PCI DSS Implementation and Its Association with Customer Retention and Fraud Prevention in E-Commerce Platforms from E-store Owners' Viewpoints

Dr. Fahad Ali Alqahtani

Department of Marketing, College of Business King Khalid University, Abha

(Submitted to the journal on 08/01 /2026 AD, and accepted for publication on 07/02 /2026 AD)

Abstract:

This paper has explored the effects of adopting the Payment Card Industry Data Security Standard (PCI DSS) to customer retention and prevention of fraud in e-commerce systems with reference to e-store owners in the Kingdom of Saudi Arabia. Past studies have mainly concerned consumer trust or technical adherence to the standard, providing little theoretical understanding of the effect of such standards on business results on the organizational level, especially in developing digital economies. The research was based on the theoretical framework of institutional theory, according to which the adoption of PCI DSS is an institutional mechanism of coercion, which raises an organizational level of legitimacy and reinforces internal control mechanisms, which affect the integration of the e-commerce performance results. Quantitative descriptive design was used in this study and an online questionnaire was used to gather data on 377 e-store owners in Saudi Arabia using a simple random sampling technique. Multiple regression analysis was used to test the proposed relationships. The results showed that the use of PCI DSS has a strong positive influence on customer retention and fraud prevention. In particular, the use of PCI DSS attributed 75.8% of the difference in retaining the customers and 86.6% of the difference in the prevention of fraud. The research has the potential to add to the theoretical literature on e-commerce security research, as well as provides practical value since it could show that investing in PCI DSS is more than just complying. It offers helpful recommendations to e-store proprietors and policymakers that advocate digital transformation initiatives in accordance with Saudi Vision 2030.

Keywords: PCI DSS, Customer Retention, Fraud Prevention, E-Commerce Platforms, Institutional Theory, E-store Owners.

معيار أمن البيانات لصناعة بطاقات الدفع وعلاقته بالاحتفاظ بالعملاء ومنع الاحتيال في منصات التجارة الإلكترونية من وجهة نظر أصحاب المتاجر الإلكترونية

د. فهد علي القحطاني

أستاذ التسويق المشارك، بقسم التسويق، كلية إدارة الأعمال، جامعة الملك خالد، أبها

المستخلص:

تناولت هذه الورقة تحليلًا لكيفية تأثير تطبيق معيار أمن البيانات لصناعة بطاقات الدفع «PCI DSS» ضمن نطاق الاحتفاظ بالعملاء ومنع الاحتيال في منصات التجارة الإلكترونية على أصحاب المتاجر الإلكترونية في المملكة العربية السعودية، ركزت الدراسات السابقة بشكل أكبر على ثقة المستهلك أو الامتثال الفني للمعيار، واستعرضت فهمًا نظريًا محدودًا عن تأثير تلك المعايير على مخرجات الأعمال على مستوى المؤسسة؛ خاصة في الاقتصادات الرقمية الجديدة، واستندت الدراسة إلى المفهوم النظري لتطبيق معيار أمن البيانات لصناعة بطاقات الدفع «PCI DSS» وفقًا للنظرية المؤسسية التي تنص على أن استخدام هذه الآلية المؤسسية كان قسريًا، وأدى إلى زيادة الشرعية التنظيمية وقوة أنظمة الرقابة الداخلية؛ مما أثر على ترسيخ مخرجات أداء التجارة الإلكترونية. واعتمدت الدراسة على المنهج الكمي من خلال النهج الوصفي واستخدم استبانة عبر الإنترنت لجمع بيانات من 377 من أصحاب المتاجر الإلكترونية في المملكة العربية السعودية باستخدام عينة عشوائية بسيطة، وتم اختبار العلاقات المقترحة من خلال تحليل الانحدار المتعدد، وتوصلت النتائج إلى أن تطبيق معيار أمن البيانات لصناعة بطاقات الدفع «PCI DSS» أثر إيجابيًا بشكل كبير على الاحتفاظ بالعملاء ومنع الاحتيال، وفسر تطبيق معيار أمن البيانات لصناعة بطاقات الدفع نسبة (75.8%) من متغير الاحتفاظ بالعملاء و (86.6%) من متغير منع الاحتيال، وقد ساهمت هذه الدراسة في المعرفة النظرية حول دراسات أمن التجارة الإلكترونية، كما أن لها قيمة عملية من خلال إثبات أن فوائد الاستثمار في معيار أمن البيانات لصناعة بطاقات الدفع «PCI DSS» ستتجاوز مجرد تحقيق الامتثال؛ مما يوفر معلومات لأصحاب المتاجر الإلكترونية وصانعي السياسات المعتمدين لفكرة التحول الرقمي المتضمنة في رؤية المملكة 2030.

الكلمات المفتاحية: معيار أمن البيانات لصناعة بطاقات الدفع، الاحتفاظ بالعملاء، منع الاحتيال، منصات التجارة الإلكترونية، النظرية المؤسسية، أصحاب المتاجر الإلكترونية.

Introduction

E-commerce platforms have seen a high rate of development in the world, especially in the emerging digital economies like Saudi Arabia where secure electronic payment systems have evolved to be a major aspect of business sustainability. Nonetheless, the rising number of cybersecurity threats and payment fraud cases are still under threat to consumer privacy and transactional security.

One of the biggest issues that concern companies of any size is the responsible and safe management of customer data, sales, as well as money. Efficient data handling is imperative to the business process, and any incompetence in data handling may jeopardize personal information to hacking by cybercriminals (Staff, 2023). In addition to this, cards have led to a revolution in financial services since they have made transactions simple, secure, and efficient. Since magnetic strip cards were developed into EMV (Europay, Mastercard and Visa) chip-based cards, the industry has been innovating to enhance security and prevent fraud. Encryption and increasing use of the tokenization and biometric authentication are being advanced to safeguard consumer data in response to emerging threats that have emerged as a result of the increase in digital transactions. One of the major influences of the card payment technologies has been the issue of security (Akinluyi et al., 2025). Also, consumer confidence is important in financial services and this is also a critical aspect of retention. It has been as a result of security innovations. Customers are more prone to utilize digital payment methods when they believe that they are safe and trustworthy (Akinluyi et al., 2025). Within the scope of international financial systems, the conceptually important term is the Payment Card Industry Data Security Standard (PCI DSS) designed to secure transactions based on the use of cards in international markets (Chippagiri, 2024; Chippagiri and Ramesh, 2025).

Problem Statement

In the Kingdom of Saudi Arabia, e-commerce is one of the key growth drivers of the economy, especially within the context of Vision 2030, wherein digital growth and secure technological advancements are prioritized (Al-Tayyar et al., 2021; Al-Jowhari et al., 2022; Authority, 2018). Nevertheless, the high rates of e-commerce platforms growth have been combined with the growth of cybersecurity threats, particularly, payment fraud scenarios and data breaches, which serve as an ongoing damage to consumer confidence and undermine the authenticity of online transactions (Alghamdi & Nor, 2023; Alhejaili, 2024). Here, developing a safe and reliable transactional setting has gained a critical position in maintaining customer relationships and increasing digital marketplace interactions (Alshehri and Meersiane, 2018; ElRaba, 2024).

In order to manage these issues, the Payment Card Industry Data Security Standard (PCI DSS) has become a worldwide compliance and technical guide to safeguard the payment card information and mitigate the risks of the electronic transactions (Chippagiri, 2024; Chippagiri and Ramesh, 2025). Although the critical role of secure environments in shaping the attitude of customers and motivating them to use e-commerce platforms further has been highlighted in previous studies (Alshehri and Meeresa, 2018), the current literature is mostly divided between the concept of technical compliance and consumer trust. These methods, though useful, offer a limited insight into the overall implications of cybersecurity standards.

To be more precise, contemporary studies have a tendency to believe that the adherence to standards

like PCI DSS will automatically translate into better business performance, yet there is a lack of careful descriptions of the organizational processes that mediate the latter (Mutemi & Bacao, 2024). More so, the majority of researchers have concentrated on consumer perceptions with limited attention to owners of e-stores who are one of the key players in adopting and putting into practice the practice of cybersecurity in organizations.

Based on this, there is a substantial theoretical gap in the interpretation of how the implementation of PCI DSS gains organizational level perceptions and measurable performance results, especially in regard to customer retention and fraud prevention. This weakness limits the explanatory ability of the available models and the necessity of more integrated frameworks that focus on the relationship between cybersecurity compliance, the legitimacy of the organization, and e-commerce performance in emerging digital economies like Saudi Arabia.

Research Questions

"What is the reality of implementing data security standards in the electronic payment card industry?"

1. "What is the reality of e-store owners' customer retention?"
2. "What is the level of fraud prevention in e-commerce platforms?"

Research Hypotheses

"There is a statistically significant effect at the significance level ($\alpha \leq 0.05$) of implementing PCI DSS standards on customer retention."

3. "There is a statistically significant effect at the significance level ($\alpha \leq 0.05$) of implementing PCI DSS standards on fraud prevention in e-commerce platforms."

Research Objectives

To identify the reality of implementing data security standards in the electronic payment card industry.

4. To discuss the reality of e-store owners' viewpoints regarding customer retention.
5. To discuss the level of fraud prevention in e-commerce platforms.
6. To verify the effect of implementing "PCI DSS" standards on customer retention.
7. To verify the effect of implementing "PCI DSS" standards on fraud prevention in an e-commerce platform

Research Significance

The proposed research helps in the current literature to expand the use of institutional theory to e-commerce cybersecurity. Its response to the study of previous literature, the institutional theory clarifies the way organizations react to formal rules and norms to attain legitimacy, and match the environmental demands (Rahman et al., 2024; Karbhari et al., 2021). It is based on this point of view that the present research refreezes the thought of the implementation of PCI DSS as not just a technical imperative or a compliance-based set of rules and regulations, but rather as a form of coercive institution that produces organizational conduct and sets of organizational controls.

In contrast to the past research that has mainly focused on the use of PCI DSS in relation to the efficiency of technical features and consumer confidence, the current study offers a more insightful approach to cybersecurity compliance by evaluating how the approach relates to organizational perception and performance results. Specifically, it describes the role of compliance with PCI DSS in promoting increased organizational legitimacy, a stronger governance practice, and, eventually, better retention of customers and a reduction in fraud rates in online stores (Chippagiri, 2024; Akinluyi et al., 2025).

Additionally, the research fills a very important gap in the existing literature as it includes the views of e-store owners, which have not received the attention of earlier studies where the dominant point of view is on the consumers or the technical systems. In this way, it will provide a more in-depth analysis on how the organization processes that bring about business value and operational effectiveness are developed through the standards of cybersecurity.

This combined methodology will help lessen the knowledge gap between compliance with cybersecurity policies and the performance of an organization and show that PCI DSS is both a regulatory instrument and a strategic framework to promote trust, mitigate threat, and ensure the sustainable development of the digital business setting, especially in Saudi Arabia.

2. Literature Review

Introduction

The chapter analyses the current studies regarding the implementation of PCI DSS, customer retention and loyalty and prevention of fraud in e-commerce. It stresses on the creation of the theoretical framework of the study, creation of the research framework, and hypotheses.

PCI DSS Implementation

According to El Alloussi et al. (2016), the Payment Card Industry Data Security Standard (PCI DSS) can be described as a harmonized approach to security that is supposed to standardize the responsibility of card data security during the transaction of payments. However, other than its technical role, it is an international framework of regulations that uphold consistent security practices by organisations that process payments.

Having complianted with Kaur (2020), PCI DSS is a federal security guideline that pertains to any organization which processes, stores, or transmits any cardholder data and its purpose is to reduce risks of card data theft and identity fraud. But it is not merely a technical standard, it forms the basis of a tier of security and reliability of digital payment systems. Online retail systems, where cards must be used to purchase products, adherence to the PCI DSS is perceived as a growing security-focused indicator of safety alongside an indicator of institutional credibility, which influences consumer attitudes and buying behaviour.

A case in point is the establishment of the PCI SSC by international suppliers of cards, which is the industry trying to deal with the fundamental weaknesses of the online payment system (Bahtiyar, 2016). Instead of compliance with PCI DSS being a list of items to be checked off, it is more of a cyclical process which is broken into three parts; assess, remediate, and report. This trifecta process compels companies to shift out of defensive mode to a more proactive mode, in which data vulnerabilities and unnecessary data storage are identified and eliminated as normal operational procedures (Council, 2017).

As such, the standard does not just provide technical guidance and standards; it becomes an overarching governance framework for securing a breadth of points of interaction, from mobile platforms to remote access (Kim & Solomon, 2018).

The position of the PCI SSC to regulate the procedure creates a consistent criterion that equalises software and hardware testing, thereby promoting the reduction of the so-called security gap that cyber-adversaries aim to compromise (Johnson, 2019). In payment gateways, compliance is not merely another regulatory requirement, but it is a major operational aspect reflecting institutional integrity; it is an indicator of a security culture (Joshi, 2024). The standards make sure that security is inherent in the electronic payment process, rather than an after-thought process, through the mandatory requirement that developers and companies must comply with some transmission and processing standards (Council, 2017).

Connection between the CIA triad (confidentiality, integrity, and availability) and the adherence to the PCI DSS standards establishes a major path of cutting down financial risks. Strong security systems in the international e-commerce business have become one of the essential elements in the robustness of an organisation towards the challenges posed by online resources (Kim and Solomon, 2018). This technical strength, in its turn, opens a psychological change in the perceptions of customers; since the work of an online payment is an inseparable component of the trust-loyalty loop (Akinluyi et al., 2025). Therefore, PCI DSS is a communication tool between the technology and consumer perceptions, with the compliance with the standard guaranteeing customers and it becoming a basis of relationship between the merchant and the end consumer (Joshi, 2024).

The development of PCI DSS as a merchant requirement to a state law is a legal modification. This makes the security environment one of their compounded compliance as the enterprise must deal with both technical and legal compliance requirements, and perhaps need to ensure a greater degree of security than they would otherwise would deal with when having to comply with either of the two compliance regimes (Chippagiri & Ramesh, 2025). This is a driver of fraud preventive; a strong authentication and monitoring mechanism in place will essentially eliminate future chances of fraud occurring, and will convert what would have been a liability to a corporate asset (Joshi, 2024; Security Standards Council, 2020).

But PCI DSS compliance is not only related to security, but it is also related to optimization. The necessity to run regular vulnerability scans and monitoring contributes to a preventative maintenance strategy that reduces downtime and improves the processing of payments (Akinluyi et al., 2025). And, in a very saturated online commerce environment, it is compliance that can be used to distinguish themselves. By emphasizing the best-practice security needs, and their compliance with payment gateways using their security features as a differentiator to increase their market share, retain risk-averse merchants, and improve customer retention (Joshi, 2024; Kosutic, 2021).

The comprehensive approach of PCI DSS enables it to serve as a universal standard of data security, not just for cardholder data but for all transactional data (Alber & Nabil, 2015). But its success depends on proper management; for instance, through the use of Web Application Firewalls (WAF), and ongoing employee education to keep up with the ever-evolving e-commerce threats (Council, 2017). Despite being criticized for its complexity and cost of implementation, a cost-benefit analysis of the standard

shows that the "cost of non-compliance" (data breaches, legal fines and penalties, reputational damage) far outweighs the cost of maintaining compliance (Seaman, 2020). In conclusion, the PCI DSS becomes a "guiding light" and a valuable defence mechanism against opportunistic and targeted cyber-attacks (Wilson et al., 2018). These standards can be reviewed as Fig.1 illustrates.

Fig 1: "PCI Data Security Standard – High-Level Overview" Source: (Council, 2017)

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	**1.** Install and Maintain Network Security Controls. **2.** Apply Secure Configurations to All System Components.
Protect Account Data	**3.** Protect Stored Account Data. **4.** Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	**5.** Protect All Systems and Networks from Malicious Software. **6.** Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	**7.** Restrict Access to System Components and Cardholder Data by Business Need to Know. **8.** Identify Users and Authenticate Access to System Components. **9.** Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	**10.** Log and Monitor All Access to System Components and Cardholder Data. **11.** Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	**12.** Support Information Security with Organizational Policies and Programs.

Customer Retention

As indicated by Alayli (2023), customer retention can be defined as an organisation's capacity to sustain customer relationships over time, not just related to satisfaction with the transaction but also to the establishment of loyalty and value. In online transactions, retention is increasingly affected by non-tangible factors such as trust in the organisation, perceived security of transactions, and institutional guarantees that mitigate risks of uncertainty in the online environment.

According to Ejibenam et al. (2021), customer retention is a key concept in explaining the long-term viability of organisations, especially in online settings where transaction costs are minimal and competition fierce. Customer retention now transcends the level of repeated transactions to include relational aspects such as trust, value, and engagement. Institutional factors e.g., compliance with security standards (e.g PCI DSS) are apt to establish institutional legitimacy which is bound to affect customer trust and eventually customer retention.

According to Das et al. (2023), customer retention has been identified as one of the major factors of profitability and organisational sustainability. However, in the digital economy, it is no longer only the quality of product and service, which determines this capability, but the degree of trust and institutional guarantees which reduce the risk as much as possible. Consequently, the variables affecting customer retention has been an important aspect in the formulation of strategies that integrate behavioural and institutional perspectives of customer loyalty.

As outlined by Alshurideh (2016), customer retention continues to be a key challenge for firms, especially in highly competitive markets where the number of switching customers is on the rise and the cost of acquiring new customers is growing. In these markets, retaining customers is more cost-effective than customer acquisition as the consequences of losing a customer are not limited to the loss of a one-time sale, but also to the loss of the customer's lifetime value. This underlines the need for a better understanding of the drivers of retention, particularly those related to trust, perceived risk, and institutional assurances in the digital environment.

In the literature, as per Artha et al. (2022), customer retention has been recognised as a measure of organisational performance, as it reflects an organisation's ability to maintain long-term relationships with customers. Yet while important, research has tended to address retention independently, with little focus on the potential impact of external institutional and security-related factors on retention performance across industries, and in digital commerce contexts in particular.

Fraud Prevention

According to Aryotama et al. (2026), fraud prevention can be viewed as a combination of institutional mechanisms and behavioural controls that reduce the risk of fraud by emphasising ethical and risk awareness. In the digital environment, fraud prevention encompasses both behaviours and institutional security and governance controls to manage access, transactions, and fraud risks.

In accordance with Awang (2023), Fraud prevention is the array of governance and control measures that seek to prevent fraud from happening in the first place. According to Yulfani et al. (2025), the Fraud Hexagon framework offers an explanation of the drivers of fraud (pressure, opportunity, rationalisation, capability, ego, and collusion) that influence an individual's propensity to act fraudulently. Therefore, fraud prevention not only involves technical protections, but also institutional and procedural controls to mitigate these behavioural and institutional determinants.

The challenge in securing e-commerce ecosystems stems from a key gap between the growth of the market and the development of consumer protections.

The issue with security in e-commerce systems is a lag between the expansion of the market and the expansion of consumer security (Moric et al., 2024; Pleskach et al., 2024). This has given fraudulent activity free rein in the past, requiring a "revolution" in payment processes. The adoption of programs such as PCI (Payment Card Industry) DSS and SCA (Strong Customer Authentication) as a mandatory pivoting force ensures a realignment between commercial interests and global cybersecurity practices (Mansell & Ang, 2015). In this context, fraud prevention becomes a mandatory part of operating the e-store, a "license to operate" within the "ecosystem" in which the e-store is embedded, where the e-store's viability depends on its ability to implement cybersecurity measures (Mutemi & Bacao, 2024).

In regulatory terms, regulatory effectiveness is contingent on its "temporal agility", i.e., to keep up to date with technology. But a punitive or excessive compliance burden could create a "compliance-innovation paradox" where the cost of compliance could limit the pace of fintech innovation or prevent small e-store owners from entering the market (Akinluyi et al., 2025). Therefore, a regulatory strategy that has a rationalist perspective requires a double approach: standardised security should be complemented by "compliance scalability" for financial inclusion. By adopting a mix of mandatory compliance, consumer education, and co-operation with industry stakeholders, regulators can establish a strong framework that provides consumer protections without excessive barriers to entry.

PCI DSS Implementation and Customer Retention

Institutionally, the customer trust will not be based only on personal perception of security, but also on the organizational legitimacy based on the ability to comply with generally accepted standards. The compliance with "PCI DSS" indicates that the set standards of data security and risk management are observed, which is especially relevant within the realm of e-commerce, with the element of information

asymmetry and perceived risk. This legitimacy could increase customer trust and promote purchasing behavioral continuity, and hence the connection between institutional compliance and customer continuity (Dong, 2026; Safa & von Solms, 2016; Rouibah et al., 2016).

PCI DSS Implementation and Fraud Prevention

The institutional theory also highlights the importance of formalized regulations and standardized controls in limiting the opportunistic activity. The requirements of "PCI DSS" include the authentication, monitoring, and control systems that lessen vulnerabilities of organizations that are used to perpetrate fraudulent actions. Although technical research comes up with evidence of decreases in data breaches after the introduction of "PCI DSS", they rarely incorporate such results into the general organizational explanations of the effectiveness of fraud prevention in the organizations (Tinonetsana & Rawjee, 2025; Owusu-Mensah et al., 2026).

Theoretical Framework

Institutional Theory

As noted by Rahman et al. (2024), institutional theory helps to explain how organizations comply with formal regulations, standards, and institutional pressures to gain and sustain legitimacy in their environment. Organizational practices are often based on a need to conform to socially and legally acceptable norms, rather than just on efficiency.

In the line of Karbhari et al. (2021), institutional theory offers a macro-level view of how institutions are created, sustained, and changed, and the pressures that they place on the behaviour and actions of individuals and organizations. The pressures are embedded in formal rules, norms, and practices that shape and guide organisational behaviour and decisions.

Institutional theory was not just born from a critique of neoclassical individualism; it was also necessary to shift the focus from individual action to economic action constrained by the structure. Unlike classical economics, which holds to the premise of isolated rational actors, institutionalism argues that formal and informal rules (such as industry standards) are the main creators of social order (Radionov, 2021; Romaniuk, 2020). The shift to neo-institutionalism is critical in acknowledging that although the institutions set the "rules of the game", actors are still an important part of the way they are translated at the organisational level (Logrono & Gallego-Bono, 2023). This enables us to better understand more sophisticated processes of how external regulations, such as cybersecurity standards, are negotiated by decision-makers rather than merely followed.

Institutions not only regulate, but also institute power structures that define an organisation's behaviour and communicative policies. Drawing on cognitive science and complexity theory, the model explains the resistance to change within organisations or, on the other hand, how organisations maintain stability through "isomorphism" (Frodin, 2024). In today's digital economy, institutional power is increasingly evident in ecological and communicative aspects, where an entity's legitimacy is based on its conformance to societal and regulatory norms (Abrutyn et al., 2025; Meyer & Vaara, 2020). Hence, the institution not only constrains but also offers the thought structures by which organizations legitimise their activities and choices.

The growth of institutional theory in sociology and management has brought to the fore the "co-constitution" of agents and the context. As such, institutions are constantly shaped by the lived realities and practices of human actors (Voronov & Weber, 2020; Meyer & Vaara, 2020). This theoretical sophistication is reflected in the recent academic shift in focus to sustainability and corporate social responsibility (CSR); it shows that institutional theory is well-positioned to explain how businesses navigate the balance between profitability and ethical (or secure) practices (Baharom & Abdullah, 2025).

In this study, institutional theory creates an adequate foundation to explain how compliance with PCI DSS functions as a coercive institutional force, which constrains the actions of social actors, and in turn interferes with e-commerce performance outcomes like customer churn and electronic fraud.

Application of Institutional Theory to the Study

This study is conceptualized under the Institutional Theory, whereby the implementation of "PCI DSS" is viewed as a coercive institutional mechanism that influences the organizational security practices as well as governance structures. The model implies that the compliance with the internal control systems and the organizational legitimacy grow due to the compliance with the "PCI DSS", which impact the key outcomes in terms of e-commerce customer retention and fraud prevention. By focusing on the perceptions of e-store proprietors, the framework is able to get a hold of the organizational processes in terms of which institutional compliance is translated into business performance outputs.

Hypotheses Development

To defend the relationship between the implementation of PCI DSS and customer retention as a theoretically justified concept, security, trust and institutional legitimacy perspectives can be combined. In e-commerce, the quality of service offered is not only what determines customer retention, but a level of security that a customer feels to conduct the business and confidence of the customer in the site also determines customer retention. It has been found that customer trust and safety significantly impact customer attitudes and make them willing to be on online shopping platforms (Alshehri and Meer, 2018; Akinluyi et al., 2025).

Moreover, adherence to security requirements, including PCI DSS, increases organisational legitimacy and sends a message of reliability to clients, thus boosting trust and promoting long-term relationships (Dong, 2026; Rouibah et al., 2016). This is consistent with institutional theory, which argues that compliance with formal standards enhances credibility in organizations and affects how stakeholders act.

Moreover, existing studies point to the fact that customer retention in online settings is highly influenced by the perceived risk and security guarantees as opposed to the purely transactional considerations (Alayli, 2023; Ejibenam et al., 2021). Thus, the adoption of PCI DSS helps to decrease the perceived risk and raise trust, and eventually retain more customers.

The findings of the study, empirically, validate that PCI DSS implementation accounts a high percentage of variance in retaining the customers (R2 =0.758), that is, there is a strong correlation between security compliance and customer continuity. On the basis of these arguments, the hypothesis below is formulated:

H1: There is a statistically significant effect of implementing PCI DSS standards on customer retention.

The interrelation between the implementation of PCI DSS and preventing fraud is based on the institutional and security control theories. Strong governance systems, monitoring systems, and access control procedures are predominantly relied on to prevent opportunistic behavior and vulnerabilities in preventing fraud in e-commerce (Awang, 2023; Yulfani et al., 2025).

The framework itself offers a set of guidelines that include encryption, authentication, continuous monitoring, and risk management practices, all of which will mitigate the risk of fraud and data breaches (Kim and Solomon, 2018; Joshi, 2024). The mechanisms directly tackle the structural and behavioral causes of fraud by reducing the opportunities and reinforcing internal controls.

Moreover, the institutional theory suggests that standardized regulatory systems such as PCI DSS are forceful mechanisms that actualize compliance and reduce deviations of safe manners, thereby limiting fraudulent activities within organizations (Rahman et al., 2024).

Empirical data also proves this correlation, with previous studies having found that with the implementation of PCI DSS, the risks of fraud and the following increase in transaction security may increase significantly (Tinonetsana & Rawjee, 2025; Owusu-Mensah et al., 2026). The findings of the research after this show that a big percentage of the difference in fraud prevention given the occurrence of the implementation of PCI DSS can be attributed to it rather than to other factors ($R2 = 0.866$), hence its high impact. According to this the hypothesis is as follows:

H2: There is a statistically significant effect of implementing PCI DSS standards on fraud prevention in e-commerce platforms.

Research Gap

Although the technical infrastructure and compliance requirements of the Payment Card Industry Data Security Standard (PCI DSS) are well documented, there is a "compliance myopia" in the current literature where compliance is viewed as an end goal rather than a means to an end. Institutional Theory suggests that, rather than coercive standards being purely bureaucratic, they are meant to align internal practices and convey institutional legitimacy to the market. Yet there is a notable empirical gap in understanding the role of this "institutional signaling" in impacting e-commerce performance, in terms of customer retention and fraud management.

The majority of research continues to be confined within technically oriented or legalistic approaches, overlooking the merchant's perception, the key driver in e-commerce processes. This is especially true in the case of nascent e-commerce markets such as Saudi Arabia. This study bridges the gap between technical compliance and business performance by refocusing its efforts on the "what" rather than the "how" of compliance for the merchant. It goes beyond documenting standards to critically examining their impact on trust-building and operational sustainability in the ever-changing e-commerce environment.

3. Field Research Procedures:

First: Research Methodology:

According to Darwish (2018), descriptive research is "a general investigation of a phenomenon in a certain group, location, and time. It aims at systematic, scientific investigation and interpretation to

achieve social problem goals." Accordingly, this study adopts a descriptive quantitative approach, which is appropriate for exploring respondents' perceptions.

Data was collected over a period of two months. To ensure confidentiality and give the intended respondents speedy access, the data was gathered via an online survey delivered via Google Forms. (377) valid responses were gathered out of (450) questionnaires distributed, yielding a response rate of over (84%). Early and late replies were examined across major dimensions and important demographic characteristics in order to evaluate potential non-response bias. Non-response bias is unlikely to have an impact on the study's findings, given that no significant differences were discovered.

Second: Research Sample and Population:

The research population contained all e-store owners in the "Kingdom of Saudi Arabia". The sample of research was drawn using a simple random sampling, containing (377) individuals from the research population.

Third: Research Sample Characteristics:

Frequencies and percentages were computed to provide general data on the individuals in the study sample, which encompassed demographic details (gender, years of experience in e-commerce) as listed below:

Table No. (1): Sample characteristics

Gender	**Frequencies**	**Percentages %**
Male	225	%59.7
Female	152	%40.3
Total	377	100٪
Number of years working in e-commerce	**Frequencies**	**Percentages %**
"Less than 5 years"	135	%35.8
"5 to less than 10 years"	173	%45.9
"More than 10 years"	69	%18.3
Total	377	100٪

The presented data indicates that the "highest" percentage achieved by individuals in gender is (59.7%) for males, while the lowest percentage is (40.3%) for females. The highest share recorded by the sample individuals in relation to years of experience in e-commerce is (45.9%) for those with (5 to less than 10 years), followed by (35.8%) for individuals with (less than 5 years), and the lowest percentage at (18.3%) for those with (more than 10 years).

Fourth: "Research Tool":

The researcher developed the questionnaire to explore the influence of "PCI DSS implementation on customer retention and fraud prevention in e-commerce platforms from e-store owners' viewpoints in the Kingdom of Saudi Arabia".

The "validity and reliability" were examined using face validity and other approaches. The questionnaire was forwarded to the reviewers to appraise the phrasing, lucidity, and relevance of the statements included in it. Certain statements in the questionnaire were removed and revised, as decided by over (80%) of the judges. Consequently, in its finalized version following the review process, the question-

naire comprised (50) statements organized into three axes.

The questionnaire's "internal consistency" was assessed through administering it to (30) respondents. The value of the validity of "internal consistency" was determined through computing the "Pearson correlation coefficient" for each statement's scores in relation to the total score of its corresponding dimension or axis in the questionnaire, where the "correlation coefficients" displayed strong values spanning (.708** and .814**) across the dimensions of the first axis. In contrast, they ranged between (.735**-.823**) in the second axis, while they ranged between (739**-.850**) in the third axis, and they were all "statistically significant" at the level of significance of (0.01).

In addition, the questionnaire axes' "general construct validity" was validated by calculating the "correlation coefficients" of the axes with the total score of the questionnaire. The results showed that the "correlation coefficients" ranged from (.986** to .996**), and that all of them were "statistically significant" at the level of significance of (0.01). The questionnaire axes' "Cronbach's alpha reliability coefficients" varied from (0.926 to 0.935), and the questionnaire's total "reliability coefficient" was (0.974). The "reliability coefficients" exhibit the feasibility and trustworthiness of the questionnaire.

Although very high correlations between constructs were observed (up to 0.996), this should not be interpreted as a redundancy problem. Rather, it reflects the conceptual closeness and theoretical alignment of the questionnaire dimensions, as all axes measure closely related aspects of "PCI DSS" operationalization and its effects on maintaining customer loyalty and preventing fraud within e-commerce platforms. The high correlations indicate that the constructs are interconnected in practice, which is consistent with the integrated nature of the studied phenomenon. The robustness and reliability of the assessment tool were further confirmed by the high "Cronbach's alpha" values and "statistically significant" item-total correlations for each axis, which showed the questionnaire's great internal consistency and distinctiveness.

A factor analysis was performed, and the findings demonstrated that the data are appropriate within this study. The "Kaiser-Meyer-Olkin (KMO)" score reached (0.726), which means that the sample size is good. Bartlett's Test of Sphericity was also "statistically significant", which means that the variables are correlated enough. The communalities values were between (0.844) and (0.940), which means that the extracted factor accounts for most of the differences in each variable. The first component explained (89.776%) of the total variation, which shows that "PCI DSS" Implementation, Customer Retention, and Fraud Prevention in E-Commerce Platforms were all well represented. The research shows that one factor can effectively summarize the three variables, which supports the strength of the measurement model.

The "five-point Likert scale (strongly disagree, disagree, neutral, agree, strongly agree) was employed to refine the research instrument: questionnaire, assigning the responses: strongly disagree (1), disagree (2), neutral (3), agree (4), strongly agree (5)".

Fifth: Assessment of Normality:

Prior to undertaking more complex statistical analysis, it is important to assess the data distribution to determine its conformity to a normal distribution. By checking for normality, you can find any problems like skewness or kurtosis that could make parametric tests like regression and correlation less reliable. By checking to see if each variable is normal, the researcher may make sure that the designated statistical methods' essential premises are met. If they aren't, they can take steps to fix the problem. So, looking

at skewness and kurtosis is the first step to making sure that data is interpreted correctly and reliably.

Table No. (2): Normality Assessment of Study Variables (Skewness and Kurtosis)

Variable	Skewness		Kurtosis	
	Statistic	Std. Error	Statistic	Std. Error
1	-1.308	.126	-1.308	.126
2	-.675	.126	-.675	.126
3	-.823	.126	-.823	.126

As shown in Table 2, the "skewness and kurtosis" values indicate that the study variables approximately follow a normal distribution. This suggests that the data conform to the basic assumption of normality, supporting the use of parametric statistical analyses in the subsequent stages of the study.

Sixth: Statistical Methods:

The researcher used SPSS to extract results using "Pearson's correlation coefficient, Cronbach's alpha coefficient, frequencies and percentages, arithmetic means and standard deviations, linear regression analysis, and the range equation".

4. Presentation of the research results:

First: "What is the reality of implementing data security standards in the electronic payment card industry?"

The following table lists these dimensions in descending order by "arithmetic mean":

Table No. (3): Payment Card Industry Data Security Standard Implementation arithmetic means and standard deviations

No.	Dimensions	Average	SD	Response score	Rank
1	Dimension one: Data Protection	3.75	1.075	High	5
2	Dimension two: Risk Management	4.06	.971	High	2
3	Dimension three: Monitoring and Alerts	3.97	1.109	High	3
4	Dimension four: Security Policy	3.82	1.051	High	4
5	Dimension five: Secure Network	4.18	.909	High	1
Overall		3.96	.840	High	

The "arithmetic mean and standard deviation" of the dimensions that have to do with putting the "Payment Card Industry Data Security Standard (PCI DSS)" into operation are shown in Table No. 3. The data show that the "arithmetic mean" for this axis was (3.96), with a "standard deviation" of (0.840). This means that a lot of individuals answered. This number shows that the companies that were looked at are very committed to following the "PCI DSS" rules.

The high response rate for the "PCI DSS" implementation axis is due to the rise in cyber risks and electronic fraud, which has forced businesses to improve their security measures and take extra steps to secure payment card data. Also, following "PCI DSS" rules is a big part of keeping the organization's credibility and building customers' trust in electronic payment systems. This could also be because following these rules is now a requirement for working with banks and payment service providers. This encourages businesses to be stricter about security measures to keep their businesses running and stay ahead of the competition.

Dimensions of the first axis, "Payment Card Industry Data Security Standard" Implementation, are presented in supplementary detail:

- **Dimension one: Data Protection**

"Means and standard deviations" for dimension's statements: "Data Protection" were calculated and arranged in a top-down sequence in accordance with the "arithmetic mean" for each statement, as depicted in the following table:

Table No. (4) Data protection arithmetic means and standard deviations

No.	Statements	Average	SD	Rank	Response score
1	"Protect Stored Account Data"	3.63	1.444	4	High
2	"Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks"	3.88	1.354	2	High
3	"Policies are in place to protect customer data for payment cards."	3.56	1.454	5	High
4	"Technologies are used to ensure the confidentiality of electronic payment data."	4.03	1.295	1	High
5	"Employees are trained to handle payment card data securely."	3.68	1.479	3	High
Overall		3.75	1.079	High	

Table No. (4) above reveals that the "arithmetic mean" for dimension one, data protection, was (3.75), with a "standard deviation" of (1.079) and a "response score of (high)". The fact that dimension one got a "high" response score is because these standards include tight rules that require institutions to follow them in order to store and process data correctly and efficiently. This high score could also be because they protect critical client data, which is easy to hack and attack. In other words, the "Payment Card Industry Data Security Standard (PCI DSS)" has become a significant means to protect credit card transactions (Chippagiri & Ramesh, 2025; Chippagiri, 2024).

- **Dimension two: Risk Management**

"Means and standard deviations" for "Risk Management" statements were calculated, then sorted according to the "arithmetic means" in descending order:

Table No. (5) Risk Management arithmetic means and standard deviations

No.	Statements	Average	SD	Rank	Response score
6	"Protect All Systems and Networks from Malicious Software"	4.09	1.363	3	High
7	"Develop and Maintain Secure Systems and Software"	3.98	1.362	4	High
8	"A clear system is depended on to identify data security risks."	4.19	1.348	1	High
9	"A periodic assessment of information security risks is conducted."	3.89	1.397	5	High
10	"Security threats are detected early."	4.13	1.347	2	High
Overall		4.06	.971	High	

Dimension two had an "overall average" of (4.06), a standard deviation of (0.971), and a response score

of (High)", as the accompanying Table No. (5) demonstrates.

Dimension two, "Risk Management", reached a "(High) response score". This can be attributed to the existence of a risk management system due to the constantly evolving security threats. Therefore, it is necessary to continuously implement a risk management system and establish mechanisms and foundations for dealing with them.

This may also be because some organizations now have security teams to identify the most important technical problems and how to deal with them. Joshi (2024) has confirmed that compliance with "PCI-DSS" standards guarantees improved customer information protection and dramatically lowers the risk of data breaches.

- **Dimension three: Monitoring and Alerts**

"Means and standard deviations" for the statements of dimension three: Monitoring and Alerts, were calculated. Then these statements were arranged in a top-down sequence in accordance with the "arithmetic mean" for each statement, as depicted in the following table:

Table No. (6) Dimension three: Monitoring and Alerts arithmetic means and standard deviations of the sample's answers

No.	Statements	Average	SD	Rank	Response score
11	"Log and Monitor All Access to System Components and Cardholder Data"	3.69	1.513	4	High
12	"Test Security of Systems and Networks Regularly"	4.15	1.360	1	High
13	"An effective system is in place to control access to payment card data."	3.62	1.458	5	High
14	"Monitoring reports are used to enhance security systems."	4.07	1.314	2	High
15	"Monitoring logs are stored for future reference if necessary."	3.81	1.404	3	High
Overall		3.87	.996	High	

The "arithmetic means" for dimension three, Monitoring and Alerts, was (3.87), the "standard deviation" was (.996), and the "response score was (High)", as shown in the above Table No. (6) demonstrates that the high score of response can be attributed to the fact that transactions are examined and suspicious activities are detected. Organizations have become more reliant on new systems compared to previous years to monitor networks and databases to respond quickly to security and cyber threats. Akinluyi et al. (2025) have confirmed that conducting vulnerability assessments, security monitoring, and similar activities can resolve problems that may impact operations before they arise.

- **Dimension four: Security Policy**

"Arithmetic means and standard deviations" were determined for dimension four's statements: Security Policy. These statements were then sorted by the "arithmetic means" in descending order. The table shows this:

Table No. (7): Arithmetic means and standard deviations for sample responses to dimension five: Security Policy

No.	Statements	Average	SD	Rank	Response score
16	"Support Information Security with Organizational Policies and Programs"	4.05	1.461	2	High
17	"Security systems are constantly updated to keep pace with ongoing threats."	3.74	1.535	3	High
18	"Training courses are organized for employees to enhance their commitment to security policies."	3.52	1.519	5	High
19	"Management's compliance with security policies is periodically evaluated."	4.17	1.419	1	High
20	"Security policy implementation is continually refined."	3.64	1.352	4	High
Overall		3.82	1.051	High	

The above Table No. (7) reveals that dimension four had an average of (3.82), a "standard deviation" of (1.051), and a "response score" of (High).

The fact that dimension four, Security Policy, reached a "response score" of (High) is potentially explained by the importance of security policies to institutions. Financial regulatory authorities have emphasized the need for compliance security policies, which have led institutions to develop systems that can counter cyber threats. That is to say, the "PCI DSS" was created to promote and improve the security of payment card account data and make it easier for uniform information protection measures to be commonly employed around the world (PCI Security Standards Council, 2022).

- **Dimension five: Secure Network**

"Arithmetic means and standard deviations" were calculated for "Dimension Six: Secure Network" statements. These statements were computed and then sorted in descending order, as depicted in the following table:

"Table No. (8) Dimension Five 'Secure Network' responses means and standard"

No.	Statements	Average	SD	Rank	Response score
21	"Install and Maintain Network Security Controls"	4.08	1.428	4	High
22	"Apply Secure Configurations to All System Components"	4.32	1.135	2	Very High
23	"There is an emergency plan for rapid response to any threats."	3.96	1.360	5	High
24	"There are clear policies to control access to devices connected to the network."	4.12	1.339	3	High
25	"The network is periodically assessed to detect security vulnerabilities."	4.44	1.138	1	Very High
Overall		4.18	.909	High	

The Table No. (8) reveals that "Secure Network" had an "arithmetic mean" of (4.18), a "standard deviation" of (0.909), and a "response score of (High)".

The reason for dimension five, the secure network, to achieve a "response score of (High)" can be accounted for by network analysis, monitoring, and control, which help speed up response and identify

and deal with security attacks. These criteria also require the use of separate IP addresses to increase security.

Second: illustrating the results of question two: "What is the reality of e-store owners' customer retention?"

Second axis responses on customer retention were calculated using "arithmetic means and standard deviations". The "arithmetic mean" for each statement was used to sort the replies in a top-down sequence, as depicted in the table below:

Table No. (9) The second axis, 'Customer Retention', individuals' responses' arithmetic means and standard deviations.

No.	Statements	Average	SD	Rank	Response score
26	"Focuses on customizing ongoing customer offerings."	4.02	1.341	2	High
27	"Encourages customer feedback."	3.42	1.543	10	High
28	"Exerts greater effort to improve and improve services"	3.92	1.482	4	High
29	"Provides open communication channels with customers."	3.54	1.559	8	High
30	"Sets clear business goals for customer acquisition and retention."	4.14	1.444	1	High
31 "Strives to provide the highest quality services to customers."		3.66	1.549	6 High	
32	"Focuses on improving customer experience through user-friendly interfaces."	3.99	1.454	3	High
33	"Provides 24/7 technical support to resolve customer issues promptly."	3.57	1.534	7	High
34	"Conducts periodic surveys to gather customer feedback."	3.83	1.480	5	High
35	"Analyzes customer behavior to efficiently meet their needs."	3.48	1.502	9	High
Overall		3.76	.940	High	

The aforementioned table shows that "the second axis, Customer Retention" had an "overall average" of (3.76), accompanied by a "standard deviation" of (0.940) and a (high) "response score".

The high response score for axis two can be explained by organizations working to improve the user experience to increase customer confidence. Some organizations also implement after-sales follow-up services to provide any assistance, developments, or actual evaluation of each product.

Third: "What is the level of fraud prevention in e-commerce platforms?"

The "arithmetic means and standard deviations" for statements in axis two, "Fraud Prevention in E-Commerce Platforms," were calculated. "Arithmetic means" was used to sort the assertions in descending order:

Table No. (10): Arithmetic means, and standard deviations of the individuals' responses in the second axis, Fraud Prevention in E-Commerce Platforms.

No.	Statements	Average	SD	Rank	Response score
36	"It relies on robust customer identity verification technologies."	3.78	1.461	6	High
37	"It applies data analytics systems to identify suspicious behavior."	4.01	1.546	2	High
38	"All customer data and information are encrypted."	3.75	1.315	7	High
39	"It educates customers on how to detect fraud."	3.94	1.442	3	High
40	"It focuses on regularly developing the software it uses."	3.61	1.606	10	High
41	"It sends immediate alerts to customers in case of suspicion."	3.85	1.432	5	High
42	"It cooperates with relevant authorities to combat fraud."	3.65	1.552	9	High
43	"It conducts periodic risk assessments to identify system vulnerabilities."	4.04	1.428	1	High
44	"It guides customers on how to easily report fraud."	3.73	1.546	8	High
45	"It provides secure and reliable payment options for customers."	3.86	1.606	4	High
Overall		3.82	.968	High	

The above Table No. (10) exhibits that the "overall average" for "the second axis, Fraud Prevention in E-Commerce Platforms", achieved an "average" of (3.82), a "standard deviation" of (0.968), and a "response score" of (High).

Axis two, "Fraud Prevention in E-Commerce Platforms," reached a high score of response due to the increase in advanced payment methods, including high security, making it difficult for threats to influence data and gain unauthorized access to sensitive data. Recently, some organizations have used artificial intelligence to analyze threats and identify methods that affect security systems.

Fourth: "There is a statistically significant effect at the significance level ($\alpha \leq 0.05$) of implementing PCI DSS standards on customer retention."

"Multiple linear regression analysis" was used to answer this hypothesis, as seen below:

Table No. (11): The Effect of 'PCI DSS' Implementation on Customer Retention

Independent Variables	B	Beta	R	R2	T-Value	T-Sig
Data Protection	.215	.246	.871a	.758	5.958	.001
Risk Management	.114	.118			3.258	.001
Access Management	.178	.189			3.249	.001
Monitoring and Alerts	.127	.150			3.450	.001
Security Policy	.172	.193			4.635	.001
Secure Network	.424	.410			8.738	.001
Dependent Variable	Customer Retention					
: Intercept (Constant)	-.135					
Adj R2	.754					
F-Value	193.256					
F-Sig	.001b					

Table 11 shows that using "PCI DSS" criteria has a "statistically significant" effect on keeping custom-

ers, with an "R-value" of (0.871) at a level of significance of (0.001). The "determination coefficient" (R2 = 0.758) says that the use of "PCI DSS" explains about (75.8%) of the changes in customer retention. The strong conceptual and practical correlation between security standards and consumer retention in e-commerce platforms is shown in this "R2 value", despite its relatively high value. The model's "explanatory power" and capacity to estimate the "dependent variable" from the "independent variable" are validated by the corresponding "F value": (193.256).

According to these results, putting strong security measures in place boosts customer trust in online transactions, which encourages retention. Practically speaking, consumers are more inclined to stick with online retailers who exhibit dependability and credibility by implementing innovative security measures. Therefore, the theoretical anticipation that security and trust are important factors influencing client retention in online commerce is supported by the high "R2 value".

Fifth: "There is a statistically significant effect at the significance level (α ≤0.05) of implementing PCI DSS standards on fraud prevention in e-commerce platforms."

"Multiple linear regression analysis" was employed to address this hypothesis, as depicted in the following table:

Table No. (12) The impact of implementing 'PCI DSS' standards on fraud prevention in e-commerce platforms.

Independent Variables	B	**Beta**	**R**	**R2**	**T-Value**	**T-Sig**
Data Protection	.254	.281	.931a	.866	9.176	.001
Risk Management	.325	.326			12.105	.001
Access Management	.151	.155			3.584	.001
Monitoring and Alerts	.136	.156			4.824	.001
Security Policy	.097	.105			3.404	.001
Secure Network	.123	.115			3.298	.001
Dependent Variable	Fraud Prevention in E-Commerce Platforms					
: Intercept (Constant)	-.455					
Adj R2	.864					
F-Value	399.988					
F-Sig	.001b					

Table 12 shows that following "PCI DSS" standards has a "statistically significant" effect on preventing fraud on e-commerce sites, with an "R-value" of (0.931) at a level of significance of (0.001). The coefficient of determination ($R^2 = 0.866$) shows that "PCI DSS" installation explains about (86.6%) of the differences in fraud prevention. This R2 value is very high, which shows that there is a strong theoretical and practical correlation between following security standards and reducing fraud in online transactions. The "F value" of (399.988) shows that the model has a lot of "explanatory power" and can consistently predict the "dependent variable" based on the "independent variable".

These results imply that following "PCI DSS" criteria, such as encryption, regulated access, and constant monitoring, greatly lowers the risk of security risks and fraud. The high "R2 value" matches the idea that good security controls are important for stopping fraud in online stores.

Summary of the results:

The study data analysis shows that "PCI DSS" standards are widely used in the electronic payment

card company. The "arithmetic mean" is (3.94), and the "standard deviation" is (0.850). Fraud prevention and client retention were also highly rated, with an "arithmetic mean" of (3.76), (SD = 0.940), an "arithmetic mean" of (3.82), and (SD = 0.968), respectively. These detailed results illustrate that e-commerce site owners know how important data security standards are for keeping customers' trust and the business running smoothly.

With an "R-value" of (0.871) ($p < 0.001$) and an "R2" of (0.758), "regression analysis" further showed that putting "PCI DSS" requirements into practice has a statistically significant impact on customer retention. Similarly, with an "R-value" of (0.931) ($p < 0.001$) and an "R2" of (0.866), "PCI DSS" installation had a considerable impact on fraud prevention. Even though these "R2" values are somewhat high, they are in line with theoretical predictions: customer confidence and the efficacy of fraud mitigation strategies are intrinsically tied to the security of payment systems. Rather than signifying methodological inflation, high explanatory power in this situation highlights the crucial role security standards play in influencing the results of online transactions.

Akinluyi et al. (2025) say that these results are in line with recent studies that stress the need to make biometric identification, tokenization, and encryption better in order to make digital payments safer. The literature has underlined the need for laws that require banks and merchants to follow tight security rules, such as "PCI DSS" and strong customer authentication (SCA) (Bahtiyar, 2016; Kim & Solomon, 2018). The plans of "PCI DSS" for discovering, fixing, and reporting security breaches (Council, 2017) show that there is a direct link between following standards and getting better results in terms of stopping fraud and keeping customers.

Additionally, the strong correlation found in this study between economic performance and security measures shows how these concepts are actually related in real-world e-commerce environments. By offering concrete proof that adhering to "PCI DSS" increases customer confidence, reduces fraudulent activity, and safeguards cardholder data, the results promote the knowledge body. This increases our understanding of how operational security requirements benefit organizations in measurable ways.

The study demonstrates that "PCI DSS" compliance is a vital element in assessing both fraud prevention and customer retention on e-commerce platforms. By combining organizational procedures, regulatory compliance, and technical safeguards, businesses can keep trust and operational resilience in a world that is growing more digital and dangerous.

6. Recommendations:

Provide comprehensive training for all employees in online stores to understand the "PCI DSS" standards and how to implement them effectively.

- Invest in modern security technologies to analyze and detect evolving forms of security and cyber threats early.
- Develop security systems to continuously monitor and evaluate financial transactions to detect any abnormal behavior.
- Regularly update and maintain security systems to keep pace with evolving threats and maintain the security and confidentiality of data.

- Develop terms and conditions to respond to any fraud attempts and provide compensation to affected customers in accordance with these policies.

7. Research proposals: Conduct future research on:

The impact of AI-powered fraud detection systems on digital transactions across websites.

- The relationship between user experience and PCI DSS implementation in financial institutions in the Kingdom of Saudi Arabia.

Declaration:

Consent to Participate Declaration:

- All participants were given a briefing on the aim of the study and signed up to participate voluntarily.

Data Availability Declaration:

The data used to support the conclusions of this article are readily available.

Declaration of Funding:

This research attained no designated grant from any sponsoring organization in the non-profit, public, or commercial sectors.

Availability of Data and Materials:

The data and materials that assist this study's results are readily accessible.

List of References:

Abrutyn, S., Uscola, C., & Feldstein, K. (2025). Institutional spheres and organizational sociology: considering the ecological and cultural dynamics of the macro realm. Journal of Organizational Sociology, 3(2), 159-186.

Akinluyi, O. I., Mbakwe-Obi, T. C., & Connor, E. (2025). The Evolution Of Card Payment Technology: How Security Risk Drives Innovation In Financial Services. *International Journal of Engineering Technology Research & Management, 4*(10), 113–127.

Alayli, S. (2023). The Impact of Loyalty on Customer Retention: The Case of Lebanon. *International Journal of Research Publication and Reviews, 4*(8), 1350-1359.

Alber, N., & Nabil, M. (2015). The Impact of Information Security on Banks' Performance in Egypt. *International Journal of Economics and Finance, 7*(9), 219–225.

Alghamdi, F. S., & Nor, R. M. (2023). Evaluating E-Commerce Engagement Factors In Saudi Arabia: Financial Loss, Identity Theft And Privacy Policies. *Intern*. *Journal of Profess*. *Bus*. *Review, 8*(12), 1–30.

Alhejaili, M. O. M. (2024). Securing The Kingdom's E-Commerce Frontier: Evaluation Of Saudi Arabia's Cybersecurity Legal Frameworks. *Journal of Governance and Regulation, 13*(2), 275–286.

Al-Jowhari, H., Ayesh, M., Mouslmani, A., & Kurdi, A. (2022). *Cybersecurity Compliance Handbook for the Kingdom of Saudi Arabia*. PWC Publications.

Alshehri, H., & Meziane, F. (2018). The Impact of Trusted and Secured Transactions in an E-Commerce Environment on Consumers' Behaviour: The Case of Saudis in the UK. *Journal of Internet Technology and Secured Transactions (JITST, 6*(3), 695–604.

Alshurideh, M. (2016). Is Customer Retention Beneficial for Customers: A Conceptual Background. *Journal of Research in Marketing, 5*(3), 382-389.

Al-Tayyar, R. S., Abdullah, A. R., Rahman, A. B., & Hareeza, M. (2021). Challenges and Obstacles Facing SMEs in adopting E-Commerce in Developing Countries: A Case of Saudi Arabia. *Estudios de Economia Aplicada, 39*(4), 1–11.

Artha, B., Zahara, I., Bahri, & Sari, N. (2022). Customer Retention: A Literature Review. *Social Science Studies, 2*(1), 30-45.

Aryotama, H., Ferisca, S., & Yonata, H. (2026). Fraud Prevention in Accounting Students: The Impact of Using Anti-Fraud Awareness, Fraud Knowledge, and Religiosity. *Greenation International Journal of Economics and Accounting, 4*(1), 61-71.

Authority, N. C. (2018). *Essential Cybersecurity Controls* (ECC – 1: 2018). Kingdom of Saudi Arabia.

Awang, N. (2023). Fraud Awareness and Prevention Mechanism from Accountant's Perception. *Jurnal Pengauditan Sektor Awam Keluaran*, 63-69.

Baharom, Z., & Abdullah, K. H. (2025). Bibliometric Analysis of Institutional Theory Research. *Fronteira: Journal of Social, Technological and Environmental Science, 14*(2), 168-184.

Bahtiyar, S., G¨ur, G., & Altay, L. . (2016). Security Assessment of Payment Systems Under PCI DSS Incompatibilities. *29th IFIP International Information Security Conference (SEC),* Jun 2014, 395–402.

Chippagiri, S. (2024). A Holistic Review of PCI Security Standards Framework for Customer Relationship Management (CRM) Software. *International Journal of Intelligent Systems And Applications In Engineering, 12*(4), 4862–4871.

Chippagiri, S., & Ramesh, A. (2025). PCI DSS: A Critical Analysis of Implementation, Effectiveness, and Legislative Impact in Payment Card Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*(1), 1258–1266.

Council., P. S. S. (2017). PCI Data Security Standard (PCI DSS). PCI Security Standards Council Publication. .

Darwish, M. A. (2018). Research Methods in the Humanities. . Arab Nation Foundation for Publishing and Distribution.

Das, L., Salman, R., Sabeer, S., & Ansari, S. (2023, December 1-3). *Customer Retention Using Machine Learning*. *10th IEEE Uttar Pradesh Section International Conference on Electrical*, Electronics and Computer Engineering (UPCON), India.

Dong, Y. (2026). Navigating trust in cross-border e-commerce: a systematic review of cultural and consumer dynamics. *Humanities and Social Sciences Communications, 13*(237), 1-14.

Ejibenam, A., Onibokun, T., Oladeji, K., Ademola, H., & Halliday, N. (2021). The relevance of Customer Retention to Organizational Growth. *Journal of Frontiers in Multidisciplinary Research, 2*(1), 113-120.

El Alloussi, H., Fetjah, L., & Chaichaa, A. (2016). Securing Card Data on the Cloud: Application of the Cloud Card Compliance Checklist. *International Journal on Advances in Security, 9*(1&2), 36-48.

ElRaba'a, R. M., & ElChamie, M. B. S. (2024). The Impact Of E-COMMERCE As A Mediator On Consumer Trust In Independent Small And Medium Lebanese Retail Enterprises. Intern. *Journal of Profess*. *Bus*. *Review, 9*(7), 1–31.

Frödin, O. (2024). Cognitive microfoundations and social interaction dynamics. The implications of complexity for institutional theory. *Theory and Society, 53*(5), 1019-1047.

Johnson, B. (2019). Impact of PCI P2PE on PCI DSS Compliance & Scope Reduction. Payway, Inc.

Joshi, P. K. (2024). Achieving PCI-DSS Compliance in Payment Gateways: A Comprehensive Approach. *Journal of Technology and Systems, 6*(7), 13 – 31.

Karbhari, Y., Alam, K., & Rahman, M. (2021). Relevance of the application of institutional theory in Shariah governance of Islamic banks. *PSU Research Review: An International Journal, 5*(1), 1-15.

Kaur, R. (2020). *PCI DSS Implementation Guidelines for Small and Medium Enterprises Using Cobit Based Implementation Approach* (Unpublished Master Thesis). Concordia University of Edmonton.

Kim, D., & Solomon, M. G. (2018). Fundamentals of Information Systems Security.

Kosutic, D. (2021). *The Impact of Cybersecurity on Competitive Advantage* [Ph.D. Thesis,

LogroÃ±o, M. F. C., & Gallego-Bono, J. R. (2023). Approaches to economic institutionalism: A theoretical review of its characteristics and elements of study. *Academic Journal of Interdisciplinary Studies, 12*(3), 66-78.

Mansell, R., & Ang, P. H. (2015). The International Encyclopedia of Digital Communication and Society. Wiley Blackwell.

Meyer, R., & Vaara, E. (2020). Institutions and Actorhood as Co-Constitutive and Co-Constructed: The Argument and Areas for Future Research. *Journal of Management Studies*. *57*(4), 898-910.

Moric, Z., Dakic, V., & Regvart, D. (2024). Protection of Personal Data in the Context of E-Commerce. *J*. *Cybersecur*. *Priv, 4*(2024), 731–761.

Mutemi, A., & Bacao, F. (2024). E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review. *Big Data Mining And Analytics, 7*(2), 419 444.

Owusu-Mensah, K., Ansong, E., Adu-Manu, K., & Yaokumah, W. (2026). A Systematic Review of Frameworks for the Detection and Prevention of Card-Not-Present (CNP) Fraud. *Journal of Cyber Security, 8*, 33-92.

Pleskach, V., Kryvolapov, Y., Kryvolapov, H., & Zelikovska, O. (2024). Investigating E-Commerce Systems for Book Sales: From Theoretical Foundations to Software Development. *In Information*

Technology and Implementation (IT&I-2024), November 20-21.

Radionov, Y. (2021). INSTITUTIONAL THEORY IN THE DEVELOPMENT OF ECONOMICS. Economy of Ukraine, 2021, 30-50.

Rahman, T., Joe, N., & Abdul Jalil, M. (2024). Governance Apathy and Systemic Barriers in Enforcing Shariah Compliance: A Critical Study of Islamic Banking Practices in Bangladesh. *International Journal of Social and Business Studies, 2*(2), 52-71.

Romaniuk, S. (2020). Social Policy: Issues of the Modern Conceptualization of Institutionalism. *Demography and social economy, 4*(42), 120-142.

Rouibah, K., Lowry, P., & Hwang, Y. (2016). The Effects of Perceived Enjoyment and Perceived Risks on Trust Formation and Intentions to Use Online Payment Systems: New Perspectives from an Arab Country. *Electronic Commerce Research and Applications (ECRA), 19*(3), 33-43.

Safa, N. & von Solms, R. (2016). Customers repurchase intention formation in e-commerce. *South African Journal of Information Management, 18*(1), 1-9.

Seaman, J. (2020). PCI DSS: An Integrated Data Security Standard Guide. Springer Science+Business Media.

Security Standards Council. (2020). Bulletin: the threat of account testing to payment security. In The PCI Security Standards Council (PCI SSC) and the National Cyber-Forensics and Training Alliance (NCFTA).

Staff., P. E. (2023). *A guide to preventing data breaches*. https://www.paypal.com/us/brc/article/data-breach-prevention

Tinonetsana, F. & Rawjee, V. (2025). Beyond the Firewall: A Critical Analysis of Payment Card Industry Data Security Standard. *International Journal of Business Ecosystem & Strategy, 7*(6), 218-225.

Voronov, M., & Weber, K. (2020). People, Actors, and the Humanizing of Institutional Theory. *Journal of Management Studies, 57*(4), 873-884.

Wilson, D., Roman, E., & Beierly, I. (2018). PCI DSS and card brands: Standards, compliance and enforcement. *Cyber Security: A Peer-Reviewed Journal, 2*(1), 73–82.

Yulfani, Ansar, M., Yamin, N., Paranoan, S., & Gunarsa, A. (2025). Fraud Prevention: The Contribution of Internal Control, Internal Audit, and Organizational Culture. *Quantitative Economics and Management Studies (QEMS), 6*(4), 612–622.

Questionnaire

Dear Brother/Sister ……...

Peace, Mercy, and Blessings of Allah Be Upon You.

The researcher is carrying out a study as part of the requirements for obtaining a doctorate in Philosophy in Business Administration at Qassim University, with the aim of identifying **"The Effect of PCI DSS Implementation on Customer Retention and Fraud Prevention in E-Commerce Platforms from E-store Owners' Viewpoints,"** Accordingly, the researcher is esteemed to introduce this questionnaire to you, hoping that you will be so kind as to provide as answer for its statements through marking with a tick (√) in the box that conveys your perspective precisely, impartially, and faithfully, because the study's findings will be contingent upon the responses that will be obtained.

The researcher confirms that all data collected through this questionnaire will be treated with utmost privacy protection and will only be employed for scientific research purposes, in accordance with approved research ethics. The researcher expresses his sincere thanks and appreciation to everyone who participated in completing this questionnaire or provided support or advice, asking God Almighty to grant them the ultimate reward.

The researcher

Gender:

Male

Female

Number of years working in e-commerce:

Less than five years

Five to less than ten years

More than ten years

Second: Questionnaire Axes

Firstly: PCI DSS Implementation

Please state the extent to which you agree or disagree with the following statements:

No.	Statement	Response Rate				
		Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Data Protection						
	"Protect Stored Account Data"					
	"Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks"					
	"Policies are in place to protect customer data for payment cards."					

No.	Statement	Response Rate				
		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
	"Technologies are used to ensure the confidentiality of electronic payment data."					
	"Employees are trained to handle payment card data securely."					
Risk Management						
	"Protect All Systems and Networks from Malicious Software"					
	"Develop and Maintain Secure Systems and Software"					
	"A clear system is depended on to identify data security risks."					
	"A periodic assessment of information security risks is conducted."					
	"Security threats are detected early."					
Monitoring and Alerts						
	"Log and Monitor All Access to System Components and Cardholder Data"					
	"Test Security of Systems and Networks Regularly"					
	"An effective system is in place to control access to payment card data."					
	"Monitoring reports are used to enhance security systems."					
	"Monitoring logs are stored for future reference if necessary."					
Security Policy						
	"Support Information Security with Organizational Policies and Programs"					
	"Security systems are constantly updated to keep pace with ongoing threats."					
	"Training courses are organized for employees to enhance their commitment to security policies."					
	"Management's compliance with security policies is periodically evaluated."					
	"Security policy implementation is continually refined."					
Secure Network						
	"Install and Maintain Network Security Controls"					
	"Apply Secure Configurations to All System Components"					
	"There is an emergency plan for rapid response to any threats."					
	"There are clear policies to control access to devices connected to the network."					

No.	Statement	Response Rate				
		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
	"The network is periodically assessed to detect security vulnerabilities."					

Secondly: Customer Retention:

Please state the extent to which you agree or disagree with the following statements:

No.	Statement	Response Rate				
		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Customer Retention						
	"Focuses on customizing ongoing customer offerings."					
	"Encourages customer feedback."					
	"Exerts greater effort to improve and improve services"					
	"Provides open communication channels with customers."					
	"Sets clear business goals for customer acquisition and retention."					
	"Strives to provide the highest quality services to customers."					
	"Focuses on improving customer experience through user-friendly interfaces."					
	"Provides 24/7 technical support to resolve customer issues promptly."					
	"Conducts periodic surveys to gather customer feedback."					
	"Analyzes customer behavior to efficiently meet their needs."					

Thirdly: Fraud Prevention in E-Commerce Platforms

Please state the extent to which you agree or disagree with the following statements:

No.	Statement	Response Rate				
		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Fraud Prevention in E-Commerce Platforms						
	"It relies on robust customer identity verificationtechnologies."					
	"It applies data analytics systems to identify suspicious behavior."					
	"All customer data and information are encrypted."					
	"It educates customers on how to detect fraud."					

	"It focuses on regularly developing the software it uses."					
	"It sends immediate alerts to customers in case of suspicion."					
	"It cooperates with relevant authorities to combat fraud."					
	"It conducts periodic risk assessments to identify system vulnerabilities."					
	"It guides customers on how to easily report fraud."					
	"It provides secure and reliable payment options for customers."					

End of Questionnaire. Thank you very much for your cooperation

For any inquiries related to the study, please contact the researcher via the email address mentioned above. All your responses will be handled confidentially and employed solely for the scientific research's purpose.

Biographical Statement

Fahad Ali Al-Qahtani is an Associate Professor of E-Commerce and Marketing in the Department of Marketing, College of Business, King Khalid University. Dr. Fahad Ali Al-Qahtani received his PhD degree in Information Security of E-Commerce (2014) from De Mont-.fort University. His research interests include e-commerce and marketing

Biographical Statement

Dr. **Fahad Ali Al-Qahtani** is an Associate Professor of Marketing in the Department of Marketing, College of Business Administration, King Khalid University, Abha, Saudi Arabia. He received his PhD degree in Information Security in E-Commerce from De Montfort University in 2014. His research interests include E-Commerce, Information Security, Digital Marketing, Online Consumer Behavior, Social Media Marketing, Trust and Privacy in E-Commerce, Marketing Analytics, Artificial Intelligence in Marketing, Electronic Customer Relationship Management, and Digital Transformation.

معلومات عن الباحث

د. فهد علي القحطاني، أستاذ مشارك بقسم التسويق، كلية إدارة الأعمال، جامعة الملك خالد، أبها (المملكة العربية السعودية)، حاصل على درجة الدكتوراه في تخصص أمن المعلومات في التجارة الإلكترونية من جامعة De Montfort University عام 2014. تدور اهتماماته البحثية حول قضايا التجارة الإلكترونية، وأمن المعلومات في بيئات الأعمال الإلكترونية، والتسويق الرقمي، وسلوك المستهلك الإلكتروني، والتسويق عبر وسائل التواصل الاجتماعي، والثقة والخصوصية في التجارة الإلكترونية، والتحول الرقمي، وتطبيقات الذكاء الاصطناعي في التسويق، وتحليلات التسويق، وإدارة علاقات العملاء الإلكترونية.

Email: falgmash@kku.edu.sa