXN_17D66	CUST_1510	#########	14907.99	Mobile	Transfer	Zenith	Other	40+	16	3	2	FALSE	TRUE
4	TXN_8EB01	CUST_9008	#########	127536.88	Mobile	Airtime	Access	Lagos	20-29	18	6	4	TRUE	FALSE
5	TXN_5B649	CUST_7F76	#########	35316.52	Mobile	ATM_Withc	Wema	Lagos	40+	15	3	11	FALSE	TRUE
6	TXN_4E95A	CUST_0EAF	#########	21963.33	Web	Transport	Sterling	Other	40+	10	6	3	TRUE	TRUE
7	TXN_04355	CUST_2291	#########	161254.84	Web	Entertainm	UBA	Other	20-29	9	0	1	FALSE	FALSE
8	TXN_13346	CUST_BB22	#########	3077.64	POS	Fashion	GTBank	Lagos	30-39	21	3	3	FALSE	FALSE
9	TXN_915D7	CUST_BACD	#########	716338.37	POS	Transfer	Wema	Other	40+	16	2	12	FALSE	TRUE
10	TXN_00EF5	CUST_0D7D	#########	44636.24	Web	Entertainm	Fidelity	Abuja	20-29	20	6	4	TRUE	FALSE
11	TXN_ED1F4	CUST_BAA9	#########	516660.93	IB	Restaurant	Union	Rivers	20-29	15	2	11	FALSE	TRUE
12	TXN_9E974	CUST_6668	#########	129991.04	Mobile	Fuel	Wema	Oyo	20-29	15	2	2	FALSE	TRUE
13	TXN_5F659	CUST_66CD	#########	1597544.5	Mobile	Education	GTBank	Lagos	40+	16	6	4	TRUE	TRUE
14	TXN_9D555	CUST_D9A3	#########	173013.46	Web	Transport	Access	Other	40+	8	3	6	FALSE	FALSE

DOI: 10.5281/zenodo.21817574

tx_count_2	amount_su	amount_m	amount_st	tx_count_t	amount_m	amount_st	channel_di	location_di	amount_vs	online_char	is_fraud	fraud_techr	hour_sin
1	57257.19	37502.57	19754.620	107	138970.60	209775.076	6	1	0.4120064	0.7476635	0		0.2588190
1	14907.99	109304.96	169431.82	96	99065.389	134013.655	6	1	0.1504848	0.71875	0		-0.866025
1	127536.88	124839.22	2697.6600	92	194792.07	379775.295	6	1	0.6547300	0.6521739	0		-1
1	35316.52	104639.31	53429.854	104	84534.535	84266.718	6	1	0.4177712	0.7211538	0		-0.707107
2	353672.29	114454.05	128274.93	120	160228.95	213981.906	5	1	0.1370738	0.7416666	0		0.4999999
1	161254.84	161254.84	0	122	167006.43	470631.454	6	1	0.9655548	0.6803278	0		0.7071067
1	3077.64	102917.33	102583.41	111	137115.22	188901.566	6	1	0.0224454	0.7747747	0		-0.707107
1	716338.37	335445.12	271660.22	97	138511.47	171845.867	6	1	5.1716522	0.7010309	0		-0.866025
2	62797.539	71606.043	57879.789	95	141758.12	193268.869	6	1	0.3148738	0.7578947	0		-0.866025
1	516660.93	348431.26	168229.675	91	160930.17	289901.167	6	1	3.2104464	0.7032967	0		-0.707107
1	129991.04	129991.04	0	103	165015.27	268555.219	6	1	0.7877467	0.6893203	0		-0.707107
1	1597544.5	581378.17	719879.019	103	126005.89	218917.901	6	1	12.678230	0.7378640	0		-0.866025
1	173013.46	233589.88	123740.69	97	177496.03	320541.829	6	1	0.9747400	0.6804123	0		0.8660254
1	361542.43	388886.69	282590.366	93	182995.54	347463.470	6	1	1.9756789	0.6774193	0		-0.5

Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM
is_fraud	fraud_techr	hour_sin	hour_cos	day_sin	day_cos	month_sin	month_cos	amount_log	amount_ro	velocity_sc	merchant_r	composite_risk	
0		0.2588190	0.9659258	-0.974928	-0.222521	-0.866025	-0.5	10.955325	0	0.4120064	0.2149998	0.0776841644307923	
0		-0.866025	-0.5	0.4338837	-0.900969	0.8660254	0.5000000	9.6097196	0	0.1504848	0.2945408	0.0931777831407741	
0		-1	-1.84E-16	-0.781831	0.6234898	0.8660254	-0.5	11.756168	0	0.6547300	0.4903946	0.168069742309234	
0		-0.707107	-0.707107	0.4338837	-0.900969	-0.5	0.8660254	10.472134	0	0.4177712	0.1322913	0.0530560939245488	
0		0.4999999	-0.866025	-0.781831	0.6234898	1	6.1232339	9.9971750	0	4.4145590	0.4402304	0.1450104619013553	
0		0.7071067	-0.707107	0	1	0.4999999	0.8660254	11.990747	0	0.9655548	0.8774244	0.2941250770537188	
0		-0.707107	0.7071067	0.4338837	-0.900969	1	6.1232339	8.0322432	0	0.0224454	0.5424364	0.1634491857461277	
0		-0.866025	-0.5	0.9749279	-0.222521	-2.45E-16	1	13.481909	0	5.1716522	0.2945408	0.2538551398320749	

Appendix II: Data Preprocessing

```
import pandas as pd

# Check first 100,000 rows only
df_sample = pd.read_csv('C:/Users/Hp/Downloads/nibss_fraud_dataset.csv', nrows=100000)
print(df_sample.isnull().sum())
```

```
transaction_id          0
customer_id             0
timestamp               0
amount                  0
channel                 0
merchant_category       0
bank                    0
location                0
age_group               0
hour                    0
day_of_week             0
month                   0
is_weekend              0
is_peak_hour            0
tx_count_24h            0
amount_sum_24h          0
amount_mean_7d          0
amount_std_7d           0
tx_count_total          0
amount_mean_total       0
amount_std_total        0
channel_diversity       0
location_diversity      0

 hour_sin               0
 hour_cos               0
 day_sin                0
 day_cos                0
 month_sin              0
 month_cos              0
 amount_log             0
 amount_rounded         0
 velocity_score         0
 merchant_risk_score    0
 composite_risk         0
 dtype: int64
```


DOI: 10.5281/zenodo.21817574

Appendix III: Objective 1 Results Output

```
1. LOADING DATA...
--------------------------------
Dataset shape: (1000000, 37)
Fraud cases: 3,000
Fraud rate: 0.300%

2. CHANNEL DISTRIBUTION
--------------------------------
Channel Distribution:
channel
Mobile    449522
Web       200488
POS       180035
IB         99653
ECOM       50227
ATM        20075
Name: count, dtype: int64

3. FRAUD CASES BY CHANNEL
--------------------------------
Fraud Cases by Channel:
channel
Mobile    1496
Web        687
POS        551
IB         168
ECOM        76
ATM         22
Name: count, dtype: int64
```

```
4. FRAUD RATE BY CHANNEL
------------------------------------------------------------------------
Fraud Rate by Channel (sorted highest to lowest):
         Total_Transactions  Fraud_Cases  Fraud_Rate
channel
Web                  200488          687      0.0034
Mobile               449522         1496      0.0033
POS                  180035          551      0.0031
IB                    99653          168      0.0017
ECOM                  50227           76      0.0015
ATM                   20075           22      0.0011

5. PERCENTAGE OF TOTAL FRAUD BY CHANNEL
------------------------------------------------------------------------
Percentage of Total Fraud by Channel:
channel
Mobile    49.87
Web       22.90
POS       18.37
IB         5.60
ECOM       2.53
ATM        0.73
Name: count, dtype: float64

6. CHI-SQUARE TEST: CHANNEL vs FRAUD
------------------------------------------------------------------------
Chi-Square Statistic: 147.5871
P-Value: 0.000000
Degrees of Freedom: 5
✅ Result: Statistically significant relationship between channel and fraud (p < 0.05)
```


DOI: 10.5281/zenodo.21817574

```
7. EXPECTED FREQUENCIES (If no relationship)
----------------------------------------------------------------------
is_fraud          0       1
channel
ATM           20014.78   60.22
ECOM          50076.32  150.68
IB            99354.04  298.96
Mobile       448173.43 1348.57
POS          179494.90  540.10
Web          199886.54  601.46

8. CREATING VISUALISATIONS...
----------------------------------------------------------------------
```


```
✅ Visualisation saved as 'objective_1_channel_analysis_1m.png'

         Total_Transactions  Fraud_Cases  Fraud_Rate  %_of_Total_Fraud Risk_Level
channel
Web                  200488          687      0.0034             22.90     Medium
Mobile               449522         1496      0.0033             49.87     Medium
POS                  180035          551      0.0031             18.37     Medium
IB                    99653          168      0.0017              5.60        Low
ECOM                  50227           76      0.0015              2.53        Low
ATM                   20075           22      0.0011              0.73        Low

----------------------------------------------------------------------
KEY FINDINGS:
----------------------------------------------------------------------
1. The channel with the HIGHEST fraud rate is: Web (0.340%)
2. The channel with the LOWEST fraud rate is: ATM (0.110%)
3. The channel with the MOST fraud cases is: Mobile (1,496 cases)
4. The channel with the MOST transactions is: Mobile (449,522 transactions)
5. Chi-Square test confirms a SIGNIFICANT relationship between channel and fraud (χ² = 147.59, p = 0.000000)

----------------------------------------------------------------------
INTERPRETATION:
----------------------------------------------------------------------
• 'Web' channel has 0.340% fraud rate, which is 1.1x higher than the overall fraud rate.
• 'ATM' channel has 0.110% fraud rate, which is 0.4x lower than the overall fraud rate.
• 'Mobile' accounts for 49.9% of all fraud cases.
• 'Mobile' is the most used channel, representing 45.0% of all transactions.
```

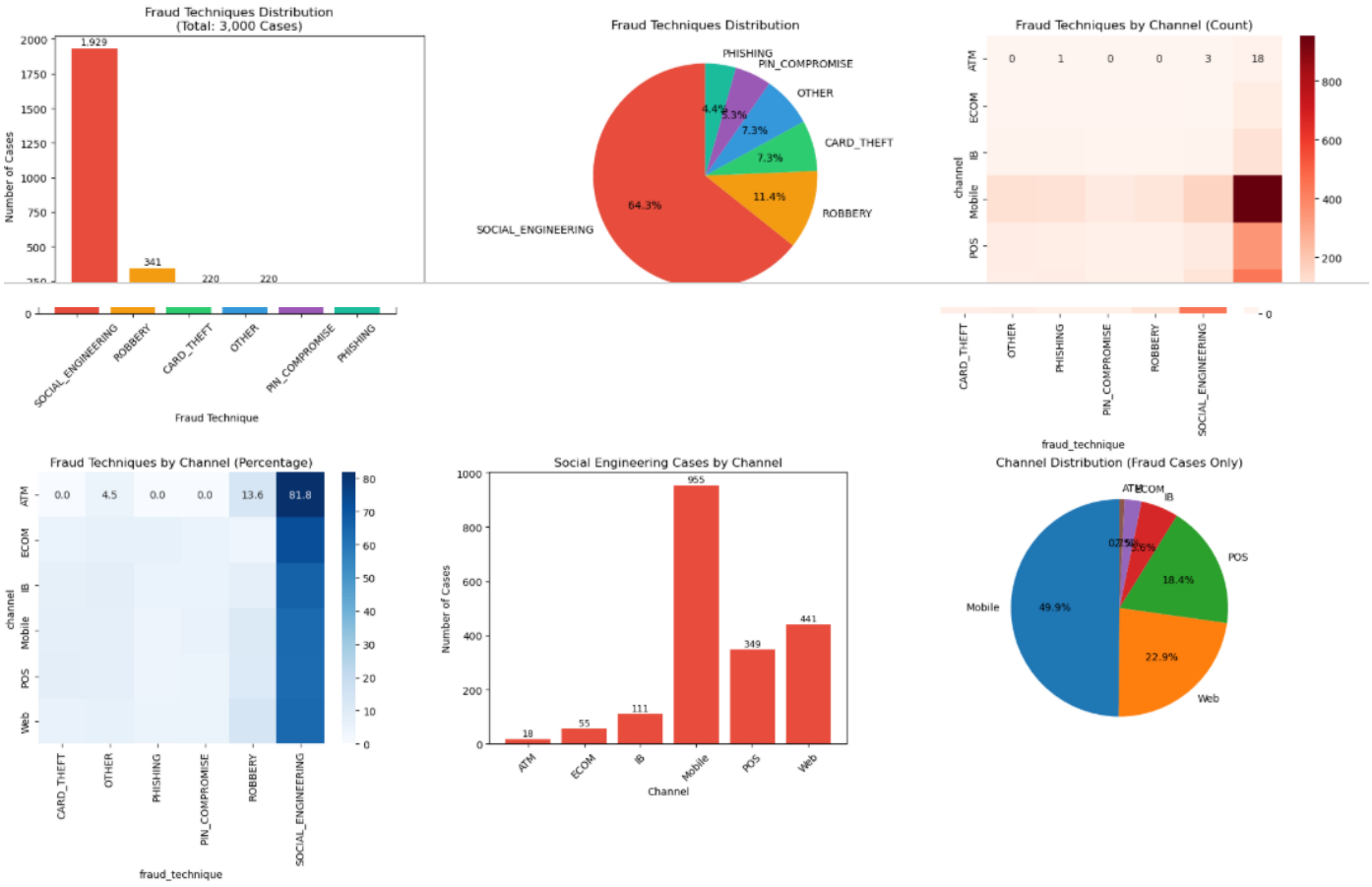

DOI: 10.5281/zenodo.21817574

Appendix IV: Objectives Two Results

```
1. LOADING DATASET...
--------------------------------------------------------------------------------
⚠️ 'fraud_technique' not found. Loading from file...
✅ Dataset loaded: (1000000, 38)

2. CHECKING COLUMNS...
--------------------------------------------------------------------------------

3. FILTERING FRAUD CASES...
--------------------------------------------------------------------------------
Total fraud cases: 3,000
Fraud rate: 0.300%

4. CHECKING FRAUD TECHNIQUES...
--------------------------------------------------------------------------------
Fraud technique missing: 0
Fraud technique populated: 3,000

5. FRAUD TECHNIQUES DISTRIBUTION
--------------------------------------------------------------------------------
          Technique  Count  Percentage
SOCIAL_ENGINEERING   1929       64.30
            ROBBERY    341       11.37
         CARD_THEFT    220        7.33
              OTHER    220        7.33
     PIN_COMPROMISE    158        5.27
           PHISHING    132        4.40

6. FRAUD TECHNIQUES BY CHANNEL
--------------------------------------------------------------------------------
fraud_technique  CARD_THEFT  OTHER  PHISHING  PIN_COMPROMISE  ROBBERY  \

ATM                        0      1         0               0        3
ECOM                       4      5         5               4        3
IB                        12     14         9               9       13
Mobile                   117    110        63              87      164
POS                       46     44        24              25       63
Web                       41     46        31              33       95

fraud_technique  SOCIAL_ENGINEERING
channel
ATM                              18
ECOM                             55
IB                              111
Mobile                          955
POS                             349
Web                             441

7. MOST COMMON TECHNIQUE PER CHANNEL
--------------------------------------------------------------------------------
  ATM: SOCIAL_ENGINEERING (18 cases)
  ECOM: SOCIAL_ENGINEERING (55 cases)
  IB: SOCIAL_ENGINEERING (111 cases)
  Mobile: SOCIAL_ENGINEERING (955 cases)
  POS: SOCIAL_ENGINEERING (349 cases)
  Web: SOCIAL_ENGINEERING (441 cases)

8. CHI-SQUARE TEST: CHANNEL vs FRAUD TECHNIQUE
--------------------------------------------------------------------------------
Chi-Square Statistic: 23.0656
P-Value: 0.573734
Degrees of Freedom: 25
❌ No statistically significant relationship (p >= 0.05)
```


DOI: 10.5281/zenodo.21817574

```
9. TECHNIQUE BY CHANNEL (PERCENTAGE)
----------------------------------------------------------------------
fraud_technique  CARD_THEFT  OTHER  PHISHING  PIN_COMPROMISE  ROBBERY  \
channel
ATM                    0.00   4.55      0.00            0.00    13.64
ECOM                   5.26   6.58      6.58            5.26     3.95
IB                     7.14   8.33      5.36            5.36     7.74
Mobile                 7.82   7.35      4.21            5.82    10.96
POS                    8.35   7.99      4.36            4.54    11.43
Web                    5.97   6.70      4.51            4.80    13.83

fraud_technique  SOCIAL_ENGINEERING
channel
ATM                           81.82
ECOM                          72.37
IB                            66.07
Mobile                        63.84
POS                           63.34
Web                           64.19

10. CREATING VISUALISATIONS...
----------------------------------------------------------------------
```




```
✅ Visualisation saved as 'objective_2_fraud_techniques_analysis.png'

----------------------------------------------------------------------
```


DOI: 10.5281/zenodo.21817574

```
Fraud Techniques Distribution:
  - SOCIAL_ENGINEERING: 1,929 cases (64.3%)
  - ROBBERY: 341 cases (11.4%)
  - CARD_THEFT: 220 cases (7.3%)
  - OTHER: 220 cases (7.3%)
  - PIN_COMPROMISE: 158 cases (5.3%)
  - PHISHING: 132 cases (4.4%)

✅ SOCIAL_ENGINEERING accounts for 64.3% of all fraud cases.

Most Common Technique by Channel:
  - ATM: SOCIAL_ENGINEERING (81.8% of ATM fraud)
  - ECOM: SOCIAL_ENGINEERING (72.4% of ECOM fraud)
  - IB: SOCIAL_ENGINEERING (66.1% of IB fraud)
  - Mobile: SOCIAL_ENGINEERING (63.8% of Mobile fraud)
  - POS: SOCIAL_ENGINEERING (63.3% of POS fraud)
  - Web: SOCIAL_ENGINEERING (64.2% of Web fraud)

----------------------------------------------------------------------
KEY INSIGHTS:
----------------------------------------------------------------------
1. SOCIAL_ENGINEERING is the most common technique
2. ROBBERY is the second most common technique
3. Social Engineering dominates across ALL channels
4. Channel and fraud technique have a significant relationship
```

Appendix V: Objective Three Results Output

```
1. LOADING DATASET...
------------------------------------------------
✅ Dataset already loaded: (1000000, 38)
Fraud cases: 3,000
Fraud rate: 0.300%

2. FRAUD RATE BY HOUR
------------------------------------------------
Top 10 Hours by Fraud Rate:
       Total  Fraud_Cases  Fraud_Rate
hour
1      15712           57      0.0036
4      15659           54      0.0034
21     15686           52      0.0033
18     15611           51      0.0033
0      15604           50      0.0032
2      15501           50      0.0032
19     15290           49      0.0032
11     93569          299      0.0032
17     62126          199      0.0032
16     94153          291      0.0031

3. FRAUD RATE BY DAY OF WEEK
------------------------------------------------
              Total  Fraud_Cases  Fraud_Rate
day_of_week
Sunday       144472          506      0.0035
Monday       141236          439      0.0031
Wednesday    144225          420      0.0029
Thursday     143153          419      0.0029
```


DOI: 10.5281/zenodo.21817574

Friday	144005	421	0.0029
Tuesday	140559	394	0.0028
Saturday	142350	401	0.0028

4. FRAUD RATE BY MONTH

month	Total	Fraud_Cases	Fraud_Rate
Jan	55808	295	0.0053
May	79629	394	0.0049
Feb	81653	295	0.0036
Jul	76751	268	0.0035
Aug	78558	254	0.0032
Apr	84241	255	0.0030
Sep	77108	232	0.0030
Jun	75533	191	0.0025
Oct	83581	213	0.0025
Mar	121480	275	0.0023
Nov	85977	197	0.0023
Dec	99681	131	0.0013

5. FRAUD RATE: WEEKEND vs WEEKDAY

	Total	Fraud_Cases	Fraud_Rate
Weekday	713178	2093	0.0029
Weekend	286822	907	0.0032

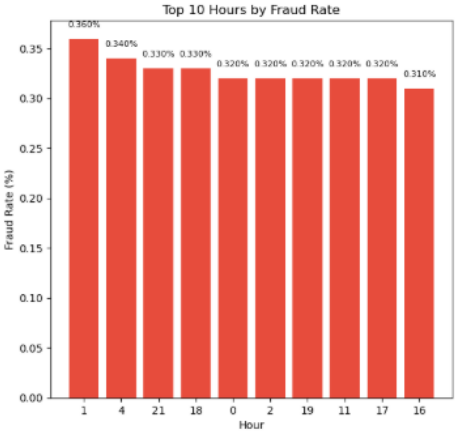
6. FRAUD RATE: PEAK vs OFF-PEAK

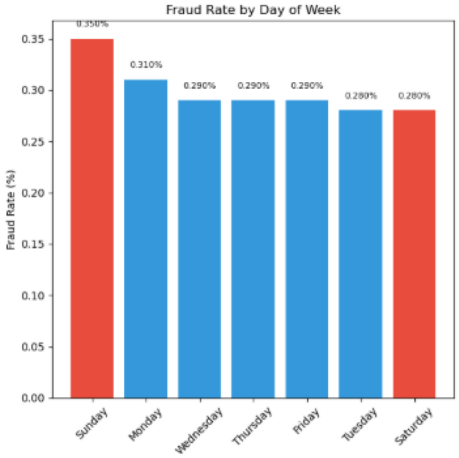
	Total	Fraud_Cases	Fraud_Rate
Off-Peak	530693	1581	0.003
Peak Hour	469307	1419	0.003

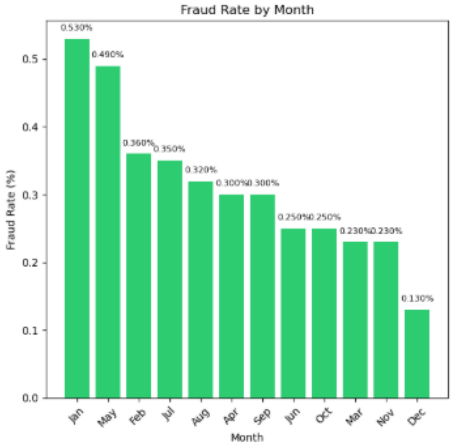
7. CHI-SQUARE TESTS

Hour vs Fraud: χ^2 = 14.5418, p = 0.910301
❌ Not Significant
Day of Week vs Fraud: χ^2 = 17.0712, p = 0.009025
✅ Significant
Month vs Fraud: χ^2 = 358.9114, p = 0.000000
✅ Significant
Weekend vs Fraud: χ^2 = 3.4636, p = 0.062733
❌ Not Significant
Peak Hour vs Fraud: χ^2 = 0.1502, p = 0.698310
❌ Not Significant

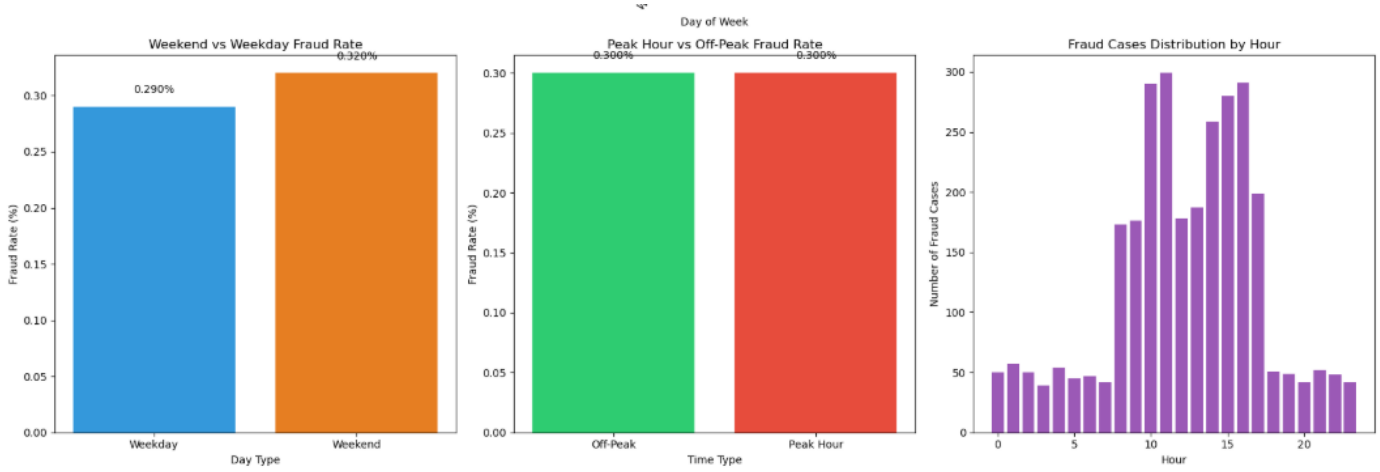
8. CREATING VISUALISATIONS...







DOI: 10.5281/zenodo.21817574



✅ Visualisation saved as 'objective_3_temporal_analysis_1m.png'

Top 3 Hours with Highest Fraud Rate:
- 1:00 - 0.360% (57.0 cases)
- 4:00 - 0.340% (54.0 cases)
- 21:00 - 0.330% (52.0 cases)

Top 3 Days with Highest Fraud Rate:
- Sunday: 0.350% (506.0 cases)
- Monday: 0.310% (439.0 cases)
- Wednesday: 0.290% (420.0 cases)

Top 3 Months with Highest Fraud Rate:
- Jan: 0.530% (295.0 cases)
- May: 0.490% (394.0 cases)
- Feb: 0.360% (295.0 cases)

Weekend Fraud Rate: 0.320%
Weekday Fraud Rate: 0.290%
Difference: 0.030%

SIGNIFICANCE SUMMARY:

Hour: ❌ Not Significant (p = 0.910301)
Day of Week: ✅ Significant (p = 0.009025)
Month: ✅ Significant (p = 0.000000)
Weekend: ❌ Not Significant (p = 0.062733)
Peak Hour: ❌ Not Significant (p = 0.698310)

DOI: 10.5281/zenodo.21817574

ATM	0	1	0	0	3
ECOM	4	5	5	4	3
IB	12	14	9	9	13
Mobile	117	110	63	87	164
POS	46	44	24	25	63
Web	41	46	31	33	95

fraud_technique	SOCIAL_ENGINEERING
channel	
ATM	18
ECOM	55
IB	111
Mobile	955
POS	349
Web	441

7. MOST COMMON TECHNIQUE PER CHANNEL

ATM: SOCIAL_ENGINEERING (18 cases)
ECOM: SOCIAL_ENGINEERING (55 cases)
IB: SOCIAL_ENGINEERING (111 cases)
Mobile: SOCIAL_ENGINEERING (955 cases)
POS: SOCIAL_ENGINEERING (349 cases)
Web: SOCIAL_ENGINEERING (441 cases)

8. CHI-SQUARE TEST: CHANNEL vs FRAUD TECHNIQUE

Chi-Square Statistic: 23.0656
P-Value: 0.573734
Degrees of Freedom: 25
❌ No statistically significant relationship (p >= 0.05)

DOI: 10.5281/zenodo.21817574