# E-COMMERCE & DIGITAL SECURITY
# Assignment-9
N Ravinder Reddy
Roll No: 2406CYS106

**E-Commerce Assignment Questions**

Q. 1. Investigate the regulatory landscape governing e-commerce security and data privacy, including GDPR, CCPA, and PCI DSS standards. Assess the impact of these regulations on e-commerce businesses and their compliance requirements. Develop a compliance framework and best practices for handling customer data, ensuring data privacy, obtaining consent, and maintaining transparency in data collection and processing practices.

Ans: CCPA and GDPR are compliance laws that aim at protecting user data from unauthorized access and processing. CCPA has often been called the 'GDPR lite' version in the compliance communities and there is a fairly supportive logical reasoning to that debate.

In today's digital age, where personal information is constantly collected, processed, and shared, data privacy has become a paramount concern for individuals and organizations alike. Data breaches and privacy scandals have highlighted the need for robust regulations to safeguard individuals' rights and hold businesses accountable for their data practices.

Both the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) of the European Union address these concerns by imposing obligations on businesses regarding the collection, use, and protection of personal data. Understanding the intricacies of these regulations is essential for businesses to navigate the complex landscape of data privacy compliance effectively.

| GDPR | PCI DSS |
|---|---|
| Government mandate | Payment card industry self-regulation |
| Concerns the rights and freedoms of those in the EU | Concerns security and processing of payment card and cardholder data |
| Applies to ANY personally identifiable information of EU citizens | Applies to payment card and cardholder data |
| Covers ALL processing of personal data | Covers storage, transmission, and processing of cardholder data |
| Data controllers and data processors must demonstrate compliance | Merchants and service providers must demonstrate compliance |
| Certifying bodies in process of being defined | Certification authority: PCI Council |
| No formal method to demonstrate compliance | Compliance demonstrated through Attestation of Compliant (AOC) |
| Supervisory Authorities from EU memberstates monitor compliance | Acquiring banks monitor compliance of merchants. Merchant monitors compliance for service providers |

The CCPA, enacted in 2018, represents a significant milestone in U.S. data privacy legislation, granting California residents greater control over their personal information. It applies to businesses that meet specific criteria, irrespective of their physical location, and imposes obligations regarding data transparency, consumer rights, and data security.

On the other hand, the GDPR, implemented in 2018, sets a high standard for data protection globally. It applies to organizations processing personal data of EU residents, regardless of their location, and establishes principles such as data minimization, purpose limitation, and accountability. While both regulations share common objectives, they have distinct requirements and enforcement mechanisms, necessitating a comparative analysis to facilitate compliance efforts.

| | CCPA | GDPR |
|---|---|---|
| Date passed or adopted: | June 28, 2018 | April 8, 2016 |
| Date effective or enforcable: | January 1, 2020 | May 25, 2018 |
| Who is regulated: | Legal entities doing business in CA w/ rev. of > $25M or process info of ≥ 50,000 | Any business in the world thatprocesses personal data of an EU citizen. |
| Who is protected: | Consumers who are California residents | Data subjects who are EU citizens |
| What is protected: | Info that identifies, relates to, describes, associates with, or links to customer. | Personal data: any info relating to an identified or identifiable data subject. |
| Security Requirements: | None specifically named but reasonable controls implied | Appropriate technical and organizational measures are mandated |
| Fines: | Privately: $100 to $750 per consumer, per incident. Civil: $2500-$7500 per violation. | Up to €20 million or 4% of the annual worldwide turnover, whichever is greater. |
| Children: | Addresses only the sale of children's information. Need opt-in consent under age 13. | Parents must provide consent for personal info use in online environment. |
| Right to be Forgotten/Deletion: | Applies only to data collected from consumer. | Applies to any data collected from or about the data subject. |

Compliance with both GDPR (General Data Protection Regulation) and PCI DSS (Payment Card Industry Data Security Standard) is crucial for businesses that handle sensitive data and want to ensure the privacy of their customers. Let's explore why:

1. GDPR (General Data Protection Regulation):
   - Impact and Changes: GDPR, adopted in 2016 and implemented in May 2018, has significantly influenced the privacy landscape worldwide. It emphasizes individual privacy rights and transparency in data collection and usage practices.
   - Applicability: GDPR applies to any organization handling data on EU citizens, regardless of where the organization is located. Even if a company complies with PCI DSS and has just one EU customer, it must also comply with GDPR.
   - Consequences of Non-Compliance: Failure to comply with GDPR can result in hefty fines and other penalties. A staggering 95% of companies required to comply with GDPR were either partially compliant or non-compliant with its requirements.

- Public Awareness: GDPR has inspired similar privacy laws in over 100 countries, emphasizing the importance of data privacy and security.

2. PCI DSS (Payment Card Industry Data Security Standard):

- Purpose: PCI DSS aims to secure payment card transactions and protect cardholder data.
- Scope: It primarily focuses on securing payment card data, whereas GDPR covers a broader range of personal data.
- Overlap: While being compliant with PCI DSS may help achieve some GDPR compliance, it doesn't guarantee full compliance. Organizations processing credit cards from EU citizens must comply with both standards.
- Consequences of Non-Compliance: Noncompliance with PCI DSS can lead to reputational damage, loss of customers, and the inability to process payment card transactions.
- Global Impact: PCI DSS has been influential globally, ensuring secure payment card transactions.

3. The e-commerce industry in India has witnessed phenomenal growth in recent years. Despite the pandemic, the sector is expected to grow at a CAGR of 20% by 2025. However, the regulatory environment in India can be complex and challenging, potentially impacting the operations and revenue of e-commerce businesses. Thus, it is essential to understand The e-commerce Regulations in India to maximize success.
4. An overview of the e-commerce industry in India
5. The e-commerce industry in India is estimated to be worth $200 billion by 2026. It consists of various players such as B2B, B2C, C2C, and hyper-local delivery models. The industry is further segmented into categories like electronics, apparel, and accessories, among others. Additionally, factors such as increasing internet penetration, growing middle-class, and the government's inclination towards digitalization have contributed to the industry's growth.
6. The importance of understanding India's regulatory landscape for e-commerce businesses
7. While the growth potential of the e-commerce industry in India is enormous, businesses must navigate the regulatory framework, which can be complex. Indian regulatory policies related to Foreign Direct Investment (FDI), intellectual property, consumer protection, employment, and labour, among others, have a substantial impact on e-commerce businesses. Non-compliance with regulations can have severe repercussions. Therefore, it is paramount for businesses to understand and comply with national and state-level laws and regulations.
8. Understanding India's Regulatory Landscape
9. Overview of India's regulatory framework for e-commerce
10. India's regulatory framework for e-commerce is governed by various laws, policies, and guidelines. The government has issued various regulations as the industry has grown over the years, such as the Press Note 2 of 2018, which sought tighter scrutiny of e-commerce firms with foreign investments.
11. India's regulatory policies and laws on e-commerce

12. India has several regulatory policies and laws related to e-commerce. These policies and laws aim to protect consumers' rights, ensure data privacy, ensure open competition, control and regulate foreign investment, and protect traditional offline retailers and manufacturers' interests. Some of the significant policies and laws that impact e-commerce are the FDI policy, Consumer Protection Act, Information Technology Act, and Prevention of Money Laundering Act.
13. The impact of India's regulations on e-commerce businesses
14. India's regulatory policies can have a significant impact on e-commerce businesses, affecting their operations, revenue, and market share. For instance, the FDI policy significantly impacts companies that have foreign investment, restricting them from selling products directly to consumers. Similarly, non-compliance with established data privacy and protection laws can damage a company's reputation.
15. The reasons for the regulations
16. India's regulatory policies for e-commerce aim to balance the interests of the stakeholders in the industry. At the core of these policies lie concerns around data privacy, consumer protection, intellectual property protection, and transparent and fair competition.
17. Compliance with the Foreign Direct Investment (FDI) Policy
18. Understanding India's FDI policy for e-commerce
19. India's FDI policy for e-commerce is aimed to ensure that foreign capital does not lead to unfair competition. According to the policy, e-commerce firms with foreign investments can operate in India, but they cannot hold inventory or sell products directly to consumers.
20. The implications of FDI regulations for e-commerce businesses
21. FDI regulations can impact e-commerce businesses, especially those with significant foreign investment. It may cause businesses to change their operating structures, such as setting up vendor entities to comply with regulations.
22. How to comply with FDI regulations in India
23. To comply with FDI regulations, e-commerce businesses must structure their operations and transactions in a manner that complies with the rules set forth by the Indian government. This can include setting up separate entities to manage inventory and engage with customers and vendors.
24. Understanding the E-commerce Guidelines for Consumer Protection

25.
26. Overview of the guidelines for e-commerce consumer protection in India
27. The E-commerce Guidelines for Consumer Protection require e-commerce firms to provide consumers with detailed information about the products, including pricing, terms of sale, and refund or return policies.
28. The key provisions of the guidelines for e-commerce consumer protection

29. The guidelines require e-commerce platforms to provide detailed descriptions of products and services promoted on their platforms. Additionally, they must display the details of the seller, including their name, address, and customer care contact details.
30. The implications of e-commerce consumer protection guidelines for businesses
31. The guidelines aim to create transparency and build consumer trust in e-commerce platforms. Thus, businesses that do not comply with these guidelines may face consumer backlash and hurt their reputation.
32. How to comply with e-commerce consumer protection guidelines in India
33. To comply with consumer protection guidelines, e-commerce businesses must provide detailed information about products and sellers, including descriptions and customer care contact information on their platforms.
34. Taxation Regulations for E-commerce Businesses in India
35. Overview of India's taxation policies for e-commerce businesses
36. E-commerce businesses in India must comply with various taxation policies, including those related to goods and services tax (GST) and income tax.
37. The applicable taxes for e-commerce businesses in India
38. E-commerce businesses with income exceeding ₹20,00,000 (approximately $27,000) are required to register under the GST and collect and pay taxes to the government.
39. The implications of taxation regulations for e-commerce businesses
40. Non-compliance with taxation regulations can lead to penalties and legal action. This can impact a business's operations and revenue negatively.
41. How to comply with taxation regulations for e-commerce businesses in India
42. E-commerce businesses in India must obtain GST registration, file GST returns on time, and collect and pay applicable taxes to stay compliant with taxation regulations.
43. Intellectual Property Rights (IPR) Regulations
44. Understanding India's IPR regulations for e-commerce businesses
45. India's IPR regulations aim to protect the rights of intellectual property holders. These include trademarks, copyrights, patents, and industrial designs.
46. The consequences of non-compliance with IPR regulations in India
47. Non-compliance with IPR regulations can lead to legal action, seizures of goods, and damages paid to the right holders, resulting in significant financial losses for a business.
48. How to comply with IPR regulations in India

49. To comply with IPR regulations, e-commerce businesses must ensure that they do not infringe on any intellectual property rights while selling products on their platforms.
50. Data Protection and Privacy Laws

51.
52. Overview of India's data protection and privacy laws for e-commerce businesses
53. India's data protection and privacy laws govern businesses' collection, storage, use, and sharing of personal data and information of consumers on e-commerce platforms. These include the Personal Data Protection Bill, 2019.
54. The implications of data protection and privacy laws for e-commerce businesses
55. Non-compliance with data protection and privacy laws can lead to regulatory action, legal liability, and loss of consumer trust and loyalty.
56. How to comply with data protection and privacy laws in India
57. To comply with data protection and privacy laws, e-commerce businesses must implement adequate cybersecurity measures, obtain consent from consumers before collecting data, and maintain data confidentiality and privacy.
58. Employment and Labour Regulations
59. Overview of India's employment and labour regulations for e-commerce businesses
60. India's employment and labour regulations aim to protect workers' rights and regulate their working conditions, wages, and work hours.
61. The implications of employment and labour regulations for e-commerce businesses
62. Non-compliance with employment and labour regulations can lead to legal action and penalties, impacting a business's reputation and revenue.
63. How to comply with employment and labour regulations in India
64. E-commerce businesses must ensure compliance with regulations related to hiring, termination, wages, working hours, safety, and social security obligations for their employees.
65. Licence and Registration Requirements for E-commerce Businesses in India
66. Overview of the licence and registration requirements for e-commerce businesses in India
67. E-commerce businesses must obtain specific licenses and registrations to operate legally in India, such as registration under the Companies Act, and GST registration.
68. The implications of non-compliance with licence and registration requirements in India
69. Non-compliance with licensing and registration requirements can lead to regulatory action and legal penalties, hindering the growth and expansion of a business.

70. How to comply with licence and registration requirements in India
71. To comply with licensing and registration requirements, e-commerce businesses must obtain the necessary licences and registrations and ensure that they are renewed and maintained according to the regulations.

72.
73. Logistics and Supply Chain Regulations in India
74. Overview of the logistics and supply chain regulations in India
75. India's logistics and supply chain regulations impact the operations of e-commerce businesses. They govern transportation, warehousing, and distribution, among others.
76. The implications of logistics and supply chain regulations for e-commerce businesses
77. Non-compliance with logistics and supply chain regulations can lead to operational disruptions and revenue losses for e-commerce businesses.
78. How to comply with logistics and supply chain regulations in India
79. To comply with logistics and supply chain regulations, e-commerce businesses must ensure proper transportation, storage, and distribution of goods while adhering to the applicable regulations.
80. Marketing and Advertising Regulations in India
81. Overview of the marketing and advertising regulations in India
82. India's marketing and advertising regulations govern advertisements' content, placement, and targeting on e-commerce platforms.
83. The implications of marketing and advertising regulations for e-commerce businesses
84. Non-compliance with marketing and advertising regulations can lead to legal action and damages, impacting a business's revenue and reputation.
85. How to comply with marketing and advertising regulations in India
86. E-commerce businesses must comply with marketing and advertising regulations and ensure that advertisements follow standards regarding their content, placement, and targeting.
87. Payment and Settlement Regulations in India
88. Overview of the payment and settlement regulations in India
89. India's payment and settlement regulations govern the transactions made on e-commerce platforms, including electronic fund transfers, prepaid payment instruments, and payment gateways.
90. The implications of payment and settlement regulations for e-commerce businesses
91. Non-compliance with payment and settlement regulations can lead to penalties and legal action, hampering a business's revenue and reputation.
92. How to comply with payment and settlement regulations in India

93. E-commerce businesses in India must comply with payment and settlement regulations by following the acceptable payment methods and ensuring safe and secure transactions for consumers.
94. E-commerce Business Models and Regulations in India
95. Overview of the different e-commerce business models in India
96. India's e-commerce industry comprises of various business models, such as B2B, B2C, and C2C, each with its specific regulatory requirements.
97. The implications of different e-commerce business models for businesses
98. E-commerce businesses must choose the right business model that complies with the specific regulations governing their model.
99. How to choose the right e-commerce business model that complies with regulations in India
100. E-commerce businesses must assess the regulatory environment and identify the most appropriate business model that aligns with the regulatory requirements.
101. Navigating the Complexities of E-commerce Regulations in India
102. The common challenges faced by e-commerce businesses in India
103. E-commerce businesses in India face several challenges, such as complying with complex regulations, dealing with multiple state-level laws, and the absence of a centralized regulatory body.
104. The strategies to overcome these challenges
105. E-commerce businesses can overcome challenges by seeking professional advice and guidance, mapping regulatory requirements, and implementing appropriate compliance processes.
106. The importance of seeking professional advice and guidance
107. Seeking professional advice and guidance can help e-commerce businesses understand and comply with the complex and evolving regulatory environment in India.

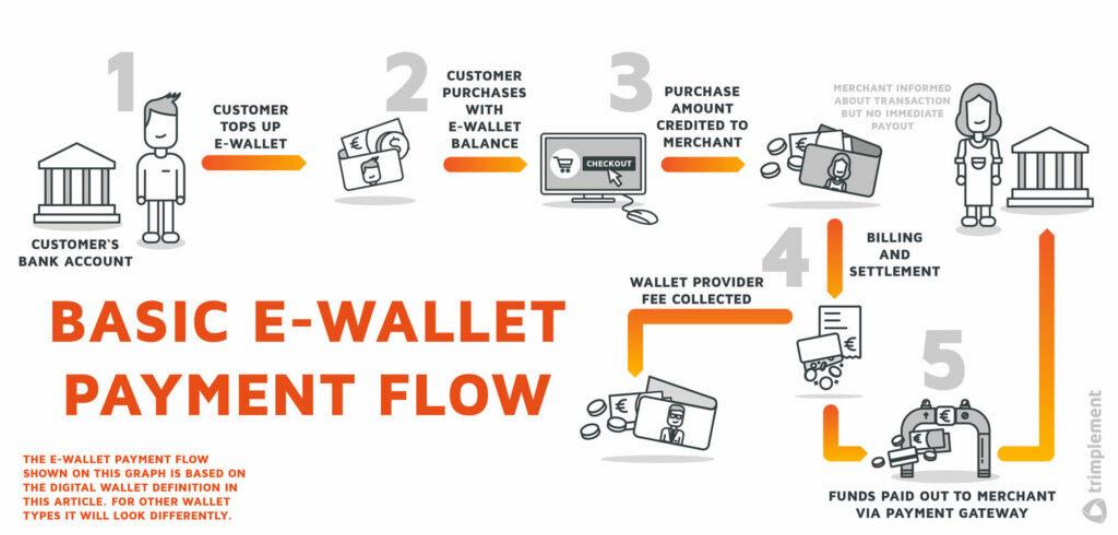
**Digital Payment Assignment Questions.**

Q.1. Analyze the factors influencing the adoption of digital payment methods such as mobile wallets, contactless payments, and peer-to-peer transfers among consumers. Investigate consumer preferences, trust issues, and perceptions of security associated with digital payment technologies.

a. Develop a research study to understand the key drivers and barriers to digital payment adoption and propose strategies to encourage widespread acceptance and usage.

Ans:

In the growing era of the digitization of the technology much of the people have using the plastic money in the form of Debit Card, Credit Card and other cards provided by the numerous respective commercial banks. The banking industry had an array of payment products – Core banking Services, immediate payment service, net banking and mobile banking; but it is found that people needed an easier, simpler way to make payments. so this gap was filled by the digital wallets or e-wallets. This paper is constructed to find out the adoption behaviour and change in the daily payment or transactions. This research is based on the various studies done on the Mobile e-wallets by the various researchers during the past two decade with an aim to find out the payment and adoption behaviour among the consumers. After the analysing the research articles the major finding is that the age group from 21-35 years are mostly using the e-wallets for the purpose of mobile and DTH recharges, booking of movie tickets, bill payments, money transfers. The reason behind is the security, easy to use, convenient method and no loss of personal information because of scan and pay method is available in the form of NFC. It is also found that many studies say that there is no significant relation between gender and the use of digital wallets.




The spring up growth in the mobile and internet phenomena. The most of the mobile users were shifted towards using of the smartphones with the heavy use of mobile internet or 3G 4G services. As the ramification of revolution in IT in the current scenario every class of society becoming more familiar with use of mobile banking, plastic money and the new era of digital payments. Mobile payment services are operated under financial regulation and performed from or via a mobile device. Instead of paying with money, cheque, or credit cards, a consumer can use a mobile to pay for a wide range of services and digital or hard goods. As on 31st May, 2017 there are 1,180,82 million wireless subscribers. High level of mobile user penetration provides immense opportunity to boost mobile banking[1]. Mobile technology, observed as a payment or banking channel, it represents an opportunity for financial

inclusion among a population that is underserved by traditional banking services (Diniz, et. al. 2011). Different ways for keeping your cash forever emerge alongside time. Sometime back, people mostly rely only on the cash, but as the time passes out, the trend of plastic money (ATM Cards) becoming popular and it's really the secure and more comfortable[3].

A Digital pocketbook refers to associate device that enables a personal to form transactions over product or product category. Here individual bank account can also be linked to digital wallet so that they can do transaction. A digital wallet is a system that securely stores users' payment information and password for number of payments methods and websites, major benefit of digital wallet services it works through application on your Smartphone [3]. The era of ICT (Information and Communication Technology) and digital innovations has come along with a dynamic change in the world business environment, whereby business transactions are constantly shifting from cash-based transactions to electronicbased ones [4]

The very first patent of the mobile e wallet was registered in the year of 2000, this was the starting of a revolution in the field of digital payments. In this research paper forty-five studies were taken for the evaluation and the time phrase is divided into four phases i.e. From 2002-2004, 2005-2009, 2010-2015 and 2016- 2019 or present. In the above said time period, many of the factors are same and many of the new, which attracts the consumers to adopt and go digitally for making payments.

In the year of 2000 there was the first patent of mobile e-wallet registered. After this regime the face of online and e-banking were being changed. Internet forces square measure poignant the banking sector transition quite the other monetary supplier cluster. E-Bank solution should deliver three key requirements: High Availability, Scalability and Security, Network security, data integrity and privacy [5]. Mobile Ecommerce addresses electronic commerce via mobile devices, where the buyer isn't in physical or eye contact with the products that square measure being purchased. On the contrary in M-Trade the buyer has eye contact with offered merchandise and services. In each cases the payment procedure is dead via the mobile network. No successful mobile payment system has yet lived up the different requirements from the market and thereby not been a success [5].There are different critical success factors and requirements considering the involvement of different factors such as Ease of use, Security, Comprehensiveness, Expenses, Technical Acceptability[5]. However, no standardised, broadly adopted mobile payment method has yet emerged, and this is supposed to be one of the factors that inhibits rife use of mobile commerce The interviewees emphasized merchant acceptance and consumer acceptance (universality), and stressed the importance of cost (transaction fees) and ease of use for both parties Security was emphasized, both for merchants and for customers, but it was usually framed in a factor that can best be described as perceived risk [6]no standardised, widely adopted mobile

payment system has yet emerged, and this is believed to be one of the factors that inhibits widespread use of mobile commerce. This paper report on a research project in which the factors are examined that affect the introduction success of mobile payment systems. We start from the venture point that a lot can be learned from research on internet paying systems, payment systems that have been introduced to faciliate payments made over the internet. First we transferred factors affecting the introduction of internet payment systems to a mobile setting. We then contrasted this list with the views of 13 executives we interviewed in Sweden and the Netherlands. We found that while many factors are at play at the same time, a subset of these stood out at the early stages of the lifecycle of mobile payment systems. In the area of consumer acceptance, these are their cost and their ease of use relative to other payment methods, and the perceived risk. In the area of merchant acceptance, transaction fees compared to debit and credit card systems are important, as is, to a significant extent, the ease of use for the merchant.

Time saving Digital wallet reduces the amount of time needed to do a transaction. Digital wallets facilitate to keep amount in electronic mode so that it will be comfortable to make online payments without enter the card details. If users' want to make me payment in other mode, they have entered the details about cards. Digital wallet keep amount in electronic form so that user can make payment without much time[32].

2. Ease of use Digital wallet is like one click pay with no need to fill details about card viz card number, passwords every time. It allows user to link digital wallet to accounts and pay immediately so that no hassles to enter the details each time[40]mobile penetration and government initiative such as Digital India are acting as catalyst which leads to exponential growth in use of digital payment. Electronics Consumer transaction made at point of sale (POS

3. Security Digital wallet can increase the transaction security since the wallet does not pass the payment card details to the website. Digital wallet allows users lock your wallet. Most of Digital wallet service provides extra security to keep your money secure from unauthorized access[40]mobile penetration and government initiative such as Digital India are acting as catalyst which leads to exponential growth in use of digital payment. Electronics Consumer transaction made at point of sale (POS.

4. Convenient and information stored under one roof Digital wallets are convenient; it helps to eliminate need to carry the physical wallet. There would synchronization of data from multiple platforms. Bank accounts, credit and debit cards, mobile accounts and bills - all will be interconnected and help in better management[3], [40]mobile penetration and government initiative such as Digital India are acting as catalyst which leads to exponential growth in use of digital payment. Electronics Consumer transaction made at point of sale (POS.

5. Attractive Discount Digital wallet provider offer discount but for this the users must make payment processes only with digital wallets [40 ]mobile penetration and government initiative such as Digital India are acting as catalyst which leads to exponential growth in use of digital payment. Electronics Consumer transaction made at point of sale (POS, [3], [25].

Major Use of Digital Wallets: As per the reviewed studies it is seen that major use of digital e-wallets by users as: • Mobile Recharges • DTH recharges • Payment of Bills • Payment at POS • Money Transfer (up to Three digits) • Payments for Online Shopping.

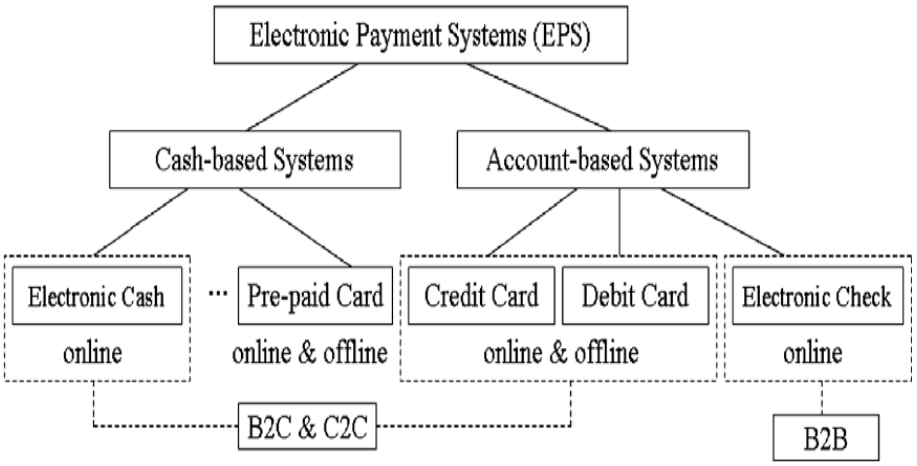



Fig. 1. Classification of electronic payment systems

It is commonly believed that good security improves trust, and that the perceptions of good security and trust will ultimately increase the use of electronic commerce. In fact, customers' perceptions of the security of e-payment systems have become a major factor in the evolution of electronic commerce in markets. In this paper, we examine issues related to e-payment security from the viewpoint of customers. This study proposes a conceptual model that delineates the determinants of consumers' perceived security and perceived trust, as well as the effects of perceived security and perceived trust on the use of e-payment systems. To test the model, structural equation modeling is employed to analyze data collected from 219 respondents in Korea. This research provides a theoretical foundation for academics and also practical guidelines for service providers in dealing with the security aspects of e-payment systems.

Electronic commerce (EC) is built upon e-payment systems (EPS). As EC becomes a major component of business operations for many companies, e-payment has become one of the most critical issues for successful business and financial services (Hsieh, 2001, Peha and Khamitov, 2004, Stroborn et al., 2004, Linck et al., 2006, Cotteleer et al., 2007, Kousaridas et al., 2008).

In comparison to the traditional payment methods, e-payment techniques have several favorable characteristics, including security, reliability, scalability, anonymity, acceptability, privacy, efficiency, and convenience (Chou et al., 2004, Stroborn et al., 2004, Tsiakis and Sthephanides, 2005, Linck et al., 2006, Cotteleer et al., 2007, Kousaridas et al., 2008). EPS have gained recognition and have been deployed throughout the world. Countries such as France, the US, and the UK have fully developed systems, while regions such as the Asia–Pacific rim provide the growth impetus to the industry.

Our research uses Korea as the site of the empirical investigation because the supporting infrastructure required for the EPS development has been put in place. Korea has aggressively pursued the development of IT and networks and created a world-class IT infrastructure (Au and Kauffman 2008). Since the mid-1990s, the Korean government has enforced a number of policies for spreading and promoting EC. As a result of these focused investments, Korea now boasts a world-class infrastructure for EC. According to the annual report of EC published by the Korea Ministry of Commerce in 2007, the total EC market size in Korea was USD 507.42 billion with a growth of 34.6% compared to the previous year. Meanwhile, Korea also has one of the highest per-capita usage statistics for the Internet; the number of Internet users was 34,430,000 (or 75.5% of the population aged six or older) and continues to rise. In the meantime, online shopping and transactions have become a normal part of life for average consumers.

The e-commerce market in Korea is expected to double annually in the next five years. Since Korea is the world's second-fastest-growing IT market, EPS will play an important role in executing wide-ranging activities and actively confronting changing economic conditions. In fact, many EPS brands such as Easycash, Easypaydirect, Inipay, iCash, eGate, eCredit, Smartpay, mypay.net, Payplus, and Paymatics have been established in the recent years.

While good EPS have a number of advantages over the traditional payment methods, they must be free of security breaches (Hegarty et al., 2003, Linck et al., 2006). The Gartner Group reports that 95% of customers are somewhat concerned about privacy or security when using credit cards on the Internet; Harris interactive also reports that six in ten respondents fear credit card theft. A key factor for the success of EPS is security, a requirement that is becoming even more crucial in the current global EC environment (Herzberg, 2003, Stroborn et al., 2004, Peha and Khamitov, 2004, Tsiakis and Sthephanides, 2005, Linck et al., 2006, Cotteleer et al., 2007). Transactions in EC can occur without any prior human contact or established interpersonal relationships. Stories about EC security threats from the media or interpersonal networks can undermine trust in EPS and cause people to fall back on the interpersonal trust that arises in human-to-human interactions. Generally, security is a set of procedures, mechanisms, and computer programs for authenticating the source of information and guaranteeing the process (Theodosios and George, 2005, Linck et al., 2006). Although extant literature extensively addresses technical details of security and trust in EPS

from the perspective of merchants or EPS service providers, consumers' perceptions of the security of EPS have not been well addressed and empirical studies are lacking in this area (Linck et al. 2006).

References

[1] P. Pushpa and S. A. Rajeshwari, "the Changing Trends in Payments : an Overview," Int. J. Bus. Manag. Invent., vol. 7, no. 7, pp. 1–5, 2018.

[2] E. H. Diniz, J. P. de J. Albuquerque, A. K. Cernew, B. Prof, and A. K. Cernev, "Mobile Money and Payment : a literature review based on academic and," SIG GlobDev Fourth Annu. Work., 2011.

[3] B. N. Kadamudimatha, "Digital Wallet : The next way of growth," Int. J. Commer. Manag. Res., vol. 2, no. 12, pp. 22–24, 2016.

[4] M. A. Kabir, S. Z. Saidin, and A. Ahmi, "Adoption of e-payment systems : a review of literature," Proc. Int. Conf. E-Commerce, vol. 2012, pp. 112–120, 2015.

[5] L. Antovski and M. Gusev, "M-Commerce Services M-Commerce Services With the growing momentum of wireless revolution and M-Commerce explosion , it is," M-commerce Serv., no. June, 2014.

[6] H. Van Der Heijden, "Factors Affecting the Successful Introduction of Mobile Payment Systems," 15th Bled Electron. Commer. Conf. eReality Constr. eEconomy Bled, no. December, pp. 430–443, 2002.

[7] A. Bradford, "Consumers Need Local Reasons to Pay by Mobile," Retrieved Oct., no. June, 2003.

[8] J. J. Chen and C. Adams, "User acceptance of mobile payments: A theoretical model for mobile payments," Proc. Int. Conf. Electron. Bus., no. January 2005, pp. 619–624, 2005.

[9] L. Da Chen, "A theoretical model of consumer acceptance of mpayment," Assoc. Inf. Syst. - 12th Am. Conf. Inf. Syst. AMCIS 2006, vol. 4, pp. 1960–1963, 2006.

[10] N. Jonker, "Payment instruments as perceived by consumers - Results from a household survey," Economist, vol. 155, no. 3, pp. 271–303, 2007.

[11] N. Mallat, "Exploring consumer adoption of mobile payments - A qualitative study," J. Strateg. Inf. Syst., vol. 16, no. 4, pp. 413–432, 2007.