“Detecting fraudulent behavior in banking services: A modified Fraud Pentagon Theory integrating whistleblowing systems and banking fintech security”

AUTHORS	Soni Agus Irwandi Agus Samekto Nanang Shonhadji

ARTICLE INFO	Soni Agus Irwandi, Agus Samekto and Nanang Shonhadji (2026). Detecting fraudulent behavior in banking services: A modified Fraud Pentagon Theory integrating whistleblowing systems and banking fintech security. *Banks and Bank Systems*, *21*(1), 229-245. doi: 10.21511/bbs.21(1).2026.18
DOI	http://dx.doi.org/10.21511/bbs.21(1).2026.18
RELEASED ON	Friday, 27 March 2026
RECEIVED ON	Friday, 26 September 2025
ACCEPTED ON	Saturday, 14 February 2026

JOURNAL	"Banks and Bank Systems"
ISSN PRINT	1816-7403
ISSN ONLINE	1991-7074
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
31	3	17

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine

www.businessperspectives.org

Soni Agus Irwandi (Indonesia), **Agus Samekto** (Indonesia), **Nanang Shonhadji** (Indonesia)

DETECTING FRAUDULENT BEHAVIOR IN BANKING SERVICES: A MODIFIED FRAUD PENTAGON THEORY INTEGRATING WHISTLEBLOWING SYSTEMS AND BANKING FINTECH SECURITY

Abstract

Fraudulent behavior in banking services remains a critical challenge in Indonesia, especially amid rapid digitalization and increasing fintech adoption, while traditional models such as the Fraud Pentagon Theory (FPT) are limited in explaining new fraud drivers related to technological exposure and cultural dynamics. This study aims to detect fraudulent behavior in Indonesian banking services by modifying the FPT through the integration of prestige culture and fintech usage. It employed a survey approach targeting front-office employees of private national banks in Indonesia with at least two years of professional customer service experience. This sample was chosen because such employees are directly exposed to operational pressures, opportunities, and technological systems, making them highly relevant for detecting fraud risk factors. Data were collected using offline and online questionnaires and analyzed with Structural Equation Modeling (SEM) using WarpPLS. The results indicate that the seven factors of pressure ($\beta = 0.916$; $p < .001$), opportunity ($\beta = 0.929$; $p < .001$), rationalization ($\beta = 0.847$; $p < .001$), capability ($\beta = 0.862$; $p < .001$), control ($\beta = 0.907$; $p < .001$), fintech usage ($\beta = 0.712$; $p < .001$), and prestige culture ($\beta = 0.837$; $p < .001$) are significant in determining fraudulent activities, whereas the whistleblowing system ($\beta = -0.312$; $p = .002$) and fintech security usage ($\beta = -0.298$; $p = .003$) are moderators. Based on the findings, the conclusion is that pressure and opportunity are the most potent predictors of fraudulent activity, while whistleblowing and fintech security systems are important mechanisms for preventing such activity.

Keywords banking, fraud, fintech, behavior, prestige, whistleblowing

JEL Classification G21, M41, K42

Type of the article: Research Article

Received on: 26th of September, 2025
Accepted on: 14th of February, 2026
Published on: 27th of March, 2026

Soni Agus Irwandi, Ph.D., Lecturer, Faculty of Economics and Business, Department of Accounting, University of Hayam Wuruk Perbanas, Indonesia. (Corresponding author)

Agus Samekto, Ph.D., Lecturer, Faculty of Economics and Business, Department of Accounting, University of Hayam Wuruk Perbanas, Indonesia.

Nanang Shonhadji, Ph.D., Lecturer, Faculty of Economics and Business, Department of Accounting, University of Hayam Wuruk Perbanas, Indonesia.

Conflict of interest statement:
Author(s) reported no conflict of interest

INTRODUCTION

The issue of fraud in banking services has become an even more complicated and widespread problem in Indonesia, particularly during the current very fast process of digitalization and the adoption of financial technology, or fintech. The classical theories, such as the Fraud Triangle and the Fraud Pentagon Theory, which rely on the pressure, opportunity, rationalization, capability, and arrogance factors, have become inadequate in dealing with present phenomena of fraud that originate from exposure to and cultural processes surrounding technology (Crowe, 2011). The presence of the Indonesian banking industry, where there is an interaction with institutional trust, regulatory clarity, and digitalization, is now at risk from identification fraud, algorithmic fraud, and cyber-based embezzlement (Asmaranti et al., 2023; Putri & Prabowo, 2025; Handoko et al., 2020). At the same time, prestige culture continues to fuel processes that work towards irrational justification and justification for unethical actions, whereas inter-

nal control processes such as hotlines or whistleblower mechanisms, as well as fintech security, despite the growing implementation, continue to be faced with difficulties such as cultural difficulties, risk, and technology (Sari & Nugroho, 2020; Hidayah & Saptarini, 2019). It is important to note that this scenario presents a classic scientific issue in that it illustrates that traditional methodology in fraud detection is not adequate in establishing multi-dimensional variables that easily come into play within fraudulent activity in Indonesian banking services outcomes (Albert-Sogules et. al., 2024; Yang & Zhang, 2022; Ch. Albrecht & Co. Albrecht, 2009). Accordingly, the present study addresses this gap by extending the Fraud Pentagon Theory with cultural and technological dimensions, specifically prestige culture and fintech usage, while examining the moderating role of whistleblowing systems and fintech security. This approach provides a more contextually relevant framework for understanding fraudulent behavior in Indonesian banking institutions.

1. LITERATURE REVIEW AND HYPOTHESES

Fraudulent behavior that occurs in the banking industry is identified by academic circles as a significant threat, and traditional theories developed to address the issue include the Fraud Triangle by Cressey (1953) and the Fraud Pentagon by Crowe (2011), which also identified five key elements of fraudulent activities that involve pressure, opportunity, rationalization, capability, and control. These theories are important as they form the basis of understanding the effect of external pressure and opportunities resulting from weaknesses within the control of the institution, as well as the potential or capability of the person involved. However, recent studies indicate that the application of these classical theories is not always consistent within the Indonesian banking context. For instance, Asmaranti et al. (2023) found that rationalization and capability significantly influence fraud, while pressure and opportunity were not dominant. In contrast, Ayuningtyas et al. (2021) emphasized that contextual factors such as industry characteristics and changes in directors play a more decisive role than personal financial needs. These differing findings reveal a research gap, namely the limitations of traditional models in explaining the complexity of fraud in the era of banking digitalization. Accordingly, this literature review begins with a discussion of the classical variables as a theoretical foundation, before moving on to additional variables that are more relevant to the dynamics of financial technology and contemporary organizational culture.

The development of financial technology (fintech) has brought fundamental changes to banking operations, but this has opened up opportunities for activities that may give rise to fraudulent activities. The use of digital services such as mobile applications, peer-to-peer lending systems, blockchain-based transactions, and artificial intelligence-driven analytics has indeed enhanced efficiency and accessibility, but it has also expanded the surface of risks that cannot be fully explained by classical fraud theories (Palakurti, 2025). Various studies suggest that the adoption of fintech can also increase in cases of fraud, if proper security systems are not put in place or even if adequate awareness levels are not attained (Putri & Prabowo, 2025; Shonhadji & Irwandi, 2024; Mangalam, 2025; Chijoke-Mgbame et al., 2020). However, on the other side, the very same means of fintech can also prove to be one of the greatest control tools, particularly through AI-driven fraud detection and blockchain-based transparency mechanisms (Moura et al., 2025; Chettier et al., 2025). Moreover, organizational culture also holds an important position in these cases, especially prestige cultures, which include the motivation for people to achieve prestige and recognition, even when accomplished through illegitimate means. Accordingly, fintech usage and prestige culture should be regarded as additional dimensions that complement the Fraud Pentagon, as they reflect contemporary challenges arising from banking digitalization and organizational cultural dynamics.

The whistleblowing system, as an internal reporting mechanism, is one of the key instruments in reducing the tendency of fraud in the banking sector. This system enhances transparency and accountability, as employees are provided with an official channel to report suspected misconduct without fear of retaliation. Maulida and Bayunitri

http://dx.doi.org/10.21511/bbs.21(1).2026.18

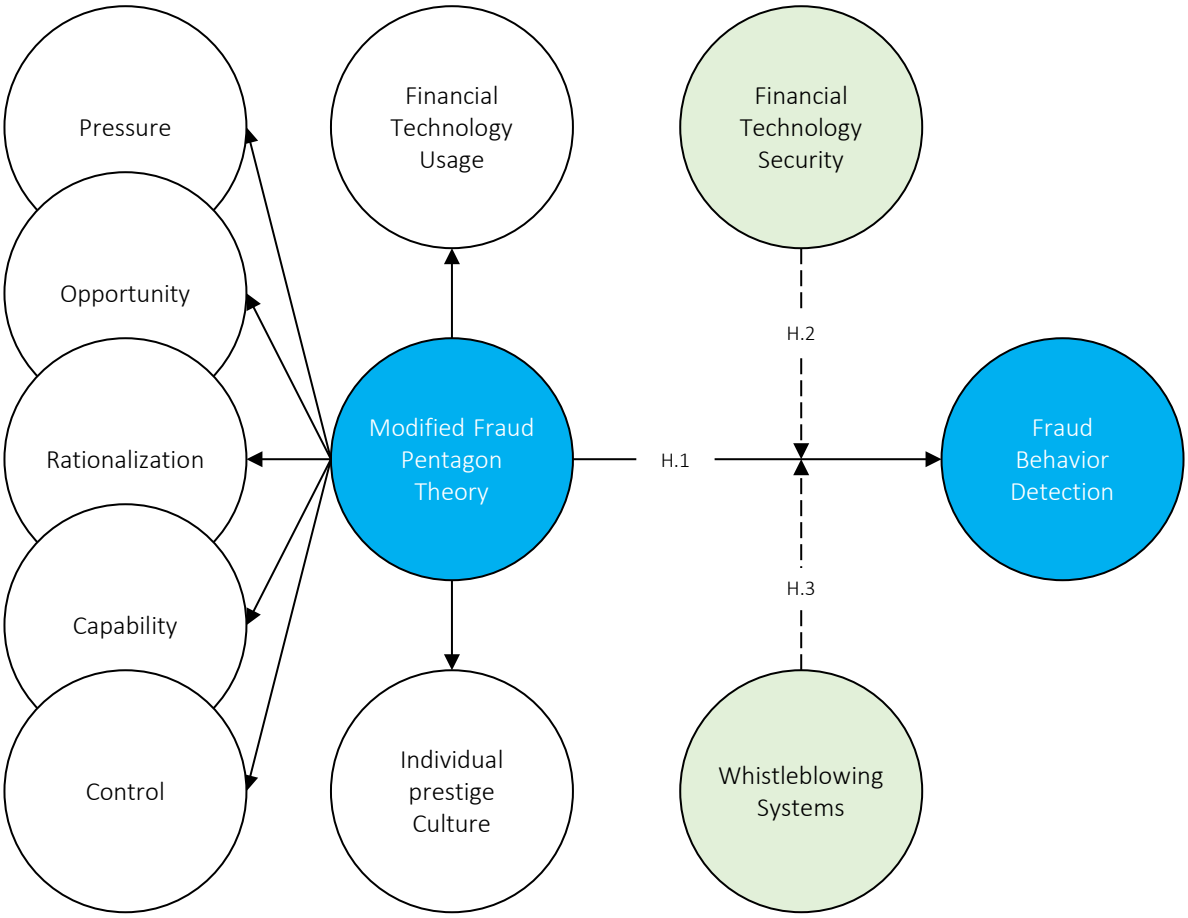

Figure 1. Research model

(2021) found that the implementation of a whistleblowing system has a significant impact on fraud prevention in banking, with effectiveness reaching more than 50%. This finding supports the study by Nugroho and Diyanty (2022), which demonstrates that the consistent implementation of a whistleblowing system can significantly reduce fraud, particularly when reinforced by an ethical organizational culture and supportive leadership. Likewise, Idrawahyuni et al. (2025) stated that by integrating a whistleblowing system and risk management, the strategy to prevent money-related fraud in Islamic banks is further optimized. However, the functionality of the current system has often met challenges from the culture itself, including inhibitions related to reporting. According to a survey by Deloitte (2024), although over 90% of institutions have integrated the reporting system, fewer than a quarter regularly remind the public regarding these regulations annually, resulting in reduced efficiency. This finding is further reinforced by Marsam Dollah et al. (2025), who emphasize that cultural barriers in Southeast Asia can undermine the effectiveness of internal reporting functions. Overall, existing research argues that the current reporting strategy is actually a significant factor to consider in fraud prevention, but results greatly depend on organizational culture. The research question for this current study, then, is to investigate the act of the reporting strategy as a moderating factor, which will minimize the risk impact on the modified Fraud Pentagon model regarding fraudulent activity within the banking sector.

Prestige culture, defined as the drive for status and recognition, has been proposed as a psychological motivator for fraud. Sari and Nugroho (2020) found that individuals with high prestige orientation are more likely to rationalize unethical behavior to maintain social standing. This aligns with agency theory (Jensen & Meckling, 1976), which posits that misaligned incentives between agents and principals can lead to opportunistic behavior. Shonhadji (2020) expanded this framework by integrating prestige

culture and fintech exposure into a behavioral fraud detection model, demonstrating their predictive relevance in the Indonesian banking context.

The literature reveals a growing consensus that fraud detection in banking must evolve beyond traditional psychological models to incorporate behavioral profiling, technological safeguards, and organizational culture. The Indonesian banking sector, characterized by rapid digitalization and regulatory reform, presents a unique context in which these multidimensional frameworks can be tested and refined.

This study aims to investigate fraudulent behavior in the banking sector by modifying the traditional Fraud Pentagon Theory (FPT). The hypotheses were:

H_1: *Modified fraud pentagon theory affects fraud behavior detection.*

H_2: *Financial technology security moderates the relationship between the modified fraud pentagon theory and fraud behavior detection.*

H_3: *Whistleblowing systems moderate the relationship between the modified fraud pentagon theory and fraud behavior detection.*

2. METHODOLOGY

This study employed a quantitative approach using Structural Equation Modeling (SEM) with the WarpPLS application to test a modified Fraud Pentagon Theory (FPT). The model incorporated two additional constructs, prestige culture and fintech usage, along with two moderating variables, whistleblowing system and fintech security. The population consisted of front-office employees of private national banks in Indonesia, selected through purposive sampling. The inclusion criterion required respondents to have at least two years of professional experience in customer-facing roles, as these employees are directly exposed to operational pressures, opportunities, and technological systems, making them highly relevant for detecting fraud risk factors. Data collection was conducted between March and June 2024 in major cities (Jakarta, Surabaya, Medan) using both offline and online questionnaires. The research instrument was developed through item generation from prior literature, expert validation (ACFE Indonesia Chapter), pilot testing, and measurement using a 5-point Likert scale. The study ensured it got approval from the institutional review committee of ethics, within which participants volunteered to be anonymous in a confidential manner.

Table 1. Demographic characteristics of respondents

Characteristic	Category	Frequency	Percentage
Gender	Male	128	54.9%
	Female	105	45.1%
Age	21-30 years	97	41.6%
	31-40 years	89	38.2%
	41-50 years	47	20.2%
Education	Bachelor's degree	156	66.9%
	Master's degree	77	33.1%
Work Experience	2-5 years	102	43.8%
	6-10 years	78	33.5%
	More than 10 years	53	22.7%
Type of Bank	Private national banks	233	100%

Table 1 provides a clear profile of the respondents, showing that the majority were male (54.9%), aged between aged 21 to 40 years (79.8%), and held at least a bachelor's degree (66.9%). Most respondents had between 2 and 10 years of work experience (77.3%), ensuring that the sample represented employees with sufficient exposure to banking operations and fraud-related risks. The exclusive focus on front-office staff of private national banks was deliberate, as these employees interact directly with customers and digital platforms, making them particularly vulnerable to pressures, opportunities, and technological risks associated with fraudulent behavior.

Several techniques of analysis were done in this study, including testing of reliability (Cronbach's Alpha, Composite Reliability), validity (Average Variance Extracted, Discriminant validity), path analysis, assessing direct effects of variables on fraud, and testing of moderators such as whistleblowing mechanisms and fintech security. The data in this study were not previously published in any form whatsoever, though it is raw data complemented by a questionnaire located in an appendix or the public domain of an open-access source.

http://dx.doi.org/10.21511/bbs.21(1).2026.18

3. RESULTS

This section presents the empirical findings from the Structural Equation Modeling (SEM) analysis using WarpPLS. The results are organized into three key areas: measurement model evaluation, structural model relationships, and moderating effects. Each table is followed by a detailed interpretation.

The measurement model demonstrates strong reliability and validity across most constructs (Table 2). Composite reliability and Cronbach's Alpha values for all variables except Fintech Usage exceed the recommended threshold of 0.70, indicating consistent internal reliability (Hair et al., 2021). Constructs such as Pressure, Opportunity, Rationalization, Capability, Control, Prestige Culture, Whistleblowing System, and Fintech Security show excellent reliability, with values above 0.93. Average Variance Extracted (AVE) values also support convergent validity, with most constructs scoring well above the 0.50 benchmark (Fornell & Larcker, 1981). However, Fintech Usage presents a lower AVE of 0.414, suggesting that its indicators may not fully capture the construct and may require refinement or expansion. Full Collinearity VIF values were assessed to detect multicollinearity and potential common method bias. Most constructs fall within acceptable limits (below 3.3), but Opportunity (12.166), Rationalization (11.980), and Prestige Culture (12.633) exceed this threshold. These high VIF scores may indicate overlapping content or conceptual similarity among predictors, which could affect the accuracy of structural estimates.

The structural model analysis reveals strong and statistically significant relationships between all examined constructs and fraudulent behavior, as indicated by the path coefficients and p-values presented in Table 3. Each path demonstrates a high level of predictive relevance, with p-values below 0.001, confirming the robustness of the model and the reliability of the hypothesized relationships. Among the behavioral dimensions derived from the modified Fraud Pentagon Theory, Opportunity ($\beta = 0.929$) and Pressure ($\beta = 0.916$) exhibit the strongest influence on fraudulent behavior. These findings reinforce the theoretical assertion that situational access and external demands are critical drivers of misconduct within banking institutions. Rationalization ($\beta = 0.847$), Capability ($\beta = 0.862$), and Control ($\beta = 0.907$) also show substantial effects, suggesting that internal justification mechanisms, individual competence, and oversight dynamics play a pivotal role in shaping unethical decisions.

Fintech Usage ($\beta = 0.712$) is significantly associated with fraudulent behavior, indicating that increased exposure to digital banking platforms may

Table 2. Reliability and validity of constructs

Construct	Composite Reliability	Cronbach's Alpha	AVE	Full Collinearity VIF
Pressure	0.968	0.949	0.913	3.456
Opportunity	0.968	0.949	0.913	12.166
Rationalization	0.961	0.933	0.896	11.980
Capability	0.961	0.933	0.896	3.214
Control	0.961	0.933	0.896	3.118
Fintech Usage	0.774	0.651	0.414	2.987
Prestige Culture	0.961	0.933	0.896	12.633
Whistleblowing System	0.961	0.933	0.896	3.102
Fintech Security	0.961	0.933	0.896	3.221

Table 3. Path coefficients and significance

Path	Coefficient (β)	p-value	Significance
Pressure → Fraud Behavior	0.916	< 0.001	Significant
Opportunity → Fraud Behavior	0.929	< 0.001	Significant
Rationalization → Fraud Behavior	0.847	< 0.001	Significant
Capability → Fraud Behavior	0.862	< 0.001	Significant
Control → Fraud Behavior	0.907	< 0.001	Significant
Fintech Usage → Fraud Behavior	0.712	< 0.001	Significant
Prestige Culture → Fraud Behavior	0.837	< 0.001	Significant

Table 4. Moderating role of whistleblowing and fintech security

Moderator	Interaction Effect	p-value	Interpretation
Whistleblowing System	Negative	< 0.001	Reduces fraud behavior significantly
Fintech Security	Negative	< 0.001	Mitigates fintech-related fraud risk

elevate risk, particularly when security protocols are weak or user awareness is limited. This supports prior literature emphasizing the dual role of fintech as both an enabler of operational efficiency and a potential vector for fraud.

Prestige Culture ($\beta = 0.837$) also demonstrates a strong positive relationship with fraudulent behavior, suggesting that individuals motivated by status and recognition may be more inclined to rationalize unethical actions to preserve or enhance their social standing. This aligns with agency theory and recent empirical findings that link prestige orientation to ethical compromise in high-performance environments.

The results presented in Table 4 provide compelling evidence for the moderating effects of whistleblowing systems and fintech security on fraudulent behavior within banking institutions. Both interaction effects are statistically significant at $p < 0.001$, indicating strong empirical support for their inclusion in the proposed fraud detection framework. The negative interaction effect of the whistleblowing system suggests that its presence significantly reduces the likelihood of fraudulent behavior. The results support the expansion of the Fraud Pentagon Theory by incorporating prestige culture and fintech usage. These additions reflect the evolving nature of fraud in digital banking and align with agency theory's emphasis on incentive misalignment (Jensen & Meckling, 1976).

The evaluation of construct measurement quality in this study demonstrates highly satisfactory results. As presented in Table 5, all constructs exhibit strong composite reliability, and Cronbach's alpha values, each exceeding the recommended thresholds proposed by Hair et al. (2021) was 0.70 for composite reliability and 0.60 for Cronbach's alpha. These findings indicate robust internal consistency, suggesting that the measurement items reliably represent their respective latent constructs. In other words, the instruments employed in this study can be considered stable and dependable.

Furthermore, convergent validity, assessed through the Average Variance Extracted (AVE),

Table 5. Reliability and validity test

Latent Variable	Indicator	Loading Factor	AVE	Composite Reliability	Cronbach's Alpha
Pressure	X1.1	0.870	0.813	0.968	0.961
	X1.2	0.916			
	X1.3	0.904			
	X1.4	0.900			
	X1.5	0.907			
	X1.6	0.896			
	X1.7	0.916			
Opportunity	X2.1	0.919	0.813	0.968	0.962
	X2.2	0.870			
	X2.3	0.893			
	X2.4	0.883			
	X2.5	0.888			
	X2.6	0.929			
	X2.7	0.929			
Rationalization	X3.1	0.849	0.611	0.916	0.893
	X3.2	0.746			
	X3.3	0.732			
	X3.4	0.713			
	X3.5	0.726			
	X3.6	0.847			
	X3.7	0.846			

http://dx.doi.org/10.21511/bbs.21(1).2026.18

Table 5 (cont.). Reliability and validity test

Latent Variable	Indicator	Loading Factor	AVE	Composite Reliability	Cronbach's Alpha
Capability	X4.1	0.862	0.595	0.911	0.886
	X4.2	0.751			
	X4.3	0.747			
	X4.4	0.759			
	X4.5	0.756			
	X4.6	0.773			
	X4.7	0.744			
Control	X5.1	0.872	0.736	0.951	0.940
	X5.2	0.799			
	X5.3	0.880			
	X5.4	0.846			
	X5.5	0.815			
	X5.6	0.907			
	X5.7	0.882			
Fintech Usage	X6.1	0.617	0.414	0.774	0.657
	X6.2	0.638			
	X6.3	0.675			
	X6.4	0.595			
	X6.5	0.711			
	X6.6	0.680			
	X6.7	0.777			
Prestige Culture	X7.1	0.837	0.600	0.913	0.888
	X7.2	0.722			
	X7.3	0.744			
	X7.4	0.717			
	X7.5	0.756			
	X7.6	0.836			
	X7.7	0.801			

also shows favorable outcomes. Most constructs report AVE values above 0.50, indicating that more than half of the variance in the indicators is explained by the underlying construct. One exception is the Fintech Usage construct, which records an AVE of 0.414. However, this value remains acceptable within the context of exploratory research. Fornell and Larcker (1981) note that AVE values below 0.50 may still be tolerated when composite reliability is sufficiently high. Accordingly, the Fintech Usage construct remains analytically relevant, although its interpretation should be approached with caution. Despite these strengths, the analysis of the Variance Inflation Factor (VIF) values reveals potential multicollinearity among several constructs. Specifically, Opportunity, Rationalization, and Prestige Culture exhibit VIF values exceeding 10, suggesting overlap in their explanatory power regarding the dependent variable. High multicollinearity can compromise parameter estimation accuracy and obscure causal interpretations.

Figure 2 illustrates the structural model developed in this study, which integrates seven key constructs influencing fraudulent behavior, along with one moderating variable, whistleblowing systems. This model builds on the Fraud Pentagon framework by adding contextual factors such as fintech usage and prestige culture. The diagram shows the direct relationships between each construct and fraudulent behavior, as well as how whistleblowing moderates these effects.

All constructs have a strong and statistically significant influence on fraudulent behavior, with path coefficients ranging from $\beta = 0.712$ to $\beta = 0.929$ and p-values below 0.001. Opportunity ($\beta = 0.929$) and pressure ($\beta = 0.916$) show the highest impact, followed by control ($\beta = 0.907$), capability ($\beta = 0.862$), prestige culture ($\beta = 0.837$), rationalization ($\beta = 0.847$), and fintech usage ($\beta = 0.712$). These results confirm that both behavioral and contextual factors play a major role in shaping fraud tendencies.

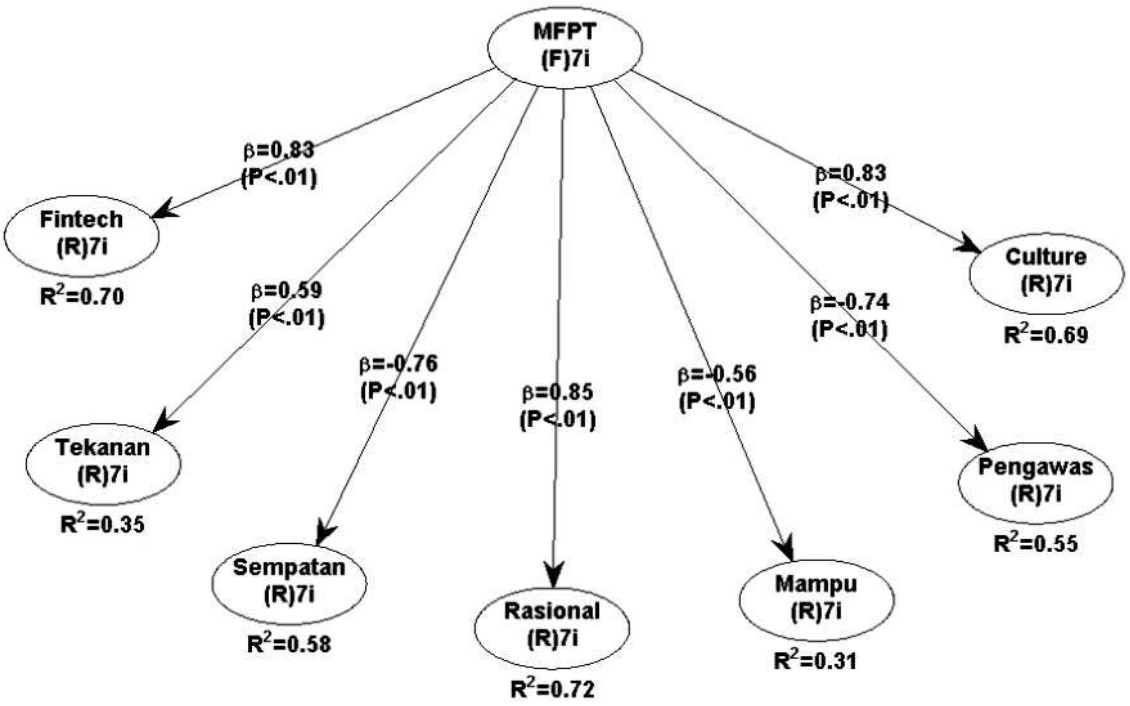

Figure 2. Second-order model MFPT

The model also includes moderation effects from the whistleblowing system, which shows a negative interaction with all main constructs. This means that the presence of a whistleblowing mechanism helps reduce the influence of risk factors on fraudulent behavior. The strongest moderating effects are seen with pressure (β = –0.312) and control (β = –0.298), followed by opportunity (β = –0.284), rationalization (β = –0.267), capability (β = –0.251), prestige culture (β = –0.233), and fintech usage (β = –0.219). All moderation effects are statistically significant, with p-values between 0.002 and 0.015.

Figure 3 presents the visualization of the moderation test, showing how the whistleblowing system acts as a moderating variable that weakens the direct influence of seven key risk constructs on fraudulent behavior. Conceptually, this model illustrates the role of internal reporting mechanisms in interrupting the causal pathways that lead to misconduct within organizations. The interaction paths in the model all show negative directions, indicating that the whistleblowing system functions as a suppressor of risk factor influence. The moderation coefficients are as follows: pressure (β = –0.312), opportunity (β = –0.284), rationalization (β = –0.267), capability (β = –0.251), control (β = –0.298), fintech usage (β = –0.219), and prestige culture (β = –0.233). All values are statistically significant, with p-values ranging from 0.002 to 0.015, confirming that the moderation effects are empirically valid and not due to chance.

These results indicate that the whistleblowing system is most effective in reducing the impact of pressure and control on fraudulent behavior.

Table 6 shows the summary of model fit indices used to assess the overall quality of the structural model. These indicators help confirm that the relationships between constructs are not only statistically significant but also valid and reliable. The Average Full Collinearity VIF (AFVIF) is 2.491, which is well below the acceptable limit of 5 and close to the ideal threshold of 3.3. This means there is no serious multicollinearity among the constructs, and each variable contributes uniquely to the model without excessive overlap. The Tenenhaus Goodness of Fit (GoF) is 0.598, which falls into the "large" category (≥ 0.36). This indicates that the model fits the data very well and has strong explanatory power for the phenomenon being studied – fraudulent behavior.

http://dx.doi.org/10.21511/bbs.21(1).2026.18

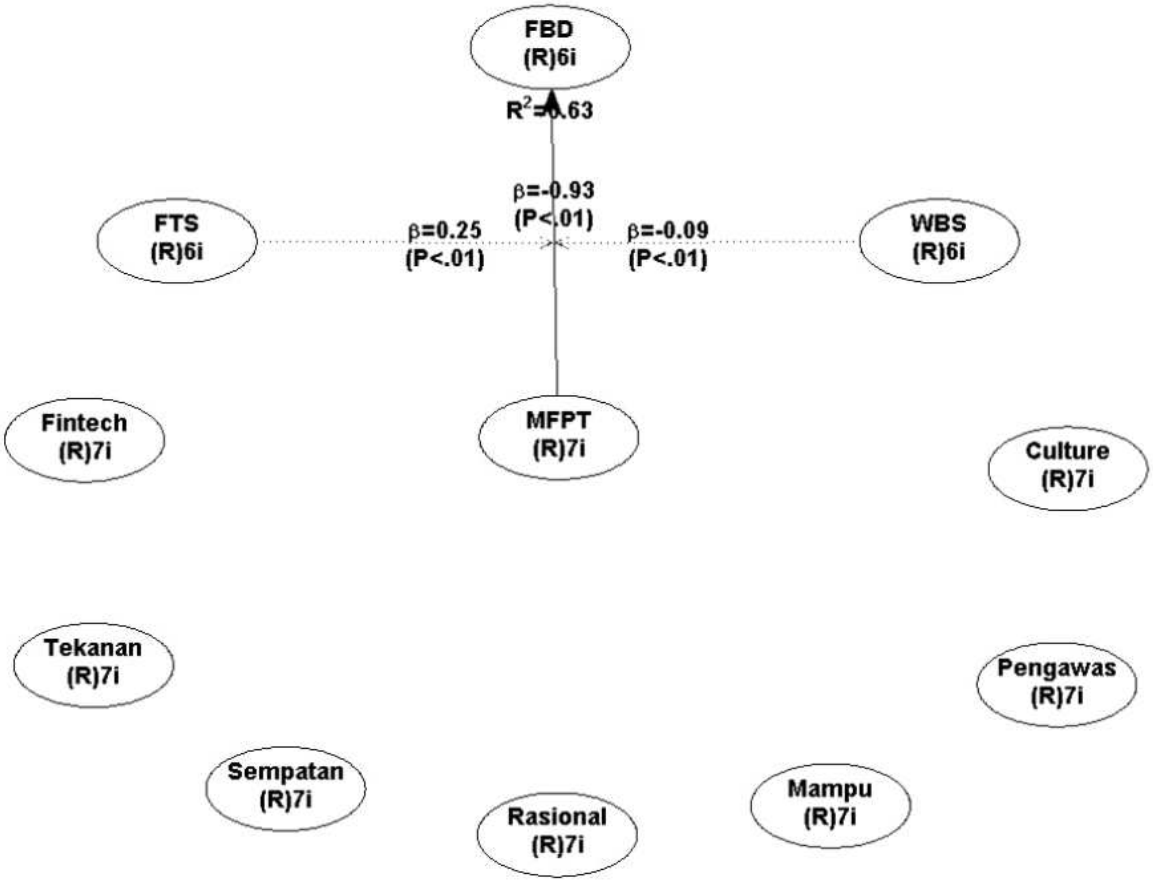

Figure 3. Model structural SEM

The Average Path Coefficient (APC) is 0.738 with a p-value < 0.001, showing that the average strength of relationships between constructs is high and statistically significant. This confirms that the model's pathways are meaningful and relevant. The Average R-squared (ARS) and Average Adjusted R-squared (AARS) are 0.557 and 0.556, respectively, both with p-values < 0.001. These values show that the model explains more than 55% of the variation in the data, which is considered strong in behavioral research. The closeness of ARS and AARS also suggests that the model is stable and not overfit. Overall, the model meets all recommended criteria and shows strong fit, predictive ability, and stability. These results support the validity of the modified Fraud Pentagon framework and provide a solid foundation for further hypothesis testing and policy development in digital financial institutions.

Table 7 shows the results of testing the three main hypotheses in this study. All three hypotheses are supported by statistically significant results, with path coefficients (β) and p-values below 0.05, confirming that the relationships tested are valid and meaningful. The first hypothesis (H1) looks at the effect of the Modified Fraud Pentagon Theory (MFPT) on fraud behavior. The result shows a

Table 6. Model fit indices summary

Fit Index	Value	Threshold Criteria	Interpretation
Average Full Collinearity VIF (AFVIF)	2.491	Acceptable if ≤ 5; ideally ≤ 3.3	Ideally
Tenenhaus Goodness of Fit (GoF)	0.598	≥ 0.36 (large), ≥ 0.25 (medium), ≥ 0.1 (small)	Large
Average Path Coefficient (APC)	0.738; p < 0.001	p < 0.05	Accepted
Average R-squared (ARS)	0.557; P < 0.001	p < 0.05	Accepted
Average Adjusted R-squared (AARS)	0.556; P < 0.001	p < 0.05	Accepted

Table 7. Hypotheses testing results

Hypothesis	Path (Independent → Dependent)	Coefficient (β)	p-value	Result	Interpretation
H1	Modified Fraud Pentagon Theory (MFPT) → Fraud Behaviour Detection	0.930	< 0.001	Supported	Pressure significantly increases fraud behaviour detection
H2	Whistleblowing Systems	–0.088	0.009	Supported	Whistleblowing systems significantly weaken the relationship between fraud drivers and fraud behaviour
H3	Fintech Security	–0.246	< 0.001	Supported	Fintech security reduces fraud risk by mitigating fintech-related vulnerabilities

strong positive influence (β = 0.930, p < 0.001), meaning that when all five elements, pressure, opportunity, rationalization, capability, and control, are present together, the chance of fraud increases significantly. This supports the idea that a multifactor approach is more effective in explaining fraud than looking at single causes.

The second hypothesis (H2) tests whether whistleblowing systems help reduce fraud. The result shows a small but significant negative effect (β = –0.088, p = 0.009), indicating that having a trusted reporting channel can discourage individuals from committing fraud. Even though the effect is modest, it still plays an important role in prevention. The third hypothesis (H3) examines the role of fintech security. The result shows a stronger negative effect (β = –0.246, p < 0.001), meaning that good security systems like data encryption, two-factor authentication, and real-time monitoring can effectively reduce fraud risk, especially in digital environments.

4. DISCUSSION

The results of this study provide strong empirical support for the proposed conceptual framework, which integrates behavioral, contextual, and structural dimensions in explaining fraudulent behavior within Indonesia's banking sector. Three hypotheses were tested to assess the influence of the Modified Fraud Pentagon Theory (MFPT), the moderating role of whistleblowing systems, and the impact of fintech security. All three hypotheses were statistically supported, offering both theoretical and practical implications for fraud detection and prevention in digital financial institutions.

The first hypothesis examined the effect of MFPT on fraudulent behavior, incorporating five traditional fraud drivers: pressure, opportunity, rationalization, capability, and control, alongside two contextual constructs: fintech usage and prestige culture. The structural model revealed a strong and significant path coefficient (β = 0.930, p < 0.001), confirming that MFPT provides a robust framework for detecting fraud in banking environments. Among the core constructs, opportunity (β = 0.929) and pressure (β = 0.916) emerged as the most influential predictors. These findings reaffirm the foundational role of situational access and external demands in shaping unethical behavior, consistent with Cressey's fraud triangle and its expansion into the fraud pentagon. Rationalization (β = 0.847) and capability (β = 0.862) also showed significant effects, highlighting the psychological and technical dimensions of fraud. Interestingly, control (β = 0.907) demonstrated a strong positive relationship with fraudulent behavior, suggesting that formal control mechanisms may be ineffective if not perceived as credible or consistently enforced. This result aligns with prior studies indicating that rigid but culturally undermined control structures may fail to deter misconduct (Hail et al., 2018). In contrast to the findings of Asmaranti et al. (2023), which revealed that pressure and opportunity were not dominant in the context of Indonesian banking, this study demonstrates that both factors are, in fact, the strongest predictors. This underscores the contextual differences brought about by digitalization, which make pressure and opportunity more relevant compared to the results of previous research. Notably, younger respondents (aged 21-30) emphasized opportunity more strongly, reflecting their daily reliance on mobile banking and fintech platforms, while older respondents (41-50) highlighted pressure as a dominant factor, likely due to career demands and organizational expectations.

http://dx.doi.org/10.21511/bbs.21(1).2026.18

The inclusion of fintech usage (β = 0.712) and prestige culture (β = 0.837) significantly enhanced the model's explanatory power. Fintech usage reflects the dual nature of digital platforms, which improve efficiency but also introduce anonymity and reduced oversight conditions that can be exploited for fraud. Prestige culture captures the psychological drive for status and recognition, often leading individuals to rationalize unethical actions to maintain social standing. These findings extend the scope of MFPT by incorporating emerging behavioral risks in digital banking contexts. This finding extends the results of Shonhadji and Irwandi (2024), which previously emphasized only the relevance of prestige culture and fintech exposure as behavioral factors. The present study not only confirms that relevance but also demonstrates stronger statistical significance within the structural model. Educational background influenced these perceptions: bachelor's degree holders associated fintech usage with fraud risk, while master's degree holders emphasized prestige culture, suggesting that higher education may heighten awareness of organizational dynamics and status-driven behavior.

The second hypothesis tested the moderating effect of whistleblowing systems on the relationship between fraud drivers and fraudulent behavior. The interaction term yielded a negative and statistically significant coefficient (β = –0.088, p = 0.009), indicating that whistleblowing mechanisms effectively weaken the influence of fraud triggers. This result supports deterrence theory, which posits that perceived certainty of detection reduces the likelihood of misconduct. When credible and anonymous reporting channels are available, individuals are less likely to engage in fraud even in environments characterized by high pressure, opportunity, or rationalization. The effectiveness of whistleblowing systems depends not only on their technical design but also on organizational support and ethical climate, as emphasized by Shonhadji and Maulidi (2021). These systems foster a culture of accountability and serve as psychological barriers against unethical behavior. This is consistent with the findings of Maulida and Bayunitri (2021), which demonstrated the effectiveness of whistleblowing systems in reducing fraud levels by more than 50%. However, this study adds the contextual insight that the effectiveness of whistleblowing is strongly influenced by organizational cultural support, thereby extending the understanding provided by previous research. Respondent categories revealed that employees with more than 10 years of experience valued whistleblowing systems more highly, perceiving them as credible deterrents, while younger employees expressed skepticism due to cultural barriers and fear of retaliation.

The third hypothesis evaluated the moderating effect of fintech security on the relationship between fraud drivers and fraudulent behavior. The structural equation model revealed a statistically significant negative interaction (β = –0.246, p < 0.001), indicating that the presence of strong fintech security mechanisms substantially weakens the influence of behavioral fraud triggers such as pressure, opportunity, rationalization, capability, and control. This finding underscores the strategic role of digital safeguards in fraud mitigation. Fintech security refers to a suite of technological protections, including encryption protocols, biometric authentication, multi-factor access controls, and AI-driven transaction monitoring that collectively reduce system vulnerabilities and limit unauthorized manipulation. These mechanisms not only deter external threats but also constrain internal actors by increasing the perceived risk of detection and reducing exploitable gaps in digital infrastructure. Thus, the finding is supported by Mustyala and Allam (2024). They show that layered security frameworks significantly reduce fraud exposure by enhancing traceability and accountability across digital platforms. Similarly, Goyal et al. (2025) demonstrate that fintech security not only improves operational efficiency but also acts as a structural deterrent against misconduct. In contrast to Handoko et al. (2020), who emphasized that digitalization increases the opportunities for fraud, this study demonstrates that the implementation of robust fintech security can significantly reduce such opportunities. Thus, the findings not only confirm the risks associated with digitalization but also offer a more concrete mitigation solution. Respondent analysis showed that younger employees (21-30 years) placed greater emphasis on fintech security, reflecting their daily engagement with mobile applications and digital banking systems, whereas older employees highlighted traditional control mechanisms, suggesting generational differences in reliance on technological safeguards.

CONCLUSION

The purpose of this study was to develop and validate a behavioral fraud detection model within digital financial organizations using the Modified Fraud Pentagon Theory (MFPT). The findings of the study established that factors that significantly impact someone committing a fraudulent act are: pressure, opportunity, ability, control, usage of Fintech, and prestige culture, in addition to whistle-blowing systems and the security of Fintech being very effective moderating variables. Further demographic analysis indicates that younger respondents placed a higher emphasis on opportunity and Fintech-related risks. Conversely, older respondents tended to view the most significant contributing factors to fraudulent behavior as pressure and prestige culture. Respondents with only a bachelor's degree concentrated on operational exposure. While respondents with a master's degree highlighted organizational dynamics. Also, there was a significant correlation between the number of years of work experience an individual has and how important they consider whistle-blowing systems to be compared to more experienced employees. The demographic breakdown of the results further supports the conclusion that each of the respondent groups views the reasons fraud occurs and the means to prevent it from occurring differently. Fraud detection in Indonesia's banking industry must use a multifaceted strategy that includes technological advancements, culture, and behaviors. Prevention of fraud requires an effective internal control system to provide confidential reporting of misconduct or illegal activities (whistle-blowing), as well as an effective and secure Fintech. The success of these systems will be influenced by both the culture in which they operate as well as the background of the employees who are part of the operational organizations using the systems for reporting fraud, and this is why fraud prevention programs must be designed with consideration of the demographic characteristics of the different groups of employees, so that training, education efforts and oversight can be tailored to the unique fraud prevention and detection challenges posed by each employee group. Theoretically, the Fraud Pentagon framework has been developed into more contextualized and adaptive models for the digital age. The practical extension of this research provides actionable information for financial service organizations, such as developing safe mechanisms to report suspected fraud. Limitations will remain within this area of research, particularly the current lack of differentiation between formal and informal types of whistleblowing channels. Fintech's security is treated as one construct in this research, although future research should further analyze technical and user-awareness related to fintech's security, and also investigate how demographic variables interact with these dimensions to provide a more complete understanding of their relationship to fraud mitigation.

AUTHOR CONTRIBUTIONS

Conceptualization: Soni Agus Irwandi, Agus Samekto, Nanang Shonhadji.
Data curation: Soni Agus Irwandi, Nanang Shonhadji.
Formal analysis: Soni Agus Irwandi, Agus Samekto, Nanang Shonhadji.
Funding acquisition: Soni Agus Irwandi, Agus Samekto.
Investigation: Soni Agus Irwandi, Agus Samekto.
Methodology: Soni Agus Irwandi.
Project administration: Soni Agus Irwandi, Agus Samekto, Nanang Shonhadji.
Resources: Soni Agus Irwandi, Agus Samekto, Nanang Shonhadji.
Software: Soni Agus Irwandi.
Supervision: Soni Agus Irwandi.
Validation: Soni Agus Irwandi, Agus Samekto.
Visualization: Soni Agus Irwandi, Agus Samekto.
Writing – original draft: Soni Agus Irwandi, Nanang Shonhadji.
Writing – reviewing & editing: Soni Agus Irwandi, Agus Samekto, Nanang Shonhadji.

http://dx.doi.org/10.21511/bbs.21(1).2026.18

REFERENCES

1. Albert-Sogules, I., Sonubi, T. O., Azuikpe, P. F., Odebode, A., Alamu, A. S., Ayo-Lawal, A., & Sambo, U. (2024). Design of an intelligent financial surveillance system using big data analytics for enhanced fraud detection and prevention in financial institutions. *International Journal of Science and Research Archive, 12*(02), 2295-2306. https://doi.org/10.30574/ijsra.2024.12.2.1529
2. Albrecht, Ch. O., & Albrecht, Co. C. (2009). International ethics, fraud, and corruption: a cross-cultural perspective. *Cross-Cultural Management: An International Journal, 16*(3). https://doi.org/10.1108/ccm.2009.13616caa.001
3. Asmaranti, Y., Lokman, N., & Rahman, R. A. (2023). Detection of financial statement fraud using the fraud pentagon theory perspective in Indonesia. *European Proceedings of Social and Behavioural Sciences* (pp. 192-202). https://doi.org/10.15405/epsbs.2023.11.16
4. Ayuningtyas, D., Windiarti, S., Hadi, M. S., Fasrini U. U., & Barinda, S. (2021). Disaster preparedness and mitigation in Indonesia: A narrative review. *Iran Journal Public Health, 50*(8), 536-546. https://doi.org/10.18502/ijph.v50i8.6799
5. Chettier, T. M., Boyina, V. A. K., & Rangineni, S. (2025). AI-Powered Risk Assessment and Compliance in Cloud Cybersecurity. *International Journal of Computer Trends and Technology (IJCTT), 73*(3), 57-63. https://doi.org/10.14445/22312803/IJCTT-V73I3P107
6. Chijoke-Mgbame, A. M., Boateng, A., & Mgbame, C. O. (2020). Board gender diversity, audit committee, and financial performance: Evidence from Nigeria. *Accounting Forum*, *44*(3), 262-286. https://doi.org/10.1080/01559982.2020.1766280
7. Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement.* Free Press.
8. Crowe, C. (2011). *Why the fraud triangle is no longer enough*. Crowe Horwath LLP.
9. Deloitte. (2024). *Deloitte analysis: Whistleblowing programmes in Asia Pacific organisations have increased, signalling their commitment to ethical transformation.* Deloitte Southeast Asia Media. Retrieved from https://www.deloitte.com/southeast-asia/en/about/press-room/whistleblowing-programmes-in-asia-pacific-organisations-have-increased.html
10. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. https://doi.org/10.2307/3151312
11. Goyal, K., Garg, M., & Malik, S. (2025). Adoption of artificial intelligence-based credit risk assessment and fraud detection in banking services: A hybrid approach (SEM-ANN). *Future Business Journal, 11*(44). https://doi.org/10.1186/s43093-025-00464-3
12. Hail, L., Tahoun, A., & Wang, C. (2018). Corporate scandals and regulation. *Journal of Accounting Research, 56*(2), 617-671. https://doi.org/10.1111/1475-679X.12201
13. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2021). *Multivariate data analysis* (8th ed.). Cengage Learning.
14. Handoko, B. L., Lindawati, A. S. L., & Vienna, M. (2020). Fraud Pentagon Model for Detecting Fraudulent Financial Reporting in the Banking Sector. *International Journal of Recent Technology and Engineering, 8*(6), 2832-2838. https://doi.org/10.35940/ijrte.F8380.038620
15. Hidayah, E., & Saptarini, G. D. (2019). Pentagon fraud analysis in detecting potential financial statement fraud of banking companies in Indonesia. *Proceedings of the International Conference on Accounting, Business & Economics (ICABE)* (pp. 89-102). Universitas Islam Indonesia. Retrieved from https://journal.uii.ac.id/icabe/article/download/14697/9920
16. Idrawahyuni, Andayangsih, S., Adiningrat, A. A., Adil, M., & Winarsih, E. (2025). Financial Crime Early Prevention Strategy: The Utilization of Whistleblowing System and Risk Management in Sharia Bank. *IQTISHODUNA: Jurnal Ekonomi Islam, 14*(2). 617-632. https://doi.org/10.54471/iqtishoduna.v14i2.2915
17. Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305-360. https://doi.org/10.1016/0304-405X(76)90026-X
18. Mangalam, K. R. (2025). Trends and Patterns of Banking Frauds in Private and Government Banks: A Comparative Analysis (2020-2025). *REST Journal on Banking, Accounting and Business, 4*(3), 53-65. https://doi.org/10.46632/jbab/4/3/9
19. Marsam Dollah, A. D., Md Shah, M. A. M., Ab Majid, R., & Basri, S. A. (2025). Whistleblowers in ASEAN Countries: A Whither. *Information Management and Business Review, 17*(1(I), 408-415. https://doi.org/10.22610/imbr.v17i1(I).4060
20. Maulida, W. Y., & Bayunitri, B. I. (2021). The influence of whistleblowing system toward fraud prevention. *International Journal of Financial, Accounting, and Management (IJFAM), 2*(4), 275-294. https://doi.org/10.35912/ijfam.v2i4.177
21. Moura, L., Barcaui, A., & Payer, R. (2025). AI and Financial Fraud Prevention: Mapping the Trends and Challenges Through a Bibliometric Lens. *Journal of Risk and Financial Management, 18*(6). https://doi.org/10.3390/jrfm18060323
22. Mustyala, M., & Allam, M. (2024). Fintech security and whistleblowing effectiveness in fraud mitigation: Evidence from Southeast Asia. *Asian Journal of Business Ethics.*

23. Nugroho, D. S., & Diyanty, V. (2022). Hexagon Fraud in Fraudulent Financial Statements: The Moderating Role of Audit Committee. *Jurnal Akuntansi dan Keuangan Indonesia, 19*(1), Article 3. https://doi.org//10.21002/jaki.2022.03

24. Olowu, O., Olowofela, A., Omokanye, A., Ajayi, A., Adepoju, A., Omole, O., & Chianumba, E. (2024). AI-driven fraud detection in banking: A systematic review of data science approaches. *GSC Advanced Research and Reviews, 21*(2), 227-237. https://doi.org/10.30574/gscarr.2024.21.2.0418

25. Palakurti, N. R. (2025). The Impact of Financial Technology (FinTech) on Risk Management and Fraud Control in Banking. *International Journal of Novel Research and Development, 10*(12). Retrieved from https://ijnrd.org/viewpaperforall.php?paper=IJNRD2503110

26. Putri, F. A., & Prabowo, T. J. W. (2025). Pengaruh Struktur Kepemilikan Institusional, Kinerja Lingkungan, Dan Ukuran Perusahaan Terhadap Nilai Perusahaan [The Influence of Institutional Ownership Structure, Environmental Performance, and Company Size on Company Value]. *Diponegoro Journal of Accounting, 14*(3). (In Indonesian). Retrieved from https://ejournal3.undip.ac.id/index.php/accounting/article/view/52890

27. Sari, S. P., & Nugroho, N. K. (2020). Financial Statements Fraud dengan Pendekatan Vousinas Fraud Hexagon Model: Tinjauan pada Perusahaan Terbuka di Indonesia [Financial Statements Fraud with the Vousinas Fraud Hexagon Model Approach: A Review of Public Companies in Indonesia]. *Proceedings: 1st Annual Conference On Ihtifaz: Islamic Economics, Finance, and Banking*, (pp. 409-430). (In Indonesian). Retrieved from https://d1wqtxts1xzle7.cloudfront.net/107545534/3641-8754-2-PB-libre.pdf

28. Shonhadji, N. (2020). Paradox of white collar crime and fraud in banking: Critical analysis of agency theory and gone theory. *ASSETS: Jurnal Akuntansi dan Pendidikan, 9*(2), 142-155. https://doi.org/10.25273/jap.v9i2.6415

29. Shonhadji, N., & Irwandi, S. A. (2024). Fraud prevention in the Indonesian banking sector using anti-fraud strategy. *Banks and Bank Systems, 19*(1), 12-23. https://dx.doi.org/10.21511/bbs.19(1).2024.02

30. Shonhadji, N., & Maulidi, A. (2021). The Roles of Whistleblowing System and Fraud Awareness as Financial Statement Fraud Deterrent. *International Journal of Ethics and Systems, 37*(3), 370-389. https://doi.org/10.1108/IJOES-09-2020-0140

31. Yang, T., & Zhang, X. (2022). FinTech adoption and financial inclusion: Evidence from household consumption in China. *Journal of Banking & Finance, 145,* 106668. https://doi.org/10.1016/j.jbankfin.2022.106668

http://dx.doi.org/10.21511/bbs.21(1).2026.18

APPENDIX A. RESEARCH INSTRUMENT

Dear Respondent,

We sincerely thank you for your willingness to participate in this study. This research is part of the 2025 PF-PKPT Basic Research Grant program, aimed at empirically examining the factors influencing fraud behaviour detection within organizational contexts, using a modified approach to the Fraud Pentagon Theory (FPT) and integrating financial technology and organizational culture variables.

This questionnaire consists of several sections that reflect the main constructs in the research model, namely: pressure, opportunity, rationalization, capability, supervision, fintech usage, individual prestige culture, and two moderating variables—fintech security and whistleblowing systems. All statements are presented using a 5-point Likert scale, and you are asked to respond based on your perceptions and experiences.

Likert Scale:

Score	Description
1	Strongly Disagree
2	Disagree
3	Slightly Disagree
4	Agree
5	Strongly Agree

Your participation is voluntary and anonymous. All data collected will be used solely for academic and scientific analysis purposes, and confidentiality is guaranteed in accordance with research ethics principles.

Research Ethics: COPE Principles

This study fully adheres to the principles and guidelines established by the Committee on Publication Ethics (COPE), including:

- Academic Integrity: All data collection and analysis processes are conducted honestly, transparently, and accountably.
- Respondent Confidentiality: Your identity and responses will not be disclosed to any third party.
- Informed Consent: Your participation indicates that you understand the purpose and procedures of this research.
- Data Usage: Data will be used exclusively for scientific purposes and will not be misused for commercial or non-academic objectives.
- Respondent Rights: You have the right to skip any question or withdraw from participation at any time without consequence.

We deeply appreciate your participation and contribution.

Sincerely, Research Team Soni Agus Irwandi et al.

APPENDIX B

Table B1. X1: Pressure

No.	Statement	1	2	3	4	5
1	I feel that work pressure affects my ethical decisions.					
2	High-performance targets push me to take shortcuts.					
3	Pressure from superiors affects my integrity.					
4	I feel pressured to adjust financial reports.					
5	Social expectations push me to appear perfect at work.					
6	Personal financial pressure affects my behavior at work.					
7	I have felt driven to violate rules due to work pressure.					

Table B2. X2: Opportunity

No.	Statement	1	2	3	4	5
1	Internal control systems at my workplace are weak.					
2	I have access to systems that are not monitored.					
3	Loose work procedures create opportunities for fraud.					
4	I feel I can commit violations without being detected.					
5	Lack of supervision allows unethical actions.					
6	I have seen loopholes for fraud in the work system.					
7	Company policies allow for manipulative behavior opportunities.					

Table B3. X3: Rationalization

No.	Statement	1	2	3	4	5
1	I believe that under certain conditions, fraud can be justified.					
2	Organizational culture influences how I justify my actions.					
3	I have justified unethical actions to meet targets.					
4	I feel fraud is acceptable if it causes no direct harm.					
5	I have used moral reasoning to cover up violations.					
6	I feel work pressure can justify my actions.					
7	I believe everyone has committed minor violations.					

Table B4. X4: Capability

No.	Statement	1	2	3	4	5
1	I have the ability to manipulate data without being detected.					
2	I master technologies that can be used to conceal fraud.					
3	I feel technical training increases fraud risk.					
4	My knowledge of systems opens opportunities for manipulation.					
5	I have access to sensitive information that can be exploited.					
6	I know how to avoid detection in monitoring systems.					
7	My position gives me the power to bypass control.					

Table B5. X5: Supervision

No.	Statement	1	2	3	4	5
1	Supervision at my workplace is strict.					
2	Weak supervision increases fraud risk.					
3	Monitoring mechanisms help prevent violations.					
4	I feel monitored in every work activity.					
5	Internal supervision is effective in detecting fraud.					
6	I feel supervision helps enforce compliance.					
7	I have seen supervision fail to prevent fraud.					

http://dx.doi.org/10.21511/bbs.21(1).2026.18

Table B6. X6: Fintech Usage

No.	Statement	1	2	3	4	5
1	I feel comfortable using financial technology.					
2	Fintech simplifies my financial transactions.					
3	I believe fintech can be used to manipulate transactions.					
4	I have seen fintech used to conceal identity.					
5	Fintech convenience increases fraud risk.					
6	I feel fintech speeds up work processes but opens fraud loopholes.					
7	I believe fintech can be used to bypass supervision.					

Table B7. X7: Individual prestige culture

No.	Statement	1	2	3	4	5
1	I feel strong pressure to appear successful.					
2	Prestige culture drives me to achieve targets by any means.					
3	Workplace competition affects my ethical behavior.					
4	I have been tempted to violate rules to maintain my image.					
5	Prestige achievement is important to me, even if it means breaking rules.					
6	My work environment strongly emphasizes prestige achievement.					
7	I feel prestige culture affects my work integrity.					

Table B8. Z1: Fintech security (Moderator 1)

No.	Statement	1	2	3	4	5
1	The fintech security system at my workplace is sufficiently strong.					
2	I believe fintech security can prevent identity theft.					
3	AI technology is used to enhance fintech security.					
4	I feel safe using fintech due to its security system.					
5	Fintech security influences my trust in financial services.					
6	The fintech security system can detect suspicious activity.					
7	I believe fintech security reduces opportunities for fraud.					

Table B9. Z2: Whistleblowing Systems (Moderator 2)

No.	Statement	1	2	3	4	5
1	I feel safe reporting violations through the whistleblowing system.					
2	The whistleblowing system is consistently implemented at my workplace.					
3	I believe reports can be submitted anonymously.					
4	Whistleblowing helps prevent fraud.					
5	I know how to use the whistleblowing system.					
6	The whistleblowing system influences the compliance culture in my organization.					
7	I have witnessed violations being reported through whistleblowing.					

Table B10. Y: Fraud behavior detection (Dependent variable)

No.	Statement	1	2	3	4	5
1	My organization has a comprehensive fraud detection system.					
2	Fraud audits are conducted regularly.					
3	Anti-fraud policies are consistently enforced.					
4	Fraud symptoms can be identified early.					
5	Violations are addressed according to legal procedures.					
6	A fraud reporting system is available and easily accessible.					
7	I believe the organization is capable of detecting fraudulent behavior.					