A GUIDE TO CONSUMER PROTECTION IN INDIA FOR MOBILE PAYMENT LANDSCAPE

***VISHNU PRABA B[1]**

Introduction:

The term "consumer protection" is used to describe a system of laws and rules designed to protect the rights of customers who utilise mobile payment services. Making sure that consumers are safeguarded against fraud, unauthorised transactions, and other types of financial misconduct has become more crucial as digital transactions have grown in popularity and mobile payment methods have become more widely used. In a nation like India, where millions of individuals are switching to digital payments for the first time, this is especially important. The Indian government has put in place a number of measures to ensure consumer protection for mobile payment methods, including guidelines for mobile payment service providers, rules for using mobile payment methods, and procedures for grievance redressal. These steps are intended to give users of mobile payment services more security, accountability, and transparency. They also seek to foster innovation and the creation of new payment systems, as well as healthy competition in the market for mobile payments. In general, consumer safety in mobile payment systems is crucial for fostering confidence and trust in India's digital payment ecosystem. The government can promote a thriving and sustainable mobile payment industry that benefits both consumers and businesses by making sure that consumers are safeguarded and that their interests are respected.

What is mobile payment method?

A mobile payment method is a digital payment system that lets customers conduct purchases using their smart phones or tablets. These exchanges can take the form of in-person transfers, internet purchases, or purchases made at physical stores.[2] Mobile payment methods are becoming more and more common because of how simple, quick, and convenient they are to use, as well as how they allow for transactions to be completed without the use of real money or credit cards. In order to help prevent fraud and unauthorised transactions, they also provide additional security features including biometric authentication and tokenization.

[1]Vishnu Praba. B, B.A. LLB (Hons.), III year, Sastra Deemed to be University.
[2]Lerner, T., 2013. *Mobile payment* (pp. 1-151). Wiesbaden: Springer.

The challenges of making mobile payment:

Mobile payments have gained popularity in recent years.While they have numerous advantages, there are certain concerns to be aware of as well. Digital payments are susceptible to fraud, including phishing schemes and shady websites. Cybercriminals can deceive you using a number of strategies to get access to your account or steal your personal data. Security flaws can also occur with digital payments. Someone who hacks into your account may take your data or carry out unauthorised transactions. Digital payment systems can be disrupted by technical challenges, such as hardware failures, connectivity issues, or other problems, making transactions challenging or impossible.[3] Technical difficulties, such as hardware breakdowns, connectivity issues, or other issues, can cause disruptions in digital payment systems, making transactions difficult or impossible. Some digital payment service providers could tack on extra or hidden costs, which can build up over time.You might need to carry cash or utilise other payment methods in some circumstances because not all retailers or vendors accept electronic payments. It's critical to utilise reputable digital payment service providers, protect your personal information, and keep an eye on your accounts for any unusual behaviour in order to reduce these dangers.

Issues of security and convenience:

India has seen a significant rise in mobile payment methods over the past few years, with many consumers using mobile wallets, UPI (Unified Payment Interface), and other digital payment systems for transactions. While these payment methods offer convenience and ease of use, there are also concerns about security and consumer protection. One of the main issues is the potential for fraud and unauthorized transactions. With mobile payments, there is a risk that someone could gain access to a user's account and make unauthorized transactions. This could happen through hacking, phishing, or other forms of fraud. To prevent such incidents, users need to be vigilant in protecting their personal information and passwords. Another issue is the lack of consumer protection laws and regulations specific to mobile payments. While there are some general consumer protection laws in place, they may not address the unique challenges posed by mobile payments. For instance, it may be difficult to determine liability for unauthorized transactions or to resolve disputes between users and payment service providers. To address these issues, there is a need for greater collaboration

[3]Kang, J., 2018. Mobile payment in Fintech environment: trends, security challenges, and services. *Human-centric Computing and Information sciences*, *8*(1), pp.1-16.

between payment service providers, government agencies, and consumer protection organizations. Payment service providers should implement robust security measures and fraud prevention systems, while also educating users on how to protect themselves. Government agencies can provide guidance on consumer protection laws and regulations specific to mobile payments, and consumer protection organizations can raise awareness about potential risks and provide assistance to users who experience issues. While mobile payment methods offer convenience and ease of use, there are also concerns about security and consumer protection. Addressing these issues will require a collaborative effort between payment service providers, government agencies, and consumer protection organizations to ensure that users are protected and have confidence in these payment systems.[4]

Directives for secure digital payments:

It is crucial to take the required safeguards to ensure secure digital payments as more and more transactions are made online. Here are some top recommendations for secure online payments:

- Use well-known payment methods that are reliable and have strong security protocols. Square, Stripe, and PayPal are a few examples.[5]
- Ensure the firewalls and antivirus programmes on your devices are current. Use secure passwords, and whenever possible, use two-factor authentication.
- When making payments, stay away from insecure or public Wi-Fi. Instead, make use of a private network or your mobile data.
- Before inputting any payment information, make sure the website is secure. Look for the secure site indicator (a padlock icon in the address bar) and the prefix "https" at the beginning of the URL.
- Don't divulge sensitive information: Unless absolutely required, avoid disclosing sensitive information such as your credit card number, CVV code, or social security number.
- Verify your claims: Keep an eye out for any unauthorised purchases on your bank and credit card statements. Any suspicious behaviour must be immediately reported.

[4]Kang, J., 2018. Mobile payment in Fintech environment: trends, security challenges, and services. *Human-centric Computing and Information sciences*, *8*(1), pp.1-16.
[5]Kang, J., 2018. Mobile payment in Fintech environment: trends, security challenges, and services. *Human-centric Computing and Information sciences*, *8*(1), pp.1-16.

- Consider utilising a virtual credit card while making purchases online. Virtual cards reduce the danger of fraud because they are transitory and can only be used once.
- Phishing schemes should be avoided. Be aware of emails or messages that request your money or personal information. Don't open attachments or click on links coming from unidentified sources.

You may protect yourself against online fraud and ensure secure digital payments by adhering to these directives.

Dispute resolution mechanism:

For consumer protection in mobile payment methods, there are numerous dispute resolution mechanisms accessible in India.The majority of mobile payment service providers have internal dispute resolution processes in place. Customers can file a complaint and seek resolution by contacting their customer care team. Providers of mobile payment services are expected to respond to complaints within a specific time frame, typically 7 to 10 days.The banking ombudsman programme was established by the Reserve Bank of India (RBI) to address complaints against banks, especially those involving mobile payments. If customers are not pleased with the response from the mobile payment service provider, they can submit a complaint with the banking ombudsman. The banking ombudsman has the authority to look into the complaint and provide a decision that is legally obligatory on the bank.Consumer courts can be established at the district, state, and federal levels under the Consumer Protection Act of 2019. If customers are not pleased with the response from the mobile payment service provider or the banking ombudsman, they can register a complaint with the appropriate consumer court. The mobile payment service provider may be ordered by the consumer court to give the consumer compensation.Some providers of mobile payment services have chosen mediation as a dispute resolution method. In order to assist the parties in coming to a mutually agreeable agreement, a mediator is appointed. Customers can take their grievances to the arbitrator chosen by the mobile payment service provider[6].It is crucial to remember that customers should first try to address their complaints with the mobile payment service provider through that company's internal complaint resolution process before using any of these dispute resolution procedures.

[6]Patil, A.R. and Bharadwaj, H., 2017. A Stakeholder's Assessment of Feasibility of Online Mediations in India. *IJCLP*, *5*, p.62.

Role of stakeholders:

In India, stakeholders are essential to guaranteeing consumer protection for mobile payment systems. Some of the stakeholders and their roles are as follows:

- Government: The Indian government is in charge of developing and implementing laws and regulations that safeguard customers in the mobile payments sector. The government has also unveiled a number of programmes, such as Digital India, which encourages financial inclusion and digital payments.
- Mobile payment companies: Companies that accept mobile payments, like Paytm, PhonePe, and Google Pay, are accountable for making sure that both the security of their payment systems and the privacy of their customers' financial and personal information are upheld. Additionally, they must be open and transparent about their fees and charges and present consumers with clear terms and conditions.[7]
- Payment Gateway Providers: Financial transactions between banks and mobile payment businesses are made easier by payment gateway providers. They must make sure that transactions are processed accurately and that their systems are secure.
- Banks: Since they are in charge of making sure that transactions are secure and that money is appropriately transferred between accounts, banks are essential to mobile payments.
- Organisations for consumer protection: These organisations, like the Consumer Protection Act of 2019, are in charge of defending the interests of consumers. They give customers a place to voice complaints and request remedy.

In verdict, guaranteeing consumer protection in mobile payment methods in India requires the cooperation of the government, mobile payment businesses, banks, payment gateway providers, and consumer protection organisations. Together, they can build a safe, open ecosystem that supports consumer protection and financial inclusion.

Consumer rights for mobile payment methods:

The use of mobile payment systems has considerably increased in India in recent years. The government has set many laws and guidelines for mobile payment service providers in order to protect the interests of consumers. Providers of mobile payment services must guarantee

[7]Pandey, S.K., 2022. A Study on Digital Payments System & Consumer Perception: An Empirical Survey. *Journal of Positive School Psychology*, *6*(3), pp.10121-10131.

the security of their systems and safeguard sensitive data belonging to customers. To prevent unauthorised access, this includes putting in place strong authentication procedures and encryption techniques. Users of mobile payment services have a right to be informed of all fees, charges, and terms and conditions. Consumers must be given clear and straightforward information from mobile payment service providers, including transaction limitations and any other pertinent details. Customers have the option to complain to the mobile payment service provider or the appropriate regulatory bodies in the event of any problems. Providers of mobile payment services are expected to have a procedure in place for handling complaints from customers[8]. Providers of mobile payment services are required to abide by all applicable data privacy laws and rules. Customers have a right to information about how the mobile payment service provider collects, uses, and shares their personal information. Customers must receive proper customer support from mobile payment service providers. This entails offering a customer service helpline, email assistance, and other means for resolving client concerns and questions. In order to safeguard the interests of customers, mobile payment service providers in India must abide by strict laws and rules. By being watchful and informing the appropriate authorities of any fraudulent or unauthorised transactions, consumers can also contribute to the protection of their rights.

Reforms in consumer protection regarding mobile payment:

India is a country where many people use digital payment methods to pay for a variety of goods and services. However, there are some ongoing worries about the security and safety of these payment options. The following adjustments could be done to enhance consumer safety for mobile payment options in India: Although India's present data privacy rules are being updated, more has to be done to guarantee that customer data is appropriately protected. Strict data protection regulations should be enforced, and mobile payment companies should be held responsible for any resulting violations. In order for customers to choose the best payment option, mobile payment businesses should be compelled to give clear and comprehensive information about their services, including fees and charges. Consumers should have access to a simple and efficient dispute resolution process in the event of a payment issue. To assist in swift and impartial dispute resolution, this could involve a specialised customer support group or an impartial mediator[9]. Stronger authentication

[8]Balasubramanian, D., 2022. E-commerce and Consumer Protection.
[9]Cheriyan, G. and TB, S., 2019. Protecting the Digital Consumers: Challenges and Possible Solution. *IJCLP*, *7*, p.85.

procedures, like multi-factor authentication and biometric verification, should be used to stop fraud and unauthorised access to mobile payment accounts. Consumers should receive information about mobile payments' advantages, hazards, and safe usage practises. Campaigns for public awareness, educational initiatives, and informational material on the websites of mobile payment companies could all help to achieve this. India may strengthen consumer protection for mobile payment methods by putting these reforms into practise, which would eventually benefit both customers and mobile payment providers by boosting trust and confidence in these payment options.

Data protection and privacy issues with mobile payments:

People now frequently use their smartphones to make purchases because to the popularity of mobile payments. When using mobile payments, there are a number of privacy and data protection concerns that must be taken into account. Some of the most important problems are as follows:

1. Personal data gathering: To complete transactions, mobile payment service providers frequently gather personal data, such as payment and location details. Hacks or data breaches could expose this data, which could lead to identity theft or financial damage.
2. Access by third parties: Some mobile payment providers may divulge user information to advertisers or third-party suppliers, which could result in spam marketing or improper use of data. To understand how their data will be used and secured, customers should carefully read the terms and conditions of their mobile payment provider[10].
3. Lack of security measures: Different mobile payment service providers employ different levels of protection. While some may utilise biometric authentication or multi-factor authentication, some may only use passwords or PINs. Users should be informed of the security precautions taken by their mobile payment provider and take action to safeguard their private information by enabling two-factor authentication and often changing passwords, among other measures.
4. User error: By accessing unprotected Wi-Fi networks or exchanging their mobile payment information with others, users run the risk of unintentionally disclosing their

[10]Wang, Y., Hahn, C. and Sutrave, K., 2016, February. Mobile payment security, threats, and challenges. In *2016 second international conference on mobile and secure services (MobiSecServ)* (pp. 1-5). IEEE.

personal information. Users must take responsibility for their own behaviour and take precautions to safeguard their personal information, such as only connecting to secure networks and refraining from disclosing payment information to third parties.

5. Compliance with regulations: In various nations or areas, mobile payment providers may be governed by various data protection and privacy laws. Users should be aware of the regulatory context in which their mobile payment provider operates and whether or not the service complies with relevant rules.

In general, users should be aware of the data protection and privacy problems related with this payment method and take precautions to protect their personal information, even though mobile payments offer convenience and flexibility.

The latest advancements in digital payments:

India has seen a substantial increase in digital payments in recent years, and mobile payment options have been essential to this shift. Here are some new developments in digital payments for India's mobile payment systems that protect consumers: Numerous mobile payment platforms now utilise fingerprint and facial recognition to verify consumers as biometric technologies advance. Customers are safeguarded against fraud and identity theft thanks to the additional layer of security provided by this. In India, QR code payments are growing increasingly popular since they give customers a simple and safe method to use their mobile devices to make purchases. The risk of fraudulent transactions is decreased by the fact that QR codes are exclusive to each transaction and can only be used once. The practise of using two distinct ways to confirm a user's identification, such as a password and a one-time code given to their mobile phone, is known as two-factor authentication (2FA), and it is becoming more and more common in India. This increases security by one layer and lowers the possibility of unauthorised access to a user's mobile payment account. Consumers in India are becoming increasingly concerned about data privacy and protection as the usage of digital payments increases. Many mobile payment systems are adopting encryption technologies to safeguard user data in order to address this[11]. These platforms also enforce strict data privacy policies. In India, a lot of mobile payment platforms now have digital dispute resolution procedures that let customers file complaints and have them settled online. Customers now have a quick and easy alternative to visiting a real branch or office to settle their problems.

[11]Androulidakis, I., Basios, C. and Androulidakis, N., 2008. Surveying Users' Opinions and Trends towards Mobile Payment Issues. *Frontiers in Artificial Intelligence and Applications*, *169*, p.9.

Digital payment providers are putting various procedures in place to ensure consumer protection since mobile payment methods in India are changing quickly. These steps, which range from biometric authentication to digital dispute resolution, are making digital payments in India for consumers safer and more practical.

Conclusion:

Consumer protection in mobile payment systems is a critical concern in India, to sum up. It is crucial to make sure that consumer rights are safeguarded as more consumers turn to mobile payments as a simple and secure method of conducting transactions. The Indian government has taken a number of steps to protect the interests of consumers, including establishing a grievance redressal process, requiring two-factor authentication, and restricting responsibility in the event of fraudulent transactions. Consumers still need to be made more aware of secure mobile payment methods, and the sector needs to embrace tougher security measures to stop fraud and data breaches. In general, establishing strong consumer protection in mobile payments will be essential for fostering adoption and increasing system trust.