LEGALITY: JURNAL ILMIAH HUKUM

Journal homepage: http://www.ejournal.umm.ac.id/index.php/legality

Privacy and Security Risks in Cross-Border Digital Payment Systems

Naeem AllahRakha[1*], Tillayeva Gulsanam Xamdamovna[2], Bozarov Sardor Sokhibjonovich[3], Otabek Narziev[4], Pulatov Temurbek [5]

[1,3,4,5] Department of Cyber Law, Tashkent State University, Tashkent, Uzbekistan

[2] Department of Social and Humanitarian Science, Tashkent State Agrarian University, Tashkent, Uzbekistan

[*] Corresponding author: chaudharynaeem133@gmail.com

Article

Keywords:
Cross-Border Digital Payments; Data Governance; Privacy and Security Risks; Regulatory Frameworks; User Rights and Protections

Article History
Received: Apr 10, 2025;
Reviewed: Aug 2, 2025;
Accepted: Sep 26, 2025;
Published: Sep 27, 2025.

Abstract

This research examines the privacy and security concerns associated with the growing adoption of digital payments. Digital payments represent a new development in payment systems being assessed by institutions, companies, and individuals. The worldwide adoption of digital payments necessitates a thorough examination of the privacy and security risks associated with these systems, particularly those operating under different regulatory frameworks. This research identifies gaps in current laws and major weaknesses in privacy and security protections, with a focus on risks to user rights. Using a mixed-methods approach, the study includes a qualitative analysis of relevant data protection laws along with a quantitative survey of user concerns and awareness. It examines practical issues and combines insights using grounded theory. The findings indicate a heavy dependence on central regulation and varying privacy standards, resulting in more frequent violations that restrict user protections and avenues for recourse. This research suggests establishing global privacy and security standards for digital payments, supported by strong enforcement and collaboration between countries. These standards should provide clear data practices, give users control over their personal information, implement robust security measures, and encourage the use of new technologies that enhance privacy. The study concludes that careful governance and cooperation are crucial for the safe development of cross-border digital payment systems, while mitigating risks to privacy, security, and user rights.

INTRODUCTION

Money, an exchange instrument for goods and services, carries no intrinsic value. It's worth is based on what society agrees upon (Jan Hogendorn & Marion Johnson, 2003). Money began to be used as a transaction tool for the first time around 3,000 BC in Mesopotamia, with the use of symbolic representations of debt. Before that, barter systems were common in regions such as Mesopotamia, dating back to approximately 6000 BC. These systems were later adopted by the Phoenicians and Colonial Americans (Arslan But et al., 2023). The introduction of metal coins took place in the 7th century BCE in Lydia and China. Paper money appeared in 11th-century China, marking a significant shift in the use of currency.

Furthermore, banking systems developed during the Middle Ages. They evolved into today's banking system with the establishment of the first US national bank in 1791 (L. Randall Wray, 1999). The gold standard was introduced in England in 1816 and adopted by the US in 1900, thereby providing the currency with greater stability (John Pickering, 1844). Today, traditional money coexists with digital options, including credit and debit cards, online payments, and cryptocurrencies. This shows how money continues to evolve (Michael Peneder, 2022).

The evolution of money transfer methods has greatly impacted global economic transactions. It started with the hawala system in the 8th century in South Asia. This system utilised a network of agents to facilitate money transfers. Since then, the money exchange system has undergone significant changes (Michael Peneder, 2022). The founding of Western Union in 1851 marked the beginning of modern money transfer methods. It allowed money transfers through the telegraph, followed by the introduction of the first credit card in the 1920s, the Diner's Club Card in 1950, and the first online payment system by First Virtual Holdings in 1994 (Timothy Wolters, 2000). The rise of the Internet further changed money transfers. This led to the launch of mobile banking and online money transfer services in the late 20th century (Victor Murinde et al., 2022).

Digital payments are transactions where money is transferred from one party to another using digital or electronic methods, without physical cash being involved. This process utilises technology to facilitate payments through devices such as smartphones, computers, and tablets. It requires both the sender and receiver to have access to a digital platform, such as a bank account linked to an online service, a mobile payment app, or a web-based payment gateway (Khando Khando et al., 2023). Key examples include bank transfers through internet banking, payments made with credit and debit cards, and mobile wallets like PayPal and Google Pay, as well as PoS terminals. The growing popularity of digital payments stems from their convenience, speed, and enhanced security, offering clear benefits over traditional cash transactions (Rizka Ramayanti et al., 2024).

In 2023, global remittance flows grew by 3% compared to the previous year, reaching about USD 860 billion. This trend is likely to continue into 2024, with a projected growth rate of 3.1%. The United States remained the top source of remittances worldwide. India led recipient countries, receiving $125 billion in remittances, followed by Mexico at $67 billion, China at $50 billion, the Philippines at $40 billion, and Egypt at $24 billion. In the competitive remittance industry, Western Union is a major player. It began in the 1850s as one of the first telegraph companies and has since expanded its operations significantly. Today, it holds a considerable share of 10-20% in the nearly $700 billion global remittance market, establishing itself as a leading sector (Dilip Ratha, 2023).

The e-commerce industry has seen tremendous growth. It increased from USD 24,029.23 billion in 2021 to approximately USD 26,673.64 billion in 2022. Its global estimated value is projected to grow to USD 62,415.2 by 2030, with an annual growth rate of 11% expected throughout the forecast period (2023 -2030) (Daniel Tolstoy et al., 2021). China is the largest e-commerce market in the world, generating over $3 trillion in annual sales, which constitutes more than half of global online sales (Jun Yong Xiang & Jing Linbo, 2021). E-commerce has removed geographical limitations, enabling merchants to sell their products or services to customers worldwide, regardless of their location, thereby allowing merchants to expand their market beyond their local one. E-commerce is a model of global selling, where international customers can purchase directly from a seller or merchant without any geographical restriction or local presence in their market, thereby allowing sellers to export their products with ease (Praveen Shanmugalingam et al., 2023).

In international trade, another traditional method of payment involves a Letter of Credit (L/C)—a financial guarantee typically issued by the buyer's bank to the seller in which the buyer's bank agrees to pay the seller once specific shipment and documentation requirements have been met. The L/C payment method addresses risk for both sellers and buyers, especially in instances where they are partners residing in regions with different legal and financial systems. The seller presents documents, which may include the bill of lading, commercial invoice, and insurance certificate, to the bank for compliance review before releasing the payment. L/C payments are governed by the International Chamber of Commerce's Uniform Customs and Practice for Documentary Credits (UCP 600), which is designed to standardise the procedures of the payments in global trade. L/Cs will always have some relevance for large export–import transactions. However, the emerging, faster, and more flexible systems of modern digital cross-border payments are prone to privacy and security risks, despite the new opportunities they create.

In recent years, several studies have examined privacy and security issues in digital payment systems. One study assessed how different countries manage data privacy risks in digital payments and recommended methods for risk evaluation

(Akanfe, Valecha, & Rao, 2020). Another analysis mapped privacy-enhancing technologies in digital payments, showing the trade-offs between ensuring privacy and maintaining auditability (Auñón et al., 2024). Research has also explored advanced tools, such as secure multi-party computation and federated learning, to secure cross-border payments without compromising user privacy (Hu et al., 2024). A further study highlighted the growing threats of cyberattacks, data breaches, and regulatory compliance difficulties in digital finance (Cremer et al., 2022). In addition, findings from the International Monetary Fund suggest that well-designed central bank digital currencies (CBDCs) can enhance cross-border payment efficiency, while also highlighting significant privacy and legal challenges (Kaur, 2024). While these works advance our understanding of digital payment privacy and security, they often overlook the unique risks associated with cross-border transactions, where mismatched regulations and inconsistent safeguards expose users to greater vulnerabilities. This research, therefore, aims to critically examine the privacy and security risks associated with cross-border digital payment systems under the following main question: *How effective are current regulatory frameworks and operational safeguards in mitigating privacy and security risks in cross-border digital payment systems to ensure user protection*?

The focus on privacy and security threats that are unique to cross-border digital payment schemes is limited in previous studies. Prior research and regulation have addressed digital payments in general, such as consumer data protection and the fundamental principles of electronic money. However, investigation and guidance on the privacy and security threats that differ from cross-border transactions across multiple regulatory jurisdictions remain limited. This study aims to bridge this gap by focusing on the threats to user rights that arise from deficiencies in existing laws and major gaps in privacy or security provisions in such cross-border systems. This research will investigate cases of fraud, data abuse, and user grievances and sensitisation to propose targeted policy and operational reforms, unlike before. The use of central regulation by payment providers and the variation in privacy norms among jurisdictions remain unexamined.

METHODS

This study utilises a mixed-methods approach to thoroughly investigate privacy and security risks in cross-border digital payment systems. The research design incorporates both qualitative and quantitative methodologies to tackle the complex nature of the research questions. The qualitative aspect employed narrative and document analysis techniques to assess the risks linked to cross-border digital payments and to scrutinise pertinent laws and regulations. A doctrinal research methodology was employed to analyse legal frameworks. The quantitative component involved a survey to assess user awareness and concerns. A case study method was

also employed to assess the effectiveness of the current operational safeguards and self-regulation measures implemented by digital payment providers.

The subjects of this study were scholarly literature, legal regulations, and individual users of digital payment systems. For the literature study, research articles focusing exclusively on the key themes of interest in the research title were sampled (approximately 80) from peer-reviewed academic journals across reputable databases, including Scopus, Web of Science, JSTOR, ERIC, ScienceDirect, CORE, PLOS, DOAJ, and BASE. As a result, the Privacy and security risk part has been derived from data analysis of this literature. The legal analysis comprised regulations from 15 countries, with a deliberate selection of countries to ensure regional coverage worldwide, given differences in population, land area, and economic provision among countries. Data collection for these regulatory documents was via government official websites. The law and regulation part in result describes the regulations. The quantitative survey was obtained by 17 participants (students) enrolled in a summer course offered by Tashkent State University of Law and Roma Tre University. The survey consisted of 13 questions to capture various aspects of users' awareness and concerns, as well as the variation in user awareness derived from the survey. Data were collected through a systematic literature search using relevant keywords, publicly accessible legal documents, and a survey questionnaire.

Qualitative data were analysed manually using thematic analysis techniques, while quantitative survey data were analysed with JASP, an open-source statistics program, to gather descriptive statistics and examine relationships between variables. Ethical considerations were important throughout the study. Participation in the survey was voluntary, and no personal identifying information was collected to ensure anonymity. All sources used in the research were cited correctly to maintain academic integrity. The study notes several limitations, including the relatively small sample size of the survey, which consisted of only 17 participants, the narrow age range of participants, who were law students aged 18-24, and the limited scope of the legal analysis, which covered only 15 countries. Additionally, the case study section focused on the policies of only two organisations. These limitations may impact the applicability of the findings and should be taken into account when interpreting the results.

RESULTS AND DISCUSSION

Privacy and Security Risk: An Overview

Privacy and security regulations for cross-border payment systems encompass a wide range of guidelines and standards designed to protect consumer data and financial transactions (Tobias Adrian & Jean Pesme, 2023). Payment networks enforce rules, such as displaying payment brands, providing receipt data, and having clear return and refund policies to avoid fines (Gillette, 1996). Data privacy laws

differ by region. They give individuals control over their personal information and require prior notice about data usage, processing, and deletion timelines (Custers & Malgieri, 2022). To fight fraud in online payments, Strong Customer Authentication (SCA) is needed. This improves security by adding multiple verification steps (Fabcic, 2021). The Payment Card Industry Data Security Standards (PCI DSS) mandate a secure setup for businesses that process card information to protect against data breaches and cyberattacks (Morse & Raval, 2008).

In the rapidly evolving digital world of financial transactions, significant gaps in privacy and security regulations within digital payment systems have become increasingly apparent. These gaps could threaten user trust and the integrity of financial transactions (Mark Fajfar, 2008). Recent studies present a variety of views and findings. Even with improvements in digital payment technologies, some areas continue to struggle with inefficiencies due to inadequate digital infrastructure (Khando et al., 2022). Regulations and oversight of digital payments are highly dynamic, particularly in relation to high-value and real-time payments, cryptocurrencies, and the development of new products (Erik Feyen et al., 2021). The plan for tackling financial crime includes a specific risk assessment, focused risk management measures, and the utilisation of new technology to rethink anti-financial crime efforts (Wiwoho et al., 2021).

The global digital payments market was valued at $111.2 billion in 2023. It is expected to grow to $193.7 billion by 2028, with a compound annual growth rate (CAGR) of 11.8%. In 2021, digital/mobile wallets, as well as credit and debit cards, became the most popular payment methods for e-commerce and point-of-sale transactions (Zlatko Bezhovski, 2016). China leads the market with a transaction value of $3,639.00 billion in 2023. Major mobile payment apps such as AliPay, WeChat Pay, and Apple Pay had significant user bases in 2022, with 650 million, 550 million, and 507 million users, respectively. A survey showed that 70% of US customers prefer using mobile apps for payments. Moreover, over half of them feel comfortable leaving their wallets at home for mobile payments. PayPal, Apple Pay, and Cash App are the top mobile payment brands among US consumers, showing a strong preference for digital payment options (Jong-Hyuok Jung et al., 2020).

Digital payments offer numerous benefits that significantly enhance business operations and customer experiences worldwide. They are delay-free and bring efficiency and speed to transactions, allowing businesses and consumers to make payments more quickly than in traditional payment methods (Zaki Irfan Al Hafizh & Anas Hidayat, 2022). Additionally, digital payments are more cost-effective. They lower transaction fees and operational costs for businesses, which can lead to improved resource utilisation and financial benefits. Security is significantly better due to encryption and fraud detection systems, ensuring safe transactions (Leora Klapper, 2023). The global reach of digital payments enables access to international

markets, expands customer bases, and facilitates easier cross-border trade. They also support financial inclusion by providing banking services to underserved areas, generating valuable data for informed decision-making, streamlining business operations, and offering various payment options to enhance customer satisfaction (Ibrahim Niankara & Rachidatou I. Traoret, 2023).

Digital payments are changing the financial sector, but they also bring several concerns for businesses and consumers. Security issues are a major concern, with an increasing number of cyberattacks, including phishing, hacking, and data breaches, threatening sensitive financial information (Zhimao Wang & Xucheng Huang, 2023). Areas with poor technological infrastructure struggle to adopt digital payments, thereby exacerbating the digital divide and affecting market competition (AllahRakha, 2024). Transaction fees, particularly for international transactions and those involving specific gateways, can erode profits. This is especially true for small and medium enterprises (Seethamraju et al., 2019). Relying on digital platforms also means operations face risks from technical failures and privacy breaches, making strong data protection measures necessary (Andrew Burt, 2023). Additionally, low technological skills and resistance to traditional payment methods hinder the adoption of digital payments (Ayatulloh, Michael Musyaffi et al., 2022).

The privacy and security measures implemented by digital payment providers, such as PayPal, aim to protect users' personal and financial information while facilitating safe and efficient transactions. Key aspects include strict information collection protocols, where PayPal gathers personal, transactional, and device-related data to provide a safe service. The policy highlights PayPal's promise not to sell or rent user information to third parties for marketing without explicit consent. It specifies the situations in which information may be shared with third parties, such as to prevent fraud, comply with the law, and deliver PayPal services, all under strict restrictions. Cross-border data transfers occur with sufficient protection, following standards set by the European Economic Area. PayPal also gives users control over their information, allowing them to review, modify, or delete their data. Security measures, such as firewalls, data encryption, and controlled access, demonstrate PayPal's commitment to protecting user data from unauthorised access and maintaining high security standards in line with industry practices.

The regulatory landscape for digital payment systems varies significantly across different regions, including both advanced economies and emerging markets. This highlights a diverse approach to overseeing non-bank payment service providers (Parma Bains & Caroline Wu, 2023). Most regions permit non-bank payment service providers (NBPSPs) to offer a broad range of digital payment and e-money services. However, e-money issuance faces the most regulation, while virtual asset services face the least. Regulatory differences reflect the challenge of promoting innovation while maintaining financial stability and protecting consumers

(Sahi et al., 2022). Notably, NBPSPs in emerging markets deal with stricter regulations than those in advanced economies. This shows the cautious approach of emerging markets as they develop their regulatory frameworks. Common themes in regulations across regions include stringent measures against money laundering, effective risk management, robust data protection, and robust consumer protection. These aim to mitigate the potential risks associated with digital payment services (Michele Braun et al., 2008).

The findings show that a large majority of US adults (81%) believe the risks of data collection by companies outweigh any potential benefits. About 66% are worried about government data collection. This concern is heightened by the fact that 70% of adults believe their personal data is less secure now than it was five years ago. Although almost everyone has been asked to agree to privacy policies, only 22% read these policies carefully. This highlights a significant gap in understanding and engagement with data privacy practices. Moreover, 63% of Americans admit to knowing very little or nothing about the laws designed to protect their privacy.

Cultural differences significantly impact the way people perceive privacy and security. For example, 68% of respondents from South Asia participated in the survey, while smaller percentages came from Southeast Asia (16%), East Asia (5%), and Australia, New Zealand, and the Pacific Islands (11%). These differences reveal distinct cultural perspectives on technology, privacy, and security. The study highlights general worries about security and privacy, but specific fears may be stronger in some regions due to cultural values, laws, and historical backgrounds. The high participation rate from South Asia may indicate a greater awareness or concern about security and privacy in this area.

The "Privacy paradox" refers to a perplexing issue in the digital age. People often voice strong worries about their online privacy and the safety of their personal data, but their behaviour frequently contradicts those concerns (Joanne K. McQuilty, 2020). This paradox is clearly shown by the fact that, while 91% of people recognise the risks of reusing passwords, an astonishing 59% admit to doing it in both their personal and work lives. This gap between what people know and how they act is even more pronounced among Millennials, with 87% acknowledging that they often reuse passwords, despite understanding the associated risks. This discrepancy highlights a notable gap between what individuals worry about regarding privacy and their actual online behaviours. It highlights the urgent need for better education and strong cybersecurity measures (Wisniewski & Page, 2022). This gap not only makes individuals more vulnerable to data breaches and cyberattacks, but it also creates a significant financial burden for businesses, increasing the costs associated with maintaining cyber resilience.

The 2018 Facebook-Cambridge Analytica scandal was a major event that revealed the manipulation of personal data for political targeting. Cambridge

Analytica, founded in 2013, utilised a Facebook API from 2010 to access data from approximately 50 million Facebook profiles without obtaining clear user consent (AllahRakha, 2025). This data influenced voter behaviour through targeted political ads. The scandal became public on March 17, 2018, when The Guardian and The New York Times reported a whistleblower's account. This led to intense scrutiny of Facebook's data privacy practices. In response, Facebook took steps to protect user data. These included shutting down API access for new apps in 2014, conducting audits, and limiting developer access to data. The scandal triggered global legislative efforts, especially in the EU, and sparked discussions about the ethics of data privacy and political microtargeting. It had a significant impact on digital democracy and social media policies (Arora & Zinolabedini, 2023).

In 2017, Equifax, a major credit reporting agency, experienced a significant data breach that compromised the personal data of approximately 13.8 million consumers in the UK. This breach happened because Equifax failed to manage and monitor the security of data outsourced to its parent company, Equifax Inc., in the US. Hackers accessed sensitive information, including names, dates of birth, phone numbers, login details, partial credit card numbers, and addresses. Equifax's lack of oversight and the delay in discovering the breach showed major flaws in its data security measures. The Financial Conduct Authority (FCA) fined Equifax £11,164,400 for these failures. This fine stressed the importance of strong cybersecurity and the responsibility companies have to protect personal data, even when outsourcing. This incident serves as a clear warning about the ongoing threats from cybercriminals and the urgent need for financial institutions to maintain high standards in data protection (Irini Kanaris Miyashiro, 2021).

Younger generations, especially those who grew up with digital technologies, have different views on privacy, security, and broader social issues compared to older generations (Goyeneche et al., 2024). This divide stems from their early and constant exposure to online platforms and social media. It allows them to challenge authority in new and powerful ways. These digital natives have used their connections to create global change, advocating for environmental sustainability and demanding social justice. Even with significant stress and anxiety, millennials and Gen Zs stay focused on pushing for societal progress (AllahRakha, 2024). Their actions, which include changing shopping habits based on a company's environmental practices and participating in political and social campaigns, show a strong desire for accountability and change (Hoofnagle et al., 2010).

Self-regulation is a method that enables individuals to manage themselves through voluntary, non-coercive, and systematic means. It is also referred to as self-control (Karoly, 1993). The PayPal Services Privacy Policy provides a clear overview of how PayPal, a leading digital payment provider, addresses privacy and security risks through its operational safeguards and self-regulation efforts. To reduce

privacy and security risks, PayPal requires users to share personal and financial information. This information is protected by strict privacy terms. It is necessary for processing transactions, verifying identities, preventing fraud, and meeting legal requirements. PayPal employs robust security measures, including data encryption and firewalls, to protect user information. The policy describes how PayPal shares information with third parties, including necessary disclosures for preventing fraud, legal matters, and providing PayPal services. These rules become stricter when state regulations are more uniform. The policy underscores PayPal's commitment to data security and transparency in handling user information (Kurt Knutsson, 2023).

The effectiveness of operational safeguards and self-regulation measures in WorldPay's privacy notice reduces privacy and security risks (Andreas Klug, 2016). By adhering to strict data protection laws, these providers demonstrate a strong commitment to safeguarding personal and business data. They avoid collecting sensitive data unless necessary, delete it when possible, and conduct thorough checks to prevent fraud and money laundering. Using encrypted data transmission and secure server storage protects against unauthorised access and data breaches. However, relying on third-party service providers and international data transfers adds complexity. This situation requires ongoing attention and adjustment to new threats (Akanfe et al., 2020a).

Laws and Regulations in Protecting Privacy and Security in Cross-Border Digital Payment Systems

Laws and regulations play a crucial role in protecting privacy and security in cross-border digital payment systems. These systems move personal and financial data across different countries, which raises the risk of misuse, fraud, and cyberattacks. Clear legal guidelines help keep sensitive information, like account details and identification records, collected, stored, and shared safely. When users feel their data is secure, they are more likely to trust and use digital payment platforms. Strong regulations also create a common standard for businesses and governments, simplifying international cooperation. Without these laws, differences in countries' regulations can lead to confusion, disputes, and security vulnerabilities.

In the legal context, "personal data" refers to information that can directly or indirectly identify a person. The EU GDPR, UK Data Protection Act 2018, and Brazil's LGPD protect personal data, including names, addresses, identification numbers, location data, financial records, and transaction histories. The UAE's Federal Decree Law No. 45 of 2021 and Mexico's Federal Law for the Protection of Personal Data include contact details, account information, and communication records. China's PIPL, Japan's APPI, and South Korea's PIPA expand this to include identity documents, online identifiers, personal habits, and internet activity. Australia's Privacy Act 1988, Canada's PIPEDA, and Argentina's Law 25.326 cover biometric and genetic data, photographs, and voice recordings. Turkey's Personal

Data Protection Law and Russia's Federal Law No. 152-FZ also protect beliefs, health records, and political opinions. Indonesia's GR 71 further includes any information processed by electronic systems (Aditya, Z. F., & Al-Fatih, S., 2021).

Global regulation of personal data in cross-border digital payments is moving toward stricter rules and higher security standards. Many countries are updating their privacy laws to keep pace with modern technology and guard against new cyber threats. A key trend involves limiting cross-border transfers unless the receiving country has equal or stronger data protection laws, as seen in the EU, China, and Brazil. Governments also require stronger user consent, quicker breach notifications, and clearer accountability from payment service providers. At the same time, demands are calling for harmonisation through regional agreements and global forums to reduce conflicts between different legal systems. International cooperation, such as among G20 members and through OECD guidelines, is helping to create common standards.

The major economies have established firm legal frameworks to protect personal data in cross-border digital payments. The EU General Data Protection Regulation (GDPR) sets high standards by requiring clear user consent, strict security measures, and limits on data transfers to countries with similar data protection standards. The USA Privacy Act of 1974 primarily focuses on federal agencies but also affects private sector practices through specific laws, particularly in the financial services sector. China's Personal Information Protection Law (PIPL) is strict about cross-border transfers, requiring security assessments and government approval before sending personal data abroad. Brazil's General Data Protection Law (LGPD) combines aspects of the GDPR with its own rules, granting individuals firm rights to access, correct, and delete their personal data. Australia's Privacy Act 1988 ensures that payment service providers manage personal data fairly and securely, and requires them to notify breaches.

Alongside national laws, many countries follow voluntary global standards and best practices to improve privacy in cross-border digital payments. The OECD Privacy Guidelines outline basic principles, including data quality, purpose limitation, and security safeguards. Many governments use these principles when drafting new laws. The APEC Privacy Framework focuses on balancing data protection with the smooth flow of information for trade, making it popular among Asia-Pacific economies. The United Nations Guidelines for the Regulation of Computerized Personal Data Files encourage fairness, transparency, and respect for human rights in data processing. Financial industry groups also promote best practices, such as encryption, fraud monitoring, and regular security audits. These standards are not legally binding, but they are widely adopted because they help harmonise different national rules, reduce compliance costs, and build trust in global payment networks.

The IMF actively guides countries in developing safe and private digital payment systems. It also helps countries adopt modern messaging standards, such as ISO 20022, to enhance data security. The Fund is creating a CBDC Handbook and providing support to over 40 emerging economies on the design, privacy, and cross-border use of CBDCs. Alongside the World Bank, the IMF promotes safe payment corridors to reduce remittance costs and improve compliance. It also suggests the XC platform, an interoperable global ledger with built-in compliance and governance standards. The IMF provides frameworks for crypto-asset policies and supports their implementation through global training initiatives. A key publication, the FinTech Note on CBDC privacy, provides tools and guidance for integrating privacy into CBDC systems.

The World Trade Organization (WTO) plays an important role in shaping the trade environment for cross-border data flows. A key policy is the ban on customs duties for electronic transmissions, established in 1998. This policy prevents tariffs on digital services, such as music or software, and promotes seamless cross-border digital commerce. The duty-free rule has made digital payments easier and more accessible. The WTO also supports the Joint Statement Initiative (JSI) on E-Commerce, which involves approximately 90 members working on a framework for digital trade. Additionally, the WTO provides technical assistance and training, particularly to developing countries, to help them establish effective legal frameworks.

The field of electronic money (e-money) and digital payment services faces several important challenges that need attention from regulators and industry players. One major issue is the lack of clear and consistent definitions and classifications for e-money and digital payment services in different regions (Tanai Khiaonarong & Terry Goh, 2020b). This inconsistency complicates the regulatory environment, making it harder for these services to operate smoothly on a global level (Ferreira & Sandner, 2021). There is a fragmented and inconsistent approach to the licensing and authorisation requirements for NBPSPs. This adds another layer of difficulty for businesses wanting to operate in multiple countries (Tanai Khiaonarong & Terry Goh, 2020a). Ensuring proper oversight and supervision of NBPSPs, particularly those that operate across borders, remains a significant challenge. This highlights the need for improved cooperation and coordination among regulators.

Consumer data protection in the digital payment sector faces challenges due to inconsistent and often weak regulations in different areas (Beduschi, 2019). This mix of laws forces digital payment service providers to self-regulate, resulting in varying levels of protection for users. This situation makes it hard to enforce data protection rules and hold providers accountable for breaches or misuse of consumer data. Additionally, users are often unaware of how these service providers collect,

use, and share their personal information. This lack of understanding hinders users' ability to control their own data, underscoring the need for stronger regulations and greater transparency in the digital payment ecosystem (Fatima et al., 2019).

The Mobile Payment Services (MPS) sector faces several major issues, showing the need for a more organised and cooperative approach within the industry (Hillman et al., 2014). Currently, there are no globally accepted principles or best practices to ensure the secure and responsible operation of MPS. This lack leads to an uneven application of existing principles, including customer due diligence, transaction limits, and agent management. Additionally, the rapid changes in digital payment technologies and business models pose a significant challenge for updating MPS principles. This makes it hard for regulations to keep up with innovation.

The difference in privacy standards across regions affects digital payment systems. This is primarily due to the significant gaps in regulatory frameworks (Ferrari, 2022). For instance, the European Union enforces the General Data Protection Regulation (GDPR). This law imposes strict control over how personal data is collected, used, and shared. In contrast, in places like the United States, data privacy rules vary by state and are generally less comprehensive than the GDPR. China, however, has been changing its standards to protect personal financial information. These updates include rights for individuals to view and delete their personal financial data (Dorfleitner et al., 2023). These rules apply to all licensed financial institutions as well as to any organisation handling personal financial data. In regions with weaker privacy laws, user data might be more vulnerable, which can undermine trust in digital payment systems worldwide.

Comparative Perspective in Southeast Asia

Indonesia is one of the fastest-growing digital payment markets in Southeast Asia. The country has a large population and high smartphone use, positioning it as a key player in cross-border digital transactions. The central bank, Bank Indonesia, regulates e-money providers. It requires them to store consumer data within the country. Indonesia also introduced the QRIS (Quick Response Code Indonesian Standard), which is now expanding to cross-border payments with Malaysia, Singapore, and Thailand. While this helps improve financial inclusion, risks remain in data privacy and cyberattacks. Many small businesses use mobile payments without strong security, making them vulnerable. Fraudulent apps and phishing attempts are common issues. Indonesia's Personal Data Protection Law, enacted as Law No. 27 of 2022, grants users stronger rights, but enforcement is still in development (Rachman, Julianti, & Arkoyah, 2024).

Malaysia has established a firm legal and financial framework to manage digital payments and safeguard consumer interests. The Bank Negara Malaysia (BNM)

regulates electronic money providers. This regulation mandates stringent cybersecurity measures and robust data protection policies. Malaysia is also part of the ASEAN Payment Connectivity initiative, which enables cross-border QR payments and enhances regional payment connectivity. These systems help travellers and businesses complete transactions across borders. However, Malaysia is facing increasing issues with online fraud, identity theft, and phishing scams. Many users, especially in rural areas, lack digital literacy. This makes them vulnerable to cybercrime. Malaysia's Personal Data Protection Act 2010 (PDPA) requires companies to safeguard customer information. However, experts argue that the penalties are not strong enough compared to international standards, such as the EU's GDPR (Ahmed & Ibrahim, 2018).

Singapore is the leader in digital payment security and regulation in the region. The Payment Services Act 2019 (PS Act) provides a clear legal framework for e-money issuers, cryptocurrency platforms, and cross-border payment services (Law, 2025). The Monetary Authority of Singapore (MAS) enforces strict anti-money laundering and cybersecurity standards. This makes Singapore one of the safest places for digital finance. Singapore has also signed agreements with Malaysia, Thailand, and India to allow for instant cross-border QR payments. Despite having strong infrastructure, Singapore faces issues from international cybercriminals who target its position as a global financial centre. The government actively promotes digital literacy and requires companies to report data breaches promptly. Singapore's strict approach serves as a model for other Southeast Asian countries.

Thailand has become a digital payment hub in Southeast Asia with its PromptPay system. This system has enabled quick mobile transfers using phone numbers or national IDs since its inception in 2016. The Bank of Thailand has partnered with neighbouring countries, such as Malaysia, Singapore, and Indonesia, to connect QR code systems for cross-border payments (Bimantara & Nugraha, 2025). This regional link lowers costs for businesses and travellers, but it also raises the risk of cross-border fraud and data security issues. Thailand's new cybersecurity law, an amendment to the Cybersecurity Act B.E. 2562 of 2019, along with the Personal Data Protection Act (PDPA) implemented in June 2022, aims to address privacy issues. However, enforcement has been slow, and many small businesses lack the resources for effective cybersecurity. Phishing scams and fake apps continue to pose significant problems. Thailand is also exploring the use of central bank digital currency (CBDC) for domestic applications, a topic that was first discussed in 2018.

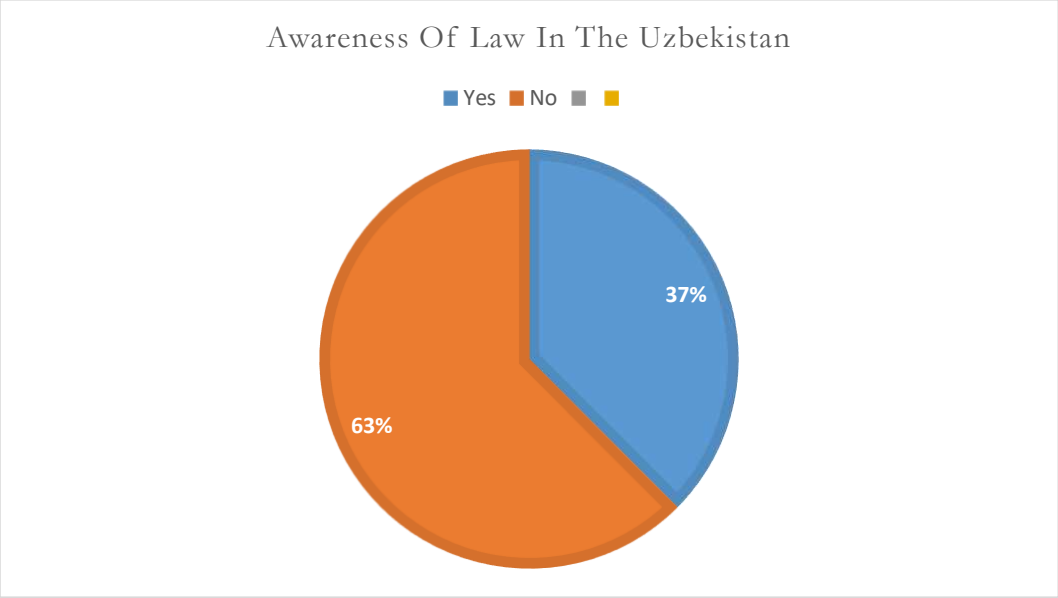
Vietnam has experienced rapid growth in digital payments. Mobile wallets like MoMo and ZaloPay are leading the market. The government supports digital transformation through its National Digital Transformation Program, which aims to reduce the use of cash. However, Vietnam does not have a strong personal data protection law, putting users at risk of financial information misuse. Cybercrime is

becoming a bigger issue, with cross-border hacking and online fraud impacting both businesses and consumers. The State Bank of Vietnam oversees payment service providers, and enforcement of security standards is underway. Vietnam is also collaborating with ASEAN partners to improve payment connectivity, particularly for remittances, which play a significant role in its economy. While digital payments promote financial inclusion, especially in rural areas, weak data privacy laws and limited consumer awareness make Vietnam one of the more vulnerable countries in Southeast Asia when it comes to digital payment security (Linh, 2025).

The Philippines has a rapidly growing digital payments market. This growth is driven by platforms like GCash, which offer financial services, resulting in a 41% reduction in cash use. The Bangko Sentral ng Pilipinas (BSP) supports digital financial inclusion and aims for 70% of adults to have financial accounts by 2025. Cross-border payments are crucial, as the Philippines is one of the world's largest recipients of remittances. To build trust, the Data Privacy Act 2012 (Republic Act No. 10173) requires financial institutions to protect personal data. However, cybersecurity risks remain high, with numerous cases of online fraud, phishing, and SIM card scams. Limited digital literacy in rural areas also makes people more vulnerable. The BSP is looking into central bank digital currency (CBDC) as part of its strategy for financial innovation. Although the Philippines is making headway, stronger enforcement of privacy laws and more public awareness campaigns are necessary to build user trust in cross-border digital payments (Velez, 2025).

Variation of User Awareness

Figure 1 Awareness of Law in The Uzbekistan



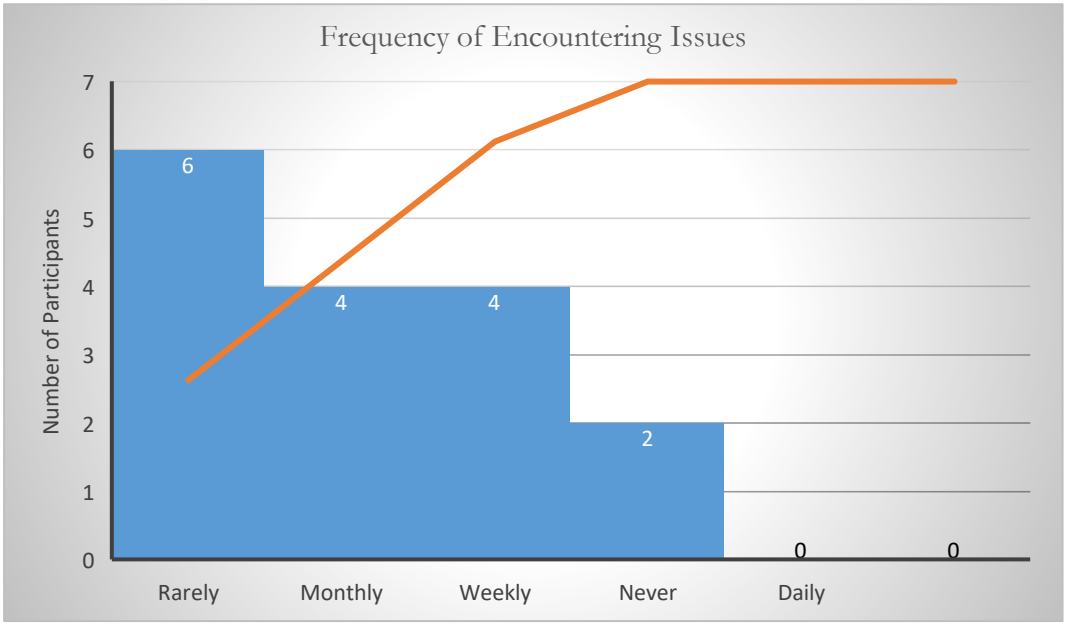
Source; Authors, 2025

The pie chart above illustrates the responses to Question 3 of the survey, which asked participants if they were aware of specific cyber laws in their country. Out of 16 participants:

1. 37.5% (6 respondents) reported being aware of the laws.
2. 62.5% (10 respondents) indicated that they were not aware.

Most participants are unfamiliar with the laws in the country. This highlights a gap in knowledge or communication about cybersecurity regulations. There is a clear need for increased awareness and education on cyber laws, particularly as digital payment systems and cross-border transactions become increasingly important.

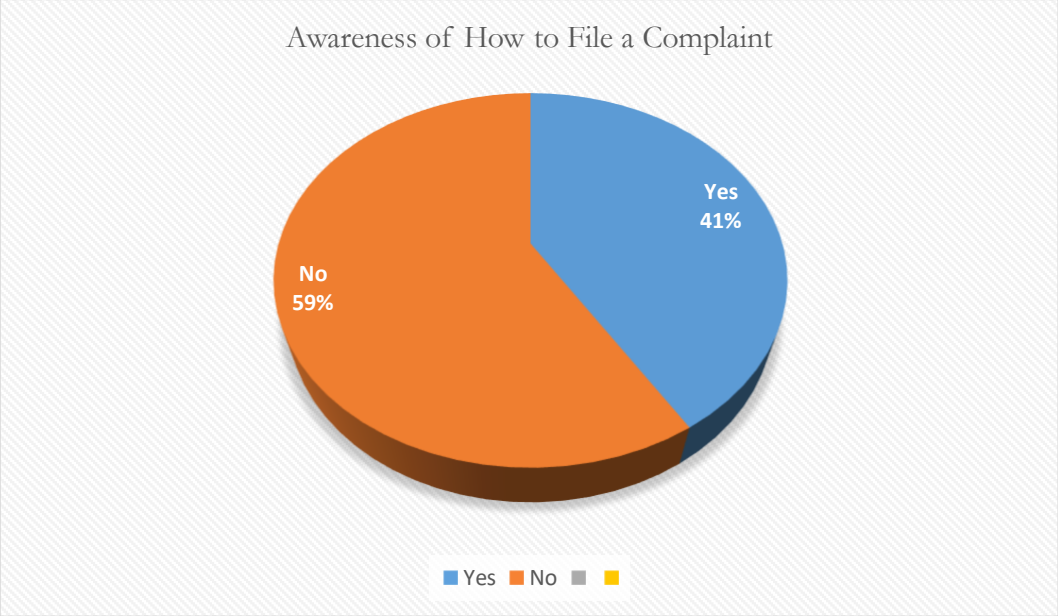
Figure 2 Frequency of Encountering Issues



Source; Authors, 2025

Most respondents, 37.5%, rarely deal with cyber law issues. This may show a low engagement with cybersecurity topics in their daily work or studies. Only a small percentage face these issues on a weekly basis, indicating that regular interaction with cyber law is uncommon among this group. This highlights the need to enhance cyber law awareness in both educational and professional sectors.

Figure 3 Awareness of How to File a Complaint



Source; Authors, 2025

The pie chart above illustrates the responses to the question about whether participants are aware of how to file a complaint about cybercrime in their country. The results indicate that:

1. 41.2% (7 respondents) are aware of how to file a cybercrime complaint.
2. 58.8% (10 respondents) are unaware.

A large portion of participants (58.8%) are not aware of how to file a cybercrime complaint. This suggests a need for better public education and clearer communication regarding legal procedures related to cybercrime. The survey data indicate a general lack of understanding about the laws, how to report cybercrimes, and the legal framework surrounding digital services. Even though participants are familiar with various types of cybercrime, their knowledge of practical legal steps and formal education on cybersecurity is limited. These gaps emphasise the need to improve public awareness and formal training, particularly as cross-border digital payment systems become increasingly complex.

The role of consumer concern and awareness in reducing data misuse is becoming increasingly important in the changing digital financial landscape (Schweidel et al., 2022). Several factors contribute to a secure digital payment system. The impact of perceived ease of use, perceived usefulness, and data security on the intention to adopt digital payment services shows how customer trust and promotion affect consumer behaviour (Zhang et al., 2023). Consumer awareness and concern about data security play a crucial role in the adoption and safe use of these services (AlHares et

al., 2024). In this context, consumer awareness is crucial, as it enables consumers to understand the importance of data protection measures and how to safeguard their personal information. As consumers become more aware of potential risks and the security measures in place, their trust in the system is likely to increase, which will encourage broader adoption.

The primary privacy and security risks in cross-border digital payment systems arise from data breaches, fraud, and non-compliance with regulations in various areas (Akanfe et al., 2020b). These systems handle sensitive financial and personal information. Compromised data can result in significant financial losses and identity theft for users. Dealing with various and sometimes conflicting international regulations presents obstacles to data protection, increasing the chance of data breaches (Cymone Gosnell, 2019). Processing delays, which happen when navigating through multiple intermediaries and regulatory rules, can make systems more vulnerable to cyberattacks and fraud. Longer transaction times leave room for malicious activities (Dinçkol et al., 2023). These issues put users' financial data at risk and lower trust in cross-border digital payment systems. This can discourage their use and slow down global financial inclusion and growth.

The rise in digital payments has raised significant concerns about privacy and security breaches. It has exposed major gaps in the protections and options available to users (De' et al., 2020). A primary concern is the inconsistency in legal and regulatory frameworks across different countries. This inconsistency may confuse consumers about their rights and accessible protections. For example, the degree of transparency and disclosure that service providers must offer about fees, exchange rates, and transaction conditions can vary widely. This can leave consumers with hidden charges or unfavourable terms that they might not be aware of. Another important issue is how service providers treat customers and conduct their business within digital payment systems. The gathering, use, and sharing of personal data across different legal areas, each with its own data protection laws, can result in weaknesses in consumer information protection (Andy Schmulow et al., 2021).

Cross-border digital payment systems allow businesses and individuals to send and receive payments between different countries. These systems have become more essential because globalisation has greatly increased trade, capital flows, and migration (Esteban Ortiz-Ospina et al., 2024). International payment gateways are key tools that authorise credit and debit card transactions for both online and offline businesses. These gateways have evolved to provide global and multi-currency payments, as well as support for various languages, for international clients (Lowry et al., 2006). Examples include PayPal, known for its wide reach and ease of setup, Worldpay, which supports multiple countries and currencies, and GoCardless, which focuses on direct bank payments. These systems enhance global commerce by simplifying transactions

and offering solutions that cater to diverse currencies, compliance requirements, and customer preferences, thereby improving the global economic landscape.

In today's connected digital world, the rise in cross-border financial activities has highlighted the need to address privacy and security risks in these systems. These risks are critical because these systems face significant vulnerabilities (Ross P Buckley et al., 2020). The shift to digital financial transactions has made international trade, investments, and remittances faster and more efficient. However, this change has also created numerous opportunities for cybercriminals to exploit system weaknesses, leading to data breaches and ransomware attacks (van Zeeland & Pierson, 2021). Financial institutions, which handle sensitive information, are prime targets. Breaches can result in significant financial losses and compromise personal data. The lack of standard rules across different regions makes cross-border transactions even more vulnerable to fraud and cyberattacks (Keman Huang & Stuart Madnick, 2020).

Examining privacy and security risks in cross-border systems is crucial because our global digital economy is highly interconnected. Financial, personal, and sensitive data often cross international borders (Kala, 2023). The rise in digital connectivity and international data flows has improved efficiency while simultaneously increasing privacy risks. The varied nature of these regulations makes it hard to enforce privacy laws and implement security measures. This situation highlights the need for international cooperation and standardisation (AllahRakha, 2024). Digital platforms that enable global interactions also raise the risks of data breaches, identity theft, and cyberattacks. These threats not only impact individual privacy and security but also undermine trust and integrity in the global digital economy (Zhghenti & Chkareuli, 2021). Cybercriminals exploit these interconnected systems, posing significant risks to personal privacy and eroding overall trust in digital systems. The challenge of navigating different regulatory jurisdictions further complicates efforts to protect data privacy and security (Srinivas & Liang, 2022).

Technological innovations, including APIs, AI, blockchain, big data, and cloud computing drive the rise of new payment methods. Although these technologies improve payment processes, they create challenges in cybersecurity and fraud (Romina Gayá, 2022). Given that technology is vital, there is a need for clear strategies to tackle the complexities of cross-border payments (Deng, 2020). It is essential to harmonise regulations across different regions to manage the challenges of cross-border digital transactions (AHMED, 2019). Direct central bank liabilities provide better stability and lower crime rates compared to private digital payment systems (Wong & Maniff, 2020). Various mechanisms lead to risks in cross-border e-commerce payments, which can be divided into credit, market, technical, and legal risks. These risks stem from liquidity issues, unexpected market fluctuations, technological gaps, and inadequate legal frameworks that struggle to keep pace with the rapid evolution of digital transactions

(Guan & Ren, 2019). The empirical study shows that security risk, online payment risk, supervisory risk, and financial risk negatively affect users (Wu et al., 2021a).

Ongoing economic and financial digitisation makes individual data a key source of value for companies. This situation highlights the need for regulations that balance privacy, social needs, and economic and financial benefits (V. Haksar et al., 2021). Access to non-traditional data can reduce adverse selection problems in credit markets. This access reveals the potential for greater financial inclusion through the use of digital footprints in credit scoring (Berg et al., 2020). The increasing reliance on digital technologies for cross-border financial transactions introduces cyber risks (Keman Huang & Stuart Madnick, 2020). Trade is essential for economic growth and prosperity. Efficient cross-border payments facilitate trade (Khando et al., 2022). High-level security breaches in cross-border payment systems are common since each country follows its own regulations (Wu et al., 2021b). These restrictions include strict requirements for local data storage or processing, supported by conditional rules that impose specific conditions for data transfer across borders (Martina F. Ferracane, 2017).

In digital transactions, digital payment systems show a strong commitment to user data privacy through careful self-regulation practices that meet strict regulatory standards. These practices involve the careful collection of personal and financial information, only to facilitate secure transactions, provide customer support, and comply with legal requirements (Krishna et al., 2023). A key part of this self-regulation includes limited information sharing with third parties, but only under closely regulated conditions. This helps prevent fraud, meet legal obligations, and improve service delivery, while protecting user privacy (Florencia Marotta-Wurgler, 2016). Cross-border data transfers can be performed securely, following policy requirements to ensure data protection across different regions (Bradford et al., 2021). Giving users significant rights over their data, such as access, modification, and the option to opt out of marketing communications, indicates a clear approach to data management. Additionally, strong security measures, such as encryption and firewalls, strengthen the protection of user information (Juliussen et al., 2023).

Despite global progress in data protection laws, a significant inconsistency in data and privacy policies persists across different countries. Over 120 countries have adopted some type of international data protection rule, but the strength, coverage, and enforcement of these regulations vary widely (AllahRakha, 2024). This difference can be attributed to the varying levels of technological development, legal systems, and cultural perspectives on privacy in different regions. Such inconsistencies create challenges for multinational companies attempting to comply with diverse legal requirements and for consumers seeking to understand their rights across various regions. Additionally, while 71% of countries have enacted privacy laws, 15% remain

without a data protection law, resulting in a significant gap in global efforts to protect personal information (Engström et al., 2023).

Global inconsistencies in data and privacy policies pose significant challenges to protecting personal information and combating identity theft (Schäfer et al., 2023). Different countries and regions have different frameworks and standards for data protection. This results in a complex environment for both consumers and businesses to navigate (Coche et al., 2024). For example, the European Union's General Data Protection Regulation (GDPR) has strict rules and heavy penalties for non-compliance. It emphasises individuals' rights over their personal data in the region. On the other hand, some areas lack these laws. At the state level, either strict or mixed approaches to data protection are applied, along with various comprehensive measures. These differences make enforcing data security less possible. They also create weaknesses that identity thieves and cybercriminals can exploit. The incidents involving First American Financial Corp. and Equifax highlight the severe consequences of inadequate data security and underscore the pressing need for unified global standards (McKay Smith & Garrett Mulrain, 2018).

The digital payment ecosystem is increasingly vulnerable to sophisticated cyber threats, including malware, phishing, and hacking attempts. This problem worsens because some payment service providers, especially smaller or newer ones, have not implemented firm security measures (John Rothchild, 1999). The lack of widely required minimum security standards and regulatory oversight in various regions exacerbates the situation, leaving both consumers and businesses vulnerable to financial loss and data breaches. Additionally, the global nature of digital payments presents significant challenges in detecting, responding to, and mitigating the impact of cross-border security incidents and fraud (Putrevu & Mertzanis, 2024a).

The instability of exchange rates creates significant risks and uncertainties for people using cross-border digital payment services. This volatility can lead to confusion about how payment service providers determine and apply exchange rates, thereby complicating transactions for users (Bénétrix et al., 2020). Additionally, there is a risk that currency conversion fees and unfavourable exchange rates will reduce the value of users' funds and transactions, making this situation a major concern. MoneyGram has margin rates that change from country to country; however, the specifics of how these rates are calculated are unclear. It is crucial to have clear disclosure requirements and protections for users to address the risks and costs that come with exchange rate fluctuations. These measures would help ensure that users are well-informed and can make choices that best fit their financial needs (Raikar & Adamson, 2020).

The rapid growth of digital payment technologies and business models has outpaced the creation of data protection and privacy laws in many areas, leaving loopholes in legal frameworks (Fahad & Shahid, 2022). Such gaps are especially evident in the absence of specific regulations or guidelines that address the privacy and security

issues associated with cross-border digital payment services. The widespread reliance on self-regulation and voluntary industry standards leads to inconsistent and often insufficient privacy and security practices (Siona Listokin, 2015). The lack of explicit and enforceable rights and remedies for users in cases of data breaches, unauthorised transactions, or other privacy and security issues worsens this problem. Additionally, regulators and supervisory authorities often lack the necessary resources and expertise to effectively monitor and enforce privacy and security standards among digital payment service providers, further complicating these issues (Putrevu & Mertzanis, 2024b).

There are serious concerns about consumer protection and rights related to cross-border digital payment services. Because regulatory frameworks are often inconsistent and insufficient, individuals face risks such as data breaches and financial losses, with limited options for recourse (David W. Opderbeck, 2023). The complexity of these payment systems makes it harder for users to understand and enforce their rights. This difficulty creates challenges in seeking redress for violations. As a result, individuals' trust and willingness to use these services decline, and their growth stalls, especially among vulnerable groups. Solving these problems requires a joint effort from different stakeholders, including regulators, industry players, consumer advocates, and international organisations. They need to create clear and unified regulations that protect user interests. Improving user rights and protections is crucial for establishing trust and confidence in digital payment services, which will encourage their adoption and growth (Aldboush & Ferdous, 2023).

CONCLUSION

This research indicates that privacy and security risks in cross-border digital payment systems are heightened due to a fragmented and poorly coordinated regulatory environment. Inconsistent laws, uneven enforcement, and too much reliance on voluntary compliance create weaknesses that cybercriminals can exploit. A key finding is that many existing frameworks focus on transaction speed, market growth, and interoperability, but do not adequately prioritise user protection. This disproportion leads to vulnerabilities such as unauthorised data access, identity theft, and large-scale fraud. Another insight is that multi-layered payment chains, with several intermediaries and jurisdictions, weaken accountability and slow down breach investigations. As payment data moves across borders, its protection relies on the weakest link in the chain, necessitating the establishment of uniform standards.

The study proposes a future model based on binding global standards, mandatory minimum-security protocols, and transparent data governance. Implementing privacy-enhancing technologies, such as encryption by default, tokenisation, and decentralised identity verification, can address risks without hindering innovation. The research also emphasises the importance of cross-border

regulatory alliances for intelligence sharing, coordinated investigations, and joint responses to cyber incidents. Introducing independent international audits and a compliance rating system could further boost accountability and public trust. By aligning technological safeguards with user rights and replacing fragmented national rules with a unified global approach, cross-border digital payment systems can be both secure and friendly to innovation. This will create a payment environment where efficiency, trust, and protection work together, ensuring resilience against current and future threats. It is time for global regulators to move beyond discussion and establish a unified, enforceable framework that ensures privacy and security rights for all users of cross-border digital payment systems.

A new Global Digital Payment Privacy Standard (GDPPS) should be created with the joint supervision of the WTO, OECD, and UNCTAD. This standard will set specific, enforceable rules for encryption strength (minimum AES-256), secure API communication, mandatory end-to-end encryption for transaction data, and multi-factor authentication for all payment authorisations. It will also require that personal data such as identity numbers, financial details, location history, and biometrics be stored in tokenised form. This ensures that even if a database is breached, raw data remains protected. Unlike existing voluntary frameworks such as the APEC Privacy Framework, the GDPPS will be binding on member countries through a treaty. Non-compliance will result in sanctions, such as temporary suspension from cross-border payment networks.

The treaty must include an International Personal Data Protection List (IPDPL) that will serve as a fixed but periodically updated catalogue of the types of personal data that must be legally protected in cross-border digital payments. This list will cover identification details, such as passport numbers and national identity documents, as well as financial records including account numbers, credit card details, and transaction logs. Additionally, it will encompass sensitive personal information, including biometrics, voice patterns, and facial recognition data. It will also include transaction-related location data and communication metadata linked to payment confirmations. All cross-border digital payment providers must classify, label, and encrypt each of these categories separately, both in storage and during transmission.

To implement the standards, a Multilateral Treaty on Cross-Border Digital Payment Privacy and Security (MT-CDPPS) should be developed under WTO trade agreements. This treaty will require member states to implement the GDPPS standards through domestic laws. It will establish a Joint Data Protection Tribunal (JDPT) that can resolve disputes across jurisdictions within ninety days. The treaty will also mandate real-time breach notifications to all affected regulators within forty-eight hours and allow joint inspections of payment service providers by international teams of certified data protection officers. A graduated system of enforcement will be

included in the treaty, encompassing official warnings, financial penalties, and possible suspension from global payment networks for repeat offenders.

To support innovation while protecting privacy, a Global Regulatory Sandbox will be launched under the treaty. This will enable fintech companies to test privacy-enhancing technologies, such as homomorphic encryption and secure multi-party computation, in live but controlled cross-border environments. Regulators from multiple countries will jointly monitor these trials. Successful technologies will be quickly incorporated into the GDPPS as mandatory best practices. This approach prevents the slow, reactive nature of traditional regulation and ensures robust future protections. For transparency and to maintain public trust, an online Global Transparency Portal will be created under the treaty's administration. This platform will require all licensed cross-border payment providers to publicly disclose their privacy policies in plain language. They must clearly identify where and how user data is stored or processed and provide a record of all data breaches over the past five years. Additionally, providers will be required to publish independent audit results showing their compliance with the GDPPS. The portal will be free for consumers, regulators, and civil society groups, allowing easy comparisons of service providers and holding them accountable for their data handling practices. This visibility will encourage companies to maintain strong privacy and security measures, as those with poor records will face reputational and competitive disadvantages.

ACKNOWLEDGMENTS

We would like to express our sincere gratitude to all those who supported us academically and personally throughout this research, despite the absence of external funding.

REFERENCES

Aditya, Z. F., & Al-Fatih, S. (2021). Indonesian constitutional rights: expressing and purposing opinions on the internet. The International Journal of Human Rights, 25(9), 1395-1419. https://doi.org/10.1080/13642987.2020.1826450.

Ahmed, H., & Ibrahim, I. R. (2018). Financial consumer protection regime in Malaysia: Assessment of the legal and regulatory framework. *Journal of Consumer Policy, 41*(2), 159–175. https://doi.org/10.1007/s10603-018-9369-0

Akanfe, O., Valecha, R., & Rao, H. R. (2020a). Assessing country-level privacy risk for digital payment systems. *Computers & Security*, *99*, 102065. https://doi.org/10.1016/j.cose.2020.102065

Akanfe, O., Valecha, R., & Rao, H. R. (2020b). Assessing country-level privacy risk for digital payment systems. *Computers & Security*, *99*, 102065. https://doi.org/10.1016/j.cose.2020.102065

Aldboush, H. H. H., & Ferdous, M. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. *International Journal of Financial Studies*, *11*(3), 90. https://doi.org/10.3390/ijfs11030090

AlHares, A., Zaerinajad, Z., & Al Bahr, M. (2024). Customer awareness and cyber security in the Organisation for Economic Co-operation and Development countries. *Corporate and Business Strategy Review*, *5*(1, special Issue), 371–381. https://doi.org/10.22495/cbsrv5i1siart11

AllahRakha, N. (2024). The Legality of Reverse Engineering and the Protection of Trade Secrets in the Software Industry. *Jurisdictie: Jurnal Hukum dan Syariah*, 15 (2), 309-334. http://dx.doi.org/10.18860/j.v15i2.28422

AllahRakha, N. (2025). Executive Discretion in Sports Awards: A Case Study of Pakistan's Olympians. *Cogent Social Science*, *11*(1), 2534414. https://doi.org/10.1080/23311886.2025.2534414

AllahRakha, N. (2025). Legislators' qualifications in Pakistan under Islamic constitutional provisions. *Journal of Human Rights, Culture and Legal System, 5*(2). https://doi.org/10.53955/jhcls.v5i2.491

Andreas Klug. (2016). *Briefing Note: Worldpay's General Approach to Privacy and EU GDPR Implementation*. https://ideas-global.org/wp-content/uploads/2018/05/External-overview-of-GDPR-strategy-for-customer-use.pdf

Andrew Burt. (2023, May 16). *The Digital World Is Changing Rapidly. Your Cybersecurity Needs to Keep Up.* Harvard Law Review. https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up

Akanfe, O., Valecha, R., & Rao, H. R. (2020). Assessing country-level privacy risk for digital payment systems. *Computers & Security, 99,* 102065. https://doi.org/10.1016/j.cose.2020.10206

Andy Schmulow, Therese Wilson, Nicola Howell, Nina Reynolds, & Paul Mazzola. (2021). Treating Customers Fairly. A concept. A framework. An alternative? *Australian Law Reform Commission Review of the Legislative Framework for Corp*. https://www.alrc.gov.au/wp-content/uploads/2023/09/Consumer-Experiences-in-Financial-Services-Results.pdf

Arora, N., & Zinolabedini, D. (2023). *The Ethical Implications of the 2018 Facebook-Cambridge Analytica Data Scandal*. The University of Texas at Austin. http://dx.doi.org/10.26153/tsw/7590

Arslan But, Pakeeza Tabassum, & Farhat Saeed Imran. (2023). Exploring The Mesopotamian Trade (C.6000-539 Bce): Types, Organization, And Expansion. *PalArch's Journal Of Archaeology Of Egypt/Egyptology*, *20*(1), 241–261. https://archives.palarch.nl/index.php/jae/article/view/11691

Auñón, J. M., Hurtado-Ramírez, D., Porras-Díaz, L., Irigoyen-Peña, B., Rahmian, S., Al-Khazraji, Y., Soler-Garrido, J., & Kotsev, A. (2024). Evaluation and utilisation of privacy enhancing technologies—A data spaces perspective. *Data in Brief, 55,* 110560. https://doi.org/10.1016/j.dib.2024.110560

Ayatulloh Michael Musyaffi, Etty Gurendrawati, Bambang Afriadi, Mario Colega Oli, & Yuni Widawati, R. O. (2022). Resistance of Traditional SMEs in Using Digital Payments: Development of Innovation Resistance Theory. *Human Behavior and Emerging Technologies*. https://doi.org/10.1155/2022/7538042

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, *6*(2), 205395171985509. https://doi.org/10.1177/2053951719855091

Bénétrix, A., Gautam, D., Juvenal, L., & Schmitz, M. (2020). Cross-Border Currency Exposures: New Evidence Based on an Enhanced and Updated Dataset. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3611655

Bimantara, A., & Nugraha, R. T. (2025). The politics of international cooperation in cross-border digital payment connectivity: A case study of QR payment system in ASEAN. *Sospol, 11*(1), 82–99. https://doi.org/10.22219/jurnalsospol.v11i1.38367

Bradford, L., Aboy, M., & Liddell, K. (2021). Standard contractual clauses for cross-border transfers of health data after *Schrems II*. *Journal of Law and the Biosciences*, *8*(1). https://doi.org/10.1093/jlb/lsab007

Coche, E., Kolk, A., & Ocelík, V. (2024). Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, *7*(1), 112–127. https://doi.org/10.1057/s42214-023-00172-1

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Cymone Gosnell. (2019). The General Data Protection Regulation: American Compliance Overview and the Future of the American Business. *Journal of Business & Technology Law*, *15*(1). https://digitalcommons.law.umaryland.edu/jbtl/vol15/iss1/6

Daniel Tolstoy, Emilia Rovira Nordman, Sara Melén Hånell, & Nurgül Özbek. (2021). The development of international e-commerce in retail SMEs: An effectuation perspective. *Journal of World Business*, *56*(3). https://doi.org/10.1016/j.jwb.2020.101165

David W. Opderbeck. (2023). Cybersecurity and Data Breach Harms: Theory and Reality. *Maryland Law Review*, *82*(4). https://digitalcommons.law.umaryland.edu/mlr/vol82/iss4/4

De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, *55*, 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

Dilip Ratha. (2023). *Remittances: Funds for the Folks Back Home*. IMF. https://www.imf.org/en/Publications/fandd/issues/Series/Back-to-Basics/Remittances

Dinçkol, D., Ozcan, P., & Zachariadis, M. (2023). Regulatory standards and consequences for industry architecture: The case of UK Open Banking. *Research Policy*, *52*(6), 104760. https://doi.org/10.1016/j.respol.2023.104760

Dorfleitner, G., Hornuf, L., & Kreppmeier, J. (2023). Promise not fulfilled: FinTech, data privacy, and the GDPR. *Electronic Markets*, *33*(1), 33. https://doi.org/10.1007/s12525-023-00622-x

Engström, E., Eriksson, K., Björnstjerna, M., & Strimling, P. (2023). Global variations in online privacy concerns across 57 countries. *Computers in Human Behavior Reports*, *9*, 100268. https://doi.org/10.1016/j.chbr.2023.100268

Esteban Ortiz-Ospina, Diana Beltekian, & Max Roser. (2024, April). *Trade and Globalization*. Our World In Data. https://ourworldindata.org/trade-and-globalization

Fahad, & Shahid, M. (2022). Exploring the determinants of adoption of Unified Payment Interface (UPI) in India: A study based on diffusion of innovation theory. *Digital Business*, *2*(2), 100040. https://doi.org/10.1016/j.digbus.2022.100040

Fatima, R., Yasin, A., Liu, L., Wang, J., Afzal, W., & Yasin, A. (2019). Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. *Journal of Information Security and Applications*, *48*, 102351. https://doi.org/10.1016/j.jisa.2019.06.007

Ferrari, M. V. (2022). The platformisation of digital payments: The fabrication of consumer interest in the EU FinTech agenda. *Computer Law & Security Review*, *45*, 105687. https://doi.org/10.1016/j.clsr.2022.105687

Ferreira, A., & Sandner, P. (2021). Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law & Security Review*, *43*, 105632. https://doi.org/10.1016/j.clsr.2021.105632

Florencia Marotta-Wurgler. (2016). Self-Regulation and Competition in Privacy Policies. *The Journal of Legal Studies*, *45*(S), 13–39. https://chicagounbound.uchicago.edu/jls/vol45/iss3/2

Goyeneche, D., Singaraju, S., & Arango, L. (2024). Linked by age: a study on social media privacy concerns among younger and older adults. *Industrial Management & Data Systems*, *124*(2), 640–665. https://doi.org/10.1108/IMDS-07-2023-0462

Hillman, S., Neustaedter, C., Oduor, E., & Pang, C. (2014). User challenges and successes with mobile payment services in North America. *Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services*, 253–262. https://doi.org/10.1145/2628363.2628389

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1589864

Hu, K., Gong, S., Zhang, Q., Seng, C., Xia, M., & Jiang, S. (2024). An overview of implementing security and privacy in federated learning. *Artificial Intelligence Review, 57*(1), 204. https://doi.org/10.1007/s10462-024-10754-9

Ibrahim Niankara, & Rachidatou I. Traoret. (2023). The digital payment-financial inclusion nexus and payment system innovation within the global open economy during the COVID-19 pandemic. *Journal of Open Innovation: Technology, Market, and Complexity*, *9*(4). https://doi.org/10.1016/j.joitmc.2023.100173

Irini Kanaris Miyashiro. (2021). *Case Study: Equifax Data Breach*. Seven Pillars Institute. https://sevenpillarsinstitute.org/case-study-equifax-data-breach/

Jan Hogendorn, & Marion Johnson. (2003). *THE SHELL MONEY OF THE SLAVE TRADE*. Cambridge University Press. https://doi.org/10.1017/CBO9780511563041

Joanne K. McQuilty. (2020). *The Privacy Paradox: An Investigation of Smart Applications, Social Relations and Privacy*. University of Wollongong. https://ro.uow.edu.au/articles/thesis/The_Privacy_Paradox_An_Investigation_of_Smart_Applications_Social_Relations_and_Privacy/27667086?file=50387322

John Pickering. (1844). The History of Paper Money in China. *Journal of the American Oriental Society*, *1*(2), 136–142. https://doi.org/10.2307/3217743

John Rothchild. (1999). Protecting the Digital Consumer: The Limits of Cyberspace Utopianism. *Indiana Law Journal*, *74*(3). https://www.repository.law.indiana.edu/ilj/vol74/iss3/5

Jong-Hyuok Jung, Eunseon Kwon, & Dong Hoo Kim. (2020). Mobile payment service usage: U.S. consumers' motivations and intentions. *Computers in Human Behavior Reports*, *1*. https://doi.org/10.1016/j.chbr.2020.100008

Juliussen, B. A., Kozyri, E., Johansen, D., & Rui, J. P. (2023). The third country problem under the GDPR: enhancing protection of data transfers with technology. *International Data Privacy Law*, *13*(3), 225–243. https://doi.org/10.1093/idpl/ipad013

Jun Yong Xiang, & Jing Linbo. (2021). Electronic Commerce in China: Current Status, Development Strategies, and New Trends. *China Finance and Economic Review*, *3*(3), 71–94. https://www.degruyterbrill.com/journal/key/cfer/3/3/html?srsltid=AfmB

OoqTTkTrlIagVFDOm9K7B8xY9Y4nh39I3QFWMuYKDbjBnH_SYL_9#issuesInVolume

Karoly, P. (1993). Mechanisms of Self-Regulation: A Systems View. *Annual Review of Psychology*, *44*(1), 23–52. https://doi.org/10.1146/annurev.ps.44.020193.000323

Kaur, G. (2024). Privacy implications of central bank digital currencies (CBDCs): A systematic review of literature. *EDPACS, 69*(9), 87–123. https://doi.org/10.1080/07366981.2024.2376794

Khando Khando, M. Sirajul Islam, & Shang Gao. (2023). The Emerging Technologies of Digital Payments and Associated Challenges: A Systematic Literature Review. *Future Internet*, *15*(1). DOI:10.3390/fi15010021

Krishna, B., Krishnan, S., & Sebastian, M. P. (2023). Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective. *Information Technology & People*. https://doi.org/10.1108/ITP-05-2023-0434

Kurt Knutsson. (2023, May 29). The dark side of PayPal and how to stay safe. *Fox News*. https://www.foxnews.com/tech/dark-side-paypal-stay-safe

L. Randall Wray. (1999). *The Origins of Money and the Development of the Modern Financial System*. https://doi.org/10.1057/9781137539922

Law, J. (2025). 11: Singapore payment services. In *Payment services*. Edward Elgar Publishing. https://doi.org/10.4337/9781035332878.00019

Leora Klapper. (2023). *How digital payments can benefit entrepreneurs*. IZA World of Labor. https://wol.iza.org/uploads/articles/648/pdfs/how-digital-payments-can-benefit-entrepreneurs.pdf

Linh, T. T. (2025). Adoption of digital payment methods in Vietnam: Key determinants and distribution analysis. *Journal of Distribution Science, 23*(2), 39–49. https://doi.org/10.15722/JDS.23.02.202502.39

Lowry, P. B., Wells, T. M., Moody, G., Humpherys, S., & Kettles, D. (2006). Online Payment Gateways Used to Facilitate E-Commerce Transactions and Improve Risk Management. *Communications of the Association for Information Systems*, *17*. https://doi.org/10.17705/1CAIS.01706

McKay Smith, & Garrett Mulrain. (2018). Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform. *JOURNAL OF NATIONAL SECURITY LAW & POLICY*, *9*, 549–588. https://nationalsecurity.law.georgetown.edu/journal/2018/07/11/equi-failure-the-national-security-implications-of-the-equifax-hack-and-a-critical-proposal-for-reform/

Michael Peneder. (2022). Digitization and the evolution of money as a social technology of account. *Journal of Evolutionary Economics*, *32*, 175–203. https://doi.org/10.1007/s00191-021-00729-4

Michele Braun, James McAndrews, William Roberds, & Richard Sullivan. (2008). Understanding Risk Management in Emerging Retail Payments. *FRBNY Economic Policy Review*, 137–159. https://www.newyorkfed.org/medialibrary/media/research/epr/08v14n2/0809brau.pdf

Naeem AllahRakha. (2024). Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations. *Pakistan Journal of Criminology*, *16*(2), 119–132. https://doi.org/10.62271/pjc.16.2.119.132

Parma Bains, & Caroline Wu. (2023). *Institutional Arrangements for Fintech Regulation: Supervisory Monitoring* (NOTE/2023/004). https://doi.org/10.5089/9798400245664.063

Praveen Shanmugalingam, Ahashraaj Shanmuganeshan, Abinaya Manorajan, Mathusany Kugathasan, & Geethma Yahani Pathirana. (2023). Does e-commerce really matter on international trade of Asian countries: Evidence from panel data. *PLOSEONE*. https://doi.org/10.1371/journal.pone.0284503

Putrevu, J., & Mertzanis, C. (2024a). The adoption of digital payments in emerging economies: challenges and policy responses. *Digital Policy, Regulation and Governance*, *26*(5), 476–500. https://doi.org/10.1108/DPRG-06-2023-0077

Putrevu, J., & Mertzanis, C. (2024b). The adoption of digital payments in emerging economies: challenges and policy responses. *Digital Policy, Regulation and Governance*, *26*(5), 476–500. https://doi.org/10.1108/DPRG-06-2023-0077

Rachman, A., Julianti, N., & Arkoyah, S. (2024). Challenges and opportunities for QRIS implementation as a digital payment system in Indonesia. *EkBis: Jurnal Ekonomi Dan Bisnis,* *8*(1), 1–13. https://doi.org/10.14421/EkBis.2024.8.1.2134

Raikar, S., & Adamson, S. (2020). Renewable project finance structures and risk allocation. In *Renewable Energy Finance* (pp. 55–66). Elsevier. https://doi.org/10.1016/B978-0-12-816441-9.00005-2

Regulatory and Policy Gaps and Inconsistencies of Digital Currencies (2/8 Digital Currency Governance Consortium White Paper Series). (2021). https://www3.weforum.org/docs/WEF_Regulatory_and_Policy_Gaps_2021.pdf

Rizka Ramayanti, Nurul Aisyah Rachmawati, Zubir Azhar, & Nik Hadiyan Nik Azman. (2024). Exploring intention and actual use in digital payments: A systematic review and roadmap for future research. *Computers in Human Behavior Reports*, *13*. https://doi.org/10.1016/j.chbr.2023.10034

Sahi, A. M., Khalid, H., Abbas, A. F., Zedan, K., Khatib, S. F. A., & Al Amosh, H. (2022). The Research Trend of Security and Privacy in Digital Payment. *Informatics*, *9*(2), 32. https://doi.org/10.3390/informatics9020032

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data-driven business and data privacy: Challenges and measures for product-based companies. *Business Horizons*, *66*(4), 493–504. https://doi.org/10.1016/j.bushor.2022.10.002

Schweidel, D. A., Bart, Y., Inman, J. J., Stephen, A. T., Libai, B., Andrews, M., Rosario, A. B., Chae, I., Chen, Z., Kupor, D., Longoni, C., & Thomaz, F. (2022). How consumer digital signals are reshaping the customer journey. *Journal of the Academy of Marketing Science*, *50*(6), 1257–1276. https://doi.org/10.1007/s11747-022-00839-w

Seethamraju, Ravi Diatha, & Krishna Sundar. (2019). Digitalization of Small Retail Stores - Challenges in Digital Payments. *Proceedings of the 52nd Hawaii International Conference on System Sciences*. DOI:10.24251/HICSS.2019.621

Siona Listokin. (2015). Industry Self-Regulation of Consumer Data Privacy and Security. *John Marshall Journal of Information Technology & Privacy Law*, *32*(1). https://repository.law.uic.edu/jitpl/vol32/iss1/2/

Tanai Khiaonarong, & Terry Goh. (2020). *Fintech and Payments Regulation: Analytical Framework*. https://www.imf.org/en/Publications/WP/Issues/2020/05/29/Fintech-and-Payments-Regulation-Analytical-Framework-49086

TIMOTHY WOLTERS. (2000). "Carry Your Credit in Your Pocket": The Early History of the Credit Card at Bank of America and Chase Manhattan. *Enterprise & Society*, *1*(2), 315–354. https://doi.org/10.5089/9781513531496.001

Velez, G. (2025). A systematic review of mobile banking, fintech innovations, and regulatory gaps to achieve financial inclusion in the Philippines. *Journal of Interdisciplinary Perspectives,* *3*(3), 390–397. https://doi.org/10.69569/jip.2025.056

Victor Murinde, Efthymios Rizopoulos, & Markos Zachariadis. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis*, *81*. https://doi.org/10.1016/j.irfa.2022.102103

Wisniewski, P. J., & Page, X. (2022). Privacy Theories and Frameworks. In *Modern Socio-Technical Perspectives on Privacy* (pp. 15–41). Springer International Publishing. https://doi.org/10.1007/978-3-030-82786-1_2

Zaki Irfan Al Hafizh, & Anas Hidayat. (2022). The role of digital payment benefits toward switching consumer behavior in the case of OVO application. *International Journal of Research in Business and Social Science*, *11*(7), 23–34. DOI: 10.20525/ijrbs.v11i7.2156

Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). Data Security, Customer Trust and Intention for Adoption of Fintech Services: An Empirical

Analysis from Commercial Bank Users in Pakistan. *SAGE Open*, *13*(3). https://doi.org/10.1177/21582440231181388

Zhimao Wang, & Xucheng Huang. (2023). Understanding the role of digital finance in facilitating consumer online purchases: An empirical investigation. *Finance Research Letters*, *55*(Part B). https://doi.org/10.1016/j.frl.2023.103939

Zlatko Bezhovski. (2016). The Future of the Mobile Payment as Electronic Payment System. *European Journal of Business and Management*, *8*(8). https://core.ac.uk/download/pdf/234627158.pdf