International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Review on Security Breach on Credit Card

Saumya Maurya[1], Smriti Kaur[2]

[1,2] Department of Computer Applications, Bbd University, Lucknow, U.P.
saumyamy786@gmail.com, smritikaur2000@gmail.com

ABSTRACT:

Web applications have seamlessly integrated into our everyday routines, offering a wide range of services and functionalities that have become indispensable to us. However, along with their increased usage, web applications have also become prime targets for security threats. So, it is important to ensure the security of web applications to protect sensitive data and maintain user trust. This research paper aims to analyze the security threats that have been highly exploited in web applications over the past four years. The study aims to identify and examine the key vulnerabilities targeted by attackers, shedding light on the evolving landscape of web application security. By understanding these threats, developers, organizations, and users can enhance their awareness and take necessary measures to mitigate risks, safeguard sensitive information, maintain user trust, and ensure the resilience of web applications in the face of relentless cyber threats.

Keywords: credit cards, vulnerabilities**,** data breach, fraud cybercrimes, secure society.

1. INTRODUCTION

E-commerce, the buying and selling goods and services online, has revolutionized how business is conducted. Transactions are carried out using electronic devices such as computers, phones, and credit cards, eliminating the need for physical documents or in-person store visits. However, this convenience has also given rise to various types of fraud, with credit card fraud being the most prevalent. Credit card fraud involves the unauthorized use of a credit card account by individuals other than the cardholder and issuer. This type of fraud allows perpetrators to obtain goods without payment or gain illegal access to funds from an account. It poses significant risks to financial institutions and banks, costing them billions of dollars annually. In 2018 alone, there were 33,305 reported cases of credit card identity fraud, according to Cifa.[1] Extensive research has been dedicated to developing innovative solutions to address these security concerns and protect credit card information. However, many existing fraud detection methods have proven ineffective, prompting further exploration and improvement. This research paper aims to delve into the world of credit card security breaches to provide valuable insights into the nature of credit card fraud and provide practical recommendations for stakeholders in the financial industry to enhance the security of credit card transactions. Financial institutions can proactively implement robust security measures, protect customer information, reduce financial losses, and maintain trust in the credit card payment ecosystem by understanding the fraud techniques utilized by fraudsters and the efficacy of different mitigation strategies. The aim is to enhance the security of credit card transactions, safeguard sensitive information, and maintain the trust and confidence of consumers in the electronic payment ecosystem.

2. LIFECYCLE OF CREDIT CARD FRAUD

The lifecycle of credit card fraud involves attackers obtaining card numbers through data breaches, skimming devices, or phishing. They then make unauthorized purchases using these card numbers, taking advantage of vulnerable payment systems. Victims usually discover fraud when they notice unauthorized charges on their statements or when their financial institution detects suspicious activity. Chargebacks are initiated to reverse fraudulent charges. However, law enforcement needs help tracing and apprehending fraudsters who employ sophisticated methods to hide their identities and launder their gains, making it difficult to take legal action against them [2].

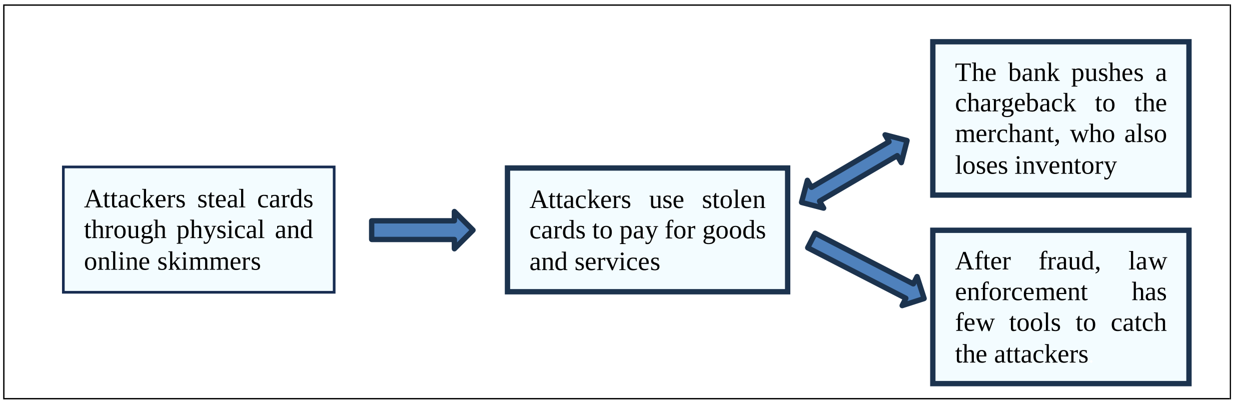
Attackers steal cards through physical and online skimmers
Attackers use stolen cards to pay for goods and services
The bank pushes a chargeback to the merchant, who also loses inventory
After fraud, law enforcement has few tools to catch the attackers

Figure 1: Flowchart representing the overall life cycle of credit card fraud

3. FRAUD TECHNIQUES

Some of the fraud techniques utilized by fraudsters to access credit card details are discussed below:

- **Card Skimming**

Fraudsters use skimming devices to capture credit card information when the card is swiped or inserted into compromised card readers, such as ATMs or point-of-sale terminals [2].

- **Triangulation Fraud**

Fraudsters set up fake online stores to collect credit card information from unsuspecting customers. They then use the stolen information for fraudulent activities [2].

- **Phishing**

Fraudsters send deceptive emails, text messages, or make phone calls impersonating legitimate institutions to trick individuals into revealing their credit card details or other personal information. Phishing attacks pose a significant challenge for defense because they are a type of socio-technical attack so to prevent them we need both technical and human-centered solutions [3].

- **Card Not Present (CNP) Fraud**

This type of fraud occurs in online or over-the-phone transactions where the physical card is not present. Fraudsters use stolen credit card information to make unauthorized purchases [4].

- **Identity Theft**

Fraudsters steal personal information, including Social Security numbers, addresses, and other details, to apply for credit cards in someone else's name. They then use these fraudulent accounts for their benefit [5].

- **Counterfeit Cards**

Fraudsters create counterfeit credit cards using stolen card information and magnetic stripe data. These fake cards are then used for fraudulent transactions [6].

It's important to stay vigilant and protect personal and credit card information to prevent falling victim to these fraud techniques.

4. NOTABLE CREDIT CARD BREACHES

Capital One Data Breach (Impacts 106 Million Customers): -

On Monday, Capital One, the fifth largest credit card issuer in the United States, made a shocking revelation. A hacker breached their security systems and gained unauthorized access to the personal information of approximately 106 million customers and applicants in the United States and Canada. This breach exposed highly sensitive details about individuals and small businesses, such as names, social security numbers, income, and dates of birth. The compromised data spanned 2005 to early 2019, encompassing multiple credit card products. In a positive development, Capital One announced that the suspected perpetrator responsible for the breach had been apprehended and is currently in federal custody. As per Capital One's statement, the hacker successfully obtained access to a wide range of information collected by the company through credit card applications. This compromised data includes names, addresses, postal codes, phone numbers, email addresses, dates of birth, and self-reported income.

Furthermore, the hacker managed to breach customer status data, encompassing credit scores, credit limits, balances, payment history, and contact information. The breach also exposed approximately 140,000 social security numbers, around one million Canadian Social Insurance Numbers, and

80,000 linked bank account numbers belonging to Capital One's secured credit card customers. The breach impacted around 100 million individuals in the United States and approximately 6 million Canadians, as confirmed by the company [7].

Home Depot (56 million credit cards compromised): -

In a significant revelation, the largest DIY retailer globally has acknowledged a highly alarming incident of customer data compromise. Over a span of five months, an astonishing 56 million credit and debit card numbers were exposed, making this breach one of the most severe in terms of compromised customer data. Home Depot disclosed that the data theft originated in April, and it was only in the current month that the malware utilized by the hackers was completely eradicated from their systems. On September 2, the security website Krebs on Security unveiled the Home Depot breach, raising concerns that all of the company's 2,200 US stores may have been impacted. However, Home Depot officially confirmed the occurrence of the data breach on September 8. As soon as the breach came to light, Home Depot engaged security firms Symantec and FishNet Security to launch an investigation into the suspected hacking.

According to Home Depot, the perpetrators utilized "unique, custom-built malware" that had not been previously encountered in similar cyber-attacks. This sophisticated approach allowed them to evade detection for an extended period. Home Depot implemented a significant payment security upgrade to enhance the security of customers' card numbers, ensuring improved encryption. Compared to Britain and numerous European countries where chip-and-PIN technology is widely adopted, US retailers have been relatively slower in its implementation. This delay can be attributed to the absence of appropriate chips in many American credit cards. To address this, the US payments industry has established a deadline of October 2015 for transitioning to chip and PIN technology, aligning with enhanced security measures [8].

Hacker Ring (Stole 160 Million Credit Cards): -

Five individuals, comprising four Russians and one Ukrainian, have been indicted by U.S. federal authorities for their alleged involvement in some of the most significant cybercrimes of the past decade. These cybercriminals are believed to be responsible for stealing over 160 million credit card numbers from major U.S. retailers, banks, and card processors. The gang is suspected of orchestrating the 2007 breach at Heartland Payment Systems, a credit card processor, which exposed approximately 130 million card numbers. They are also linked to the 2011 breach at Global Payments, which affected nearly one million accounts and resulted in significant financial losses of around $100 million for the company. The case, described by federal prosecutors in New Jersey as the largest hacking scheme ever prosecuted in the U.S., highlights the magnitude of their criminal activities. The Justice Department officials have stated that these individuals were part of a larger criminal organization led by Albert "Soupnazi" Gonzalez, a notorious hacker who was arrested in 2008 and is currently serving a 20-year prison sentence for his involvement in various breaches, including the theft of approximately 90 million credit cards from retailer TJX. The hackers employed SQL injection attacks to infiltrate their targets, exploiting vulnerabilities in server configurations to inject malicious code into the database connected to the publicly accessible web server. This unauthorized access enabled the attackers to upload software and extract data from the compromised systems [9].

5. MITIGATION STRATEGIES

Some of the preventive measures used for preventing credit card fraud are discussed below:

- **Cutting Off the Supply of Stolen Card Numbers:** Fraudsters employ two methods to obtain card information: physical skimming and online skimming. It is essential to develop systems that can detect tampering and ensure the safety of payment machines. Although progress has been made in this area, fraudsters continuously find new ways to modify machines. Additionally, preventing online skimming, which often goes undetected for extended periods, requires new approaches to safeguard our card details during online transactions. Researchers are actively working on solutions to protect our credit card information, ensuring its safety when we shop online or use our cards in stores [2].

- **Empower Merchants to Reduce Fraud:** Empowering merchants offers two key advantages. Firstly, merchants possess detailed transaction information, enabling them to identify unusual or potentially fraudulent activities. Secondly, merchants have the ability to intervene and stop a transaction before any fraud occurs, preventing potential harm. For example- modern approaches, like step-up authentication, allow apps to collect additional information from suspicious users, distinguishing legitimate users from fraudsters. Examples include Apple's FaceID, Uber and Boxer's credit card scanning systems, and Coinbase's ID verification flow [2].

- **Empower Law Enforcement to Reduce Fraud:** While developing new tools and algorithms is important for businesses to detect fraud, what happens after fraud is detected is often unclear. One common advice is to alert law enforcement about the fraud, but it's not always clear which agencies to contact and how they can effectively investigate the fraud [2].

- **Be Aware of Phishing and Skimming Scams:** Beware of unsolicited messages or calls asking for your card details. Only click on suspicious links or share personal/financial info after verifying the request. Access websites directly or contact the merchant/bank for confirmation. Stay alert to card readers when shopping or using ATMs, watching for skimmers. When unsure, opt for tap-to-pay if possible [3].

- **EMV Chip Technology:** EMV (Europay, Mastercard, and Visa) chip technology is designed to enhance security by using embedded microchips in credit cards. These chips generate unique transaction codes for each purchase, making it difficult for fraudsters to clone or counterfeit cards [10].

- **Two-Factor Authentication (2FA):** Two-factor authentication adds a layer of security by requiring users to provide additional verification, such as a one-time password sent to their mobile device and entering their credit card information [11].
- **Tokenization:** Tokenization replaces sensitive card data with a unique identifier called a token. Even if intercepted, this token is useless to fraudsters since it can only be used to make fraudulent transactions with the corresponding sensitive data [12].
- **Secure Online Payment Gateways:** E-commerce websites and online merchants use secure payment gateways that encrypt and protect customers' credit card information during online transactions. These gateways ensure that sensitive data is transmitted securely and not accessible to unauthorized parties [13].
- **PCI DSS Compliance:** The Payment Card Industry Data Security Standard (PCI DSS) sets requirements for businesses that handle credit card information. Compliance with these standards ensures merchants implement security measures to protect cardholder data, reducing the risk of data breaches and fraud [14].
- **Geolocation and IP Address Verification:** Geolocation and IP address verification help identify suspicious transactions by comparing the location of the transaction with the cardholder's usual location. A transaction from an unfamiliar location or through a suspicious IP address may trigger additional security measures or verification steps [15].
- **Biometric Authentication:** Biometric authentication methods, such as fingerprint or facial recognition, provide secure verification of the cardholder's identity. These methods add an extra layer of security by using unique physiological or behavioral characteristics that are difficult to replicate [16].

It's important to note that while these methods significantly reduce the risk of credit card fraud, no system is entirely foolproof. Remaining vigilant, regularly monitoring credit card statements, and promptly reporting any suspicious activity to the relevant authorities or card issuers are essential in combating fraud.

6. FUTURE TRENDS AND CHALLENGES

As technology continues to shape the way we conduct transactions, the need for robust credit card security has become more critical than ever. With cybercriminals employing increasingly sophisticated tactics, protecting sensitive credit card information is a constant challenge. However, innovative trends in biometric authentication, tokenization, and advanced fraud detection are poised to transform the landscape, offering hope for a more secure future. Here are some noteworthy future trends and challenges listed below: -

- **Advanced Cyber Threats:** As technology continues to evolve, so do cyber threats. Future trends suggest that cybercriminals will employ more sophisticated techniques, including advanced malware, artificial intelligence (AI)-powered attacks, and targeted social engineering. The challenge lies in staying ahead of these evolving threats and developing robust security measures to mitigate risks effectively [17].
- **Emerging Technologies:** The rapid development of technologies such as the Internet of Things (IoT), blockchain, and cloud computing introduces both opportunities and challenges for credit card security. While these technologies enhance convenience and efficiency but create new attack surfaces and vulnerabilities. Securing these technologies will require innovative approaches and adaptive security measures [18].
- **Biometric Authentication:** Biometric authentication, such as fingerprint scanning and facial recognition, is gaining popularity as a more secure and convenient method of verifying identities. However, the challenge lies in ensuring the integrity and privacy of biometric data. Protecting biometric information from theft, forgery, and unauthorized access will be a critical focus in the future [19].
- **Data Privacy Regulations:** With the increasing public concern over data privacy, governments worldwide are implementing stricter regulations to protect consumer information. Compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) poses challenges for credit card issuers, who must navigate complex legal requirements and implement robust data protection measures [20].
- **Insider Threats:** Insider threats, including employees with malicious intent or compromised credentials, pose a significant challenge to credit card security. Future trends indicate the need for comprehensive employee training programs, strict access controls, and continuous monitoring to effectively detect and mitigate insider threats [20].
- **Global Collaboration and Information Sharing:** As cyber threats become increasingly global, collaboration among credit card issuers, financial institutions, and cybersecurity organizations becomes crucial. Sharing threat intelligence and best practices can help proactively identify emerging threats, develop effective countermeasures, and enhance overall security posture [20].
- **User Education and Awareness:** User education and awareness are critical in preventing credit card fraud. Future challenges include educating users about emerging threats, promoting secure online practices, and encouraging responsible card usage. User awareness campaigns and interactive training programs will be essential to combat evolving security risks [20].
- **Mobile Payments and Contactless Technology:** The widespread adoption of mobile payments and contactless technology presents new challenges in securing transactions and protecting payment data. The future will require robust encryption, secure mobile payment applications, and additional authentication mechanisms to ensure the security and integrity of mobile-based transactions [19].

- **Artificial Intelligence and Machine Learning:** Integrating artificial intelligence (AI) and machine learning (ML) in credit card security offers opportunities and challenges. While AI and ML can enhance fraud detection and prevention capabilities, cybercriminals can also exploit them to develop more sophisticated attacks. Striking a balance between leveraging AI/ML for security purposes and safeguarding against misuse will be a future challenge [21].
- **Evolving Regulatory Landscape:** The regulatory landscape surrounding credit card security is continuously evolving. Staying compliant with existing regulations and adapting to new requirements can take time for credit card issuers. Organizations must maintain a proactive approach, regularly assess regulatory changes, and invest in compliance measures to navigate this dynamic landscape successfully [22].

7. CONCLUSION

By understanding the fraud techniques employed by fraudsters and implementing robust mitigation strategies, stakeholders in the financial industry can work together to create a safer and more secure environment for credit card transactions. The paper has highlighted that fraudsters utilize diverse methods, such as data breaches, skimming devices, and phishing scams, to obtain card numbers. These techniques exploit vulnerabilities in payment systems and compromise the security of sensitive cardholder information. Consequently, unsuspecting victims face the risk of financial loss and potential damage to their credit reputation. To address these challenges, the research has outlined effective mitigation strategies. Implementing robust security measures and encryption technologies can help safeguard cardholder data and prevent unauthorized access. Fraud detection systems equipped with advanced analytics and machine learning algorithms can proactively identify suspicious transactions and patterns, enabling timely intervention to mitigate potential fraud. Additionally, raising awareness among individuals about the importance of secure online practices, such as avoiding suspicious links and protecting personal information, can reduce the likelihood of falling victim to fraud. Continuous research, innovation, and collaboration are essential to stay one step ahead of evolving fraud techniques and protect the interests of cardholders, businesses, and the overall economy.

References

1. Online Available at: Cyber Security Issues and Challenges in E-Commerce by Dr. Shazia W. Khan :: SSRN Last accessed on 21 June 2023
2. Online Available at: Credit Card Fraud Is a Computer Security Problem | IEEE Journals & Magazine | IEEE Xplore Last accessed on 21 June 2023
3. Online Available at: How Experts Detect Phishing Scam Emails | Proceedings of the ACM on Human-Computer Interaction Last accessed on 21 June 2023
4. Online Available at: Applied Sciences | Free Full-Text | Credit Card Fraud Detection in Card-Not-Present Transactions: Where to Invest? (mdpi.com) Last accessed on 21 June 2023
5. Online Available at: Credit and identity theft - ScienceDirect Last accessed on 21 June 2023
6. Online Available at: An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection | IEEE Journals & Magazine | IEEE Xplore Last accessed on 21 June 2023
7. Online Available at: https://www.investopedia.com/capital-one-reveals-massive-hack-exposing-millions-4707235 Last accessed on 21 June 2023
8. Online Available at: https://www.theguardian.com/business/2014/sep/19/home-depot-56m-credit-card-numbers-compromised Last accessed on 21 June 2023
9. Online Available at: https://krebsonsecurity.com/2013/07/hacker-ring-stole-160-million-credit-cards/ Last accessed on 21 June 2023
10. Online Available at: Microsoft Word - 6522-20880-1-SM-New1-Jenny (researchgate.net) Last accessed on 21 June 2023
11. Online Available at: IJCSI-9-4-2-457-462-libre.pdf (d1wqtxts1xzle7.cloudfront.net) Last accessed on 21 June 2023
12. Online Available at: 602.pdf (iacr.org) Last accessed on 21 June 2023
13. Online Available at: Online Payment Gateways Used to Facilitate E-Commerce Transactions and Improve Risk Management by Paul Benjamin Lowry, Taylor Michael Wells, Gregory D Moody, Sean Humphreys, Degan Kettles :: SSRN Last accessed on 21 June 2023
14. Online Available at: A Security Awareness Program for PCI DSS Compliance: Implementation and Legal and Ethical Issues to Be Considered (isaca.org) Last accessed on 21 June 2023
15. Online Available at: *TR-06-05.pdf (carleton.ca) Last accessed on 21 June 2023
16. Online Available at: 34._Biometric_Authentication_of_Financial_Transactions-libre.pdf (d1wqtxts1xzle7.cloudfront.net) Last accessed on 21 June 2023
17. Online Available at: https://pdfs.semanticscholar.org/01be/7624aa0e0251182593350a984411c2e5128a.pdf Last accessed on 21 June 2023

18. Online Available at: https://www.sciencedirect.com/science/article/abs/pii/S2214785321045752 Last accessed on 21 June 2023
19. Online Available at: https://popcenter.asu.edu/sites/default/files/problems/credit_card_fraud/PDFs/Bhatla.pdf Last accessed on 21 June 2023
20. Online Available at: https://www.sciencedirect.com/science/article/pii/S1319157822004062 Last accessed on 21 June 2023
21. Online Available at: https://www.sciencedirect.com/science/article/pii/S187705092030065X Last accessed on 21 June 2023
22. Online Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167404815001261 Last accessed on 21 June 2023
23. Online Available at:https://scholar.google.com/citations?view_op=view_citation&hl=en&user=NqR8-fkAAAAJ&citation_for_view=NqR8-fkAAAAJ:u-x6o8ySG0sC Last accessed on 21 June 2023
24. Online Available at:https://scholar.google.com/citations?view_op=view_citation&hl=en&user=NqR8-fkAAAAJ&citation_for_view=NqR8-fkAAAAJ:zYLM7Y9cAGgC Last accessed on 21 June 2023
25. Online Available at:https://scholar.google.com/citations?view_op=view_citation&hl=en&user=NqR8-fkAAAAJ&citation_for_view=NqR8-fkAAAAJ:d1gkVwhDpl0C Last accessed on 21 June 2023
26. Online Available at:https://scholar.google.com/citations?view_op=view_citation&hl=en&user=NqR8-fkAAAAJ&citation_for_view=NqR8-fk AA AAJ:qjMakFHDy7sC Last accessed on 21 June 2023