Jurnal Manajemen
Vol. 22 No. 2 November 2025 Page 107-133 doi: https://doi.org/10.25170/jm.v22i2.6735
P-ISSN: 1829-6211 E-ISSN: 2597-4106 http://ejournal.atmajaya.ac.id/index.php/JM

INTERGENERATIONAL INSIGHT OF FRAUD INTENTION IN DIGITAL BANKING: WHAT MAKES CUSTOMERS GO ROGUE?

Ali Maskur[1], Ignatius Hari Santoso[2]

[1,2] Faculty of Economic and Business, Universitas STIKUBANK, Indonesia
[1]*maskur@edu.unisbank.ac.id* [2]*ignatiusharisantoso@edu.unisbank.ac.id*

ABSTRACT

This study investigates the factors influencing customers' intention to commit fraud in the context of mandatory digital banking, with a focus on intergenerational differences between Generation Y and Millennials. Guided by the Fraud Triangle Theory, the research explores how perceived opportunity, financial pressure, and rationalization contribute to fraud intention. A mixed-method approach was employed, beginning with in-depth qualitative interviews followed by a quantitative survey of 100 digital banking users in Indonesia. The constructions were validated through factor analysis, and the model was tested using Partial Least Squares (PLS-SEM). The findings reveal that perceived opportunity and rationalization significantly influence fraud intention, while financial pressure does not. Furthermore, generational differences do not moderate the relationships between the predictors and fraud intention. These results highlight the importance of improving digital system integrity and addressing ethical rationalizations to prevent fraud. The study contributes to a deeper understanding of consumer-initiated financial fraud in the digital age and suggests avenues for more targeted fraud prevention strategies.

Keywords: *Digital Banking, Fraud Intention, Perceived Opportunity, Financial Pressure, Intergenerational*

Article history: Submission date 23 May, 2025 Accepted date 2 November, 2025
To cite: Maskur, A., Santoso, I. H. (2025). Intergenerational Insight Of Fraud Intention In Digital Banking: What Makes Customers Go Rogue?. Jurnal Manajemen, 107–133.

1. INTRODUCTION

The way that consumers engage with financial institutions has changed because of Indonesia's banking services' quick digitization. Digital banking is becoming more required, particularly for customer onboarding and transaction services, thanks to the government's encouragement of financial inclusion and the backing of regulatory organizations like Otoritas Jasa Keuangan (OJK). The rapid digital transformation of banking services has fundamentally changed the way consumers interact with financial institutions. In Indonesia, digital banking adoption has accelerated due to regulatory encouragement by OJK and Bank Indonesia, which promote the financial inclusion and digital financial literacy (Ahmed et al., 2024).

Globaly, digital banking has also grown into a core channel for customer engagement, providing convenience, efficiency and 24/7 access to financial services (Lai, 2021; Garg et al., 2022). The use of mobile banking, e-wallets, and application-based service, reflect a paradigm shift from branch centric to technology driven financial ecosystem (Alalwan et al., 2017). This transformation is widely considered as a cornerstone of financial modernization and consumer empowerment. However, alongside these benefits, digitalization also creates a new vulnerability that exposes both institutions and customers to fraud action. Unlike the traditional banking, where face-to-face verification and physical documentation act as natural safeguard, digital banking opens the door to the fraud such as phishing, synthetic identity fraud, SIM swap scam, and exploitation of promotional program (Hoffman & Birnbrich, 2022; Wang & Dincelli, 2021). This change has increased operational effectiveness and service accessibility, but it has also created new security flaws that have led to an increase in financial theft.

For digital banking platforms to be adopted and used consistently trust plays a central role. Numerous studies confirm that clients' trust in the digital interface and perceived security significantly affect their intention to use and maintain engagement with digital banking services (Handayani et al., 2020; Nugroho & Situmorang, 2023). When emotional assurance and perceived reliability are established, users are more likely to commit to long term usage (Dimitriadis & Kyrousi, 2023).

However, the absence of in-person touch and tangible assurance can make clients particularly older or less tech savvy feel less secure when the interaction with banks becomes more virtual (Naimi et al., 2022; Bueno et al., 2024). The transition from human assisted to digital only service environment may erode emotional connection and weaken the trust if banks fail to substitute physical reassurance with digital transparency and empathetic design (Mohammed et al., 2024)

At the same time, the rising plrevalence of digital fraud, including phising, identity theft, and social engineering, has created an environment, of uncertainty. This growing cybercrime landscape undermines clients' confidence and increases risk perceptio toward digital channels. (DeLiema et al., 2020; Oktaviani & Prasetyo, 2024). In some cases, individuals may even engage in opportunistic fraudulent behavior when expsed to such uncertainty or when pressured to transact thorugh untested digital platform (Sari & Rahman, 2023). Therefore, consisten digital banking adoption depends not only on technological functionality but also on the institution's ability to sustain consumer's trust in the face of perceived risk and impersonality.

This terrain is further complicated by generational disparities. Digital behaviors, trust patterns, and risk perceptions vary each generation (Mulia, 2023; Thasleena & Santhi, 2025). For example, older generations like Gen X and Baby Boomers may be more trusting in banks but more susceptible to online scams because they are less accustomed to digital interfaces,

whereas Gen Z and Millennials, who are digital natives, may have higher digital literacy but lower institutional trust. These variations imply that, particularly considering a mandated digital migration, the relationship between trust and fraud intention varies by age group.

Bank Central Asia (BCA) experienced a surge in social engineering fraud incidents in 2022 and 2023, in which clients were tricked by phony websites, phishing links, and WhatsApp and SMS impersonations of bank employees. On fraudulent banking portals, scammers tricked consumers into entering personal information or an OTP (one-time password), which led to the unapproved withdrawal of funds from their accounts. The victims said that their balances vanished overnight, even though they had never disclosed their passwords. Users frequently voiced a great deal of mistrust in the bank's digital security and recovery procedures and were ignorant of how their SIM cards had been compromised. To further erode confidence in the digital services required, some even accused the bank of being insensitive to complaints.

Another case is several users of "Livin' by Mandiri," Bank Mandiri's digital platform, claimed unexpected account breaches and unauthorized financial transfers in 2022. Following an inquiry, it was discovered that many of these occurrences involved SIM swap fraud, in which criminals used telco operators to manipulate a victim's phone number, giving them the ability to intercept OTPs (One-Time Passwords) and access Mandiri accounts. These cases illustrate how criminals exploit system weakness and customer unawareness and not only erode the clients' trust but also highlight that fraud in digital banking is no longer limited to external cybercriminals, but clients themselves may actively exploit the loopholes for personal gain.

Even though this problem is becoming more important, little empirical study has been done to examine how generational variations affect the relationship between fraud intention and trust in the age of required digital banking. This study aims to close that gap by investigating the relationship between consumers' intention to commit fraud (or susceptibility to fraud) across generations and their level of trust in the digital system and the banking institution. This study offers a relevant contribution to comprehending fraud risk from a multifaceted, generational viewpoint by combining theories from behavioral finance, technology acceptance, and criminology (such as the Fraud Triangle Theory and the Technology Acceptance Model).

Trust is essential to consumer engagement, retention, and compliance in the digital banking ecosystem. Traditional in-person cues like physical presence, personal relationships, and human reassurance are being replaced by trust as financial services move from in-person to virtual platforms (Suhartanto et al., 2022). In this case, trust has multiple dimensions, including confidence in the banking organization, faith in technology, and trust in regulatory protections. Despite the urgency of these risks, most digital banking research has predominantly focused on positive behavioral aspect such as technology adoption (Nguyen & Hyunh, 2020), customer satisfaction (Rahu et al., 2017), and loyalty (Suhartanto et al., 2022). The darker side of clients'

behavior such as fraud intention remains underexplored, even though first party fraud by clients is now recognized as a growing concern (Puspitasari & Hermawan, 2021; Brenig & Hildebrandt, 2022).

Furthermore, existing fraud studies often apply the Fraud Triangle or Fraud Diamond Theory primarily to organizational or employee misconduct (Abdullahi & Mansor, 2015; Nawawi & Hermawan, 2021; Brenig & Hildebrandt, 2020), leaving an open question about how this theoretical framework can be applied to client-initiated fraud in digital context.

Research continuously shows that user adoption of digital banking platforms is strongly influenced by trust (Lai, 2021; Yasa et al., 2021). Customers in Indonesia, where cybercrime is on the rise and digital infrastructure is unequal, are frequently hesitant to use digital services unless they have faith in the platform's integrity and security. When digital banking becomes required and consumers have no other option, this trust becomes even more important. Lack of trust not only discourages legitimate usage—it can also increase fraud intention. Customers who perceive banks as opaque, unresponsive, or unfair may justify unethical behavior such as misreporting transactions, exploiting system loopholes, or tolerating phishing attempts. The Fraud Triangle Theory (pressure, opportunity, rationalization) suggests that distrust in the institution can serve as a rationalization for fraud, especially among frustrated or digitally excluded users.

Understanding the factors that influence clients to commit fraud is crucial because customer driven fraud arises from motives and perception that differ from organizational or employee misconduct. Clients often exploit the system weakness when they perceive the opportunity such as bypassing verification, abusing promotional program, or taking advantage of transaction delay. They may also rationalize their behavior by believing that digital banks are wealthy institutions that are not harmed by small scale fraud, or by framing their actions as a form of compensation for the perceived unfair fee or policy. Without clearly identifying these client-side drivers, banks underestimating the role of user behavior in fraud and relying too heavily on back-end monitoring, rather than addressing the psychological and situational triggers that motivate the clients to act dishonestly.

In the digital banking setting, the need for further study is far greater compared to traditional or semi digital banks. This is because digital expands both the perceived opportunity and the rationalization space for the clients. For example, digital only is more anonymous, automated and less supervised, making it easier for the clients to test the system vulnerabilities or misuse the digital promotions without face-to-face accountability. By contrast, traditional and semi digital banks have natural safeguards such as branch interaction, physical identity checks and direct employee oversight that limit clients to make misconduct action.

Therefore, while comparative research across the channel is useful, additional study in

digital banking must go deeper to capture how the application designs, transaction speed and user experience create the new forms of opportunity and justification for the fraudulent acts by clients. Such understanding is vital for building the fraud prevention strategies that are not only technologically robust but also psychologically attuned to clients' behavior.

Previous literature on digital banking has predominantly focused on the positive aspects such as customer satisfaction, loyalty and adoption, while the darker side of consumer behavior such as fraud intention remains underexplored. Similarly, research of fraud using the Fraud Triangle Theory has often concentrated on organizational or employee misconduct, but little is known about how these elements manifest in client-side fraud, particularly in digital banking. Moreover, although intergenerational differences have been widely researched in digital adoption issues, few studies have investigated whether such differences contribute to clients' fraud intention. By addressing these gaps, this study contributes to extending the fraud theory into consumer context while offering a generational perspective in digital financial service.

Most of the research on digital banking focuses on customer happiness, loyalty, or technological adoption such as TAM and UTAUT (Alalwan et al., 2021; Gard et al., 2022; Sing & Srivastawa (2020). But less is known about the darker side of consumer behavior—fraud intention—particularly as trust declines. By establishing a connection between fraud intention and trust, the gaps are filled. Another dimension that complicates this phenomenon is intergenerational differences in digital trust, risk perception and technology use. Generational cohort differs in their digital literacy and trust in institutions, while the younger (millennials and Z) are more digitally fluent, they may have lower institutional trust, whereas older cohort may trust the banks but lack awareness of online risk (Yasa et al., 2021). Yet, little empirical research has tested whether such intergenerational difference shapes the fraud intention in digital banking environment.

Based on the identified gap, this research guided by several research questions. First, it asks what factors influence the clients' intention to commit fraud in digital banking. Second, it explores to what extent the rationalization acts as a justification mechanism for clients in shaping fraudulent behavior. Third, it examines whether the financial pressure significantly predicts the clients' fraud intention in digital banking context. Finally, it investigates whether the intergenerational difference between Y Generation and Millennials moderates the relationship between these three drivers and fraud intention.

In line with this question, the purpose of this study is to investigate the key drivers of fraud intention among banking clients in the era of mandatory digital banking, using the Fraud Triangle Theory as the underlying framework. The research aims to test the predictive power of opportunity, rationalization, and pressure, while also examining whether the effect is different across the generational cohort. By doing so, the research provides new empirical evidence such

as client-initiated fraud and offers insights into more fraud prevention strategies from the customer perspective.

1. LITERATURE REVIEW

Fraud Triangle Theory

Fraud research has traditionally been grounded in the Fraud Triangle Theory (Cressey, 1953), which emphasized the opportunity, pressure and rationalization as the main drivers of fraudulent behavior. Opportunity refers to the situation where weakness in systems, process or oversight make it possible to commit fraud with a low risk of detection. Pressure is typically linked to financial strain, lifestyle demands, or social expectation that drive individuals to seek illicit financial gain. Rationalization captures the cognitive justification that offenders use to view their fraudulent behavior as acceptable, excusable or not truly harmful. This tripartite framework has been widely validated in organizational and financial context, making it a strong foundation for studying client fraud in digital banking.

Fraud Elements

Opportunity is often regarded as the most controllable element of the fraud triangle because it relates directly to systemic weakness. In traditional banking, opportunities for fraud may arise from inadequate segregation of duties or weak monitoring system. In digital banking, however, opportunities take new forms such as system loopholes, identity manipulation, phising or the exploitation of promotional programs. Research by Puspitasari & Hermawan (2021), in Indonesian banking, highlight that clients perceive the digital banking system as more vulnerable, which encourage opportunistic behavior. Likewise, Hoffman and Birnbrich (2012) previously noted that gaps in online verification system can create fertile ground for fraudulent practices. Thus, in the digital context, opportunity is amplified by the increasing complexity of technological platforms and the difficulties bank in monitoring every transaction in real time.

Pressure represents the motivational aspect of fraud. Traditionally, financial pressure has been examined in the context of employee facing the debt, job insecurity, and performance demands. However, for clients in digital banking, pressure may stem from personal financial instability, consumerism, or economic shock such as inflation and unemployment. Research by Nguyen and Huynh (2020) found that individuals experiencing financial stress are more likely to consider the exploitation of digital finance services inappropriately. Similarly, Nawawi & Salin (2018) emphasized that financial pressure not only pushes individuals toward fraudulent action but also can intensify their research for the opportunity within weak system. In consumer context, this pressure is often situational especially when clients are facing urgent financial need may view digital banking fraud as a temporary solution to immediate problems.

On the other hand, rationalization is the most complex and culturally nuanced element of the fraud triangle. It refers to the mental process through which individuals justify fraud as acceptable behavior. In employee fraud, rationalization often involves feelings of underpayment or mistreatment. In the digital banking context, clients may rationalize fraud by framing it as harmless to large institutions or as compensation for service failure. Reinstein & Taylor (2017) and Mintchik & Riley (2019) highlighted that rationalization is a crucial psychological mechanism that allows clients to maintain a positive self-image while engaging in fraudulent action. Yang & Chen (2023) also pointed out that in first party fraud case, rationalization enables the clients to see themselves not as criminals but as opportunistic consumer that responding to systemic flaws.

Collectively the Fraud Triangle Theory provides a robust lens to analyze the client-initiated fraud in digital banking. While opportunity, pressure and rationalization have been extensively studied in the organizational fraud, their application to consumer-driver fraud remains relatively limited. Digital banking adds new dimensions to each element such as opportunities are shaped by technological vulnerabilities, pressure is heightened by economic uncertainty and consumer demands, and rationalizations are influenced by the evolving perception of fairness in financial service.

In the world of digital banking, fraud is increasingly committed by bank clients themselves in addition to by internal staff members or outside attackers. A range of dishonest practices intended to get money through unethical means are included in customer-initiated fraud. These include dishonestly submitting credit applications, contesting valid transactions, abusing promotional offers, and voluntarily taking part in money laundering schemes by acting as "money mules." Although first-party fraud has not received much attention in the past, new research has begun to recognize it as a serious and expanding problem in banking, particularly as financial services move toward entirely digital channels (Puspitasari & Hermawan, 2021).

Application or documentation fraud, in which people use fictitious income statements, tax identification numbers, or business licenses to get bank loans or credit cards, is a prevalent type of consumer fraud. In their research on the fraud triangle in the Indonesian banking sector, Puspitasari & Hermawan (2021) found that opportunity, financial pressure, and the justification of dishonest action frequently combine to cause client fraud. This is consistent with traditional fraud ideas that are still quite applicable in the digital age, including Cressey's Fraud Triangle.

Friendly fraud, sometimes known as bogus transaction disputes, is another common type. Here, after obtaining goods or services, clients purposefully contest legitimate transactions by claiming things like "unauthorized use." In their analysis of behavioral patterns in these fraudulent chargebacks, Van Vlasselaer et al. (2021) highlighted the difficulty banks face in differentiating between legitimate situations and intentional deception. This type of fraud is more prevalent in e-commerce transactions and is made worse by the growing use of mobile banking and digital

payments.

Even when they carried out certain digital transactions (such as QR payments or mobile banking transfers) knowingly, some consumers make up the story that they were not allowed (Wang & Dincelli, 2021). Reversing the transaction or getting a refund are frequently the objectives. Another fraud case which is conducted by customers is to open several digital bank accounts and take advantage of marketing initiatives like cashback incentives or referral bonuses, customers fabricate multiple false or synthetic identities. There has been widespread misuse of sign-up and cashback programs by digital banks such as Jenius (BTPN), blu by BCA Digital, and SeaBank, where scammers have used incentives using various phone numbers and identification numbers.

Even more, consumers fraudulently obtain personal loans, credit cards, or Kredit Usaha Rakyat (KUR) from state-owned banks by forging documents such as pay stubs, tax ID numbers (NPWP), or fictitious business licenses. False KUR applications in Central and West Java have been the subject of numerous fraud cases where people filed fictitious paperwork or conspired with insiders to obtain money.

The Fraud Triangle Theory is still a useful paradigm for comprehending fraudulent activity in the context of digital banking. According to this idea, fraud happens when three factors come together: opportunity, pressure, and justification. Among these, clients' awareness and understanding of the financial system have a significant impact on opportunities. Amoh et al. (2021) evaluated consumers' awareness and understanding of electronic banking fraud in Ghana. The results showed that although consumers were aware of several fraudulent practices, institutional elements including inadequate client education and a lack of oversight greatly increased the risk of electronic banking fraud for both banks and customers. This emphasizes the idea that customer knowledge may unintentionally lead to fraud opportunities if it is not combined with strong institutional controls and education.

One of the crimes with the greatest rate of growth in industrialized nations is consumer financial fraud (CFF), which is defined as unauthorized access to a person's bank account or payment card information for fraudulent transactions (Engels et al., 2020) (Kadoya et al., 2020). Criminals can target potential victims anywhere in the world thanks to the digitalization of financial services, the pervasive use of social media and electronic payment methods, and the growing complexity of financial goods (Goel, 2021; Nasi et al., 2023).

Fraud by Customer

According to Vuori et al. (2019), organizational knowledge is the "provision of organisational histories, knowledge, competencies, and skills" that arises from human thought and interpretation (Galeazzo & Furlan, 2019) interpretation. According to Eslamkhah & Hosseini

(2019) it represents the different "understandings" that exist regarding the organization, its procedures, and its contents. Organizational performance depends on managing this knowledge since, once processed and codified, it can provide significant benefits to the organization as well as, occasionally, to competitors, outsiders, and other stakeholders (Laihonen and Huhtamaki, 2020).

Occupational fraud, as defined by Nawawi and Salin (2018), is the intentional misuse or misapplication of the resources or assets of the employing organization to leverage one's profession for personal benefit. Regardless of the industry, fraud encompasses a broad range of offenses, deceptions, and breaches of employee trust. What motivates someone to act unethically is related to perceived pressure. This kind of pressure needs only be felt; it need not be actual. The culprit can be coerced into committing a crime if they think they are under pressure (Abdullahi & Mansor, 2015).

Christian et al., (2019) said that there may be social, political, non-financial, or financial pressure to commit fraud. Non-financial pressure, for instance, could come from a lack of self-control and a desire to conduct fraud to support one's gambling or drug addiction. Chepkoech & Rotich (2017) assert that pressure can be either positive or negative factor. Another factor is perceived opportunity which predicated on the claim that people fraudulently use any system's flaws to further their own agendas (Mhlangga, 2020).

The term "pressure component" describes the internal or external pressures that lead someone to commit fraud. In the context of the consumer, these pressures may take the form of financial difficulty, economic instability, or social pressure, all of which can lead people to commit fraud, including chargeback fraud, identity theft, and filing false claims (Abiodun, 2020). Finding high-risk client segments requires an understanding of the type and origin of these pressures. The second component is opportunity, refers to how simple it is thought to commit fraud without getting caught. This could include disjointed data monitoring systems, insufficient verification procedures, or weak cybersecurity safeguards in digital banking systems. Consumers may be more inclined to act unethically if they believe there are systemic flaws, particularly if there seems to be no oversight (Asmah et al., 2019)

Further, people use the process of rationalization to defend dishonest behavior to themselves. From the viewpoint of the consumer, rationalization could involve ideas like "no one is really harmed" or "the company overcharges anyway." These explanations are essential in reducing the psychological barrier to misconduct, which makes it easier for otherwise law-abiding people to engage in deviant activity (Baten, 2020). The most unique aspect of Fraud Diamond Theory may be the fourth component, capacity. It describes a person's characteristics or skills that allow them to commit fraud. This could include knowledge of financial systems, digital literacy, or past exposure to fraudulent activity in the context of consumer behavior (Wood et al., 2021).

A competent consumer has the skills and resources to successfully take advantage of system flaws in addition to being pressure-driven and aware of opportunities (Van Scotter & Roglio, 2020).

The applicability of FDT outside of its initial organizational context is supported by recent empirical research. For example, Dias-Oliveira et al. (2024) showed that academic dishonesty, a type of personal wrongdoing outside the corporate sphere, was highly influenced by all four components of the theory among university students. This study offers strong proof that FDT can be modified to comprehend rogue consumer behavior, particularly in situations where customers behave as autonomous agents. Similarly, Ristiana et al. (2022) discovered that while opportunity was not a major predictor, pressure, justification, and ability all had a substantial impact on students' desire to commit academic fraud (Kim & Choi, 2021; Kocakulah & Eser, 2023). These results imply that although FDT is still a useful model, the relative importance of each component may change based on the situation and the subject profile.

Grounded in the Fraud Triangle Theory (Cressey, 1953) and supported by prior studies (Puspitasari & Hermawan, 2021; Wang & Dincelli, 2021) this research develops the following hypothesis to be tested empirically.

H1: Perceived opportunity has a significant impact on clients' fraud intention in digital banking landscape

H2: Financial pressure has a significant impact on clients' fraud intention in digital banking landscape.

H3: Rationalization has a significant impact on clients' fraud intention in digital banking landscape.

Despite the increasing academic intention to digital banking, the intergenerational dynamics of trust, risk perception, and fraudulent intention remain an understudied area. Prior studies have acknowledged that the generational cohort exhibits distinct patterns in digital literacy, technology adoption and institutional confidence, yet most of this research stops describing the behavioral differences, rather than explaining their fraud related implications. For instance, Mulia (2023) found that Baby Boomers and older Generation X clients tend to exhibit higher trust in financial institutions but lower familiarity with cybersecurity mechanisms which increase their vulnerability to deception.

Conversely, younger cohort, such as Millennials and Generation Z demonstrate greater confidence in navigating digital interface but show lower institutional trust and a higher tolerance for opportunistic behavior, possibly because they perceive financial system as impersonal or profit-driven (Thasleena & Santhi, 2025). These contrasting tendencies imply that each generations construct and interpret trust differently, one anchored in relational assurance, the other in technological performance, which shape how individuals reationalize or justify unethical conduct when interacting with digital banking platforms. Since generational

differences are believed to influence the risk perception, trust and digital behavior (Yasa et al., 2021; Lai, 2021), this research further hypothesized:

H4a: Generation moderates the relationship between financial pressure and fraud intention

H4b: Generation moderates the relationship between perceived opportunity and fraud intention.

H4c: Generation moderates the relationship between rationalization and fraud intention.

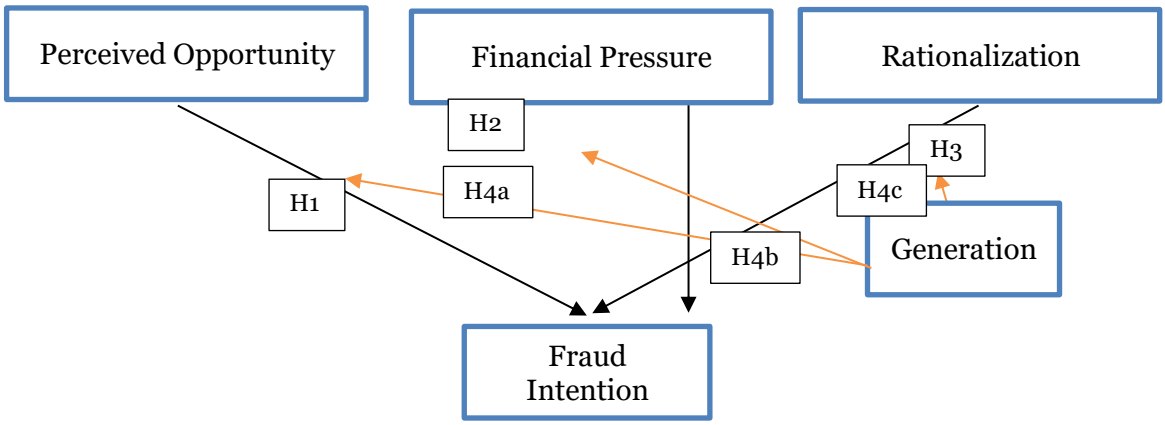

Figure 1. Research Framework

3. RESEARCH METHODOLOGY

Qualitative Study

This study uses a qualitative exploratory technique to begin the first pre-test investigating the reasons for consumer fraud in the banking industry. To explore the complex motives, attitudes, and environmental elements driving such immoral or unlawful actions, the qualitative design was selected. Because of the intricacy and delicate nature of the subject, qualitative research offers more flexibility and depth in comprehending personal experiences and mental processes than can be achieved with formal quantitative techniques.

Before each interview and survey session, the participants are provided with a clear explanation of the research's objectives, the voluntary nature of participation, and the confidentiality of their responses. They are assured that their personal identity will remain anonymous and that the data is used for academic purposes only. Consent is obtained verbally during the qualitative interview.

The data collection is conducted in two stages. The qualitative phase is carried out in early 2024, where 10 digital banking clients with prior experience related to fraud cases or high awareness of fraud risk are interviewed using a semi-structured interview guide. Each session lasted approximately 10 minutes and focused on exploring the clients' perception about the

opportunity, financial pressure and rationalization in relation to fraud intention. A snowball sampling technique is applied to identify the participants who have relevant experiences.

The main technique for gathering data for the study is in-depth semi-structured interviews. Researchers can delve further into participants' opinions, feelings, and experiences with banking fraud thanks to these interviews. The original statement and body language are obtained through in-person interviews, which last 10 to 15 minutes each. Key topics such as participants' perceptions of fraud, their explanations or justifications, the impact of digital banking technologies, their level of trust or mistrust in the banking system, and any social or personal pressures that might encourage fraudulent behavior are all covered in detail in the interview guide.

In this qualitative stage, participants are selected based on the following criteria such as active user of digital banking service in Indonesia, has several previous epxerience related to digital fraud, aged 20 years and olders, capable to articulate their perception about digital banking and fraudulent behavior. Individuals who never use digital banking are unable to provide informed consent, employee of bank, fraud investigators and who work as regulator are excluded to aviod the professional bias.

People with pertinent knowledge of the topic are chosen using a purposeful approach. Ten banking customers with prior fraud-related experience are making up the sample. To maintain confidentiality, the researchers do not disclose any personal information and handle all collected data in a private manner. It is possible to find more people with pertinent experiences by using snowball sampling. The purpose of this pre-test is to provide deep and contextually based insights into the factors that influence banking clients' fraudulent behavior. The results are used as practical guidance tactics for risk mitigation and fraud prevention in the banking sector, as well as to build more thorough models and hypotheses for the quantitative stage.

Quantitative Study

The quantitative phase is conducted in middle of 2024 and involved an online survey which distributed to 100 active digital banking clients in Indonesia. Respondents represented different generation chores (42 from Y Generation and 58 from Millennials) to examine the potential of intergenerational differences. A structured questionnaire is developed from both prior literature and themes which identified during the qualitative pre-test. Response iscollected using five-point Likert-like scale. In terms of analysis, data validity and reliability are first confirmed through loading factors, Average Variance Extracted and Cronbach’s Alpha. Structural Equation Modeling is applied to test the hypothesized relationship.

The survey received approximately 130 responds, and after excluding the incomplete

responses, and invalid entries, 100 valid questionnaires are retained for further analysis, yielding an effective response rate of around 77%. After completing the theme analysis and qualitative pre-test, the study moves on to the quantitative phase, which attempts to confirm the variables influencing bank customers' fraudulent conduct. Measureable variables or constructs are created by combining the themes derived from the interview data, such **as perceived opportunity, financial pressure, and rationalization.**

In this stage, inclusion is limited to active digital banking users who had online banking application for at least six months and belong to the generational cohort understudy, namely Generation Y and Z. All respondents participated voluntarily and required them to provide complete and valid survey responses. Exclusion criteria included incomplete or inconsistent survey submission, respondents who do not directly use digital banking services.

A systematic survey instrument is developed based on these constructions. Items from the qualitative results and pertinent earlier research are used to create a structured questionnaire. To gauge respondents' levels of agreement or perception with each element, each question is scored on a Likert scale, with 1 denoting strongly disagreement and 5 strongly agree. The questionnaires are going through a pilot test before being widely distributed to evaluate its clarity and reliability and make sure the indicators appropriately represent the components that have been discovered.

Structural equation modeling (SEM) is used to evaluate each factor's impact on fraudulent intention. A greater comprehension of the behavioral mechanisms at work is made possible by this method, which evaluates both direct and indirect effects among variables. Active users of Indonesian digital banking platforms would be among the target group for this phase. To guarantee sufficient representation across a range of demographic categories, including age groups (e.g., Gen Z, millennials, older adults), income levels, and educational backgrounds, stratified random selection may be employed. Statistical power analysis is used to establish the necessary sample size, however for adequate model validity and generalizability, it is anticipated to 100 respondents.

It is crucial that the measurement tool utilized in this study pass rigorous validity and reliability testing before moving further with model building. These tests guarantee that the data produced is reliable and consistent for statistical analysis, and that each construct obtained from the qualitative phase appropriately reflects the concepts it aims to measure. The first step in the validity testing process is the expert evaluation of the content validity. Each survey item is examined by academic experts and professionals working in the domains of consumer behavior, fraud prevention, and digital banking to see if it accurately captures the intended construct—such as opportunity, rationalization, or mistrust. The validity of each construction is tested by Average Variance Extracted and Loading Factor. Each parameter should surpass 0.50 point to

be accepted. On the other hand, reliability is tested by Cronbach's Alpha parameter, and should surpassed 0.70 point.

The Connection of Phase 1 and Phase 2 Study

This research is deliberately designed as a sequential mixed-method study, where the first phase (qualitative) and second phase (quantitative) are methodologically and conceptually interdependent. First phase functioned as exploratory foundation, while second phase served as the confirmatory extension. In the first phase, semi-structured interviews conducted to capture the lived experience, perception and rationalization underlying the fraud related behavior. This phase also provides two critical contributions. First, it ensured the contextual sensitivity, where the many frauds related constructs in the literature such as opportunity, rationalization and financial pressure have been primarily tested in organizational settings.

The interviews revealed how these constructions manifest client behavior within digital banking landscape. For example, respondents identified transaction delays, weak document verification and the exploitation of cashback promotion as unique form of opportunity in digital system. This context specific insight allows us to refine and supplement the existing measurement items, ensuring that the constructs are not imported from prior research in a purely generic form but instead tailored to the Indonesian digital banking environment.

Second, the qualitative findings improve the content validity. Rationalization, for instance, is well-known concept in the Fraud Triangle Theory, but how clients frame it differs from employee. Respondents describe rationalization such as banks are wealthy, so a small fraud is harmless, or hidden fee justify my action. By capturing these naratives, we can construct the survey items which directly reflect how clients rationalize the fraud in practice, thereby strengthening the theoretical ground and measurement accuracy of the phase two.

Building on this foundation, phase two used a survey of 100 active digital banking clients to achieve the statistical test and validate the construction derived from the phase one and prior literature. The quantitative phase confirmed the reliability and validity of the items through factor analysis and testing the proposed hypothesis using PLS-SEM. In this way, phase one acted as item-development phase, while the second phase is acting as theory testing and generalization phase.

In the qualitative stage, data are analyzed usin a thematic coding scheme developed through both deductive and inductive procedures. The deductive codes are derviced from the three principal constructs of the Fraud Triangle Theory namely perceived opportunity, financial pressure, and rationalization which served as theoretical foundation. Meanwhile, inductive codes emerged from participants narative during the interviews, allowing the new contectual insight specivif to digital banking fraud in Indonesia to be identified. The coding process

followed a three-step procedure such as initial open coding to capture relevant statements and behavioral descriptions, axial coding to group similar responses into conceptual categories related to opportunity, presure and rationalization, and selective coding to refine these categories into measurable constructs that informed the quantitative instrument.

4. RESULTS AND DISCUSSIONS

Result

Our first step, which is in-depth interview, has 10 respondents. Based on the interview, this step generates multiple answers which have been classified into relevant construct. A total of 100 respondents took part in the quantitative research process for the current study. These individuals were chosen to reflect several generational cohorts pertinent to the goals of the study. 42 respondents out of the entire sample were classified as members of Generation Y. People who were born between the early 1980s and the mid-1990s and who have seen the shift from analog to digital technology are usually included in this cohort.

The 58 respondents that remained were classified as belonging to Gen Z. Generation Z, who are frequently seen as having some overlap with Generation Y, are distinguished by their early exposure to digital technologies and their important influence on contemporary consumer behavior. In line with the purpose of the research, this generational distribution was specifically chosen to look at any possible behavioral distinctions between these two age groups. Below is the grouping result of the multiple answer from the in-depth interview into the relevant construction.

The participants in this qualitative stage are selected through purposive and snowball sampling techniques based on specific inclusion criteria such as active user of digital banking services aged 20 years and above, have prior experience or awareness rlated to digital fraud casees and can articulate their perception of fraud-related behavior. The ten respondents consisted of six maes and four females, representing both Generation Y and Z cohorts.

The qualitative findings revealed several significant insights that shaped the direction of the overall research. First, Perceived Opportunity emerged as a key driver of fraud intention, with participants highlighting the system weakness such as transaction delay, lack of direct document verification, and exploitable cashback program as the opportunity to commit unethical acts without immediate detection. Second, Financial Pressure is found to play a relatively minor role, altough the participations acknowledge that financial stress could increase temptation, it did not independently lead to fraudulent intention unless accompanied by perceived opportunity or moral justification. Third, Rationalization appeared as the most psychologically powerful factor influencing fraud intention. Respondents commonly justified unethicl action with statements such as Bank are rich, so a small fraud will not harm them or “hidden charge justify my actions” refelcting

how consumer use moral disengagement to maintain a positive self-image while considering misconduct.

Building upon these insights, the quantitative phase is conducted to statistically test and validate the relationship identified in qualitative phase. A total of 100 respondents participated in this stage, consisting of 42 individuals from Gen Y and 58 individuals from Gen Z. All participants are active users of digital banking platforms such as BCA Mobile, Livin by Mandiri, and Blu by BCA Digital with at least six months of consistent usage experience. The sample is almost balanced across gender and represents a range of educational and occupational backgrounds, including university students, office employees, SME owners, and professionals. This generational and demographic diversity provide a robust foundation for examining the moderating role of generational cohorts.

Table 1. Grouping The Open-ended Question to Perceived Opportunity Construct

No	Open-ended Question	Item	Indicator
1	In what situation do you think that you will commence fraudulent behavior to your financial provider / bank / insurance company?	The transaction system is not closely monitored	Opp1
		The system does not verify all documents directly	Opp2
		The system can be bypassed easily	Opp3
		I know about the delay between transaction confirmation and the actual debit in the system	Opp4
		I believe that the system itself made it easy to be exploited	Opp5

Table 2. Grouping The Open-ended Question to Financial Pressure Construct

No	Open-ended Question	Item	Indicator
2	In what situation do you think that you will commence fraudulent behavior to your financial provider / bank / insurance company?	When I am under financial stress, I am more likely to consider actions I would normally reject	Fin1
		I have experienced situations where urgent financial needs made me consider unethical financial actions	Fin2
		I sometimes feel forced to take risky or dishonest financial steps due to lack of income or resources	Fin3
		Breaking the regulations when interacting with financial service providers can be justified by dire financial circumstances.	Fin4
		Taking advantage of system vulnerabilities appears to be a vital alternative during financial crises.	Fin5

Following response collection, the researcher used the content analysis technique based on our research partner in campus to group multiple-answer questions into their appropriate constructs. Every piece was meticulously categorized to guarantee that it appropriately represented the planned architecture. Each item underwent a validity and reliability test after the grouping procedure. This test served to confirm that the indicators were conceptually and statistically consistent with the

constructions they were meant to measure.

Table 3. Grouping The Open-ended Question to Rationalization Construct

No	Open-ended Question	Item	Indicator
3	In what situation do you think that you will commence fraudulent behavior to your financial provider / bank / insurance company?	A minor act of fraud doesn't truly harm anyone because banks are insured and generate enormous profits	Rat1
		If the bank makes frequent mistakes or charges hidden fees, I feel less guilty about taking advantage of them.	Rat2
		If I discover a system flaw and take advantage of it, the bank is responsible for not protecting it, not me.	Rat3
		Breaking the regulations when interacting with financial service providers can be justified by dire financial circumstances.	Rat4
		In challenging circumstances, breaking the rules is permissible as long as no one is harmed directly.	Rat5

If an object satisfied two important requirements, it was deemed a valid indicator. For the item to have a strong enough link with its related construction, it must first have a loading factor with a p-value better than 0.5. Second, the item must not show cross-loading on more than one construct, as this would indicate that the item's measurement was unclear. To preserve the accuracy and dependability of the measurement model, items that did not fit these requirements were not included in subsequent analysis. The validity test results are shown by Table 4, 5 and 6 respectively.

Table 4. Validity Check Result for Perceived Opportunity

No	Item	Indicator	Outer Loading P-values	Average Variance Extracted	Parameter Used
1	The transaction system is not closely monitored	Opp1	0,659	0,590	>0,5
	The system does not verify all documents directly	Opp2	0,921		
	The system can be bypassed easily	Opp3	0,609		
	I know about the delay between transaction confirmation and the actual debit in the system	Opp4	0,873		
	I believe that the system itself made it easy to be exploited	Opp5	0,732		

A validity test was performed on each construct to guarantee the measurement model's precision and coherence. After being categorized into pertinent constructs according to theoretical alignment, the items were put through an outer loading analysis. If an item did not exhibit cross-loading with other constructs and its p-value was greater than 0.5, it was considered valid. The indicators were examined in relation to the Perceived Opportunity generated values ranging from 0.609 to 0.921, all five indicators (Opp1 until Opp5) had outer loading levels over the 0.5 criterion.

This concept had a satisfactory convergent validity, as indicated by its Average Variance Extracted (AVE) of 0.590. Therefore, every item in this category was kept for additional examination.

Table 5. Validity Check Result for Financial Pressure

No	Item	Indicator	Outer Loading P-values	Average Variance Extracted	Parameter Used
2	When I am under financial stress, I am more likely to consider actions I would normally reject.	Fin1	removed	0,586	>0,5
	I have experienced situations where urgent financial needs made me consider unethical financial actions.	Fin2	0,864		
	I sometimes feel forced to take risky or dishonest financial steps due to lack of income or resources.	Fin3	0,776		
	Breaking the regulations when interacting with financial service providers can be justified by dire financial circumstances.	Fin4	0,640		
	Taking advantage of system vulnerabilities appears to be a vital alternative during financial crises.	Fin5	removed		

Table 6. Validity Check Result for Rationalization

No	Item	Indicator	Outer Loading P-values	Average Variance Extracted	Parameter Used
3	A minor act of fraud doesn't truly harm anyone because banks are insured and generate enormous profits.	Rat1	0,758	0,627	>0,5
	If the bank makes frequent mistakes or charges hidden fees, I feel less guilty about taking advantage of them.	Rat2	0,740		
	If I discover a system flaw and take advantage of it, the bank is responsible for not protecting it, not me.	Rat3	0,812		
	Breaking the regulations when interacting with financial service providers can be justified by dire financial circumstances.	Rat4	0,774		
	In challenging circumstances, breaking the rules is permissible as long as no one is harmed directly.	Rat5	0,869		

Five indicators were first tested in the Financial Pressure construct. However, because Fin1 and Fin5 have low loading values and did not satisfy the necessary validity standards, they are eliminated. The allowed loading values for the final three components (Fin2, Fin3, and Fin4) ranged from 0.640 to 0.864, yield an AVE score of 0.586. These findings imply that the financial pressure construct is sufficiently represented by the updated set of items. The removal of item FIN1 and FIN5 is based on the result of the measurement validity test. Both items showed the loading

factor value below the recommended threshold of 0.50.

Table 7. Validity Check Result for Fraud Intention

No	Item	Indicator	Outer Loading P-values	Average Variance Extracted	Parameter Used
4	I have the intention to commit fraud.	Fraud1	0,619	0,565	>0,5
	With the financial pressure I face, the desire to commit fraud arises.	Fraud2	0,780		
	I will commit fraud when the opportunity arises.	Fraud3	0,838		
	I consider committing fraud, even though it is wrong.	Fraud4	0,752		

There are two possibilities for this result. First, our respondents are relatively financially stable, which may explain why the direct link between financial stress and fraudulent intention is not strongly perceived. As a result, items that are explicitly framed as financial distress (FIN1 and FIN5) are not consistent with the overall responses. Second, compared to other items (FIN2-FIN4), these two statements may have been interpreted by respondents as overlapping between opportunity or rationalization rather than purely financial pressure, thereby reducing their conceptual clarity.

Further, all five of the items in the Rationalization construct demonstrated strong validity. Rat1 through Rat5 had outer loading values between 0.740 and 0.869. No indicators were eliminated from this category since the AVE of 0.627 demonstrated that this construction had enough convergent validity. With loading values ranging from 0.619 to 0.830, all four items for the Fraud Intention construct met the validity criteria. The construct accurately assessed the intention to commit fraud, as evidenced by the computed AVE of 0.565. These results show that the indicators employed for this construction are conceptually consistent and statistically passed. Before going to the path analysis, we run the reliability test. The result is shown below.

Table 8. Reliability Check Result for All Construct

No	Item	Composite Reliability	Cronbach's Alpha	Parameter Used
1	Perceived Opportunity	0,989	0,832	>0,5
2	Financial Pressure	0,718	0,670	
3	Rationalization	0,887	0,860	
4	Fraud Intention	0,796	0,747	

Composite Reliability (CR) and Cronbach's Alpha are the two main measures used to evaluate the measurement model's reliability. Table 11 demonstrates that every construction has good internal consistency, surpassing the dependability requirement of 0.5. With a composite reliability score of 0.989 and a Cronbach's Alpha of 0.832, the Perceived Opportunity construct generates the best reliability score, indicating excellent internal consistency among the items. With

Cronbach's Alpha of 0.860 and a composite reliability of 0.887, the rationalization construct likewise demonstrated high reliability. Acceptable dependability was attained by the Fraud Intention construct, which had respective values of 0.796 and 0.747.

Last but not least, despite having the lowest reliability scores of the four, the Financial Pressure construct's items consistently measure the same concept, as evidenced by its composite reliability of 0.718 and Cronbach's Alpha of 0.670, both of which were above the acceptable threshold By using the Smart PLS 4 application, we test all path with criterion single tailed at 0.05 significance level. The results shown by Table 9 below include the role of generational difference as moderator variable.

Table 9. Path Analysis

No	Independent Construct	Dependent Construct	P-values	Parameter Used	Result
1	Perceived Opportunity	Fraud Intention	0,031	<0,05	supported
2	Financial Pressure		0,100		not supported
3	Rationalization		0,005		supported
4	Generation x Financial Pressure		0,212		not supported
5	Generation x Perceived Opportunity		0,085		not supported
6	Generation x Rationalization		0,149		not supported

According to the path analysis results, which are displayed in Table 9, bank clients' intention to commit fraud is significantly predicted by perceived opportunity ($p = 0.031$). This result confirms the theory that people are more prone to develop fraud intentions when they believe the financial system has exploitable flaws, like inadequate oversight or transaction processing delays. The Fraud Triangle Theory, which highlights opportunity as a major facilitator of unethical behavior, is consistent with this finding. In practice, it implies that fraud risks could be considerably reduced by minimizing perceived gaps through improved transparency, real-time transaction verification, and stronger internal controls.

Financial pressure, on the other hand, has no significant impact on the intention to commit fraud ($p = 0.100$). This finding implies differently in the context of this study, even though prior research and theoretical frameworks frequently portray financial stress as a driving force behind unethical action. This finding could be explained by several reasons. First, even in the face of financial strain, immoral action may be discouraged by cultural and moral norms within the respondent group. Second, it's possible that the study participants—who are probably employed or financially secure—do not encounter financial strain that might lead them to commit fraud. Furthermore, two elements from the financial pressure construct are eliminated because of the validity test, which would have compromised the measurement's capacity to fully represent the range of financial stress. Therefore, without enabling circumstances and mental explanation, financial pressure alone is not enough to motivate dishonest intention.

The significance of the rationalization construction in the fraud decision-making process is further supported by the considerable link it exhibits with fraud intention ($p = 0.005$). This lends credence to the notion that people frequently need internal rationalization before engaging in unethical behavior, such as thinking that banks can cover minor losses or that no harm is done directly. Even when acting dishonestly, this psychological process aids people in overcoming remorse and maintaining their sense of self. Therefore, it may be possible to lessen fraud inclinations by limiting reasoning through ethics instruction, personal accountability, and unambiguous penalties.

Additionally, it was discovered that there was no statistically significant relationship between generation and the three primary dimensions (financial pressure, perceived opportunity, and rationalization). There was no evidence to support the moderating effect of generation on the associations between financial pressure and perceived opportunity ($p = 0.085$), fraud intention ($p = 0.212$), and rationalization ($p = 0.149$). These findings imply that there is no discernible difference between Generation Y and Millennial respondents in the impact of the primary variables on fraud intention. This suggests a degree of uniformity in the ways that different generations react to the fundamental causes of deception.

Discussion

The result of the path analysis provides a nuanced understanding of the behavioral mechanism underlying fraud intention in digital banking. Out of the six hypothesized relationships, only two paths are statistically significant and supported, while the financial pressure and all moderation effects of generation are found to be insignificant. The significance of Perceived Opportunity reinforces the central argument of the Fraud Triangle Theory that situational enabler, such as system loopholes, plays a critical role in motivating unethical actions when detection risk is low.

In a digital context, where the anonymity and automation are high, perceived opportunity becomes more salient than external financial pressure. The strong effect of rationalization also suggests that psychological justification is a key mechanism driving customers' willingness to engage in fraud. Respondents who believe that "banks are large and wealthy" or that "hidden fees justify the misconduct" examplify a moral disengagement process that allows individual to normalize unethical behavior wothout self-blame.

In contrast, the non-significant influence of financial pressure indicates that economic hardship alone is insuficient to trigger fraudulent action among digital banking users. This finding departs from traditional interpretation of the Fraud Triangle, where financial strain is often a core motivator of fraud. The outcome may be exlplained by the relative financial stability of the respondents, most of whom are employed or in higher education, and by the

psychological distance between digital actions and the real-world moral accountability.

Furthermore, the absence of significant moderating effects of generation suggests that both cohorts share relatively similar cognitive patterns when interacting with digital financial platforms. Despite the differences in age and literacy, both generations appear to perceive fraud opportunities and rationalization in comparable ways. This convergence may be attributed to their shared immersion in digital culture, where technological familiarity reduces the generational gap in ethical perceptions and online decision making.

5. CONCLUSION AND SUGGESTION

Conclusion

This research provides both theoretical enrichment and practical implication in understanding fraud intention within the context of mandatory digital banking. Theoretically, the research extends the application of the Fraud Triangle Theory from its conventional organizational or employee misconduct setting into the consumer behavior domain. Empirically this study demonstrates that only Perceived Opportunity and Rationalization significantly influence the fraud intention and highlights the shifting nature of fraud motivation in the digital era, where the system-based vulnerability and cognitive justification outweigh the traditional economic pressure.

The integration of intergenerational analysis between Generation Y and Z further contributes to the literature by testing whether generational cohort shaped by differing digital experiences, moderate fraud-related behavior. The finding that generational differences did not significantly alter the predictive relationship indicates a theoretical refinement: in highly digitalized environment, technological familiarity converges ethical and behavioral pattern across generations, suggesting that fraud intention is more a function of contextual affordance and moral reasoning than demographic variation. Hence, this study advances behavioral fraud by bridging the criminological and consumer perspective in the digital financial ecosystem.

Practically, the findings provide actionable insight for banks, regulators and digital finance providers in designing more effective fraud prevention strategies. Since Perceived Opportunity emerged as a dominant factor, financial institutional should prioritize the system transparency enhancement, real-time monitoring and multi layered verification to minimize clients' perception of expliotable loopholes. Simultaneously, because Rationalization strongly influences unethical decision, preventive measure must adress the psychological and ethical dimension of user behavior through awareness campaigns, transparent communication of financial policies, and digital ethics education. The absence of generational differences suggests that such intervention can be designed universally across age group, emphasizing shared digital

trust, and accountability principles rather than demographic segmentation.

Suggestion

Even though your study found that financial pressure did not significantly predict fraud intention, further research could examine mediating or moderating factors that might account for this link. Personal values, religious beliefs, or financial literacy, for example, may mitigate or enhance the impact of financial hardship on unethical behavior. Furthermore, employing qualitative techniques like focus groups can reveal emotional aspects and hidden perceptions that are difficult to measure with surveys.

To determine whether age-related factors affect ethical reasoning, digital literacy, or exposure to fraud chances, future research might include Generation Z and baby boomer generations, but this study concentrated on Generation Y and Millennials. Furthermore, a more thorough picture of fraud behavior across demographic groups might be obtained by integrating respondents from a range of socioeconomic backgrounds, professions, and geographic locations (rural vs. urban).

REFERENCE

Abdulahi, R., & Mansor, N. (2015). Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance, and Management Science*, 5(4), 38-45.

Abiodun, E.A. (2020). Internal control procedures and firm's performance. *International Journal of Scientific and Technology Research,* 9(2), 6407-6415.

Ahmed, F., Hussain, A., Khan, S., Malik, A.H., Asim, M., Ahmad, S., & El-Affendi, M. (2024). Digital risk and financial inclusion: Balance between auxiliary innovation and protecting digital banking customer. *Risk,* 12(8), 133

Alalwan, A.A., Dwivedi, Y.K., & Rana, N.P. (2017). Digital banking adoption: A quantitative study of the role of customer satisfaction and technology accepntance. *International Journal of Bank Marketing*, 35(6),1018-1038

Amoh, J.K., Awunyo-Vitor, D. & Ofori-Boateng, K. (2021). Customers' awareness and knowledge level of fraudulent acts in electronic banking in Ghana: Evidence from a universal bank. *Journal of Financial Crime*, 28(3), 870-882

Asmah, A.E., Antuilik, W.A., Ofori, D., & Futter, A. (2019). Antecendents and consequences of staff related fraud in the Ghanian banking industry. *Journal of Financial Crime*, 26(3), 669-682.

Baten, A.N. (2020). Basic understanding of fraudulent activities in corporate organization.

Review of Business Accounting and Finance, 1(1), 1-13.

Bueno, L.A., Sigahi, T.F., Rampasso, I.S., Leal Filho, W., & Anholon, R. (2024). Impacts of digitalization on operational efficiency in the banking sector: Thematic analysis and research agenda proposal. *International Journal of Information Management Data Insights*, 4(1), 100230, doi: 10.1016/j.jjimei.2024.100230.

Brenig, C., & Hildebtrandt, A. (2020). Money mules: The untapped weakness in the fraud chain. *Journal of Financial Crime,* 27(2), 419-435.

Chepkoech, F., & Rotich, G. (2017). Effect of risk management process on motor insurance fraud in Kenya. *International Journal of Social Science and Information Technology*, 3(3), 1934-1951

Christian, N., Basri, Y.Z., & Arafah, W. (2019). Analysis of fraud triangle, fraud diamond and fraud pentagon theory to detecting corporate fund in Indonesia. *The International Journal of Business Management and Technology*, 3(4), 1-6.

DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O.S. (2020). Financial fraud among older Americans: Evidence and implications. *The Journal of Gerontology: Series B,* 75(4), 1042-1059.

Dias-Oliveira, M., Ferreira, C., Morais, C., & Almeida, L.S. (2024). Academic dishonesty and the fraud diamond: An explanatory model. *SAGE Open,* 14(1).

Dimitriadis, E., & Kyrousi, A. (2023). Between firewals and feelings: Modelling trust and commitment in digital banking platforms. *Journal of Cybersecurity and Privacy*, 5(4), 845-862.

Eslamkhah, M., & Hosseini-Seno, S.A. (2019). Identifying and ranking knowledge management tools and techniques affecting organizational information security improvement. *Knowledge Management Research & Practice*, 17(3), 276-305.

Engels, C., Kumar, K., & Philip, D. (2020). Financial literacy and fraud detection. *The European Journal of Finance,* 26(4), 420-442

Galeazzo, A., & Furlan, A. (2019). Good problem solvers? Leveraging knowledge sharing mechanism and management support. *Journal of Knowledge Management*, 23(6), 1017-1038.

Garg, P., Gupta, B., & Chauhan, S. (2022). Consumer intention to adapt digital banking in India: Extending UTAUT 2 with security trust and privacy. *Journal of Financial Service Marketing*, 27(2), 79-95.

Goel, R.K. (2021). Masquerading the government: Drivers of government impersonation fraud. *Public Finance Review*, 49(4), 1-25

Handayani, R., Sutanto, J., & Purwanto, A. (2020). Trust role in acceptance of digital banking in Indonesia. *International Journal of Trade, Economics and Finance*, 11(5), 129-135.

Hoffmann, C., & Birnbrich, C. (2022). Synthetic identity fraud: A digital challenge for banking risk management. *Journal of Financial Regulation and Compliance,* 30(1), 115-130.

Kadoya, Y., Khan, M.S.R., & Yamane, T. (2020). The rising phenomenon of financial scams: Evidence from Japan. *Journal of Financial Crime*, 27(2), 387-396.

Kim, Y., Lee, S., & Choi, J. (2021). The impact of job insecurity on fraud: Evidence from the financial sector. *Journal of Financial Crime,* 28(3), 788-805.

Kocakulah, M., & Eser, Z. (2023). Mangerial discretion and opportunities for fraud in financial reporting. *International Journal of Accounting and Finance*, 12(2), 245-267.

Lai, P.C. (2021). Digital trust: the critical factor for the adoption of digital banking in developing countries. *International Journal of Electronic Finance*, 10(1), 23-37.

Laihonen, H., & Huhtamaki, J. (2020). Organisational hybridity and fluidity: Deriving new strategies for dynamic knowledge management. *Knowledge Management Research & Practice*, 1-13.

Mhlangga, D. (2020). Industry 4.0 in finance: the impact of artificial intelligence on digital financial inclusion. *International Journal of Financial Studies,*8(3), 45

Mintchik, N., & Riley, J. (2019). Rationalizing fraud: how thinking like a crook can help prevent fraud. *The CPA Journal*, 89(3), 44-50.

Mohammed, A.B., Al-Okaily, M., Qasim, D., & Al-Majali, M.K. (2024). Towards an understanding of business intelligence and analytics usage: Evidence from the banking industry. *International Journal of Information Management Data Insights*, 4(1), 100215.

Mulia, D. (2023). The differences in risk perception between millennials and baby boomers in online transactions. *Jurnal Manajemen*, 23(3), https://doi.org/10.24912/jm.v23i3.570

Naimi-Sadigh, A., Asgari, T., & Rabiei, M. (2022). Digital transformation in the value chain disruption of banking services. *Journal of Knowledge Economy*, 13(1), 1212-1242.

Nasi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime victimization and polyvictimisation in Finland – prevalence and risk factors. *European Journal on Criminal Policy and Research,* 29(2), 283-301

Nawawi, A., & Salin, A.S.A.P. (2018). Internal control and employee's occupational fraud on expenditure claims. *Journal of Financial Crime*, 25(3), 891-906

Nguyen, T.H., & Huynh, T.L.D. (2020). The roles of perceived risk and trust on e-banking adoption: Evidence from Vietnam. *International Journal of Electronic Finance*, 27(2), 79-95.

Nugroho, F., & Situmorang, Z. (2023). Internet banking adoption in Indonesia: TAM extension with the moderation role of customer knowledge and trust. *Jurnal Akuntansi, Keuangan dan Bisnis*, 16(1), 33-45.

Oktaviani, M. & Prasetyo, R.E. (2024). The influence of perceived risk on digital banking is on

customer intention to use digital banks in Jabodetabek. *Jurnal Integrasi Sains dan Media*, 2(1), 55-63

Puspitasari, I.N., & Hermawan, A. (2021). Fraud triangle in banking industry: Evidence from Indonesia. *Journal of Financial Crime*, 28(3), 935-946.

Rahi, S., Ghani, M.A., & Alnaser, F.M. (2017). Adoption of internet banking: Extending the role of technology acceptance model with e-customer service and customer satisfaction. *World Applied Science Journal*, 35(9), 1918-1924.

Reintstein, A., Taylor, E.Z. (2017). Fences as controls to reduce accountants' rationalization. *Journal of Business Ethics*, 141(3), 477-488

Ristiana, A., Mukhtar, S., & Sariwulan, R.T. (2024). Factors influencing academic fraud are based on the fraud diamond theory of economics education students at Jakarta State University. *International Journal of Economy, Education and Entrepreneurship,* 4(2).

Sari, D.N., & Rahman, I. (2023). Fraud intent in Indonesian banking industry: an Empirical study of employee and consumer behavior. *Jurnal Ilmiah Manajemen dan Akuntansi Retail*, 4(2), 112-125

Suhartanto, D., Wibisono, D., & Triyuni, N.N. (2022). Trust and customer loyalty in digital banking: Evidence from Indonesia. *Journal of Asian Finance, Economcs and Business*, 9(2), 197-205

Thasleena, K.F., & Santhi, P. (2025). Generational divide in digital banking: Caomparing experience and expectation across Generation X,Y, and Z. *Indian Journal of Information Sources and Sevices*, 15(2), 268-274, https://doi.org/10.51983/ijiss-2025.IJISS.15.2.34

Van Scotter, J.R., & Roglio, K.D.D. (2020). CEO bright and dark personality: Effects on ethical misconduct. *Journal of Business Ethics,* 164(3), 451-475.

Van Vlasselaer, V., Eliassi-Rad, T., Akoglue, L., Snoeck, M., & Baesens, B. (2021). Mining behavioral patterns for credit card fraud detection. *Expert System with Application*, 173, 114765.

Vuori, V., Helander, N., & Maenpaa, S. (2019). Network level knowledge sharing: Leveraging riege's model of knowledge barriers. *Journal of Knowledge Management*, 21(1), 57-70.

Wang, Y., & Dincelli, E. (2021). Anonymity, trust, and fraud behavior in digital banking. *Computer in Human Behavior Reports*, 4, 100127.

Wood, B.P., Eid, R., & Agag, G. (2021). A multilevel investigation of the link between ethical leadership behavior and employee's green behavior in the hospitality industry. *International Journal of Hospitality Management*, 97, 102993.

Yang, M., & Chen, Y. (2023). Cognitive rationalization in occupational fraud: structure exploration and scale development. *Frontiers in Psychology*, 14, 1112127 https://doi.org/10.3389/fpsyg.2023.1112127

Yasa, I.N.N.K., Suparna, G., & Astawa, I.N. (2021). The effect of digital banking trust on customer satisfaction and loyalty. *Jurnal Ventura: Jurnal Ekonomi dan Bisnis*, 24(1), 67-75.