Extending the Fraud Diamond Theory: An Adaptive Framework for Preventing Customer-initiated Fraud in the Digital Banking Ecosystem

Ali Maskur
Universitas STIKUBANK
maskur@edu.unisbank.ac.id

Ignatius Hari Santoso
Universitas STIKUBANK
ignatiusharisantoso@edu.unisbank.ac.id

Abstract
The rapid expansion of digital banking ecosystem has transformed financial service accessibility while simultaneously creating new opportunities for customer-initiated fraud. Compared to conventional banking systems, digital platforms present unique vulnerabilities arising from technological complexity, remote transaction, and reduced direct oversight. Although the Fraud Diamond Theory has been widely used to explain fraudulent behavior through pressure, opportunity, rationalization and capability, its applicability in customer-driven fraud within digital environment remains underexplored. This study aims to extend the Fraud Diamond Theory by introducing perceived severity as an adaptive construct to explain customer-initiated fraud intention. A mixed-method approach is employed using two sequential stages, which is in-depth interview and partial least square method to empirically test the new construct using 111 digital banking users. The findings reveal that financial pressure, rationalization, and perceived severity significantly influence customer-initiated fraud intention, meanwhile, perceived opportunity and capability are found to have no significant effect. This study contributes theoretically by extending Fraud Diamond Theory through the inclusion of deterrence-oriented perspective. Practically, the findings suggest that financial institution should complement technological security measures with behavioral interventions, user education and communication strategies emphasizing the consequences of fraudulent actions.

Keywords: *fraud diamond theory, customer-initiated fraud intention, digital banking, perceived severity, digital banking*

INTRODUCTION

In recent years, fraud in the banking sector has shown an increasing trend, in line with the rapid digital transformation of the financial industry. Report from various international institution indicate that fraud is no longer limited to internal manipulation or conventional crimes, but has evolved into digital-based fraud involving various methods such as phishing, account takeovers, social engineering and identity theft. This situation is exacerbated by the increasing number of users of digital financial services, which opens up

wider opportunities for perpetrators to exploit system loopholes and weakness in user behavior. Empirical studies show that the digitalization of financial services significantly increases exposure to fraud risk due to the increasing complexity of systems and technology-based interaction (Kou et al., 2021; Omarini, 2018).

Data from the Financial Service Authority (Otoritas Jasa Keuangan) shows that complaints related to fraud in the financial service sectors continue to increase, with thousands of reports annually, dominated by cases of digital fraud and misuse of customer accounts (Otoritas Jasa Keuangan, 2023). This phenomenon raises fundamental questions about why fraud has become increasingly prevalent in the modern banking industry. One key factor is the shift in transaction characteristics from a physical to a fully digital one. In a digital environment, interaction between customers and financial institutions tend to be indirect, reducing the traditional controls and increasing the opportunity for manipulation.

Furthermore, technological advances have provided broader access to tools and methods that can be used to commit fraud, even by individuals with relatively limited technical skills. Research also shows that easy access to technology, low digital security literacy, and increased anonymity in transactions are key factors driving the rise in fraud opportunities in the banking sector (Levi & Smith, 2021; Button & Cross, 2017). In line with this, Bank Indonesia reported that the value of digital transaction in Indonesia has experienced very rapid growth in recent years. BI noted that electronic money and digital banking transactions have grown by double digits annually, reflecting the high public adoption of digital financial services (Bank Indonesia, 2023). While this growth offers benefits in term of efficiency and convenience, the increased volume of digital transaction also directly increases exposure to fraud risk, as more points of interactions can be exploited by criminals.

Furthermore, the development of the digital banking ecosystem has exacerbated the complexity of fraud issues. This ecosystem involves not only banks as primary institutions, but also various other parties such as fintech, payment services providers and integrated digital platforms. While this integration provides convenience and efficiency for users, it also creates a wider attack surface, opening up more vulnerabilities that fraudster can exploit. Furthermore, the characteristic of digital service that emphasize speed and convenience often come at the expense of stringent verification and control, increasing the opportunity for abuse.

According to Bank Indonesia, the integration of payment system through initiatives such as BI-Fast and QRIS has significantly accelerated the flow of digital transactions (Bank Indonesia, 2023). However this integration also creates a wider risk surface, as each integration also creates a wider risk surface, as each integration point has the potential to become a security gap if not properly managed. On the other hand, the shifting role of customers in the digital ecosystem is also a crucial factor. Customer are no longer merely passive users but also active participants in digital transaction process. This makes customer behavior and perception key elements in the occurrence of fraud, both as victims and perpetrators. In this context, various studies have begun to emphasize the importance of a behavioral approach to understanding fraud, as factors such as rationalization, financial pressure, and perceptions of risk and consequences play a significant role in driving fraudulent intentions (Vousinas 2019; Free, 2015).

Thus, the rise in fraud cases in digital banking is not only caused by technological system weakness but also by the complex interaction between technological factors, the environment, and individual behavior. Therefore, a theoretical approach capable of comprehensively explaining this phenomenon is needed. One relevant approach is the Fraud Diamond Theory, which emphasize the role of pressure, opportunity, rationalization and

capability in driving fraud. However, in the context of the ever-evolving digital ecosystem, this theory requires adaptation to accommodate new dynamics, particularly those related to customer behavior in the digital environment. This provides an important foundation for this research in developing an adaptive model to understand and prevent fraud in the digital banking ecosystem.

On the other hand, OJK report also emphasized that most digital fraud cases involve customer behavioral factors, such as a lack of awareness of social engineering-based fraud and a tendency to share sensitive information with unauthorized parties (Otoritas Jasa Keuangan, 2023). This suggest that fraud in the digital ecosystem is not solely caused by system weakness but also by the complex interaction between technology and individual behavior.

Research Gap

Although research on fraud and security in digital financial service has advanced rapidly over the past decade, several significant research gaps remains. First, most previous studies have focused more on technical approaches and fraud detection, such as the use of machine learning and data analytics to identify suspicious transactions, rather than understanding the behavioral factors that drive individuals to commit fraud (Kou et al., 2021). This approach tend to ignore the psychological and cognitive aspects of users as actors in the digital ecosystem.

Second, research examining fraud in the banking context is still dominated by internal organizational perspective, such as fraud by employees or management. Studies specifically addressing customer-initiated fraud in the digital environment are relatively limited (Maskur & Santoso, 2025; Vousinas, 2019; Leukfeldt, 2017). Yet digital transformation has transformed customers into more active participants in the system,

increasing their potential for fraud involvement.

Third, although the Fraud Diamond Theory has been widely used to explain fraudulent behavior, its application in the context of the digital banking ecosystem remains largely unexplored empirically. Most studies still use this model in traditional context, thus failing to fully capture new dynamics such as digital anonymity, ease of access and system complexity (Kassem & Higson, 2016). This highlights the need to adapt and expand theoretical models to suit evolving digital environments.

Fourth, the literature on deterrence in the digital context generally focuses on compliance with information security policies, not specifically on fraudulent behavior. Although variables such as perceived severity have been shown to be influential in reducing fraudulent intentions, their integration with fraud models such as Fraud Diamond remains rare (Ifinedo, 2019; Cheng et al., 2017). This suggests an opportunity to develop a more comprehensive model that incorporates motivational and deterrence perspectives.

Finally, from a methodological perspective, most previous researches used a single quantitative approach, potentially overlooking deeper empirical context. The use of mixed-method approaches, particularly the combination of PLS-SEM with in-depth interview relatively limited in digital fraud studies. Based on this gap, this research seeks to address this gap by developing an adaptive model based on Fraud Diamond Theory contextualized within the digital banking ecosystem and integrating it with a deterrence perspective through the perceived severity variable.

LITERATURE REVIEW

Fraud Diamond Theory

The Fraud Diamond Theory is a development of the Fraud Triangle Theory,

originally introduced by Cressey (1953), and then expanded by Wolfe and Hermanson (2004) by adding capability as a fourth factor in explaining fraud. Within this framework, fraudulent behavior is influenced by four main elements such as pressure, opportunity, rationalization and capability. Pressure refers to the incentive or pressure experienced by an individual whether financial or non-financial. Opportunity reflects the existence of gaps or weakness in the system that allow fraud to occur. Rationalization is the moral justification process an individual uses to justify their actions, while capability refers to the individual's ability to carry out the fraudulent act.

In recent literature developments, the Fraud Diamond Theory remains relevant, but requires adaptation to the digital context. A study by Abdullahi & Mansor (2018) shows that the complexity of digital system and increased user anonymity can increase the opportunities and expand the scope of individual capabilities beyond traditional organizational boundaries. Furthermore, research by Kaseem & Higson (2016) confirms that the elements of the Fraud Diamond need to be reinterpreted in the context of a digitalized environment, where interactions are no longer physical and traditional control are limited.

Deterrence Theory and Perceived Severity

In addition to the internal factors described in the Fraud Diamond, criminology literature emphasizes the importance of external factors through Deterrence Theory, which states that deviant behavior can be prevented if individuals perceive the consequences of such actions to be severe and unfavorable. In this context, perceived severity is a key determinant in shaping an individual's decision not to commit a crime.

Recent empirical research continues to demonstrate that perceived severity is a crucial determinant in reducing the intention to commit violations in digital environments.

A study by Ifinedo (2019) found that the perception of severe sanctions significantly reduced the individual's intention to violate information security policies, as individuals tend to consider negative consequences before acting. This finding confirms that severity serves as an effective external control mechanism in shaping compliance behavior.

Furthermore, research by Cheng et al. (2017) showed that the combination of perceived severity and perceived certainty significantly influenced compliance with information security policies. In this context, severity plays a role in increasing individual's awareness of the serious consequences of violations, thereby reducing the tendency to engage in deviant behavior. Another study by Posey et al. (2018), showed that perception of negative consequences, including punishments and personal loss, significantly reduce the unethical behavior in information technology environments. This research emphasize that when individuals perceive that the consequences are serious and detrimental, they are more likely to avoid violating the behavior.

Thus, recent literature consistently shows that perceived severity remains a key factor in the deterrence framework, particularly in digital context, where individual decisions are heavily influenced by evaluations of the potential consequences of their actions.

Pressure on Customer-initiated Fraud Intention

Within the Fraud Diamond Theory framework, pressure is understood as the drive or pressure experienced by individuals that can trigger fraudulent acts. This pressure tis generally related to financial conditions, lifestyle demands, and social pressure that encourage individuals to seek instant solutions, including through deviant means. In the context of digital banking, pressure becomes even more relevant because easy access to the financial system can accelerate the decision-making process, including opportunistic

decisions.

Several empirical studies show that pressure has a positive influence on the tendency to commit fraud. A study conducted by Abidin et al. (2017) found that financial pressure is a significant factor which driving individuals to engage in fraudulent behavior, particularly when individuals face limited economic resources. Furthermore, research by Said et al. (2018) showed that personal and economic pressure contribute significantly to fraudulent intention, as individuals tend to seek quick solutions to problems they face. Similar findings are also presented by Nawawi and Salin (2018) who stated that external pressure can increase an individual's tendency to commit the fraud, especially when combined with the opportunities within the system.

However, the relationship is not always consistent. Several studies have shown that pressure is not always lead to deviant behavior, depending on the individual's internal control. A study settled by Aghghaleh et al. (2016) found that even when individuals experience pressure, they do not necessarily commit fraud if they possess high level of ethic and integrity. Furthermore, research by Dorminey et al. (2018), emphasized that factors such as organizational culture and control system can weaken the effect of pressure on fraudulent behavior. This suggest that pressure is not the sole determinant, but rather operates in interaction with other factors.

These contradictory findings indicate that the influence of pressure is contextual, especially in digital environment. in the digital banking ecosystem, customer pressure can more easily translate into fraudulent intention due to ease of access, speed of transactions, and minimal direct supervision. Logically, individuals under high stress especially financial stress will tend to seek quick solution to meet their needs. When digital system provides easily accessible, and relatively anonymous opportunities, the psychological

barriers to committing fraud become lower. Thus, this research proposes the following hypothesis to be empirically tested.

H1. Pressure provides significant impact on customer-initiated fraud intention.

Opportunity on Customer-initiated Fraud Intention

In the Fraud Diamond Theory, opportunity refers to the existence of gaps in a system that allow individuals to commit fraud without being easily detected. In the context of digital banking, these opportunities can arise from security system weaknesses, lack of oversight and technological complexity that is not fully understood by users.

Several empirical studies have shown that opportunity has a positive influence on fraudulent behavior. Research by Albrecht et al. (2017) showed that weakness in the internal control systems significantly increase the likelihood of fraud. Furthermore, a study by Suryandari and Yuesti (2017) found that the greater the opportunity individual perceive, the higher their tendency to commit fraud. In the digital context, research by Bhasin (2017) also confirms that the lack of control and oversight in technology-based systems increases the opportunity for individuals to commit fraud.

However, some studies have shown conflicting results. A study by Ngo and Nguyen (2020) found that even when opportunities are available, individuals do not always commit fraud if they have high ethical awareness. In addition, research by Alzoubi (2018) shows that the effectiveness of governance and control mechanism can reduce the impact of opportunity on fraud, so that opportunities are not always translated into action.

Logically, in the digital banking ecosystem, opportunities play a crucial role because minimal interaction and complex systems can create gaps that are difficult to detect. When individuals are aware of system weaknesses and perceive that their actions

will remain undetected, the barriers to committing fraud are lower. Therefore, the greater the perceived opportunity, the higher the individual's tendency to have the intention to commit fraud. Thus, this research proposes the following hypothesis to be empirically tested.

H2. Opportunity provides significant impact on customer-initiated fraud intention

Rationalization on Customer-initiated Fraud Intention

Rationalization is a cognitive process in which individuals justify fraudulent acts to maintain their moral values. Research by Murphy and Dacin (2016) shows that rationalization plays a crucial role in enabling individuals to commit unethical acts without feeling guilty. Furthermore, a study by Barbaranelli et al. (2018) found that individuals who are able to justify deviant behavior tend to have higher intention to do so. In the technological context, research by Moore and Gino (2017) also confirms that self-justification mechanism is a significant factor in unethical behavior.

However, some findings are note entirely consistent. A study by Kaptein (2017) showed that in environment with a strong ethical culture, rationalization is not always lead to the fraud action. Furthermore, Hsieh et al. (2018) suggest that moral awareness can weaken the influence of rationalization on fraudulent intentions.

Logically, in digital banking, rationalization becomes increasingly important because the psychological distance between the actor and the system tend to be greater. Individuals can easily justify their actions because they do not see the direct impact on the victim. Thus, the higher level of rationalization, the greater individual's tendency to have the intention to commit fraud. Thus, this research proposes the following hypothesis to be empirically tested.

H3. Rationalization provides significant impact on customer-initiated fraud intention.

Capability on Customer-initiated Fraud Intention

Capability refers to an individual's ability to commit fraud, including knowledge, skills, and confidence in utilizing systems. In the digital banking context, capability is often related to technological literacy and understanding of digital banking systems. Research by Seetharaman et al. (2017) shows that an individual's technical ability plays a significant role in enabling technology-based fraud. A study by Bada and Nurse (2019) also found that individuals with high levels of digital literacy have a greater ability to exploit systems. Furthermore, research by Leukfeldt and Holt (2020) in the context of cybercrime shows that perpetrators with higher technical skills tend to be more active in committing digital crimes.

However, some studies suggest that capability does not always lead to fraud. A study by Crossler et al. (2017) found that even individuals with technical capabilities do not always misuse them if they possess a strong ethical conscience. In addition, research by Hadlington (2017) shows that psychological factors such as self-control can inhibit the use of abilities for deviant purposes. Logically in the digital banking ecosystem, capability is a crucial factor because technology-based system requires a certain level of understanding to be utilized. Individuals with high capability are more likely to identify loopholes and exploit them for personal gain. Therefore, the higher an individual's capability, the greater the likelihood of fraudulent intent. Thus, we propose following hypothesis to be empirical tested

H4. Capability provides significant impact on customer-initiated fraud intention

Perceived severity on Customer-initiated Fraud Intention

Perceived severity is an individual's perception of the severity of the consequences they will face if they commit fraud. Within the framework of deterrence theory, severity function as an external control mechanism. Research by Dodel and Mesch (2018) shows that the perception of serious consequences can reduce an individual tendency to engage in cybercrime. A study by Yu et al. (2020) also found that the perception of severe penalties significantly reduced fraudulent intentions in digital environments. Furthermore, research by Hu et al. (2019) showed that the threat of strong sanctions increases user compliance with system rules.

However, there are conflicting result. Pahnia et al. (2017) showed that perceived severity is not always significant when individuals are familiar with digital systems. Furthermore, research by Workman (2016) before suggest that individuals may ignore the threat of punishment if they perceive a low likelihood of being caught. When individuals perceive the consequences of fraud to be severe, whether legal, financial or reputational, they are more likely to avoid such acts. Conversely if the consequences are perceived as light or insignificant, the barrier to committing fraud is lower, thus this research propose following hypothesis to be tested

H5. Perceived severity provides significant impact on customer-initiated fraud intention.

METHODS

In-depth Interview Stage

This research combines in-depth interview and quantitative testing based on PLS-SEM which is known as sequential exploratory mixed-methods design. The literature shows that this approach is highly relevant for a research aimed at developing new constructs or

contextualizing classic theories in underexplored domains, such as customer fraud in digital ecosystems (Creswell & Creswell, 2018; Venkatesh et al., 2013).

In the first stage, in-depth interviews serve as conceptual exploration to capture empirical realities that cannot be fully explained by existing theories. In the context of digital banking fraud, a qualitative approach allows researchers to identify the dynamics of customer behavior, including how they interpret the opportunities, construct the justification, and respond to the pressure in digital environment. Previous studies have shown that qualitative methods are highly effective in uncovering hidden dimensions of fraudulent behavior, such as moral disengagement mechanism, perceived anonymity and user's subjective experiences with digital systems (Free 2015; Vousinas, 2019). Thus interview results serve not only as a basis for constructing or reconstructing research variables.

Data collection is conducted through semi-structured interviews with 12 informants, selected using a purposive sampling technique. This number is deemed adequate because it reached data saturation, the point at which new insight no longer emerge significantly from additional interviews (Guest et al., 2017). Informant selection is based on specific criteria to ensure the information obtained accurately reflects the phenomenon under study.

The informant qualifications are who active customers of digital banking services (mobile banking, internet banking and digital wallets), possess experiences conducting regular digital transaction, within the productive age including Generation Z and early millennials who are known to be dominant users of digital services, and have a basic understanding of digital security risk, both through personal experience and exposure to information. Furthermore, to broaden perspectives, several informants are selected from

diverse backgrounds, such as banking practitioners, active fintech users, and individuals with high digital literacy, allowing for a more comprehensive view of the consequences of fraud.

Interviews focused on exploring informant's perception regarding the various possible consequences of fraud such as legal sanctions, financial loss, account suspension and reputational impacts. The result of this process indicate that perception of the severity of consequences extend beyond legal aspects and encompass other dimensions such as loss of access to service, direct financial losses, and long-term impacts on personal reputation. These findings are then used as the basis for developing indicators to measure perceived severity in the quantitative stage.

Validity and Reliability

Next, the findings from the qualitative phase are translated into measurable and empirically testable construct using Partial Least Square-SEM. The use of PLS-SEM in this study is strongly justified, primarily because the model developed is predictive and exploratory, and involves the possibility of new constructs or adaptation of existing theories. The literature indicates that PLS-SEM is highly suitable for research focused on theory development, with high model complexity, and not always meeting the assumption of normal distribution (Hair et al., 2022; Sarstedt et al., 2021).

Measurement model evaluation is conducted to ensure that each construct has adequate validity and reliability. Convergent validity is tested through outer loading and Average Variance Extracted values. An indicator is considered valid if its outer loading value is above 0.70, although values between 0.60 and 0.70 are acceptable in exploratory research. Furthermore, the AVE value must exceed 0.50, indicating that the construct is able to explain more than 50% of the indicator's variance (Hair et al., 2022).

Construct reliability is measured using Composite Reliability and Cronbach's Alpha. A CR value greater than 0.70 indicates good internal consistency, while a Cronbach's Alpha above 0.70 indicates that the indicators within the construct have adequate reliability. In the context of developing new construct such as perceived severity, greater emphasis is placed on composite reliability values because they are considered more accurate in the PLS-SEM approach.

Structural Model Testing

After the measurement model meets the validity and reliability criteria, the next step is to evaluate the structural model through path analysis. This test aims to examine the causal relationship between constructs in the research model. The evaluation is conducted by examining the path coefficient, t-statistic and p-values obtained through the bootstrapping procedure. The relationship between variables is declared significant if the t-statistic is greater than 1.96 at the 5% significant level or the p-value less than 0.05. Furthermore, model strength is also evaluated through the R2 value, which indicates the ability of the independent variables to explain the dependent variable. R2 value of 0.25, 0.50, and 0.75 are interpreted as weak, moderate, and strong respectively.

RESULTS

The Respondents' Demographic

This study involved 111 respondents who are active users of digital banking services. The demographics profiles of the respondents are presented to provide an overview of the sample's characteristics and to ensure their suitability for the research context regarding customer behavior in the digital banking ecosystem. Based on age group, the majority of respondents are between 17 and 26 years old for 65 respondents, followed by the aged 27 and 35 for 34 respondents, and 12 respondents are over than 35 years old.

The dominance of Generation Z, indicated that the study samples represent a user group with high level of interaction with digital technology and app-based banking services.

In term of gender, respondents consisted of 63 women and 48 men. This composition shows a relatively balanced distribution and indicates that the use of digital banking services has been evenly distributed across various user groups. Based on their most recent educational level, the majority of respondents had a bachelor degree for 59 respondents, followed by a high school or equivalent for 31 respondents and a diploma or postgraduate degree for 21 respondents. This educational profile indicates that most respondents have a sufficient level of literacy to understand the use of digital services and the risk inherent in digital financial activities.

In terms of occupation, the respondents are predominantly students for 47 respondents, followed by private sector employee for 38 respondents, entrepreneur for 14 respondents, and other occupations for 12 respondents. This variety of occupational background provide a diverse range of perspectives regarding digital service usage behavior, economic conditions, and responses to fraud-related situation. Furthermore, based on experience using digital banking services, majority of respondents for 74 respondents had used this service for more than a year, while 37 respondents have less than a year of experience. In terms of usage intensity, 79 respondents used digital banking service more than three times a week, indicating a high level of engagement in digital activities.

Validity and Reliability Result

Based on the test results, all indicators in the Opportunity construct demonstrated outer loading values above the recommended threshold of 0.70 (Hair et al., 2022). These results indicate that all indicators have a good ability to represent the Opportunity construct as shown on Table 1.

Table 1. Validity and Reliability of Opportunity Construct

No	Item	Indicator	Outer Loading	AVE
1	The transaction system is not closely monitored	Opp1	0.771	0.61
	The system does not verify all documents directly	Opp2	0.782	
	The system can be bypassed easily	Opp3	0.741	
	I know about the delay between transaction confirmation and the actual debit in the system	Opp4	0.823	
	I believe that the system itself made it easy to be exploited	Opp5	0.840	

Source: Data Processed (2026)

Among all indicators, item Opp5 has the higher outer loading value of 0.840, indicating that respondents' perception of the systems' ease of exploitation are the strongest representation of the Opportunity construct. In contrast, the Opp3 has the lowest loading value of 0.741, but is still above the minimum acceptable limit so it is retained in the model. Furthermore, the Opportunity construct achieved an AVE value of 0.61, exceeding the minimum threshold of 0.50. This value indicates that the Opportunity construct is able to explain approximately 61 % of the variance in its indicators, with the remainder influenced by factors outside the research model. Thus, these results indicate that the Opportunity construct has met convergent validity.

Based on the analysis shown on Table 2 below, all indicator in the Financial Pressure construct showed outer loading values above the minimum threshold of 0.70 as recommended in the PLS-SEM approach. The outer loading value for each indicator ranged from 0.761 to 0.869. This finding indicate that all items contribute significantly to explaining the Financial Pressure construct and do not require indicator elimination. Indicator Fin1 has the higher outer loading value of 0.869. This result indicates that financial pressure, which drives individuals to consider deviant actions, is the most dominant representation of the Financial Pressure construct. This finding indicate that condition of economic stress can influence individual decision-making process, including the tendency to consider deviant behavior.

Table 2. Validity and Reliability of Financial Pressure Construct

No	Item	Indicator	Outer Loading	AVE
2	When I am under financial stress, I am more likely to consider actions I would normally reject	Fin1	0.869	0.683
	I have experienced situations where urgent financial needs made me consider unethical financial actions	Fin2	0.828	
	I sometimes feel forced to take risky or dishonest financial steps due to lack of income or resources	Fin3	0.809	
	Breaking the regulations when interacting with financial service providers can be justified by dire financial circumstances.	Fin4	0.761	
	Taking advantage of system vulnerabilities appears to be a vital alternative during financial crises.	Fin5	0.860	

Source: Data Processed (2026)

Meanwhile, indicator Fin4 achieved the lowest loading value of 0.761. However, this value is still above the recommended minimum threshold, indicating that the indicator still contributes adequately to the Financial Pressure construct. Furthermore, the AVE value fo 0.683 indicates that the Financial Pressure construct explains 68,3% of the variance in its constituent indicators, with the remainder influenced by factors outside the research model. An AVE value exceeding the minimum threshold of 0.50 indicates that the construct meets the convergent validity requirements. Overall, the test result indicate that the Financial Pressure construct adequately represent the financial pressure felt by individuals, particularly in the context of fraudulent behavior tendencies in the digital financial services ecosystem. All indicators meet the recommended validity criterial and are suitable for use in the next stage of the structural model analysis.

Based on the Table 3 below, all indicators in the Rationalization construct demonstrated outer loading value above the minimum threshold of 0.70, as recommended in the PLS SEM approach. The loading values for each indicator are ranged from 0.779 and 0.893, thus these results indicate that all items have a good ability to represent the Rationalization construct. Indicator Rat1 achieved the highest outer loading value of 0.893. This value indicates that the beliefs that fraudulent acts do not have a significant impact on

banking institutions is the most dominant form of justification used by respondents. This findings indicates an individual tendency to reduce perception of guilt by justifying that the injured party has substantial financial capacity, thus deeming the impact minor.

Table 3. Validity and Reliability of Rationalization Construct

No	Item	Indicator	Outer Loading	AVE
3	A minor act of fraud doesn't truly harm anyone because banks are insured and generate enormous profits	Rat1	0.893	0.694
	If the bank makes frequent mistakes or charges hidden fees, I feel less guilty about taking advantage of them.	Rat2	0.802	
	If I discover a system flaw and take advantage of it, the bank is at responsibility for not protecting it, not me.	Rat3	0.863	
	Breaking the regulations when interacting with financial service providers can be justified by dire financial circumstances.	Rat4	0.823	
	In challenging circumstances, breaking the rules is permissible as long as no one is harmed directly.	Rat5	0.779	

Source: Data Processed (2026)

Furthermore, indicator Rat3 scored 0.863, indicating that shifting responsibility to system weaknesses is also a fairly strong form of rationalization. This align with the concept of neutralization in fraudulent behavior, where individuals shift moral responsibility from themselves to external parties. Meanwhile, indicator Rat5 has the lowest loading value compared to other indicators, but still considered valid in forming the Rationalization construct.

Furthermore, the Rationalization construct achieved and Average Variance Extracted value of 0.694, indicating that the construct explained approximately 69.4% of the variance in its constituent indicators. This value exceeded the minimum threshold of 0.50, thus concluding that the construct met the convergent validity criteria. Overall, the test result indicate that the Rationalization construct has excellent measurement quality. The high outer loading and AVE value indicate that the indicators used are able to robustly describe the

process of justifying fraudulent behavior in the context of customer in the digital banking ecosystem. Therefore, all indicators are deemed suitable for retention and use in the next stage of the structural model analysis.

The outer loading value of each Capability's construct are ranged from 0.694 until 0.853 which indicate that each indicators have a strong contribution to explaining the Capability construct. Indicator Cap2 such as I am capable of identifying potential vulnerabilities in digital financial service system, obtained and outer loading value of 0.853, while Cap5 such as I have sufficient experience using various digital banking or financial services has a value of 0.845. Both indicators demonstrated a very strong contribution to formation of the Capability construct. These findings indicate that the ability to recognize system weakness and experience using digital banking service is a key indicator of capability in the context of fraudulent behavior in the digital banking industry.

Table 4. Validity and Reliability of Capability Construct

No	Item	Indicator	Outer Loading	AVE
4	I have a good understanding of how digital banking service systems work	Cap1	0.694	0.620
	I am capable to identify potential vulnerabilities in digital financial service system	Cap2	0.853	
	I feel have sufficient technical skills to utilize digital system according to my needs	Cap3	0.727	
	I believe that individual with technical skills can perform certain activities in digital systems without being easily detected	Cap4	0.803	
	I have sufficient experience using various digital banking or financial services.	Cap5	0.845	

Source: Data Processed (2026)

Meanwhile, indicator Cap4 such as I believe that individuals with technical skills can perform certain activities in digital system without being easily detected also showed a high loading value of 0.803, indicating that perception of technical ability to avoid detection are also important in explaining capability. Conversely, indicator Cap1 such as I have a good understanding of how digital banking service system work has the lowest outer loading value

at 0.694. Although slightly below the ideal value of 0.70, this indicator is retained because it close to the recommended limit and theoretically has strong relevance to the capability construct. Furthermore, removing this indicator has the potential to reduce the conceptual scope of the construct, particularly in the technical knowledge dimension.

Furthermore, the Capability construct obtained and Average Variance Extracted value of 0.620, which has exceeded the minimum value of 0.50. This result indicate that the Capability construct is able to explain approximately 62% of the variance of its constituent indicators, while the remainder is influenced by other factors outside the research model. Thus the Capability construct has met the requirement for convergent validity. The Perceived Severity construct in this study is an adaptive construct developed through in-depth interview during the qualitative exploration phase. This construct is developed because research on customer-initiated fraud in digital banking ecosystem has yet to integrate perspective on individual perception of the severity of fraud consequences. Unlike the main elements of the Fraud Diamond Theory, which focus on factors driving fraudulent behavior, the Perceived Severity construct is develop to represent deterrent mechanism, specifically related to customer perception of the severity of consequences if fraudulent acts are committed.

During the qualitative exploration phase, the in-depth interview revealed several dominant themes that emerged consistently which is legal consequences, formal sanctions, blocking of service access, reputational impact, and long-term consequences. These themes are then converted into measurement indicators that are further tested in quantitative phase. Based on the result of the measurement model test, all indicators in the Perceived Severity construct demonstrated outer loading value at acceptable levels. Indicator Sev1 such as If I committed fraud in digital banking, the legal consequences I would face would be very severe, achieved the highest outer loading value of 0.821, indicating that the perception of

the severity of legal consequences is the most dominant dimension in shaping the Perceived Severity construct. This finding indicate that the threat of legal consequences remains a primary factor individuals will consider when evaluating the impact of fraud in the digital banking system.

Table 5. Validity and Reliability of Severity Construct

No	Item	Indicator	Outer Loading	AVE
5	If I committed fraud in digital banking, the legal consequences I would face would be very severe	Sev1	0.821	0.586
	The sanctions imposed on perpetrators of fraud in digital financial services are very serious.	Sev2	0.802	
	Account blocking due to fraud is a very detrimental consequence	Sev3	0.751	
	The reputational impact of fraudulent acts can be very damaging	Sev4	0.782	
	Overall, the consequences of fraud in digital financial services are very severe	Sev5	0.663	

Source: Data Processed (2026)

Furthermore, indicator Sev2 such as the sanctions imposed on perpetrators of fraud in digital financial services are very serious, also displayed a high loading value of 0.802, indicating that perception regarding the seriousness of formal sanction are an important aspect of this construct. This finding suggest that individuals consider not only the likelihood pf punishment but also the severity of the punishment the perpetrator could receive.

Meanwhile, indicator Sev3 and Sev4, representing the dimension of loss of system access and reputational impact, obtained values of 0.751 and 0.782, respectively, indicating a strong contribution to the construct. This demonstrates that respondents view fraud not only from the legal consequences perspective but also consider the social operational impacts that arise after the act is committed.

On the other hand, indicator Sev5 such as Overall, the consequences of fraud in

digital financial service are very severe, achieved an outer loading of 0.663, the lowest value compared to other indicators. Although slightly below the ideal value of 0.70, this indicator is still considered acceptable because it meets the minimum acceptable threshold for new construct development (Hair et al., 2022),. Furthermore, this indicator plays an important theoretical role as a representation of a global assessment of the Perceived Severity of fraud consequences. This construct also achieved an AVE value of 0.586, exceeding the minimum threshold of 0.50. This value indicate that the construct explains 56.6% of the variance in tis constituent indicators, thus meeting the requirement of convergent validity.

Overall, the test result indicate that the Perceived Severity construct has adequate measurement quality despite being a new construct developed contextually. these result indicate that the indicators developed from in-depth interview are capable of capturing respondents' perception regarding the severity of fraud consequences in digital banking services. Therefore, the Perceived Severity construct can be retained and used in subsequent structural model testing.

The test result on Table 6 showed that all indicators in the Customer-initiated Fraud Intention construct have outer loading values above the recommended minimum limit. The loading values of all indicators are ranged from 0.779 to 0.879. These results indicate that all items have a good ability to represent the construct of customer fraud intention. Indicator Int1 such as If there is an opportunity in the digital banking system that benefits me without being easily detected, I might consider it, achieved the highest outer loading value of 0.879. These results indicate that the existence of opportunity in the system that provide benefits with a low risk of detection is the strongest proxy for customer fraud intention. These findings indicate that the perception of opportunity and the low likelihood of detection are key considerations in shaping fraudulent behavior tendencies.

The Int3 indicator obtained a high loading value of 0.872, thus indicate that the acceptance of deviant behavior under certain conditions also contributes significantly to the formation of fraudulent intentions. This finding indicates that situational factors can influence individuals' assessment of whether a behavior is acceptable. Furthermore, the Int2 indicator related to perceived benefits, obtained a value of 0.829, while the Int4 indicator, concerning willingness to take risk, obtained value of 0.796. Both indicators demonstrate a strong contribution in explaining the tendency for fraudulent behavior in the context of digital banking services.

Meanwhile, indicator Int5 achieved the lowest outer loading value of 0.779. Although this is the lowest value compared to the other indicators, it remains above the recommended threshold and indicates an adequate contribution to the formation of the Customer-initiated Fraud Intention construct. In addition to the outer loading value, this construct achieved and Average Variance Extracted value of 0.692, and meets the criteria of convergent validity.

Table 6. Validity and Reliability of Customer-initiated Fraud Intention Construct

No	Item	Indicator	Outer Loading	AVE
6	If there is an opportunity in the digital banking system that benefits me without being easily detected, I might consider it	Int1	0.879	0.692
	I might consider taking certain actions in digital banking services if the benefits are significant enough	Int2	0.829	
	Under certain circumstances, deviant behavior in digital financial services is acceptable	Int3	0.872	
	I am willing to take certain risk in using digital banking service to gain additional benefits	Int4	0.796	
	If the situation allows, I am likely to engage in illegal behavior in digital banking service	Int5	0.779	

Sources: Data Processed (2026)

After convergent validity testing is conducted using outer loading and AVE values, the next step is to evaluate construct reliability. Based on Table 7 below, all construct in this

study demonstrated Composite Reliability and Cronbach's Alpha values that exceeded the recommended minimum limits. These results indicate that all construct have a good level of internal consistency and are suitable for use in structural model analysis.

The Rationalization construct achieved the highest Composite Reliability value of 0.919, with a Cronbach's Alpha value of 0.889. These result indicate that the indicators in the Rationalization construct have very high consistency in measuring an individual's internal justification process for fraudulent acts. This high reliability indicates that each indicator within the construct is strongly interrelated.

Table 7. Reliability Check Result for All Construct

No	Item	Composite Reliability	Cronbach's Alpha
1	Perceived Opportunity	0.886	0.840
2	Financial Pressure	0.915	0.883
3	Rationalization	0.919	0.889
4	Customer-initiated Fraud Intention	0.918	0.888
5	Capability	0.890	0.884
6	Severity	0.876	0.823

Source: Data Processed (2026)

The Customer-initiated Fraud Intention construct also demonstrated excellent reliability, with a Composite Reliability value of 0.918 and a Cronbach's Alpha of 0.888. These findings indicate that the items used to measure customer fraud intention in the digital banking context have high measurement stability and consistency. Furthermore, the Financial Pressure construct demonstrated a Composite Reliability value of 0.915 and a Cronbach's Alpha of 0.883, while the Capability construct obtained values of 0.890 and 0.884. These values indicate that both constructs have strong reliability in representing financial pressure and individual capabilities in the context of digital banking fraud.

The Perceived Opportunity construct also demonstrated good reliability, with a Composite Reliability value of 0.886 and a Cronbach's Alpha of 0.840. These results indicate that the indicators measuring perceived opportunity in digital system have adequate

consistency. Meanwhile, the Perceived Severity construct, a new construct developed through in=depth interviews, achieved a Composite reliability value of 0.876, and a Cronbach's Alpha of 0.823. Although it has the lowest value compared to the other constructs, all values are still well above the recommended minimum threshold. These findings are an important indication that this new construct has a good level of reliability and demonstrates adequate internal consistency, despite being developed through a qualitative exploration process.

Path Analysis Result

Based on the test result, the Financial Construct demonstrated a significant influence on Customer-initiated Fraud Intention with p-value of 0.000 and t-statistic value of 4.999. Among all variables, Rationalization demonstrated the highest t-statistic value, indicating that internal justification process are the strongest factor in shaping fraudulent intentions. These results demonstrate that individuals are more likely to consider deviant behavior when they are able to construct personal justifications for their actions.

The Severity construct, a new construct developed in this research, also demonstrated a significant effect toward Customer-initiated Fraud Intention with p-value of 0.015, and t-statistic value of 2.465. This finding suggests that perception of the severity of fraud consequences plays a role in shaping customer behavioral tendencies. These result indicate that inhibiting factor based on perception of punishment and consequences play a role in fraud models in the digital ecosystem.

Table 8. Path Analysis

No	Independent Construct	Dependent Construct	P-values	T-Statistic
1	Perceived Opportunity	Customer-initiated Fraud Intention	0.191	1.316
2	Financial Pressure		0.001	3.382
3	Rationalization		0.000	4.999
4	Capability		0.058	1.916
5	Severity		0.015	2.465

Source: Data Processed (2026)

On the other hand, the Perceived Opportunity construct did not demonstrate a significant effect on Customer-initiated Fraud Intention (p-value 0.191, t-statistic value is 1.316). These result suggest that the perception of opportunities within the system does not necessarily directly drive fraud intentions.

Furthermore, the Capability construct also did not show a significant effect at the 5% significance level with p-value of 0.058 and t-statistic value of 1.916. This value is very close to the significance limit and can therefore be categorized as a marginal or near-significant relationship. This indicates that an individual's technical ability does not necessarily directly increase fraud intentions without the influence of other factors. Overall, the test result indicate that of the five construct tested. Financial Pressure, Rationalization, and Severity significantly influence Customer-initiated Fraud Intention, while Perceived Opportunity and Capability do not show a significant effect in this research model.

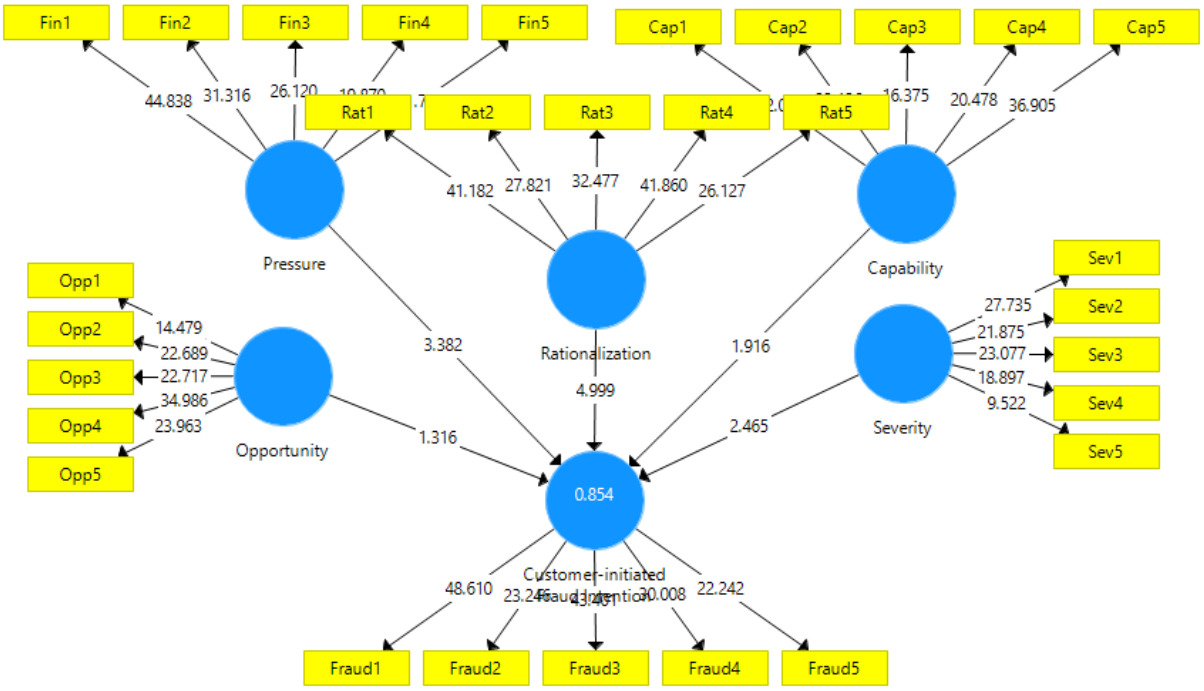

Figure 1. Research Model

The Effect of Perceived Opportunity on Customer-initiated Fraud Intention

In the Fraud Diamond Theory, opportunity is viewed as a condition that allows fraud to occur due to system weakness, poor supervision, or control gaps (Wolfe & Hermanson, 2004). however, in the context of modern digital banking, the mere existence of opportunity appears insufficient to generate fraudulent intentions. Current digital system has integrated various layers of security such as multi-factor authentication, real-time monitoring, and fraud detection systems, so the perception of opportunity may not necessarily translate into a realistic opportunity to be exploited.

These findings align with research by Nurunnabi & Nurunnabi (2020), which showed that opportunity does not always have a direct relationship with fraudulent behavior because psychological factors and individual perception often predominate. These results are also consistent with research by Zakaria et al. (2021), which found that opportunity can lose its

direct influence when the environment has a robust digital control system.

However, these findings contradict research by Abdullahi & Mansor (2018), which showed that opportunity is a primary factor driving fraudulent tendencies, especially when individuals are aware of system weakness and a low probability of detection. These findings indicate that in the context of customer-initiated fraud, the perception of opportunity appears to require a combination of other factors, such as financial pressure or rationalization process, before developing into fraudulent intent.

The Effect of Financial Pressure on Customer-initiated Fraud Intention

The finding is consistent with the pressure element in the Fraud Diamond Theory, which explains that economic pressure is the primary trigger for individuals to cnsider deviant behavior. In the context of digital banking, financial pressure can arise in the form of economic need, debt, decreased income, or economic instability. These result are supported by research by Islam et al. (2021), which shows that economic pressure has a significant influence on the intention to commit deviant acts in digital environment. Research by Merima & Rafique (2022) also found that financial pressure can increase an individuals' tendency to seek alternative means of profit through illegal means.

However, Shuhidan et al. (2017) found different result, finding that financial pressure is not always a strong predictor of fraudulent behavior because some individuals maintain moral standards despite economic hardship. Thus, financial pressure is an important factor, but its impact is likely influenced by other psychological mechanism such as rationalization or perceived consequences.

The Effect of Rationalization on Customer-initiated Fraud Intention

The result of this study inform that the internal justification process is the most dominant

factor in the research model. This finding suggest that individuals are more likely to consider fraud when they can construct certain moral justification, such as believing the institution will not suffer significant harm or believing that the system has weakness that are the responsibility of the service provider.

This result is supported by research which conducted by Free (2015) which show that rationalization is a crucial component bridging the gap between fraudulent intention and action. Albrecht et al. (2018) also shows that an individual's ability to construct internal justification can reduce moral barriers to fraudulent behavior. Conversely, Jaffar et al. (2019) proposed that rationalization is not always the dominant predictor, as in some cases situational pressure is more influential. Thus, even when opportunities or pressure exist, individuals tend to require psychological justification mechanism before fraudulent intention are formed.

The Effect of Capability on Customer-initiated Fraud Intention

The test result show that Capability does not significantly impact the Customer-initiated Fraud Intention. Although approaching the significance level, these results indicate that an individual's technical capability is not sufficient to directly drive fraudulent intentions. In the Fraud Diamond Theory, capability explains an individuals' ability to commit fraud, including skills, experience and knowledge. However, in teh context of digital banking customer, technical capability may be used more to improve service efficiency than for exploitation purposes.

These results are supported by bolivar-Ramos & Garcia-Morales (2020), which showed that technological capability is not always associated with deviant behavior. Individuals with high capability do not necessarily have the intention to commit fraud. However, Vousinas (2019) found that capability plays a significant role in explaining fraud when the individuals also have high opportunities and motivation. These findings, indicate that technical skills may

play more a supporting role than a primary driver of fraudulent intention.

The Effect of Severity on Customer-initiated Fraud Intention

The result of this study indicate that Severity construct has a significant effect on Customer-initiated Fraud Intention. This finding is important because Severity is a new construct developed through in-depth interviews. These results indicate that perceptions of the severity of fraud consequences, such as legal penalties, account suspension and reputational damage, play a role in shaping behavioral intentions.

This finding is consistent with Deterrence Theory, which explains that individuals tend to avoid deviant behavior when the consequences are perceived as severe. Research by Ifinedo (2018) found that perception of severe penalties can reduce intentions to commit digital fraud. Similar result is also found by Herath and D'Acrcy (2017) who showed that perception of sanction severity can suppress deviant behavior intention in digital environment.

However, the research by Marett et al. (2019) found that perception of punishment are not always effective because some individuals are more influenced by the probability of being caught than the severity of the punishment. The findings of this study, demonstrate that the development of the Severity construct provides additional theoretical contributions in expanding th Fraud Diamond Theory, particularly in the context of customer-initiated fraud in the digital banking ecosystem.

CONCLUSION AND IMPLICATIONS

This research aims to develop the Fraud Diamond Theory in the context of customer-initiated fraud in the digital banking ecosystem by adding a new construct. Perceived Severity, obtain through in-depth interview and empirically tested using PLS-SEM. The research involved 111 digital banking service users to understand the factors influencing customer fraud

intentions. The test result indicate that Financial Pressure, Rationalization, and Perceived Severity have a significant influence on Customer-initiated Fraud Intention, while Perceived Opportunity and Capability do not show a significant influence.

Specifically, Rationalization is the factor with the strongest influence in the research model. These result indicate that individuals are more likely to consider fraudulent behavior when they can construct an internal justification for the action. Furthermore, Financial Pressure has also been shown to increase the likelihood of fraudulent intention, indicating that economic pressure remains a significant factor in deviant behavior in the digital environment. Another interesting finding is the significance of Perceived Severity as a new construct in this research. These results indicate that an individual's perception of the severity of consequences , such as legal sanction, account suspension, and reputational impact, contribute to the formation of fraudulent intentions.

These findings demonstrate that consequences-based inhibitory mechanism play a significant role in the context of digital fraud. Conversely, Perceived Opportunity and Capability do not show a significant influence. This finding indicate that the presence of system opportunities and an individual's technical capabilities are not necessarily sufficient to directly trigger fraudulent intentions without the involvement of other psychological and situational process. Overall, this study demonstrates that fraudulent behavior among digital customers is influenced not only by structural factors as explained in the Fraud Diamond Theory, but also by cognitive factors, and the individuals' perception of behavioral consequences.

Practical Implication

This research provides several practical implications for the digital banking industry. First, because rationalization is the most dominant factor, banking institution need to develop prevention strategies that focus not only on technological security but also on user psychology

and behavior. Educational programs should emphasize that system exploitation remains fraud, even if it occurs due to system weakness or is not considered to directly harm the institution.

Second, the significance of financial pressure demonstrates the importance of early detection mechanism for customer risk. Financial institution can develop data-driven approach to identify transaction behavior patterns that indicate high financial stress.

Third, the research result on perceived severity indicates that communication regarding the consequences of fraud need to be strengthened. To date, banking security system have primarily emphasized technical aspects. This research demonstrates the need for more explicit information regarding legal implication, account blocking, violation history recording, and reputational impact on fraud perpetrators.

REFERENCES

Abdullahi, M., & Mansor, N. (2018). Fraud triangle theory and fraud diamond theory. *International Journal of Academic Research ini Accounting, Finance and Management Science*, 8(3), 106-112, https://doi.org/10.6007/IJARAFMS/v8-i3/4543

Aghghaleh, S.F., Mohamed, Z.M., & Rahmat, M.M. (2016). Detecting financial statement frauds in Malaysia: Comparing the abilities of Beneish and Dechow models. *Asian Journal of Accounting and Governance*, 7, 57-65, https://doi.org/10.17576/AJAG-2016-07-06

Alzoubi, E.S.S. (2018). Audit committee, internal audit function and earnings management. *Journal of Applied Accounting Research*, 19(3), 398-414, https://doi.org/10.1108/JAAR-06-2017-0062

Bada, M., & Nurse, J.R.C. (2019). Developing cybersecurity education and awareness programmes for small-medium-sized enterprises. *Information & Computer Security*, 27(3), 393-410, https://doi.org/10.1108/ICS-07-2018-0080

Bank Indonesia. (2023). *Laporan Sistem Pembayaran Indonesia 2023*. Bank Indonesia, https://www.bi.go.id/id/publikasi/laporan/Pages/Laporan-Sistem-Pembayaran-Indonesia-2023.aspx

Barbaranelli, C., Farnese, M.L., & Chirumbolo, A. (2018). Moral disengagement and unethical behavior. *Frontiers in Psychology*, 9, 1-12, https://doi.org/10.3389/fpsyg.2018.00001

Button, M., & Cross, C. (2017). Technology and fraud: The fraud justice network and the challenge of fraud investigation. *Journal of Financial Crime*, 24(4), 562-577, https://doi.org/10.1108/JFC-06-2016-0040

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2017). Understanding the violation of information security policy: an Integrated model based on social control and deterrence theory. *Computers & Security*, 68, 1-14, https://doi.org/10.1016/j.cose.2017.04.003

Crossler, R.E., Belanger, F., & Ormond, D. (2017). The quest for complete security: an Empirical analysis. *Computer & Security*, 73, 1-16, https://doi.org/10.1016/j.cose.2017.10.001

Dodel, M., & Mesch, G. (2018). Cyber-victimization preventive behavior. *Computers in Human behavior*, 83, 1-9, https://doi.org/10.1016/j.chb.2018.01.012

Dorminey, J.W., Fleming, A.S., Kranacher, M.J., & Riley, R.A. (2018). The evolution of fraud theory. *Issues in Accounting Education*, 33(1), 1-15, https://doi.org/10.2308/iace-52104

Free, C. (2015). Looking through the fraud triangle : a Review and call for new directions. *Meditari Accountancy Research*, 23(2), 175-196, https://doi.org/10.1108/MEDAR-02-2015-0009

Guest, G., Namey, E., & Mitchell, M. (2017). *Collecting qualitative data: a field manual for applied research.* SAGE Publications.

Hadlington, L. (2017). Human factors in cybersecurity. *Computers in Human Behavior*, 69, 1-6, https://doi.org/10.1016/j.chb.2016.11.027

Hair, J.F., Hult, G.T.M., Ringle, C.M., & Sarstedt, M. (2022). *A primer on partial least square structural equation modeling (PLS-SEM) 3rd edition*. SAGE Publication_

Hair, J.F. (2021). Partial least square structural equation modeling. *Handbook of Market Research*, Springer, https://doi.org/10.1007/978-3-319-05542-8_15-2

Henseler, J., Ringle, C.M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135, https://doi.org/10.1007/s11747-014-0403-8

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2019). Does deterrence work in reducing information security policy abuse? *Information & Management*, 56(70, 103-115, https://doi.org/10.1016/j.im.2019.02.005

Ifinedo, P. (2018). Determinants of employee's information system security policy compliance. *Information & Computer Security*, 26(3), 289-310, https://doi.org/10.1108/ICS-08-2017-0057

Ifinedo, P. (2019). The effect of deterrence factors on employees' information security policy compliance intentions. *Information System Frontiers*, 21(2), 413-432, https://doi.org/10.1007/s10796-017-9801-1

Kassem, R., & Higson, A.W. (2016). External auditors and corporate corruption: Implications for external audit regulators. *Current Issues in Auditing*, 10(1), 1-10, https://doi.org/10.2308/ciia-51391

Kou, Y., Shi, Y., Wang, Z. (2021). Machine learning methods for fraud detection: a review. *Decision Support Systems*, 50(3), 1-12, https://doi.org/10.1016/j.dss.2020.113513

Leukfeldt, E.R. (2017). Phising for suitable targets in the Netherlands: Routine activity theory and phisinig victimization. *Cyberpsychology Behavior and Social Networking*, 20(3),

183-188, https://doi.org/10.1089/cyber.2016.0556

Levi, M., & Smith, R.G. (2021). Fraud and its relationship to pandemics and economics crises. *Journal of Financial Crime,* 28(3), 801-815, https://doi.org/10.1108/JFC-09-2020-0185

Maskur, A., & Santoso, I.H. (2025). Intergenerational insight of fraud intention in digital banking: What makes customers go rogue? *Jurnal Manajemen*, 22(2), 107-133, https://doi.org/10.25170/jm.v22i2.6735

Moore, C., & Gino, F. (2017). Ethically adrift: How others pull our moral compass. *Harvard Business Review*, https://doi.org/10.2139/ssrn.2596303

Nawawi, A., & Salin, A.S.A.P. (2018). Internal control and employees occupational fraud on expenditure claims. *Journal of Financial Crime,* 25(3), 891-906, https://doi.org/10.1108/JFC-07-2017-0067

Nurunnabi, M., & Nurunnabi, M. (2020). Fraud and governance in digital environments. *journal of Financial Crima,* 27(4), 1021-1038, https://doi.org/10.1108/JFC-06-2019-0081

Omarini, A., (2018). Banks, and fintechs: How to develop a digital open banking approach for the bank's future. *International Business Research*, 11(9), 23-36, https://doi.org/10.5539/ibr.v11n9p23

Otoritas Jasa Keuangan. (2023). *Laporan perlindungankonsumen sektor jasa keuangan 2023*. Otoritas Jasa Keuangan, https://www.ojk.go.id/id/kanal/edukasi-dan-perlindungan-konsumen/Pages/Laporan-Perlindungan-Konsumen.aspx

Otoritas Jasa Keuangan. (2022). *Statistik pengaduan konsumen sektor jasa keuangan*. Otoritas Jasa Keuangan. https://www.ojk.go.id/id/kanal/edukasi-dan-perlindungan-konsumen/data-dan-statistik/Pages/Statistik-Pengaduan-Konsumen.aspx

Pahnila, S., Siponen, M., & Mahmood, A. (2017). Employee's behavior towards IS security policy compliance. *Information & Management*, 54(1), 1-13, https://doi.org/10.1016/j.im.2016.08.004

Posey, C., Bennett, R.J., Roberts, T.L., & Lowry, P.B. (2018). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Information System Research*, 29(2), 309-326, https://doi.org/10.1287/isre.2017.0739

Said, J., Alam, M.M., & Karim, Z.A. (2018). Integrating religiosity into fraud triangle theory: Empirical findings from Malaysia. *Journal of Financial Crime*, 25(2), 436-450, https://doi.org/10.1108/JFC-02-2017-0016

Seetharaman, A., Senthilvelmurugan, M., & Raj, J.R. (2017). Cybersecurity: Issues and challenges. *Journal of Cyber Security Technology*, 1(2), 1-10, https://doi.org/10.1080/23742917.2017.1288491

Venkatesh, V., Brown, S.A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quartertly*, 37(1), 21-54, https://doi.org/10.25300/MISQ/2013/37.1.02

Vousinas, G.L. (2019). Advancing theory of fraud: The SCORE model. *Journal of Financial Crime*, 26(1), 372-381, https://doi.org/10.1108/JFC-12-2017-0128

Yu, S., Niu, X., & Chen, Y. (2020). Understanding cybercrime prevention behavior. *Computers & Security*, 92, 101751, https://doi.org/10.1016/j.cose.2020.101751

Zainal Abidin, A., Hashim, H.A., & Ariff, A.M. (2017). Ethical commitments and financial performance: Evidence from Malaysian public listed companies. *Journal of Financial Crime*, 24(2), 206-219, https://doi.org/10.1108/JFC-06-2016-0036

Zakira, N.B., Haron, R., & Zainol, M.S. (2021). Fraud prevention and internal control in digital settings. *Journal of Financial Crime*, 28(2), 533-549, https://doi.org/10.1108/JFC-07-2020-0131