Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

June 2026. Vol. 5. No. 3; e-ISSN: 2808-4519

Customers' Loss of Confidence in Banking Security Systems: A Case Study of the Loss of BRI Customers' Funds

Aisyah Safitri[1]*, Sitti Nur Aini[2], Moh. Ali Fajar Sidiq[3], Achmarul Fajar[4*]

[1,2,3,4]*Department of Management, University of Madura, Madura, Indonesia*
aisyahsafitri355@gmail.com[1], azkaroliaini@gmail.com[2], sidiqaliffajar@gmail.com[3], fajar@unira.ac.id[4*]

Abstract

The phenomenon of customer funds going missing in the banking sector, particularly in the case of Bank Rakyat Indonesia (BRI), has raised concerns about the security of the digital banking system and has led to a decline in public confidence. This study aims to analyse the crisis of customer confidence in banking security systems by examining influencing factors, such as cyber risk, risk perception, and the role of social media. The research method employed is a qualitative approach using case studies, utilising secondary data obtained from academic journals, institutional reports, and case documentation. The research findings indicate that the loss of customer funds is influenced by vulnerabilities in digital security systems and the rise in cybercrime, such as phishing and social engineering. Furthermore, these incidents have led to a decline in customer trust, a trend exacerbated by the dissemination of information via social media. This study concludes that the crisis of customer trust is caused not only by technical factors, but also by risk perceptions and the dynamics of public information. Therefore, improvements in banking system security, strengthened consumer protection, and effective communication strategies are required to maintain customer trust.

Keywords: *customer trust; banking security; cyber risk; social media; digital banking*

1. Introduction

The phenomenon of customer funds going missing in the banking sector has once again come to public attention following a case involving Bank Rakyat Indonesia (BRI) that went viral on social media. This case highlights vulnerabilities in the banking security system that have a direct impact on customer confidence. According to the Bank for International Settlements (BIS, 2021), incidents of fund loss in modern banking systems are generally caused by a combination of weaknesses in security systems and exploitation by external parties. This situation indicates that although the banking sector has adopted digital technology, the risks to the security of customer funds remain significant.

In the context of digital security, threats to banking systems are becoming increasingly complex as technology advances. Research by Krombholz et al. (2015) in ACM Computing Surveys explains that attacks on digital financial services are often carried out using phishing, malware and social engineering techniques that target users. Furthermore, Böhme and Moore (2012) emphasise that authentication systems based on one-time passwords (OTPs) and telephone numbers have vulnerabilities that can be exploited by cybercriminals. This demonstrates that the security of banking systems depends not only on internal technology, but also on user behaviour and the security of the digital ecosystem as a whole.

On the other hand, customer trust is a key factor in the sustainability of the banking industry. Mayer, Davis, and Schoorman (1995) define trust as an individual's willingness to accept vulnerability based on expectations of another party. In the context of financial services, Gefen et al. (2003) state that trust has a significant influence on the use of technology-based services. Consequently, incidents of customer funds being lost have the potential to reduce public trust in banks and drive changes in customer behaviour, such as a desire to switch banks or reduce the use of digital services.

Globally, the digitalisation of banking has brought benefits in terms of efficiency and ease of access, but has also increased exposure to security risks. The World Bank (2022), in its report on Financial Consumer Protection and Digital Finance, states that the growth of digital financial services is accompanied by an increase in cyber risks that could affect the stability of the financial system. Furthermore, Arner, Barberis, and Buckley (2016) emphasise that the development of fintech requires adaptation in regulation and consumer protection to address emerging risks.

Although various studies have addressed banking system security and risk management, most still focus on technical aspects and have not comprehensively linked real-world incidents to perceptions of customer trust or the influence of social media in shaping public opinion. Kim, Ferrin, and Rao (2008) demonstrate that research on trust in digital services still has limitations in integrating actual risk factors with user perceptions. Consequently, there is a research gap in understanding the relationship between banking security incidents, customer trust, and information dynamics in the digital age.

In light of this, this study aims to analyse the crisis of customer trust in banking security systems through a case study of the loss of customer funds, as well as to examine the relationship between system security, risk perception and customer behaviour in the context of digital banking. It is hoped that this study will contribute to the development of research on banking security and customer trust, and serve as a reference for financial institutions in improving consumer protection systems.

2. Literature Review

2.1. Customer Trust

Trust is a crucial aspect of the relationship between customers and banking institutions. Mayer, Davis and Schoorman explain that trust is a person's willingness to accept risk based on the belief that the other party will act as expected. In the context of banking , customers entrust their funds and personal data to the bank; consequently, trust forms the cornerstone of the ongoing relationship between customers and the bank.
Gefen, Karahanna and Straub state that, in technology-based services, trust plays a key role in shaping users' intention to continue using digital services. This means that when customers feel that a bank's digital services are secure, trustworthy and capable of protecting their interests, they are more likely to continue using those services.

2.2. Digital Banking Security Systems

Digital banking makes it easier for customers to carry out transactions, but it also presents more complex security risks. Krombholz et al. explain that digital attacks can be carried out through social engineering, phishing, malware and psychological manipulation of users to gain access to sensitive data. In cases where customers' funds are lost, this risk is particularly relevant as criminals often exploit technological vulnerabilities and user negligence.
Furthermore, research on the adoption of mobile banking indicates that security, risk, institutional trust and trust in technology are key factors in the use of digital banking services. Consequently, system security is understood not only as technical protection, but also as a factor that shapes customers' perceptions of whether banking services are secure or not.

2.3. Cyber Risks And Customer Perception of Risk

Cyber risks in digital financial services can influence customers' perceptions of a bank's security. Kim, Ferrin and Rao explain that trust and risk perception influence consumers' decisions regarding the use of electronic services. If perceived risk increases, user trust tends to decline, leading to a decision to avoid or abandon the service.
In the context of digital banking, perceived risk—or the risk as perceived by customers—can arise in the event of lost funds, data breaches, unauthorised transactions, or negative media coverage. Consequently, perceptions of risk are shaped not only by personal experience but also by information circulating in the public domain.

2.4. Consumer Protection in Banking

Consumer protection is a key aspect of the financial services sector, as customers are in a vulnerable position in the event of a dispute or loss. The World Bank states that the increasing use of digital financial services also heightens risks for consumers and creates a need for stronger consumer protection policies.
In Indonesia, consumer protection in the financial services sector is regulated by POJK No. 22 of 2023 on Consumer and Public Protection in the Financial Services Sector. This regulation emphasises the importance of consumer protection in line with the development of the digitalisation of financial products and services.

2.5. Social Media and The Crisis of Trust

Social media plays a major role in shaping public opinion regarding banking cases. When cases of lost customer funds go viral, information can spread rapidly and influence public perception, including that of customers who have not been directly affected by the incident. In this context, social media can exacerbate a crisis of confidence, as the public judges banks not only on the basis of personal experience, but also on the basis of narratives circulating online.
Research on fintech indicates that the development of digital financial services has heightened concerns regarding security and trust in banking services. This literature review also confirms that issues of trust and security remain a key focus in understanding the behaviour of users of digital financial services.

2.6. Previous Research

Several previous studies have shown that trust, security and risk are closely linked to the use of digital services. Mayer et al. emphasise that trust is related to a willingness to accept risk. Gefen et al. demonstrated that trust influences the intention to use digital services. Kim et al. showed that risk perception and trust influence consumer decisions regarding electronic services. Meanwhile, Krombholz et al. explained that digital attacks such as phishing and social engineering pose a real threat to technology-based systems.

However, these studies generally still discuss trust, risk and security in general terms. There have not yet been many studies that specifically link actual cases of customer fund losses, crises of trust and the role of social media within the context of the Indonesian banking sector. Therefore, this study aims to fill this gap by using the case of the loss of BRI customer funds as a case study.

2.7. Theoretical Framework

Based on this literature review, it is clear that the crisis of customer confidence is influenced by several factors, namely the security of the banking system, cyber risks, risk perception, consumer protection, and social media coverage. When security systems are perceived as weak and cases of lost funds go viral, public risk perception increases. This heightened perception of risk can erode customer trust and lead to behaviours such as switching banks, reducing the use of digital services, or withdrawing funds from accounts.

3. Research Method

3.1. Type and Research Approach

This study employs a qualitative approach using the case study method. The qualitative approach was chosen because this study aims to gain an in-depth understanding of the phenomenon of a crisis of customer trust based on real-life cases. According to Creswell (2014), qualitative research is used to explore and understand the meaning of a social phenomenon or human issue.
The case study method was used to conduct an in-depth analysis of the disappearance of customer funds as a specific phenomenon within the context of digital banking. Yin (2018) states that case studies are well-suited to investigating contemporary phenomena in real-life contexts, particularly when the boundaries between the phenomenon and its context are not clearly defined.

3.2. Data Types and Sources

This study utilises **secondary data** obtained from various sources, including:
1.Scientific journals relevant to the topics of trust, banking security, and cyber risk
2.Reports from international institutions such as the World Bank, BIS, and OECD
3.Reliable news regarding the case of missing BRI customer funds
4.Official regulations such as OJK regulations regarding consumer protection

According to Sugiyono (2019), secondary data is a data source that does not provide data directly to the data collector, but rather through documents or other relevant sources.

3.3. Data Collection Techniques

Data collection techniques in this study were carried out through:
1. **Literature Review**
   Data collection was carried out by reviewing various literature such as journals, books, and previous research reports relevant to the research topic.
2. **Documentation**
   Data was also obtained through documentation in the form of news reports and case studies relating to the loss of customer funds. According to Bowen (2009), document analysis is a systematic method for reviewing and evaluating documents, whether in printed or electronic form.

3.4. Data Analysis Techniques

The data analysis technique used is qualitative descriptive analysis. The data collected was analysed as follows:
1. Data reduction → selecting data relevant to the research focus
2. Data presentation → organising the data into a systematic narrative
3. Drawing conclusions → interpreting the results of the analysis

Miles and Huberman (1994) state that qualitative data analysis consists of three main stages, namely data reduction, data presentation, and drawing conclusions.

3.5. Data Validity

To ensure the validity of the data, this study employs source triangulation, which involves comparing data from various sources such as journals, official reports and news articles.
According to Patton (1999), triangulation is a technique for enhancing the credibility of data by utilising various sources of information.

4. Research Results

An analysis of various secondary data sources has revealed that cases of customer funds going missing in the banking sector, particularly at Bank BRI, are influenced by several key factors, namely vulnerabilities in digital security systems, the rise in cybercrime, and weaknesses in customer data protection. These cases demonstrate that, despite the banking system's use of advanced digital technology, there are still loopholes that can be exploited by unscrupulous parties.

Furthermore, the research findings also indicate that the incident had a direct impact on a decline in customer confidence. This is evident from the public's growing concerns regarding the security of their funds, as well as a tendency to consider switching to another bank or reducing their use of digital banking services.
On the other hand, the role of social media in disseminating information regarding this case has been significant. Viral information has accelerated the spread of risk perceptions within the public, thereby amplifying the psychological impact on customers, even for those who were not directly affected by the incident.

5. Discussion

5.1. Analysis of Banking System Security

Research findings indicate that the security of banking systems still faces significant challenges in the digital age. These findings are consistent with the research by Krombholz et al. (2015), which states that cyberattacks such as phishing and social engineering pose a major threat to digital financial systems. This suggests that vulnerabilities lie not only in the technological systems themselves, but also in the interaction between the systems and users.
Furthermore, vulnerabilities in authentication systems, such as the use of phone-based OTPs, represent a key weakness that criminals can exploit. Consequently, banking security must be viewed holistically, encompassing technological, human and operational aspects.

5.2. A Crisis of Customer Trust

Based on the theory of trust put forward by Mayer et al. (1995), trust is formed from perceptions of an institution's competence, integrity, and goodwill. In cases of customer funds being lost, all three of these aspects can be compromised, thereby triggering a crisis of trust.
The findings of this study are also consistent with those of Gefen et al. (2003), who state that trust is a key factor in the use of digital services. When customers feel that the banking system is not secure, their trust diminishes, which in turn affects their behaviour regarding the use of these services.

5.3. The Influence of Social Media on Risk Perception

Social media acts as a catalyst in accelerating the spread of information and shaping public opinion. In this case, the viral nature of news regarding the loss of customer funds increased risk perception among the public.
These findings support the research by Kim et al. (2008), which states that risk perception can be influenced by external information, including news reports and public opinion. Thus, social media serves not only as a means of communication, but also as a factor that can exacerbate a crisis of confidence.

5.4. Implications for Customer Behaviour

A decline in trust and an increased perception of risk lead to changes in customer behaviour. Customers tend to:
1. Reduce their use of digital services
2. Exercise greater caution when transacting
3. Consider switching to another bank

This is consistent with theories of digital consumer behaviour, which state that decisions regarding the use of services are heavily influenced by levels of trust and perceptions of risk.

5.5. Implications For Banking Institutions

The results of this study indicate that banks need to:
1. Enhance digital security systems
2. Strengthen customer data protection
3. Improve transparency and communication with the public
4. Manage reputation crises on social media swiftly and effectively

According to the World Bank (2022), consumer protection and system security are key factors in maintaining the stability of the financial sector in the digital age. Therefore, banks are not only required to be innovative but must also be able to maintain public trust.

6. Summary of Discussion

Based on the findings and discussion, it can be concluded that the crisis of customer trust is not caused solely by incidents of lost funds, but also by the interplay between weaknesses in security systems, perceptions of risk, and the influence of social media.
This finding reinforces the view that in the era of digital banking, customer trust is becoming increasingly vulnerable as it is influenced by rapidly evolving technological and informational factors.

7. Conclusion

Based on the findings of the research and the discussion, it can be concluded that the phenomenon of customer funds going missing in the banking sector, particularly in the case of Bank BRI, reflects serious challenges within the digital banking security system. Although banking technology has advanced rapidly, there are still vulnerabilities that can be exploited by cybercriminals, such as through phishing, social engineering and weaknesses in authentication systems.

Furthermore, the incident has had a significant impact on a decline in customer confidence. Trust, as the cornerstone of the banking industry, is undermined when customers feel that the system is unable to protect their funds and data effectively. This decline in confidence is further exacerbated by the spread of information via social media, which accelerates the formation of perceptions of risk within the public.
Furthermore, this study shows that the crisis of confidence is influenced not only by technical security factors, but also by risk perceptions and the dynamics of public information. These three factors are interrelated and contribute to shaping customer behaviour, such as increased vigilance, reduced use of digital services, and a tendency to switch banks.
Thus, it can be asserted that in the era of digital banking, the success of banking institutions is determined not only by technological innovation, but also by the ability to maintain system security and customer trust on an ongoing basis.

8. Recommendations

Based on the findings of the study, banking institutions are expected to comprehensively enhance their digital security systems, covering technological aspects, operational procedures and customer education regarding the risks of cybercrime. Banks also need to strengthen their early detection systems for suspicious activity and improve transparency in handling cases of lost customer funds, so as to maintain public confidence.
In addition, regulators such as the Financial Services Authority (OJK) and the government are expected to strengthen oversight of the implementation of digital security in the banking sector and update consumer protection regulations to make them more responsive to the evolution of cybercrime in the digital age. Strengthening policies relating to personal data protection and digital transaction security is also crucial to minimising the risk of customer losses.
Customers are also expected to increase their awareness and vigilance when using digital banking services, such as safeguarding the confidentiality of personal data, not sharing OTP codes with others, and being more cautious regarding the increasingly sophisticated methods of digital fraud.
For future researchers, this study is expected to serve as a reference in developing research on digital banking security and customer trust. Future studies may adopt a quantitative approach or expand the scope of the research to include several banks in order to obtain more comprehensive findings regarding the factors that influence customer trust in digital banking systems.

References

[1] Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.
[2] Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook (2nd ed.). SAGE Publications.
[3] Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40.
[4] Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90.
[5] Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce. Decision Support Systems, 44(2), 544–564.
[6] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. ACM Computing Surveys, 48(1), 1–36.
[7] Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organisational trust. Academy of Management Review, 20(3), 709–734.
[8] Bank for International Settlements. (2021). Principles for operational resilience. https://www.bis.org/publ/bcbs240.htm
[9] World Bank. (2022). Financial consumer protection and digital finance. https://openknowledge.worldbank.org/handle/10986/36750
[10] Financial Services Authority. (2023). Financial Services Authority Regulation No. 22 of 2023 on Consumer and Public Protection in the Financial Services Sector. https://peraturan.bpk.go.id/Details/302699/peraturan-ojk-no-22-tahun-2023