Journal of Theoretical and Applied Information Technology
15th May 2024. Vol.102. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STRENGTHENING PAYMENT CARD DATA SECURITY: A STUDY ON COMPLIANCE ENHANCEMENT AND RISK MITIGATION THROUGH MFA IMPLEMENTATION UNDER PCI DSS 4.0

PIETERS NICHOLAS PARADONGAN TAMBUNAN[1], NILO LEGOWO[2], DENNIS RYDARTO TAMBUNAN[3]

[1]Information System Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Jakarta, Indonesia 11480

[2]Information System Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Jakarta, Indonesia 11480

[3]Faculty of Economics, Dehasen University Bengkulu, Bengkulu, Indonesia

E-mail: [1]pieters.tambunan@binus.ac.id, [2]nlegowo@binus.edu, [3]tambunandennis376@gmail.com

ABSTRACT

The increasing use of electronic payments and the growing reliance on payment card transactions have underscored the importance of robust security measures to protect payment card data. The Payment Card Industry Data Security Standard (PCI DSS) has long been recognized as a crucial framework for ensuring security and compliance in handling payment card data. Amidst evolving cyber threats, the adoption of Multi-Factor Authentication (MFA) has emerged as a critical strategy to enhance the security of payment card data, improve compliance with PCI DSS 4.0, and mitigate associated risks. This study involves payment gateway organizations subject to PCI DSS 4.0 compliance requirements. Qualitative data confirms the effectiveness of MFA in thwarting cyber threats and enhancing overall payment card data security. In an era marked by evolving cyber threats, this research emphasizes the importance of implementing MFA to bolster payment card data security, achieve compliance with PCI DSS 4.0, and mitigate risks. The findings of this study offer actionable insights for organizations seeking to strengthen their payment card data security measures and align with regulatory standards.

Keywords: *Payment Card Data Security, PCI DSS 4.0, Multi-Factor Authentication (MFA), Compliance Enhancement, Risk Mitigation.*

1. INTRODUCTION

In today's increasingly interconnected and digital world, information systems play a critical role in the operations of companies across various industries, especially those involved in finance. These systems store critical data, sensitive information, and intellectual property that are vital for business continuity. However, the rapid expansion of technology has also opened doors to a myriad of security threats and vulnerabilities. To protect these invaluable assets, organizations must prioritize information system security and risk management [1].

While technology has brought numerous benefits, it also makes us vulnerable to various security threats and vulnerabilities. These threats pose significant risks to individuals, organizations, and even nations, underscoring the importance of understanding and mitigating them. The swift pace of technological advancements has led to the creation of sophisticated systems, networks, and devices that empower us in unprecedented ways. From the Internet of Things (IoT) to cloud computing and artificial intelligence, these innovations have transformed industries and enriched our lives. However, with great technological advancements comes great responsibility, as these advancements also introduce new avenues for malicious actors to exploit. Technological security threats encompass a range of malicious activities and potential hazards that can compromise the confidentiality, integrity, and availability of digital assets [2].

Every company needs something to secure their assets, which is why the introduction of Multi-Factor Authentication (MFA) has emerged as a crucial tool in combating cyber security threats. MFA is a security mechanism that requires users to provide two or more authentication factors from different categories before gaining access to a system. These categories typically include something the user knows (e.g., a password), something the user has (e.g., a smart phone or token), and something the user is (e.g., biometric data such as fingerprints or facial recognition). MFA significantly enhances the security of information systems by adding an additional layer of protection beyond traditional single-factor authentication methods, which often rely solely on usernames and passwords [3].

MFA is critically important for fintech, especially Payment Gateway Companies. As the financial backbone of e-commerce and digital payments, payment companies handle sensitive financial information, making them prime targets for cyber-attacks. Payment gateway companies act as intermediaries between customers, merchants, and financial institutions, facilitating the authorization and processing of online payments. These intermediaries enable smooth fund transfers, supporting various payment methods such as credit cards, digital wallets, and cryptocurrencies. In doing so, they bridge consumers and businesses, driving the growth of e-commerce and digital financial inclusion [4].

In the ever-evolving digital financial landscape, payment gateway companies play a critical intermediary role in facilitating secure online transactions. These companies handle sensitive financial data daily, making them prime targets for cyber-attacks. To address these security challenges, compliance with the Payment Card Industry Data Security Standard (PCI DSS) is crucial [5]. This introduction delves into the technological security threats and vulnerabilities faced by payment gateway companies and highlights the crucial role of Multi-Factor Authentication (MFA) in meeting PCI DSS requirements and enhancing overall security. The critical role played by payment gateway companies in managing financial transactions makes them attractive targets for malicious actors seeking security weaknesses. This research project aims to address the increasingly important issue of information system security and risk management by exploring the implementation and evaluation of Multi-Factor Authentication (MFA). Its primary goal is to enhance awareness and understanding of the effectiveness of MFA in reducing security risks and protecting critical data [6].

2. LITERATURE REVIEW

2.1 Information Systems Security

Information System Security is the practice of protecting information by mitigating information risks. It involves implementing a series of strategies, technologies, and best practices to protect data and information systems from unauthorized access, disclosure, disruption, modification, or destruction. Information System Security is a crucial aspect of modern organizations, as the proliferation of digital data and reliance on information technology make organizations vulnerable to a variety of threats and cyber risks. Effective information security measures are essential for protecting sensitive data, maintaining business continuity, and safeguarding the organization's reputation [7].

Key aspects and principles of Information System Security include Confidentiality, Integrity, and Availability (CIA). The CIA triad is the foundation of information security, emphasizing the protection of confidentiality, integrity, and availability of data. Information System Security also addresses threats and vulnerabilities by understanding the various threats (e.g., malware, insider threats) and vulnerabilities (e.g., outdated systems) that can jeopardize security. Information System Security also requires Authentication to verify the identity of users or systems to ensure that only authorized entities gain access to resources. In addition, Authorization is necessary to determine what actions or resources an authenticated user or system is allowed to access or perform [8].

2.2 PCI DSS 4.0

PCI DSS stands for Payment Card Industry Data Security Standard. It is a set of security standards designed to ensure the secure handling of payment card data. PCI DSS was developed by major credit card companies, including Visa, MasterCard, American Express, Discover, and JCB, to establish a common framework for organizations that process, store, or transmit payment card information. The primary goal of PCI DSS is to protect sensitive cardholder data from theft, fraud, and unauthorized access. The standard provides specific requirements and best security practices that organizations must follow to achieve compliance [9].

The PCI Security Standards Council (PCI SSC) published the PCI Data Security Standard (PCI DSS) version 4.0 on March 31, 2022. PCI DSS is a global standard that sets the baseline of technical and operational standards for protecting account data. PCI DSS v4.0 replaces version 3.2.1 of PCI DSS to better address emerging threats and technologies and provide innovative ways to combat new threats. The latest standard and a Summary of Changes can be found and reviewed on the PCI SSC website. The updates to PCI DSS v4.0 aim to meet the increasing security needs within the payment industry, promote security as an ongoing process, enhance flexibility, and improve procedures for organizations using different methods to achieve their security objectives. PCI DSS (Payment Card Industry Data Security Standard) is a global standard that establishes the technical and operational criteria for protecting payment data [10].

2.3 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security process that requires users to provide two or more different authentication factors to verify their identity before they can access a system, application, or online account. MFA adds an extra layer of security beyond traditional username and password authentication, making it more difficult for unauthorized users to gain access. The requirements for MFA apply to all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and cover both direct access to the network or entity's systems as well as web-based access to applications or functions. MFA for remote access to the Cardholder Data Environment (CDE) can be implemented at the network or system/application level; it is not necessary to apply it at both levels. For example, if MFA is used when a user connects to the CDE network, MFA does not need to be used again when the user logs into any system or application within the CDE [11].

The aim of Multi-Factor Authentication (MFA) is to enhance the level of confidence in the identity of someone accessing a resource. To achieve this, MFA employs a layered authentication approach that requires an individual to present at least two of the three authentication factors to gain access to the resource. In accordance with PCI DSS Requirements, the three authentication factors are something the user knows (such as a password), something the user has (such as a security key), and something biometric (such as a fingerprint) [12].

2.4 Risk Management

Risk Management is a systematic process for identifying, assessing, prioritizing, and mitigating risks to an organization or project to achieve its objectives while minimizing potential negative impacts. It is a fundamental practice in business, finance, project management, and many other areas where uncertainty and potential threats exist. The main goal of risk management is to make informed decisions about how to address risks to reduce potential losses or to capitalize on potential opportunities [13].

Within the context of PCI DSS (Payment Card Industry Data Security Standard), Risk Management refers to the systematic process of identifying, assessing, prioritizing, and mitigating risks related to payment card data security. PCI DSS is a set of security standards designed to protect sensitive payment card information and applies to organizations that handle, process, or store such data. Organizations are required to conduct risk assessments to identify potential threats and vulnerabilities that could affect the security of payment card data. These assessments help in understanding the potential impact and likelihood of risks that may occur.

2.5 Awareness and Training

Information Security (IS) awareness and training are critical components of an organization's cybersecurity strategy. It involves providing knowledge to employees, contractors, and other relevant parties about the importance of information security and equipping them with the knowledge and skills to identify, mitigate, and respond to security threats effectively. The goal is to create a security-conscious culture within the organization and empower individuals to play an active role in protecting sensitive information.

PCI DSS (Payment Card Industry Data Security Standards) awareness and training are essential aspects of achieving and maintaining compliance with the standards. PCI DSS requires that organizations handling payment card data implement training and awareness programs to ensure that employees and related personnel understand their roles and responsibilities in protecting payment card information.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. RESEARCH METHODS

This research adopts a qualitative research design method. Its aim is to provide a comprehensive assessment of the implementation of Multi-Factor Authentication (MFA) in payment gateway organizations subject to PCI DSS 4.0 compliance. The focus of this study will be on payment gateway companies, as PCI DSS 4.0 is designed to ensure secure handling and transmission of payment card data. Payment gateways act as intermediaries processing credit card transactions on behalf of merchants. They handle sensitive customer data during these transactions. Compliance with PCI DSS helps protect this data from breaches and theft.

3.1 Data Collection Methods

In order to gain a deeper understanding of Multi-Factor Authentication (MFA) implementation, this research will utilize a qualitative approach. Data will be collected through in-depth interviews with key stakeholders from a selection of organizations previously surveyed. These organizations will be purposively chosen based on their unique experiences in implementing MFA, as reflected in their previous survey responses. Qualitative data obtained from interviews will be analyzed using thematic analysis method, allowing for the identification of key themes and extraction of meaningful narratives.

3.2 Data Analysis Method

To enhance the validity of findings, triangulation is conducted by comparing and contrasting data obtained from surveys and interviews. This approach helps ensure that the results are consistent and reliable. Qualitative research techniques using both non-PCI DSS and PCI DSS 4.0 perspectives are applied during the interview phase. Staff checks are implemented during the interview stage. After conducting interviews, employees are given the opportunity to review and validate interview transcripts. This iterative process ensures that the data accurately reflect their views and experiences. The researcher also ensures that a comprehensive data audit trail is maintained throughout the research process. This includes detailed records of survey distribution and response rates, interview transcripts, and data analysis procedures. This audit trail not only facilitates transparency but also enables future researchers to track the steps taken in data collection and analysis, thereby contributing to the overall study's auditability and replicability.

3.3 Review and Data Validation

Quantitative data will be analyzed using Narrative Synthesis, where related themes and narratives are synthesized to develop a comprehensive understanding of qualitative findings. Representative quotes from interviews will be included to illustrate and support key insights to estimate the relationship between MFA implementation and PCI DSS compliance. This will provide a data analysis on why PCI DSS 4.0 needs to be implemented in many companies, especially in payment gateway companies. Qualitative findings will be scrutinized to ensure alignment with the research objectives. Narratives will be evaluated for relevance to the main research questions.

To enhance the validity of findings, triangulation is conducted by comparing and contrasting data obtained from surveys and interviews. This approach helps ensure that the results are consistent and reliable. Qualitative research techniques using both non-PCI DSS and PCI DSS 4.0 perspectives are applied during the interview phase. Staff checks are implemented during the interview stage. After conducting interviews, employees are given the opportunity to review and validate interview transcripts. This iterative process ensures that the data accurately reflect their views and experiences. The researcher also ensures that a comprehensive data audit trail is maintained throughout the research process. This includes detailed records of survey distribution and response rates, interview transcripts, and data analysis procedures. This audit trail not only facilitates transparency but also enables future researchers to track the steps taken in data collection and analysis, thereby contributing to the overall study's auditability and replicability.

4. RESULT AND DISCUSSION

4.1 Adoption of MFA and PCI DSS Compliance in Companies

The company has made every effort to maintain the security of its information systems, yet many companies remain targets of attacks by irresponsible parties. One such incident occurred in 2022, where Bank Indonesia became aware of hacking attempts in the form of ransomware. There were 16 folders containing various types of data, ranging from the public's savings positions in rupiah, foreign exchange (forex) from commercial banks, to receipts. This ransomware, known as Conti, is operated by the Wizard Spider hacker group. They are based in Russia and have been targeted by Europol, Interpol, the FBI, and the UK's National Crime Agency. This malware can steal or lock victims' data until a ransom is paid. Typically, the ransom is paid with cryptocurrencies such as Bitcoin. If not paid, the hacked data and systems will be rendered unusable and ultimately destroyed. To date, it is unknown if the hackers also demanded a ransom from Bank Indonesia [13].

A company requires validated standards in maintaining the security of its information systems. According to the PCI DSS survey results, there is a positive correlation between the implementation of Multi-Factor Authentication (MFA) and compliance with the PCI DSS 4.0 standards among surveyed organizations. Out of 150 surveyed organizations, 85% reported implementing MFA as part of their security protocols. Of this number, 92% showed higher compliance rates with PCI DSS 4.0 compared to organizations that did not adopt MFA. One example is a Payment Gateway company, which adheres to the PCI DSS 4.0 standards as security guidelines for the information systems they use. With the assistance of PCI DSS 4.0, Payment Gateway companies become more compliant with regulations set by Bank Indonesia as Payment Gateways.

Multi-Factor Authentication (MFA) serves the fundamental purpose of instilling a heightened sense of assurance regarding the identity verification of individuals seeking access to various resources, spanning from physical locations and computing devices to networks and databases. By incorporating multiple layers of authentication mechanisms, MFA effectively erects barriers that unauthorized users must navigate through in order to obtain access privileges. Within the domain of information security, the PCI DSS 4.0 document stands as a comprehensive guide delineating the foundational principles and widely accepted best practices pertaining to multi-factor authentication. Designed to cater to organizations at every stage of their journey, whether it involves evaluating, implementing, or enhancing MFA solutions, PCI DSS 4.0 serves as an indispensable resource for both entities and solution providers vested in fortifying their authentication protocols.

4.2 Impact of MFA on Risk Mitigation

The implementation of Multi-Factor Authentication (MFA) has emerged as a crucial step in significantly enhancing risk mitigation strategies among surveyed organizations. One such example is a Payment Gateway company in Indonesia, where respondents consistently emphasized that MFA played a crucial role in strengthening their defenses against unauthorized access to payment card data. The effectiveness of MFA in preventing unauthorized access to systems and sensitive data is evident from the responses of key stakeholders. By requiring multiple factors for authentication, including something known to the user (e.g., password) and something owned by the user (e.g., mobile device), MFA creates a robust barrier for potential attackers. This additional layer of security ensures that even if one factor is compromised, the risk of a security breach remains significantly reduced. The following is an explanation of MFA from the PCI DSS 4.0 standard, where passwords and other "something known" data must be difficult to guess or brute-force, and protected from disclosure to unauthorized parties. Furthermore, Biometric and other "something you are" data must be protected from replication or unauthorized use by others with access to the device where the data resides. After that, Smart cards, software certificates, and other "something you have" data should not be shared and must be protected from replication or ownership by unauthorized parties.

Interviewed participants reported a significant decrease in credential-based attacks, such as phishing and brute force attempts, after implementing MFA. The cases of compromised user credentials were much lower among organizations that had implemented MFA as part of their security protocols. Interviews with key stakeholders provided valuable insights into the impact of MFA implementation on risk mitigation. Respondents consistently highlighted that MFA significantly enhanced their organization's ability to

mitigate security risks associated with payment card data. One respondent stated, "The implementation of MFA drastically reduces the risk of unauthorized access to our payment processing systems. It is very difficult for criminals to compromise user accounts and gain access to sensitive data." MFA acts as a barrier to credential-based attacks that rely on stolen or guessed passwords. Even if attackers manage to obtain a user's password through phishing or other means, they still need access to the second authentication factor (e.g., mobile app or hardware token) to gain entry. The higher level of complexity for these attackers significantly reduces the success rate of attacks.

Companies like one Payment Gateway in Indonesia that implement MFA report an improvement in incident response capabilities. Timely detection of unusual login patterns and the ability to quickly identify and mitigate potential threats were recurring themes in interviews. MFA not only prevents unauthorized access but also enhances organizations' ability to detect and respond promptly to security incidents. These proactive efforts play a crucial role in reducing the impact of security breaches and minimizing potential data exposure. MFA fosters confidence among stakeholders in their risk mitigation strategies. Organizations feel more prepared to face security challenges and are better equipped to protect payment card data. Trust in risk mitigation strategies is a critical aspect of cybersecurity. When organizations feel confident in their security measures, they are more effective in responding to emerging threats and taking proactive steps to further enhance security. The role of MFA in strengthening this confidence cannot be underestimated, as it forms a strong foundation for risk mitigation efforts.

4.3 Compliance and Competitive Advantage

Although MFA has proven effective in enhancing security and compliance, respondents also shared challenges encountered during the implementation process. The most frequently mentioned challenges include user resistance to MFA adoption, complexity of integration with legacy systems, and the need for user education and training. One respondent from a Payment Gateway company in Indonesia commented, "Engaging our employees in MFA was a challenge initially. However, once they understood the importance of protecting patient payment data, the resistance decreased."

Research findings indicate that organizations complying with PCI DSS 4.0 standards, including implementing MFA, often gain competitive advantages in the market. Customers and partners view compliance as a sign of trust and commitment to data security. A respondent from one Payment Gateway company in Indonesia stated, "PCI DSS compliance, coupled with MFA, has opened up opportunities for us to collaborate with other financial institutions and acquire new customers prioritizing secure payment processing." Here is an exploration of some common authentication scenarios and considerations for multi-factor authentication provided by PCI DSS 4.0:

4.3.1 Scenario 1

An individual uses a set of credentials (password A) to log in to a device and also to access a software token stored on the device. Then, the individual establishes a connection to the CDE/corporate network, providing a different set of credentials (password B) and the OTP generated by the software token as authentication. The authentication system grants the requested access if both provided factors are valid:

- Something you know - Password B
- Something you have - Software token

Figure 1: Scenario 1

In Figure 1, to ensure the autonomy of the authentication factor remains intact, this scenario necessitates a software token ("something you have") embedded within a physical device in such a way that it cannot be duplicated or used on another device. Additionally, the physical security of the device becomes a security control to be verified as proof of device ownership. Conversely, if access to the software token is merely a reflection of the ability to log into the device (either locally or remotely),

the entire authentication process becomes a dual usage of "something you know."

4.3.2 Scenario 2

In this scenario, an individual uses a set of credentials (e.g., username/password or biometrics) to log into the device, and these credentials also grant access to a software token stored on the device. To initiate a connection to the CDE/corporate network, the user opens a browser window pre-filled with a different set of credentials (e.g., cached on the device or using a password manager) along with the software token.

Figure 2. Scenario 2

In Figure 2, it is explained that this scenario does not provide autonomy between authentication factors because one set of credentials (Password A) grants access to both factors (Password B and software token).

4.3.3 Scenario 3

In this scenario, an individual uses a set of credentials (e.g., username/password) to log into the computer. Connecting to the CDE/corporate network requires an initial set of credentials and an OTP generated by the software token on the mobile device.

Figure 3. Scenario 3

In Figure 3, it is explained that although the individual uses the same password (something we know) to authenticate to the laptop and the CDE/corporate network, the software token on the mobile device provides the second factor (something you have) that maintains autonomy between the authentication mechanisms. If the mobile device is also used to initiate the connection to the CDE/corporate network, additional security controls will be required to demonstrate the autonomy of the authentication mechanism.

4.3.4 Scenario 4

In this scenario, an individual uses multi-factor authentication (e.g., password and biometric) to log into a smartphone or laptop. To establish a non-console connection to the CDE/corporate network, the individual then provides one factor of authentication (e.g., a different password, a digital certificate, or a signed challenge response).

Figure 4. Scenario 4

In Figure 4, it is explained that the device (smartphone or laptop) must be fortified and controlled to ensure that multi-factor authentication is implemented correctly and consistently before initiating a connection to the CDE/corporate network. This includes ensuring that users cannot modify or disable security configurations, such as bypassing or disabling multi-factor authentication, and that the autonomy of authentication factors is maintained. Additionally, additional controls may be required to prevent unauthorized parties from gaining constructive "trust" usage between the device and the CDE/corporate network. An example of constructive usage is malicious users running processes on a device that allows them to interact with the CDE/corporate network without knowing the password or biometrics used by legitimate users. If users manage their own devices — for example, in a BYOD environment — user-managed devices must maintain a strong and isolated execution environment (such as TEE, SE, or TPM) that cannot be influenced or bypassed by users. If not, organizations will not have assurance that MFA is properly implemented and enforced on these devices.

4.4 Recommendations

Respondents emphasize the importance of continuous education and training programs for users. While MFA enhances security, its effectiveness depends on users' understanding of the technology and their willingness to engage with it. User education remains a critical component in MFA implementation. It is important to bridge knowledge gaps and encourage user engagement. Organizations should invest in comprehensive training initiatives to ensure that employees and customers not only understand MFA but also are proficient in using it effectively. Looking ahead, this research identifies emerging trends in payment card data security, such as the increasing use of biometric authentication methods in MFA systems. Recommendations for organizations like One Payment Gateway Company in Indonesia include:

4.4.1 Continuous Investment in MFA

Organizations should prioritize ongoing investment in Multi-Factor Authentication (MFA) technologies and solutions to adapt to evolving threats and ensure robust payment card data security. This includes staying abreast of advancements in MFA technologies and incorporating them into existing security frameworks.

4.4.2 Comprehensive User Education

Implement comprehensive user education programs to familiarize employees and stakeholders with the importance of MFA, its functionalities, and best practices. Educated users are more likely to understand the significance of MFA in safeguarding payment card data and actively participate in security measures.

4.4.3 Exceeding Regulatory Compliance

While compliance with PCI DSS 4.0 is essential, organizations should view it as a baseline rather than the ultimate goal. Strive to exceed regulatory requirements by implementing additional security measures and best practices to further fortify payment card data security.

4.4.4 Facilitating Collaboration and Information Sharing

Foster collaboration among industry peers, regulatory bodies, and security experts to share insights, experiences, and emerging threats related to payment card data security and MFA implementation. Collaborative efforts can lead to more robust security strategies and better protection against evolving threats.

4.4.5 Tailoring MFA Strategy to Organizational Context

Develop a customized MFA strategy aligned with the unique context, needs, and risk profile of the organization. This includes conducting risk assessments, identifying specific threats, and implementing tailored MFA solutions that address the organization's vulnerabilities effectively.

Research findings indicate that organizations are increasingly focusing on strengthening their security strategies moving forward. They view MFA as a fundamental element in these efforts, with the hope that MFA will continue to play a central role in securing payment card data. It is important to acknowledge some limitations of this research. The sample size may not represent the entire spectrum of organizations subject to PCI DSS 4.0 compliance, as it only focused on One Payment Gateway Company in Indonesia.

5. CONCLUSION

This study has explored the critical role of Multi-Factor Authentication (MFA) in enhancing security, compliance, and risk mitigation within organizations subject to the Payment Card Industry Data Security Standard (PCI DSS) 4.0. The findings emphasize the significant impact of MFA on the landscape of payment card data security. In conclusion, the study underscores the critical. The findings highlight the significant impact of MFA on the landscape of payment card data security, emphasizing its effectiveness in enhancing security, compliance, and risk mitigation.

Organizations that have adopted MFA demonstrate higher levels of compliance with PCI DSS 4.0, reinforcing the alignment of MFA with regulatory requirements. MFA serves as a robust barrier against unauthorized access and credential-based attacks, effectively reducing the risk of data breaches. Moreover, organizations implementing MFA observe improvements in incident response capabilities, enabling swift action during security incidents.

The recommendations put forth emphasize the importance of continuous investment in MFA technologies, comprehensive user education, and exceeding regulatory compliance standards. Facilitating collaboration and information sharing, along with tailoring MFA strategies to the organizational context, are also essential for maximizing the effectiveness of MFA in safeguarding payment card data. Ultimately, Multi-Factor Authentication stands as a cornerstone in securing payment card data in compliance with PCI DSS 4.0. Its multifaceted impact on security, compliance, and risk mitigation reinforces its central role in protecting sensitive financial information in today's rapidly evolving digital landscape.

Limitations of this research sample may not fully represent all industries (focused only on Payment Gateway Companies). It primarily focuses on organizations subject to PCI DSS 4.0 compliance, which may result in a biased sample. Some of the data collected, particularly through surveys and interviews, relies on self-reporting. This creates potential for response bias and subjective interpretation. In future research, researchers could compare the effectiveness of various MFA methods and technologies in enhancing payment card data security and compliance. Assessing their strengths and weaknesses in various organizational contexts. Exploring unique challenges and best practices associated with MFA implementation in specific industries, such as healthcare, finance, or e-commerce, where payment card data security is paramount.

REFERENCES:

[1] Fotouhi, M., Bayat, M., Das, A. K., Far, H. A. N., Pournaghi, S. M., & Doostari, M. A. (2020). A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks*, *177*, 107333. https://doi.org/10.1016/j.comnet.2020.107333

[2] Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

[3] Hameed, M. A., & Arachchilage, N. A. G. (2021). The role of self-efficacy on the adoption of information systems security innovations: A meta-analysis assessment. *Personal and Ubiquitous Computing*, *25*(5), 911–925. https://doi.org/10.1007/s00779-021-01560-1

[4] Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W.-C. (2021). Internet of Things: Evolution, Concerns and Security Challenges. *Sensors*, *21*(5), Article 5. https://doi.org/10.3390/s21051809

[5] Mehraj, H., Jayadevappa, D., Haleem, S. L. A., Parveen, R., Madduri, A., Ayyagari, M. R., & Dhabliya, D. (2021). Protection motivation theory using multi-factor authentication for providing security over social networking sites. *Pattern Recognition Letters*, *152*, 218–224. https://doi.org/10.1016/j.patrec.2021.10.002

[6] Robinson, P. (2022). Can PCI DSS 4.0 reverse the decline in compliance? *Computer Fraud & Security*, *2022*(6). https://doi.org/10.12968/S1361-3723(22)70579-9

[7] Seaman, J. (2020). An Introduction to the PCI DSS Controls Framework. In J. Seaman (Ed.), *PCI DSS: An Integrated Data Security Standard Guide* (pp. 231–284). Apress. https://doi.org/10.1007/978-1-4842-5808-8_9

[8] Silaban, M., & Ramli, K. (2022). Desain Kerangka Kerja Keamanan Infrastruktur Dompet Digital Menggunakan PCI DSS 4.0 dan COBIT 2019 Berbasis Analisis Manajemen Risiko. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *7*(12), Article 12. https://doi.org/10.36418/syntax-literate.v7i12.11645

[9] Sinigaglia, F., Carbone, R., Costa, G., & Zannone, N. (2020). A survey on multi-factor authentication for online banking in the wild. *Computers & Security*, *95*, 101745. https://doi.org/10.1016/j.cose.2020.101745

[10] Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. E. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change*, *167*, 120743. https://doi.org/10.1016/j.techfore.2021.120743

[11] Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*, 2172–2175. https://doi.org/10.1016/j.matpr.2021.11.121

[12] Wang, D., Zhang, X., Zhang, Z., & Wang, P. (2020). Understanding security failures of multi-factor authentication schemes for multi-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

server environments. *Computers & Security*, *88*, 101619. https://doi.org/10.1016/j.cose.2019.101619

[13] Wijanarko, R. P., Setiawan, M. R., Mukaromah, S., & Najaf, A. R. E. (2023). ANALISIS DAN SIMULASI SERANGAN RANSOMWARE TERHADAP DATABASE BANK SYARIAH INDONESIA. *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, *3*(1), Article 1. https://doi.org/10.33005/sitasi.v3i1.436