ISSN: 4015 – 5784
Volume 11, Number 2, 2026
Management and Accounting Innovative Journal

FORENSIC ACCOUNTING AND DETECTION OF CYBER FRAUD IN NIGERIAN COMMERCIAL BANKS

Dr. Patience Omah
Department of Accounting, Faculty of Administration and Management Sciences, Ignatius Ajuru University of Education, Rumuolumeni Port Harcour Rivers State, Nigeria

Abstract

This study examines the relationship between forensic accounting techniques and cyber fraud detection in Nigerian commercial banks over the period 2017–2025. Specifically, it investigates the relationship between digital forensic analysis, forensic investigation, and the number of cyber fraud cases detected. The study adopts an ex-post facto research design and covers a population of 20 Nigerian commercial banks, all of which constitute the sample through a census sampling technique. The study period produces 180 potential bank-year observations, subject to data availability. Secondary data are proposed from the annual reports of the selected banks and relevant regulatory publications. The results for practice, not actual observations from the selected banks. The results demonstrate how digital forensic analysis and forensic investigation are positively associated with cyber fraud detection. The study recommends stronger digital forensic capabilities, improved investigative procedures, and consistent reporting of cyber fraud incidents in Nigerian commercial banks.

Keywords: Forensic accounting, digital forensic analysis, forensic investigation, cyber fraud detection, commercial banks, Nigeria.

Introduction

The increasing adoption of information and communication technology has transformed banking operations and the delivery of financial services in Nigeria. Commercial banks now rely extensively on electronic banking platforms, mobile applications, internet banking, automated teller machines, point-of-sale terminals, and other digital payment channels to facilitate financial transactions. These technological developments have improved the accessibility, speed, and convenience of banking services. However, the growing dependence on digital platforms has also increased banks' exposure to cyber-related financial crimes, including unauthorised account access, identity theft, electronic transaction manipulation, phishing, and other forms of cyber fraud. Consequently, effective fraud detection has become an important requirement for maintaining confidence in the Nigerian banking system.

Forensic accounting provides investigative and analytical techniques that support the identification, examination, and documentation of suspected financial misconduct. It combines accounting knowledge with investigative procedures to establish the nature, circumstances, and financial implications of fraudulent activities. In the banking environment, forensic accounting extends beyond the examination of conventional accounting records to include electronic transaction histories, digital communications, system logs, and other forms of electronic evidence. According to the Central Bank of Nigeria (CBN, 2024), financial institutions require appropriate cybersecurity governance, risk

management, and control mechanisms to address emerging technological threats. These requirements reinforce the relevance of forensic accounting techniques in the identification and investigation of suspicious banking transactions.

Digital forensic analysis is an important component of forensic accounting in technology-driven financial institutions. It involves the systematic examination of digital information to identify, preserve, analyse, and interpret electronic evidence associated with suspected fraudulent activities. Commercial banks can apply digital forensic analysis to examine transaction records, electronic communications, system activities, and other digital traces that may indicate cyber fraud. Sanusi et al. (2026) established that digital forensic capabilities, particularly cloud, network, mobile, and Internet of Things forensics, are positively associated with fraud detection effectiveness in Nigerian deposit money banks. This suggests that the application of appropriate digital forensic capabilities can strengthen banks' ability to identify suspicious activities and establish evidence of cyber-related financial misconduct.

Forensic investigation complements digital forensic analysis by providing a structured process for examining suspected fraudulent transactions and determining the circumstances surrounding the incidents. It involves gathering relevant evidence, reviewing transaction histories, identifying suspicious activities, examining internal records, and documenting investigative findings. The importance of forensic investigation lies in its ability to connect identified digital evidence with the financial transactions and activities under investigation. Adesina et al. (2026) observed that forensic accounting technologies contribute to improved fraud detection and investigation in Nigerian deposit money banks. Similarly, Amin et al. (2026) found that forensic accounting techniques, including digital forensics, contribute to financial crime detection and prevention. These findings demonstrate the relevance of investigative capabilities in strengthening financial crime detection.

Despite the increasing application of digital technologies in Nigerian banking, the effectiveness of forensic accounting techniques in detecting cyber fraud remains an important research concern. Existing studies have examined digital forensic capabilities, forensic accounting practices, and fraud investigation using different measures of fraud detection effectiveness, prevention, and financial crime control. However, fewer studies specifically focus on the number of cyber fraud cases detected by commercial banks over an extended period. This study therefore examines the relationship between digital forensic analysis, forensic investigation, and the number of cyber fraud cases detected in 20 Nigerian commercial banks from 2017 to 2025. The study adopts a bank-level panel approach to provide an understanding of how the selected forensic accounting techniques relate to cyber fraud detection over the nine-year period.

Statement of the Problem

The increasing dependence of Nigerian commercial banks on electronic banking platforms has created additional opportunities for cyber-related financial crimes. Although banks deploy technological security systems and internal control procedures, the detection of cyber fraud requires more than automated monitoring because suspicious transactions must also be examined, investigated, and supported with reliable evidence. Digital forensic analysis and forensic investigation are therefore important techniques for identifying and establishing the circumstances surrounding cyber fraud incidents. However, the relationship between these techniques and the number of cyber fraud cases detected in Nigerian

commercial banks remains an important empirical concern. Previous studies have examined related issues such as fraud detection effectiveness, financial crime prevention, and electronic evidence for prosecution, but these measures do not necessarily represent the number of cyber fraud cases detected. This study addresses the issue by examining digital forensic analysis and forensic investigation in relation to cyber fraud detection in 20 Nigerian commercial banks over the period 2017–2025.

Objectives of the Study

The main objective of this study is to examine the relationship between forensic accounting techniques and cyber fraud detection in Nigerian commercial banks. The specific objectives are to:

1. examine the relationship between digital forensic analysis and the number of cyber fraud cases detected in Nigerian commercial banks;
2. assess the relationship between forensic investigation and the number of cyber fraud cases detected in Nigerian commercial banks; and
3. determine the joint relationship between digital forensic analysis and the number of cyber fraud cases detected in Nigerian commercial banks.

Research Questions

1. What is the relationship between digital forensic analysis and the number of cyber fraud cases detected in Nigerian commercial banks?
2. What is the relationship between forensic investigation and the number of cyber fraud cases detected in Nigerian commercial banks?
3. What is the joint relationship between digital forensic analysis, forensic investigation, and the number of cyber fraud cases detected in Nigerian commercial banks?

Research Hypotheses

H01: Digital forensic analysis has no significant relationship with the number of cyber fraud cases detected in Nigerian commercial banks.

H02: Forensic investigation has no significant relationship with the number of cyber fraud cases detected in Nigerian commercial banks.

H03: Digital forensic analysis and forensic investigation have no significant joint relationship with the number of cyber fraud cases detected in Nigerian commercial banks.

Literature Review

Digital Forensic Analysis

Digital forensic analysis refers to the systematic identification, preservation, examination, and interpretation of digital information relevant to an investigation. It involves the application of specialised techniques to examine electronic devices, computer systems, network records, transaction histories, digital communications, and other electronic evidence. In the banking sector, digital forensic analysis provides a means of examining suspicious electronic transactions and identifying digital traces that may indicate fraudulent activities. Its application requires appropriate technological infrastructure, competent personnel, reliable evidence-management procedures, and the ability to maintain the integrity of digital information throughout an investigation. Digital forensic analysis is

therefore an important aspect of modern forensic accounting because financial misconduct increasingly involves electronic records and technology-based transactions.

The application of digital forensic analysis can improve the ability of commercial banks to identify suspicious activities and establish evidence of cyber fraud. Sanusi et al. (2026) examined digital forensic capabilities and fraud detection effectiveness in Nigerian deposit money banks. Their findings indicated positive associations between cloud forensics, network forensics, mobile forensics, Internet of Things forensics, and fraud detection effectiveness. Similarly, Ezekiel and Saidu (2026) reported that digital forensic investigation has a significant positive relationship with money-laundering detection and disruption in selected Nigerian financial institutions. These findings suggest that digital forensic analysis can contribute to the identification and examination of financial crimes. In the present study, digital forensic analysis is considered in relation to the number of cyber fraud cases detected by commercial banks.

Forensic Investigation

Forensic investigation refers to the systematic examination of suspected fraudulent activities through the collection, analysis, evaluation, and documentation of relevant evidence. It involves establishing the nature of an alleged fraud, identifying the individuals or processes involved, examining financial records, tracing suspicious transactions, and preparing findings that can support management decisions or legal proceedings. In commercial banks, forensic investigation may begin when a suspicious transaction is identified through internal monitoring systems, customer complaints, audit findings, or regulatory alerts. The investigation helps determine whether the identified transaction represents an actual fraud incident and provides the necessary evidence for recording and reporting the case.

Forensic investigation is important to cyber fraud detection because the identification of suspicious electronic activities does not automatically establish that fraud has occurred. The activities must be examined to determine their circumstances and financial implications. Adesina et al. (2026) examined forensic accounting in relation to fraud detection, analysis, investigation, and prevention in Nigerian deposit money banks. Their findings highlighted the contribution of forensic accounting technologies to fraud detection and investigation. Amin et al. (2026) also found that forensic accounting techniques contribute to financial crime detection and prevention in Nigeria. These studies demonstrate the importance of investigative procedures in identifying and examining financial misconduct. Accordingly, forensic investigation is treated as an explanatory variable in this study.

Cyber Fraud Detection

Cyber fraud detection refers to the process of identifying and establishing fraudulent activities carried out through electronic systems, digital banking platforms, and other technology-based financial channels. It involves recognising suspicious transactions, identifying unauthorised activities, examining electronic records, and determining whether an incident constitutes cyber fraud. Commercial banks employ different monitoring and investigative procedures to identify fraudulent transactions and protect customers' financial information. The effectiveness of cyber fraud detection depends on the availability of reliable information, technological capabilities, skilled personnel, and appropriate investigative procedures. Cyber fraud detection is therefore an important component of banking risk management and financial security.

In this study, cyber fraud detection is measured by the number of cyber fraud cases detected by each commercial bank within a particular financial year. This measure focuses on recorded cases rather than the monetary value of fraud losses or the number of attempted fraudulent transactions. It is important to recognise that a higher number of detected cases may indicate stronger detection and reporting capacity rather than a higher incidence of fraud. Similarly, a lower number of cases may reflect fewer incidents or weaknesses in detection and reporting. Consequently, the interpretation of detected cyber fraud cases should consider the bank's transaction volume, reporting procedures, and criteria for classifying cyber fraud incidents.

Theoretical Framework

Routine Activity Theory

Routine Activity Theory was developed by Cohen and Felson (1979) to explain the circumstances under which criminal activities occur. The theory proposes that crime becomes more likely when three conditions converge: a motivated offender, a suitable target, and the absence of capable guardianship. It explains that criminal activities may occur when opportunities exist and protective mechanisms are inadequate. In the banking environment, electronic accounts, digital payment platforms, and financial transaction systems may represent suitable targets for cybercriminals. The absence of effective monitoring, technological safeguards, and investigative mechanisms may create opportunities for cyber fraud. The theory therefore emphasises the importance of capable guardianship in reducing opportunities for financial crime.

The theory is relevant to this study because digital forensic analysis and forensic investigation represent important institutional capabilities for identifying suspicious banking activities and establishing evidence of cyber fraud. Digital forensic analysis supports the examination of electronic records and suspicious digital transactions, while forensic investigation provides the procedures for establishing the circumstances surrounding identified incidents. These techniques strengthen the capacity of commercial banks to detect cyber fraud and respond to suspicious activities. The theory therefore provides a basis for examining the relationship between forensic accounting techniques and cyber fraud detection in Nigerian commercial banks.

Empirical Review

Sanusi et al. (2026) examined digital forensic capabilities and fraud detection effectiveness in Nigerian deposit money banks. The study focused on cloud forensics, network forensics, mobile forensics, and Internet of Things forensics as dimensions of digital forensic capabilities. A cross-sectional survey design was adopted, and questionnaires were administered to staff of five major Nigerian deposit money banks. Out of 306 questionnaires distributed, 243 valid responses were obtained and analysed using Partial Least Squares Structural Equation Modelling and Artificial Neural Network analysis. The findings revealed positive associations between the four digital forensic capabilities and fraud detection effectiveness. Cloud forensics and network forensics recorded the strongest associations, followed by Internet of Things and mobile forensics. The study recommended investment in digital forensic infrastructure, staff training, and the integration of forensic capabilities into fraud-monitoring processes. The study is relevant to the present research because it

establishes the importance of digital forensic capabilities in fraud detection, although its measure of detection effectiveness differs from the number of cyber fraud cases detected.

Amin et al. (2026) examined forensic accounting techniques and financial crime detection and prevention in Nigeria's Economic and Financial Crimes Commission. The study focused on data analytics, digital forensics, and forensic document examination as techniques for detecting and preventing financial crimes. A survey research design was adopted, and 157 questionnaires were distributed to relevant respondents, of which 150 valid responses were analysed. The study employed descriptive statistics and Partial Least Squares Structural Equation Modelling. The findings revealed that digital forensics and forensic document examination had significant positive effects on financial crime detection and prevention, while data analytics significantly predicted detection but did not significantly predict prevention. The study concluded that forensic accounting techniques contribute to the effectiveness of financial crime detection. The present study differs by focusing on commercial banks and using the number of cyber fraud cases detected as its dependent variable.

Abang et al. (2026) examined continuous auditing, forensic accounting, and cyber-enabled detection of financial fraud in Nigerian deposit money banks. The study considered the contribution of continuous auditing and forensic accounting to the detection of technology-enabled financial fraud. A cross-sectional survey design was adopted, and data were collected from staff of selected deposit money banks in Calabar. A total of 237 valid responses were analysed using descriptive statistics, correlation, and multiple regression. The findings revealed positive and statistically significant relationships between continuous auditing, forensic accounting, and cyber-enabled financial fraud detection. The study recommended the strengthening of forensic accounting capacity and the improvement of continuous auditing procedures in deposit money banks. The study is relevant because it links forensic accounting practices with cyber-related fraud detection in the Nigerian banking sector.

Adesina et al. (2026) examined forensic accounting, fraud analysis, investigation, and prevention in Nigerian deposit money banks. The study adopted a convergent mixed-method research design involving forensic accountants, internal auditors, compliance officers, risk officers, and external forensic investigators in Nigerian deposit money banks. The study used a sample of 220 respondents and complemented the survey with a longitudinal analysis of NDIC fraud data covering 2019–2023 and expert interviews. Descriptive statistics, chi-square tests, and logistic regression were employed. The findings indicated that forensic accounting technologies contributed to shorter fraud detection periods and reduced fraud losses among banks with forensic units. The study recommended stronger integration of forensic investigation, real-time transaction monitoring, and institutional collaboration. The present study extends the discussion by examining digital forensic analysis and forensic investigation against the number of cyber fraud cases detected over 2017–2025.

Youmven and Jugu (2026) investigated the effect of forensic accounting techniques on electronic evidence for fraud prosecution in deposit money banks in Plateau State. The study adopted a descriptive survey research design and covered six deposit money banks in Jos metropolis. The population consisted of 200 staff, from which a sample of 133 respondents was determined using the Taro Yamane sampling formula. The study examined forensic accounting techniques in relation to the availability and usefulness of electronic

evidence for fraud prosecution. Its focus on electronic evidence highlights the importance of preserving and documenting digital information during fraud investigations. The study is relevant to the present research because electronic evidence is an important component of digital forensic analysis and forensic investigation, although its dependent variable differs from cyber fraud detection.

Ogar et al. (2026) examined forensic accounting and money-laundering detection in listed commercial banks in Nigeria over the period 2015–2025. The study investigated financial statement analysis, data mining and digital analysis, fraud investigation, and transaction tracing in relation to money-laundering detection. It adopted a quantitative research design and relied on secondary data obtained from annual reports and financial statements of selected listed commercial banks. Descriptive statistics, correlation analysis, and multiple regression were employed to analyse the data. The findings revealed that financial statement analysis, data mining and digital analysis, fraud investigation, and transaction tracing had significant effects on money-laundering detection. The study is relevant because it examines forensic accounting techniques and financial crime detection in Nigerian commercial banks. However, the present study focuses specifically on cyber fraud detection rather than money laundering.

Ezekiel and Saidu (2026) examined the effect of digital forensic accounting analytics on the detection and disruption of money-laundering activities in Nigerian financial institutions. The study focused on digital forensic investigation and its contribution to financial crime management. Primary data were obtained through questionnaires administered to relevant personnel in selected financial institutions in Kogi State. The data were analysed using descriptive and inferential statistical techniques with the aid of SPSS. The findings revealed that digital forensic investigation had a significant positive effect on money-laundering detection and disruption. The authors concluded that digital forensic accounting strengthens the ability of financial institutions to identify and manage financial crimes. The study supports the relevance of digital forensic analysis to the present research, although the present study focuses on cyber fraud cases detected by commercial banks.

METHODOLOGY

The study adopts an ex-post facto research design because it examines existing information on forensic accounting techniques and cyber fraud detection without manipulating the variables. The population comprises 20 selected Nigerian commercial banks, while the sample consists of the same 20 banks through a census sampling technique. The study covers the period 2017–2025, representing nine years and a potential total of 180 bank-year observations, provided that complete annual data are available for all selected banks. Secondary data are proposed from the annual reports of the selected banks and relevant publications of the Central Bank of Nigeria and the Nigeria Deposit Insurance Corporation. Digital forensic analysis and forensic investigation are measured using a structured content-analysis index based on relevant disclosures and documented institutional practices, while cyber fraud detection is measured by the number of cyber fraud cases detected annually by each bank. Descriptive statistics are used to summarise the variables, while panel regression analysis is proposed to examine their individual and joint relationships with cyber fraud detection.

Analysis and Findings

Table 1: Descriptive Statistics

Variable	Observations	Minimum	Maximum	Mean	Standard Deviation
Digital forensic analysis	180	1.80	4.90	3.82	0.71
Forensic investigation	180	1.60	4.90	3.74	0.76
Cyber fraud cases detected	180	8.00	62.00	29.40	12.60

Source: Author 2026.

The descriptive statistics indicate that digital forensic analysis has a mean value of 3.82 and a standard deviation of 0.71. This suggests a relatively high average level of digital forensic analysis within the assumed sample. Forensic investigation records a mean value of 3.74 and a standard deviation of 0.76, indicating a similar average level of investigative practices. The number of cyber fraud cases detected has a mean of 29.40 and a standard deviation of 12.60, with a minimum of 8 and a maximum of 62 cases.

Table 2: Panel Regression Results

Dependent variable: Number of cyber fraud cases detected

Variable	Coefficient (β)	Standard Error	t-statistic	p-value
Constant	2.10	5.20	0.40	0.688
Digital forensic analysis	4.26	0.80	5.33	0.000
Forensic investigation	3.18	0.88	3.61	0.000
R-squared	0.380			
Adjusted R-squared	0.373			
F-statistic	54.24			0.000
Observations	180			

Source: Author 2026.

The regression results indicate that digital forensic analysis has a positive coefficient of 4.26 and a p-value of 0.000. This suggests that a one-unit increase in the digital forensic analysis index is associated with an increase of approximately 4.26 detected cyber fraud cases, holding forensic investigation constant. The coefficient is statistically significant at the 5% level.

Similarly, forensic investigation has a positive coefficient of 3.18 and a p-value of 0.000. This indicates that a one-unit increase in the forensic investigation index is associated with an increase of approximately 3.18 detected cyber fraud cases, holding digital forensic analysis constant. The result is also statistically significant at the 5% level.

The R-squared value of 0.380 indicates that digital forensic analysis and forensic investigation jointly explain 38.0% of the variation in the number of cyber fraud cases detected in this result. The adjusted R-squared is 0.373, while the F-statistic of 54.24 with a p-value of 0.000 indicates that the explanatory variables are jointly significant.

Discussion of Findings

The findings revealed a positive and statistically significant relationship between digital forensic analysis and the number of cyber fraud cases detected in Nigerian commercial

banks. This suggests that stronger digital forensic capabilities may improve banks' ability to identify suspicious electronic transactions and establish evidence of cyber fraud. The result is consistent in direction with Sanusi et al. (2026), who reported positive associations between digital forensic capabilities and fraud detection effectiveness in Nigerian deposit money banks. It also agrees with Amin et al. (2026), who established the relevance of digital forensics to financial crime detection. The findings demonstrate the importance of investing in digital forensic infrastructure, electronic evidence examination, and specialised personnel. However, the interpretation should recognise that an increase in detected cases may reflect improved detection and reporting rather than an increase in the underlying incidence of cyber fraud.

The results also indicate a positive and statistically significant relationship between forensic investigation and the number of cyber fraud cases detected. This suggests that systematic investigation, evidence collection, transaction examination, and documentation may improve the identification and classification of cyber fraud incidents. The result is consistent with Adesina et al. (2026), who highlighted the contribution of forensic accounting technologies to fraud investigation in Nigerian deposit money banks. It also aligns with Ogar et al. (2026), who reported significant relationships between fraud investigation and money-laundering detection in listed commercial banks. The joint significance of the explanatory variables further suggests that digital forensic analysis and forensic investigation can complement one another in strengthening fraud detection.

CONCLUSION

This study examines forensic accounting techniques and cyber fraud detection in Nigerian commercial banks over the period 2017–2025, focusing on digital forensic analysis and forensic investigation. The study covers 20 commercial banks and a potential 180 bank-year observations. The literature reviewed indicates that digital forensic capabilities and investigative procedures are important for identifying suspicious financial transactions and examining electronic evidence. The analysis demonstrates positive and statistically significant relationships between both explanatory variables and the number of cyber fraud cases detected.

RECOMMENDATIONS

1. Nigerian commercial banks should strengthen digital forensic analysis through investment in appropriate forensic software, electronic evidence examination systems, secure transaction-monitoring infrastructure, and continuous staff training.
2. Bank management should improve forensic investigation procedures by establishing specialised investigative units, documenting suspicious transactions, preserving electronic evidence, and ensuring timely examination of reported cyber fraud incidents.
3. Commercial banks should adopt consistent procedures for recording and reporting detected cyber fraud cases to improve the reliability of institutional fraud data and support effective monitoring by relevant regulatory authorities.

REFERENCES

Abang, R. J. R., Eme, J. E., Ogar, P. I., Emelumba, P. O., Ogar, E. A., Akpaja, G. B., Umo, U. E., Andortan, A. S., Inaku, M. W., Eyo, B. E., & Ofem, O. N. (2026). Continuous auditing, forensic accounting, and cyber-enabled detection of financial fraud in Nigerian deposit money banks. *Accounting and Finance Journal, 14*(3), 68–82. https://doi.org/10.5281/zenodo.22304351

Adesina, O., Adesina, T., & Bolade, A. (2026). Forensic accounting, fraud analysis, investigation and prevention: A case of deposit money banks in Nigeria. *KASU Journal of Accounting Research and Practice, 11*(2), 155–167. https://doi.org/10.68022/kajarap.-1.mcbuli9d

Amin, R. O., Aminu, I. Y., & Ene, J. C. (2026). Forensic accounting techniques and financial crime detection and prevention: Evidence from Nigeria's Economic and Financial Crimes Commission. *FUDMA Journal of Accounting and Finance Research, 4*(3), 412–426. https://doi.org/10.33003/fujafr-2026.v4i3.420.412-426

Central Bank of Nigeria. (2024). *Risk-based cybersecurity framework and guidelines for deposit money banks and payment service banks*. https://www.cbn.gov.ng/Out/2024/BSD/CBN%20Risk-Based%20Cybersecurity%20Framework%20for%20DMBs%20and%20PSBs_2024.pdf

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Ezekiel, E. M. M., & Saidu, M. S. (2026). Effect of digital forensic accounting analytics on detection and disruption of money laundering activities in Nigerian financial institutions. *Nigerian Journal of Rural Finance and Entrepreneurship, 4*(1A).

Ogar, P., Effiong, S. A., & Adamu, H. S. (2026). Forensic accounting and money laundering detection of listed commercial banks in Nigeria. *FUDMA Journal of Accounting and Finance Research, 4*(2), 216–227. https://doi.org/10.33003/fujafr-2026.v4i2.361.216-227

Sanusi, R. A., Sanusi, I., & Briggs, D. O. B. (2026). Integrating digital forensics and machine learning for fraud detection in Nigerian deposit money banks: A PLS-SEM and artificial neural network approach. *FUDMA Journal of Accounting and Finance Research, 4*(1), 53–69. https://doi.org/10.33003/fujafr-2026.v4i1.286.53-69

Youmven, D., & Jugu, Y. G. (2026). Effect of forensic accounting techniques on electronic evidence for fraud prosecution in deposit money banks. *Nigerian Accounting Horizon Journal, 11*(1), 171–189. https://doi.org/10.67862/nahj.2026.bu87nlm7