Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487 editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1111

E-Commerce & Digital Wallet Payment Fraud

Kishore Bellamkonda Sunderajulu

Product Manager – Payments Technology

Abstract

Payment transaction security is a cornerstone of modern financial systems, essential for safeguarding sensitive financial data as digital transactions proliferate across mobile, online, and in-person platforms. It relies on advanced technologies, including cryptographic protocols and tokenization, which replace sensitive card details with secure digital tokens to minimize the risk of data breaches. Regulatory mandates such as Reg II, PSD2/SCA, RBI, and GDPR alongside industry standards like PCI-DSS and ISO 8583, drive the adoption of stringent security measures to protect both consumers and financial institutions.

However, the increasing complexity of the payments ecosystem and the rise of emerging technologies present ongoing challenges. The integration of mobile wallets, contactless payments, and eCommerce transactions necessitates security frameworks that combine robust protection with scalability and ease of implementation. Future innovations will focus on enhancing interoperability across payment platforms, leveraging AI-driven anomaly detection to identify fraud patterns, and evolving cryptographic techniques to counter new threats.

A secure transaction environment is paramount for maintaining consumer trust and enabling the continued growth of digital payment solutions globally, as the industry navigates the intersection of technological advancement, regulatory compliance, and user-centric design

Introduction

As the adoption of digital payments and online commerce accelerates, the financial risk associated with fraud targeting these ecosystems continues to grow. Digital wallet mobile app fraud involves the misuse of mobile applications or devices for illegal financial gain, often leading to significant loss of revenue and compliance challenges. Examples include account takeovers, click fraud, SMS fraud, and In-app purchase fraud. Fraudsters employ sophisticated techniques such as social engineering, spoofed websites, and malicious code to compromise sensitive payment data, resulting in financial risk, reputational damage, and increased chargeback rates. Businesses must implement proactive compliance measures and robust detection systems to mitigate these risks.

Similarly, eCommerce fraud exposes businesses to a range of financial and reputational risks by exploiting vulnerabilities in online transactions. Common methods include payment fraud with stolen credit card data, account takeovers, refund abuse, interception fraud, and triangulation schemes. These fraudulent activities not only erode consumer trust but also result in revenue loss, chargebacks, and potential regulatory compliance breaches.

To address these challenges, businesses must adopt comprehensive strategies that integrate fraud prevention, compliance measures, and payment security. By doing so, they can safeguard against fraud,

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487 editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1111

reduce financial and reputational risk, and ensure sustainable growth in the increasingly digital payments ecosystem. Let's review the types of fraud and how they occur.

Payment fraud, risk & mitigation

eCommerce fraud type:

a. Online shopping Fraud

This is the most prevalent type of card-not-present (CNP) fraud, where criminals use stolen credit card details to make purchases on eCommerce platforms. Since these transactions do not require physical card verification, fraudsters exploit this vulnerability to their advantage.

Risk: This leads to financial losses for merchants in the form of chargebacks, loss of revenue, and increased compliance obligations to secure payment systems. It also erodes consumer trust in online shopping platforms, resulting in reputational risk.

Mitigation: Implementing robust authentication measures such as 3D Secure, tokenization, and AI and Machine learning-driven fraud detection systems can help identify suspicious activities and anomaly detection early on before the transactions are processed.

b. Phone Order Fraud

This occurs when a fraudster places an order over the phone using stolen card details. This type of fraud often targets businesses that manually process payments without robust verification procedures.

Risk: Businesses face chargebacks and financial losses, as well as operational inefficiencies due to handling disputes. There is also a reputational risk if fraud becomes prevalent.

Mitigation: Merchants can require additional verification, such as the card verification value (CVV) and billing address, before processing phone orders. Training staff to recognize red flags in phone orders is also crucial.

c. Mail Order Fraud

This involves fraudulent transactions conducted through mail order forms, where stolen card information is sent in writing to merchants. Although less common today due to digitization, it remains a concern for certain businesses.

Risk: Similar to phone order fraud, mail order fraud can result in chargebacks, compliance risks, and revenue loss.

Mitigation: Encouraging secure online payment options over traditional mail orders and verifying customer identities before processing transactions can mitigate risks.

d. Recurring Payment Fraud

Fraudsters set up unauthorized subscriptions or recurring payments using stolen card details. These fraudulent activities are often difficult to detect until the legitimate cardholder notices unusual charges on their statements.

Risk: Financial losses occur because of disputed charges and associated chargeback fees. It also leads to reputational damage for subscription-based services.

Mitigation: Implementing strong customer authentication (SCA), requiring consent for recurring payments, and notifying users about upcoming charges can help reduce the likelihood of fraud.

e. Account Takeover Fraud

Criminals gain unauthorized access to a legitimate user's account, often through credential stuffing,

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487 editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1111

phishing, or brute-force attacks. Once inside, they exploit stored card details to make fraudulent purchases.

Risk: This leads to significant financial risk, reputational damage, and potential loss of customer trust. Businesses may face operational challenges when compensating affected customers and securing compromised accounts.

Mitigation: Using multi-factor authentication (MFA), monitoring for suspicious login activities, and implementing behavioral analytics can protect against account takeovers.

f. Phishing Fraud

Fraudsters use deceptive emails, messages, or websites to trick users into revealing sensitive payment information. These attacks often imitate trusted brands to increase their effectiveness.

Risk: Phishing results in financial losses for victims and increases chargeback rates for merchants. The reputational damage to businesses impersonated by fraudsters is also a significant concern.

Mitigation: Educating customers about phishing tactics, deploying anti-phishing tools, and monitoring for fraudulent use of brand assets can help mitigate the risk.

g. Synthetic Identity Fraud

In this type of fraud, criminals combine real and fabricated personal information to create a fake identity, which is then used to open new credit accounts and make fraudulent purchases.

Risk: Synthetic identities are difficult to detect, causing long-term financial losses for financial institutions and merchants. The cost of investigating and addressing synthetic identity fraud is substantial.

Mitigation: Employing advanced verification techniques, such as biometric authentication and identity proofing during account setup, can help prevent the creation of synthetic identities.

h. Triangulation Fraud

Fraudsters set up fake online stores to collect payments from unsuspecting customers. They then use stolen card details to purchase goods from legitimate merchants, which are delivered to the fake store's customers.

Risk: Legitimate merchants suffer financial losses due to chargebacks, while customers lose trust in online platforms. Fraudsters profit from both the stolen card data and the proceeds from fake store sales.

Mitigation: Monitoring for unusual purchasing patterns, implementing fraud detection systems, and educating consumers about identifying legitimate online stores can help mitigate this type of fraud.

Digital wallet Fraud

a. Click Fraud

Bots simulate user behaviour by repeatedly clicking on ads, often on mobile platforms, to generate fraudulent revenue for publishers or deplete advertising budgets.

Risk: Businesses lose advertising spend with no genuine customer engagement, which can distort analytics and ROI metrics. Financial risk and loss of revenue are significant, alongside reputational damage when fraud is detected.

Mitigation: Deploying bot detection tools, using CAPTCHAs, and monitoring traffic patterns can help identify and prevent click fraud.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487 editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1111

b. Chargeback Fraud (Friendly Fraud)

Customers dispute legitimate purchases by requesting chargebacks from their credit card issuers, claiming unauthorized transactions or undelivered goods.

Risk: Chargeback fraud results in financial losses for merchants, increased chargeback fees, and higher compliance obligations with payment processors. It also damages merchant reputations and impacts customer trust.

Mitigation: Clear return policies, strong transaction records, and implementing 3D Secure authentication can help reduce chargeback occurrences.

c. Card-Not-Present (CNP) Fraud

Fraudulent transactions occur when stolen card details are used in online or mobile app purchases without the physical card.

Risk: Leads to direct financial losses, compliance risks, and reputational damage for merchants. Businesses also bear the burden of chargeback fees and fraud mitigation costs.

Mitigation: Advanced fraud detection tools, tokenization, multi-factor authentication (MFA), and encryption protocols are essential to combating CNP fraud.

d. Mobile Deposit Fraud

Fraudsters deposit counterfeit checks via mobile banking apps and trick victims into withdrawing and returning funds before the checks are discovered as fake.

Risk: Financial institutions and victims face monetary losses, reputational harm, and potential legal challenges in recovering funds.

Mitigation: Real-time check verification, delayed fund availability for large deposits, and educating users about fraud schemes can mitigate risks.

e. Authorized Push Payment (APP) Fraud

Fraudsters manipulate victims into making electronic payments to accounts controlled by them, often through social engineering tactics.

Risk: Victims lose funds directly, and financial institutions face reputational risks and compliance scrutiny over inadequate fraud detection measures.

Mitigation: Educating users, using transaction monitoring systems, and implementing confirmation-of-payee systems can help reduce APP fraud.

f. Romance Scams

Fraudsters develop fake online relationships with victims to manipulate them into transferring money, which is quickly laundered through multiple accounts.

Risk: Significant financial losses for victims and reputational risk for platforms used by scammers. These scams also create compliance challenges for financial institutions.

Mitigation: Raising awareness, monitoring suspicious transactions, and implementing fraud detection systems that flag unusual activity can help reduce these scams.

g. Advance Fee Fraud

Victims are promised a significant benefit (e.g., loans, prizes) in return for an upfront fee, which they pay but never receive the promised benefit.

Risk: Victims face monetary losses, and businesses linked to fraudsters suffer reputational damage. Financial institutions may face compliance investigations for facilitating such schemes.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487 editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1111

Mitigation: Public education campaigns, robust anti-fraud mechanisms in payment platforms, and collaboration with law enforcement can help prevent these frauds.

h. Account Takeover

Fraudsters gain unauthorized access to user accounts via phishing, credential stuffing, or brute force attacks and misuse stored payment details.

Risk: Results in financial losses, compromised data, chargebacks, and reputational risks for businesses and consumers.

Mitigation: Enforcing strong passwords, MFA, and monitoring for unusual login activities are critical for account protection.

i. Identity Theft

Fraudsters steal personal information to impersonate victims, opening fraudulent accounts or conducting unauthorized transactions.

Risk: Victims face financial harm and reputational damage, while financial institutions deal with compliance breaches and fraud mitigation costs.

Mitigation: Identity verification tools, biometric authentication, and secure data storage can reduce the risk of identity theft.

j. Ransomware Attacks

Malicious software encrypts user or organizational data, with attackers demanding payment for its release. Ransomware often targets mobile platforms via malicious apps or phishing schemes.

Risk: Results in operational disruptions, data loss, financial losses, and reputational risks for businesses.

Mitigation: Regular software updates, secure app installations, employee training, and anti-malware tools can mitigate the threat of ransomware.

Conclusion

In today's rapidly evolving digital payments landscape, the threat of payment fraud—whether in the form of payment transactions, eCommerce vulnerabilities, or mobile app exploitation—remains a critical concern for businesses and consumers alike. Each fraud type introduces unique complexities, ranging from financial losses and compliance challenges to reputational harm and operational disruptions. To combat these threats effectively, businesses must prioritize a multi-faceted fraud prevention strategy. Implementing advanced authentication protocols, leveraging real-time monitoring systems, and fostering ongoing customer awareness is essential to mitigating risks and maintaining the integrity of payment ecosystems. A proactive and adaptive approach not only safeguards against current threats but also enhances consumer trust and confidence, ensuring the sustainable growth of digital payment solutions in an increasingly interconnected world.

Abbreviations and Acronyms

Abbreviation	Acronym
PSD2	Revised Payment Service Directive
RBI	Reserve Bank of India
GDPR	General Data Protection Regulation
PCI	Payment Card Industry

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487 editor@aijmr.com
Volume 2, Issue 6, November-December 2024
CrossRef DOI: 10.62127/aijmr.2024.v02i06.1111

AI	Artificial Intelligence
eCommerce	Electronic Commerce
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
SCA	Strong Customer Authentication
Reg II	Regulation II - Debit Card Interchange Fees and Routing
ISO	International Standard Organization
DSS	Data Security Standards
SMS	Short Message Service
3D Secure	3Domain Secure

References

Investopedia:

1. [https://www.investopedia.com/terms/c/cardnotpresent-fraud.asp]
2. Federal Reserve: *Regulation II: Debit card interchange fees and access to payment systems*. [https://www.federalreserve.gov/paymentsystems/regii-about.htm]

Allure Security:

1. [https://alluresecurity.com/what-is-mobile-app-fraud/]
2. PCI Security Standards Council:
3. [https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf] World Bank
4. [https://fastpayments.worldbank.org/sites/default/files/2021-10/Customer_Authentication_Final.pdf]
5. EuropeanCentralBank: [https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf]
6. European Banking Authority (EBA):
7. [https://www.eba.europa.eu/publications-and-media/press-releases/eba-clarifies-application-strong-customer-authentication]

EMVCo:

1. [https://www.emvco.com/knowledge-hub/emv-3-d-secure-enabling-strong-customer-authentication/]
2. European Union:
3. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389]