ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

Enhancing Transactional Security in U.S. Banking Systems by Implementing OTP-Based Two-Factor Authentication to Mitigate Debit and Credit Card Fraud

Chiedozie M. Okafor[1]*, Dickson O. Oseghale[2], Stephen Ayanlaja[3]

[1]ISACA–Abuja Chapter, Financial Analyst Independent Researcher Certified Information System Auditor, Nigeria

[2]Division of Global HIV & TB, U.S. CDC, Budget Analyst, Nigeria

[3]U.S. CDC, Financial Analyst Auditor, Nigeria

***Corresponding Author**

DOI: https://doi.org/10.51244/IJRSI.2025.120800111

Received: 09 Aug 2025; Accepted: 15 Aug 2025; Published: 30 July 2025

ABSTRACT

The rapid rise in debit and credit card fraud within the United States has become a significant threat to financial institutions and consumer trust. Despite the widespread use of encryption and secure socket layer (SSL) technologies, traditional single-factor authentication methods such as static passwords and Card Verification Value (CVV) codes remain susceptible to cyber threats, including phishing, data breaches, and credential stuffing. This paper proposes the implementation of One-Time Password (OTP)-based Two-Factor Authentication (2FA) as a scalable and effective mechanism to enhance the security of card-based transactions in the U.S. banking system. By combining a user-known credential with a dynamic, time-sensitive OTP, the study presents a robust authentication framework designed to reduce unauthorized access and transactional fraud. The discussion draws on a comprehensive review of current fraud trends, limitations of existing authentication models, and a conceptual OTP-integrated security architecture adaptable to banking infrastructures. The paper also considers technical feasibility, user experience implications, and regulatory compliance. Findings offer practical insights and implementation strategies to support U.S. financial institutions in mitigating fraud risks while maintaining accessibility and usability for consumers.

Keywords: One-Time Password (OTP), Two-Factor Authentication (2FA), Card-Not-Present (CNP), Time-Based One-Time Password (TOTP), Authentication

INTRODUCTION

Background

The financial services sector in the United States has experienced a significant and sustained increase in payment card fraud, particularly involving debit and credit cards. This trend has been exacerbated by the growth of digital banking and e-commerce, especially following the COVID-19 pandemic, which contributed to a sharp rise in online and card not present (CNP) transactions (Sato, 2024). CNP transactions are especially vulnerable, as they bypass physical card verification processes and rely solely on digital credentials, which are increasingly targeted by cybercriminals.

According to the Federal Trade Commission (FTC), over 390,000 cases of credit card fraud were reported in 2023 alone, and for the first time, total reported fraud losses in the U.S. surpassed $10 billion, representing a 14% increase over the previous year (Federal Trade Commission, 2023). This aligns with growing concerns that account takeover fraud is outpacing malware as a dominant threat in the financial sector (Hoffman, 2022).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

Reinforcing the urgency of this issue, the Nilson Report projects that global card fraud losses will exceed $403.88 billion over the next decade, with the United States bearing a disproportionate share of 42% in the global card fraud losses, despite accounting for only 25% of transaction volume (Marek, 2025). The report attributes this disparity to reluctance among U.S. merchants and card issuers to adopt stricter fraud prevention technologies, a vulnerability increasingly exploited by international criminal actors.

Together, these findings underscore the systemic weaknesses of current authentication systems and highlight the need for urgent reform. Traditional single factor authentication methods, such as static passwords, PINs, and CVVs, lack contextual verification and are highly susceptible to phishing, credential stuffing, and replay attacks (Simmons, 2024; Yuza, 2024). In response, financial institutions must pursue adaptive, layered approaches to transaction security, such as the implementation of OTP-based two factor authentication (2FA), to effectively safeguard user accounts and digital payment systems in the evolving threat landscape.

Problem Statement

While the adoption of encryption technologies and fraud monitoring systems has advanced in U.S. financial institutions, the continued reliance on single factor authentication (SFA) remains a significant vulnerability. Methods such as static passwords, PINs, and CVV codes offer no contextual validation, are easily phished or stolen, and are frequently reused across multiple platforms (Aibangbee, 2023; Brown et al., 2021). These weaknesses allow attackers to exploit even minor credential leaks to gain unauthorized access to user accounts. The risk is further amplified by the fact that many e-commerce platforms such as Amazon, Walmart, and some ride-hailing or subscription-based services do not require OTP-based two-factor authentication prior to payment settlement. This lack of enforcement enables fraudulent transactions to be processed without additional user verification, exposing debit and credit card credentials to misuse and increasing financial liability for the issuing banks in the event of chargebacks or unauthorized claims.
The problem is further compounded by the lack of real-time response mechanisms in most SFA systems. Unlike multi-factor approaches, single-layer models cannot dynamically verify a user's identity based on device, location, or transactional behavior. As a result, attackers who successfully obtain user credentials through phishing or malware can execute fraudulent transactions with little resistance (Simmons, 2024; Yuza, 2024).

Although regulatory bodies such as the Federal Financial Institutions Examination Council (FFIEC) and National Institute of Standards and Technology (NIST) have issued guidelines advocating for multi-factor authentication, adoption across U.S. banks remains inconsistent. Many institutions continue to delay or limit implementation due to perceived user friction, cost, or legacy infrastructure limitations. This disconnects between regulatory expectations and practical implementation has created a gap in the security posture of digital banking systems.

What is urgently needed is a secure, scalable, and user-friendly solution that enhances authentication without introducing bureaucratic bottleneck. OTP-based Two-Factor Authentication (2FA), which introduces a dynamic, time-sensitive credential alongside the user’s primary login information, offers a practical approach to closing this security gap. However, its widespread adoption requires not only technical adaptation but also organizational commitment and customer education.

Research Aim and Objectives

This study aims to enhance the security of transactional systems within U.S. banking institutions through the implementation of OTP-based Two-Factor Authentication (2FA). Specifically, it will:

- Analyze the current landscape and methodologies of debit/credit card fraud in the U.S.
- Examine the limitations of traditional authentication methods.
- Propose a secure and adaptable 2FA framework based on OTPs.
- Evaluate the potential effectiveness of the proposed system in reducing fraudulent activities.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

- Identify implementation challenges, user adoption factors, and regulatory considerations.

Significance of the Study

The proposed research holds practical and strategic value for financial institutions, cybersecurity professionals, and policymakers. By addressing a critical vulnerability in card-based transaction systems, this study seeks to contribute to the development of a more secure banking environment. The implementation of OTP-based 2FA is not only technologically feasible but also aligns with industry best practices and emerging regulatory standards, including those set forth by the Federal Financial Institutions Examination Council (FFIEC, 2021). The outcomes of this research are intended to guide future policy formulations, technical upgrades, and customer security education initiatives.

LITERATURE REVIEW

Trends in Debit and Credit Card Fraud in the U.S

Over the past decade, the frequency and sophistication of debit and credit card fraud in the United States have steadily increased. According to the Federal Reserve's 2023 Payments Study, card fraud accounted for more than 40% of all fraud losses in the retail payments ecosystem (Federal Reserve Financial Services, 2023). Card-Not-Present (CNP) fraud, often associated with online transactions, is now the dominant form, exacerbated by increased e-commerce usage during and after the COVID-19 pandemic (Aboulaiz et al., 2024).

Criminal tactics range from phishing and credential stuffing to more advanced man-in-the-middle attacks and data breaches. In many instances, fraudsters bypass weak authentication protocols by exploiting stolen or reused login credentials(Liu et al., 2022; Mutemi & Bação, 2024). The FTC's Consumer Sentinel Network Data Book notes that financial fraud involving cards is now more prevalent than identity theft or check fraud, demonstrating a shift in threat priorities within the financial sector (Federal Trade Commission 2023).

The FTC's Consumer Sentinel Network Data Book 2024 further reinforces this narrative. With 2.6 million fraud reports filed in 2024 alone, card-related fraud particularly involving credit cards, bank transfers, and payment apps has outpaced both identity theft and check fraud. The data indicates a seismic shift in fraud vectors within the U.S. financial system.

The map below illustrates the ten states with the highest reported total fraud losses in 2024, based on data from the FTC report. These states represent key regions of vulnerability.

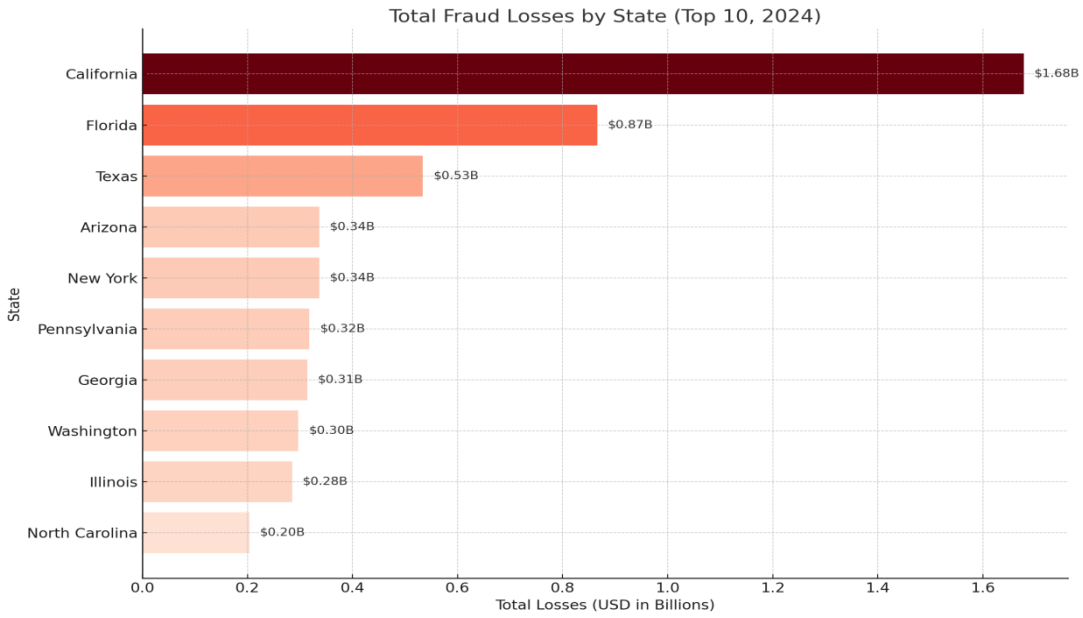


Figure 1: Total Fraud Losses by State (Top 10, 2024).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

Data Source: FTC Consumer Sentinel Network Data Book 2024 – Appendix C.

California reported the highest total fraud losses over $1.67 billion followed by Florida and Texas. In states like Illinois and Arizona, although total losses were lower, median losses exceeded $600 per report, suggesting more damaging fraud events per case.

This geographic distribution of losses highlights both high-volume and high-impact regions, underscoring the need for state-specific fraud prevention frameworks. It also supports ongoing calls for the implementation of secure multi-factor authentication, especially in card-not-present environments, to curb fraud exposure.

As U.S. payment systems continue to digitize, protecting consumers through enhanced authentication protocols, anomaly detection models, and consumer education will be crucial to reversing this trend and restoring confidence in card-based transactions.

Limitations of Traditional (Single-Factor) Authentication

Single-factor authentication (SFA) methods, such as passwords, PINs, or static security questions, rely on a single form of verification, typically something the user knows. This model, while easy to implement and use, is increasingly regarded as insufficient in modern threat environments (Ometov et al., 2018). Studies in Transactions on Privacy and Security show that over 80% of breaches involve compromised credentials, and many users tend to reuse weak passwords across multiple platforms (Das et al., 2014).

SFA systems lack transactional context and real-time adaptability, making them especially vulnerable to phishing, SIM swapping, and replay attacks. These vulnerabilities persist despite the presence of encryption and fraud monitoring systems, indicating a critical need for layered security solutions (Ali et al., 2020; Jakobsson, 2020). The U.S. Federal Financial Institutions Examination Council (FFIEC) and National Institute of Standards and Technology (NIST) have both issued recommendations for financial institutions to move beyond SFA and adopt stronger authentication frameworks (Authentication in Internet Banking: A Lesson in Risk Management, 2023).

Further compounding the limitations of SFA is the ongoing rise in fraud report categories linked to credential-based attacks. According to Appendix B2 of the 2024 Consumer Sentinel Network Data Book, categories such as Identity Theft and Imposter Scams have seen substantial increases over the past three years, closely associated with weak or compromised authentication mechanisms.

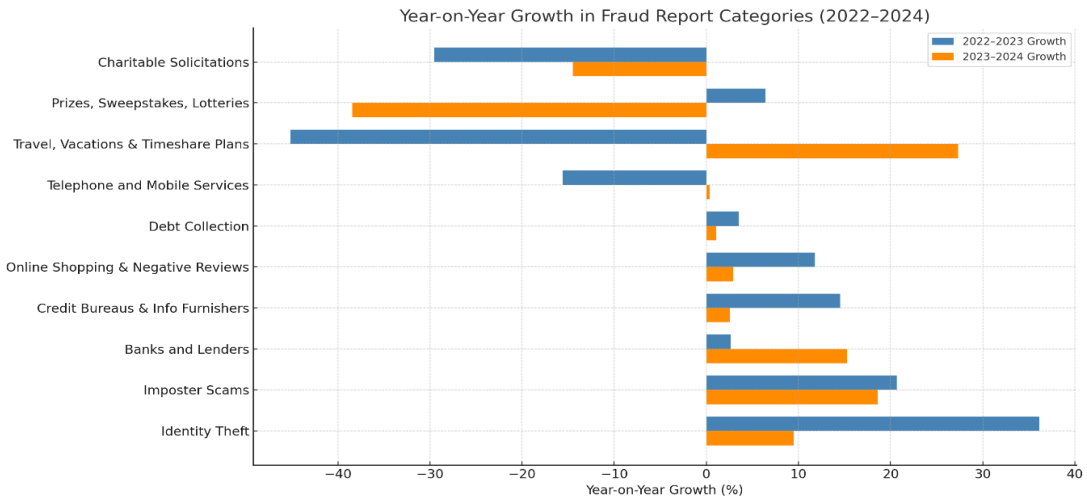


Figure 2: Year-on-Year Growth Trends in Credential-Based Fraud Categories (2022–2024).

Data Source: FTC Consumer Sentinel Network Data Book 2024 – Appendix B2.

Figure 2 illustrates the year-on-year growth rates for selected credential-based fraud categories over the 2022 to 2024 period, derived from Appendix B2 of the FTC Consumer Sentinel Network Data Book 2024. The chart

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

provides a comparative analysis of annual growth trends, highlighting areas of accelerating fraud activity and shifts in consumer risk exposure.

Notably, identity theft exhibited the most pronounced growth, with a 36.11% increase between 2022 and 2023, followed by a further 9.49% increase in 2024. This steady rise reflects ongoing vulnerabilities in personal data protection and the growing exploitation of stolen credentials in financial fraud.

Imposter scams, which are strongly associated with social engineering tactics, grew by 20.68% in 2023 and an additional 18.62% in 2024, marking it as the most persistently aggressive fraud category. These scams often exploit weak authentication controls and the absence of multi-factor identity checks.

While credit bureau and information furnisher-related complaints also rose significantly in 2023 (14.52%), growth tapered in 2024 to just 2.56%, suggesting either improved dispute resolution mechanisms or saturation in reporting.

Interestingly, banks and lenders experienced modest growth of 2.67% in 2023, followed by a sharper 15.29% rise in 2024, potentially driven by the proliferation of neobanking platforms and peer-to-peer lending frauds.

Lastly, online shopping and negative reviews, though smaller in volume, showed consistent growth year over year, 11.78% in 2023 and 2.93% in 2024 reflecting continued consumer vulnerability in e-commerce transactions.

This visualization reinforces the urgency of strengthening authentication frameworks, especially for fraud types that are disproportionately driven by compromised credentials. The disparities in growth across categories also support a risk-based security approach, where resources are strategically allocated to the fastest-growing and highest-impact fraud vectors.

The Role and Effectiveness of OTP-Based Two-Factor Authentication

Two-Factor Authentication (2FA) is defined as the combination of two distinct verification elements typically "something the user knows" (e.g., password) and "something the user has" (e.g., an OTP sent to a device). OTP-based 2FA is among the most widely adopted solutions due to its balance between security and usability(Abhishek et al., 2013; Schneier, 2005).

Empirical studies support the effectiveness of OTPs in reducing unauthorized access. Google's internal research found that OTPs sent via SMS blocked 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks (Google Security White Paper, 2020). However, OTPs sent via SMS are themselves subject to vulnerabilities such as SIM hijacking and SMS interception. This has led to the emergence of more secure alternatives, including TOTP (Time-Based OTPs) generated via mobile apps and hardware tokens like YubiKeys (Jover 2020).

Notably, a study by Alam et al. (2021) in the *Journal of Cybersecurity and Privacy* evaluated OTP-based 2FA implementations in Southeast Asian banking institutions and concluded that multi-factor models reduced fraud-related losses by up to 60% within the first 12 months of deployment. While U.S. institutions have been slower to adopt these models at scale, several major banks have already taken steps to incorporate them. For example, Capital One and Wells Fargo have integrated OTP and multi-factor authentication into their digital platforms, using mobile authenticator apps and device-based validation as an added layer of protection. These banks have reported measurable improvements in fraud prevention and customer trust, demonstrating the viability of OTP-based 2FA frameworks in the U.S. banking ecosystem.

Taken together, the reviewed literature demonstrates a clear consensus that traditional single-factor authentication mechanisms are no longer adequate in securing digital transactions, especially in high-risk environments like online banking. The widespread adoption of OTP-based 2FA offers a viable and proven means of mitigating fraud, particularly in scenarios involving remote and card-not-present payments (Mohammed et al., 2023; Yoo et al., 2014). Nonetheless, the effectiveness of such systems depends on proper

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

technical integration, regulatory support, and end-user acceptance each of which warrants careful consideration in any proposed implementation framework(Mekterović et al., 2021; Vanini et al., 2023).

System Architecture Design

This section presents the conceptual architecture for integrating OTP-based Two-Factor Authentication (2FA) into the transaction processes of non-compliant U.S. debit and credit card systems. The goal is to enhance security during remote and card-not-present (CNP) transactions by requiring an additional, time-sensitive credential that can only be used once and is contextually bound to the transaction.

Overview of the OTP- Based 2FA Model

The architecture integrates OTP-based 2FA into the payment authorization layer of banking infrastructure. It supplements the standard authentication process (e.g., card number, PIN/CVV) with a time-bound OTP, delivered or generated after the initial credential is verified.

Authentication Phases:

Credential Submission Phase

- User initiates a transaction (e.g., online payment).
- Enters primary credentials (card number, expiry, CVV, password/PIN).

OTP Generation and Transmission Phase

- Server verifies initial credentials.
- An OTP is generated:
  - Option A: SMS-based OTP sent to the registered mobile number.
  - Option B: TOTP generated by a tokenized banking or authenticator app (e.g., using RFC 6238 standard).
- OTP is bound to:
  - Transaction amount
  - Merchant ID
  - Timestamp

Verification and Authorization Phase

- User enters the received OTP.
- System validates the OTP for correctness, expiry time, and transaction binding.
- If verified, transaction is authorized.

System Components

Component	Function
Authentication Server	Handles primary credential validation and OTP logic.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

OTP Generator	Uses HMAC-based or time-based algorithms (e.g., SHA-1, SHA-256).
Token Delivery System	Sends OTP via SMS, email, or push notification, or enables app-based generation.
Transaction Binding Module	Binds OTP to transaction parameters (to prevent reuse or interception).
Client Interface	Customer-facing platform (mobile/online banking interface or POS).

Security Features

- Time Sensitivity: OTP expires after 30–60 seconds.
- Transaction Binding: OTP is only valid for a specific transaction (based on hash of transaction metadata).
- Rate Limiting: Prevents brute-force attacks by limiting OTP entry attempts.
- Device Fingerprinting: Optionally logs device/browser fingerprint to detect anomalies.
- Fallback and Recovery: Secure recovery methods in case of mobile number change or device loss.

Integration with Banking Systems

The proposed architecture is designed to work with:

- Core Banking Systems: Acts at the transaction approval layer.
- Payment Gateways: Integrates with third-party processors (e.g., Visa/MasterCard).
- Mobile and Web Banking Interfaces: Embeds directly into apps and online banking portals.

A sandbox prototype or simulation can be created using technologies such as:

- Node.js / Python (Flask/Django) for backend logic
- TOTP libraries (e.g., pyotp or otplib)
- Twilio / Firebase / Push APIs for OTP delivery
- SQLite/MySQL for storing user-device-token relationships

Diagram – OTP-Based 2FA Flow

This diagram illustrates the architecture and process flow of an OTP-based Two-Factor Authentication (2FA) mechanism designed to enhance transactional security during debit and credit card payments. The system involves five key components: the Cardholder, Merchant Website, Payment Gateway, Issuing Bank (Authentication Server and Database), and the Cardholder's smartphone used to receive the One-Time Password (OTP).

The authentication sequence proceeds as follows:

Card Information Entry

The cardholder initiates an online payment by submitting their card details—such as the card number, expiration date, and CVV—on the merchant's checkout page. This step triggers the payment authorization process.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

Transaction Request and OTP Generation

The merchant forwards the transaction request through the payment gateway to the issuing bank. If the transaction is flagged for additional verification under the 3D Secure protocol, the issuing bank generates a unique, time-sensitive OTP linked to the specific transaction.

OTP Transmission

The OTP is transmitted to the cardholder's registered smartphone via SMS, mobile push notification, or an authenticator application. This step ensures that the individual completing the transaction has possession of the trusted device.

OTP Submission and Verification

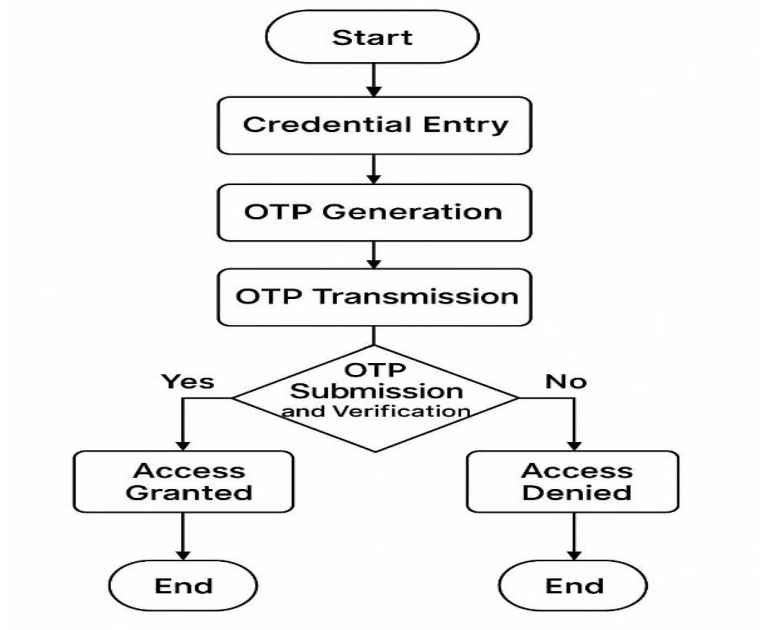
The cardholder inputs the received OTP into a secure 3D Secure verification page. The issuing bank validates the OTP along with transaction metadata, confirming both card ownership and user authorization.

Access Decision (Authorization Outcome)

If the OTP is successfully verified, the issuing bank authorizes the transaction and returns an approval to the merchant. If the OTP is incorrect, expired, or not provided, the transaction is denied, and the payment is not processed.

This structured OTP-based 2FA model significantly reduces the risk of fraudulent card-not-present (CNP) transactions by adding a dynamic verification step, reinforcing cardholder authentication, and supporting a more resilient and secure payment environment.

Diagram – OTP-Based 2FA Flow



The diagram clearly illustrates the data flow between each stage of the authentication process, with directional arrows indicating the logical sequence of interaction. It includes the outcome of the authentication check, either Access Granted or Access Denied as final steps in the process. These conclusive states enhance the clarity of the model and reflect the complete decision path based on verification results, completing the authentication lifecycle without requiring further explanation in the flowchart. This structured 2FA model significantly reduces the risk of unauthorized access due to credential theft or reuse, supporting a more secure and resilient authentication environment.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

Evaluation And Strategic Outcome

Evidence-Based Expectations for 2FA Implementation

The implementation of an OTP-based Two-Factor Authentication (2FA) system has the potential to significantly reduce fraudulent transactions involving debit and credit cards, particularly in online and card-not-present (CNP) scenarios (Gualdoni et al., 2017; Hassan et al., 2020). By combining traditional static credentials with a dynamic, time-sensitive One-Time Password (OTP), the framework establishes a robust authentication barrier. This layered approach helps prevent unauthorized access even in cases where a user's card information has been compromised (Gualdoni et al., 2017; Khattri & Singh, 2019). Based on existing literature and industry reports, the adoption of OTP and TOTP-based two-factor authentication (2FA) systems has been associated with substantial security and usability benefits. These include reported reductions of 50–70% in account takeover fraud, enhanced levels of customer trust and satisfaction, and a notable decline in phishing-related breaches due to diminished effectiveness of stolen static credentials (Moepi & Mathonsi, 2023; Yousafzai et al., 2004). These outcomes suggest that, with appropriate operational controls and user engagement strategies, the proposed architecture has the potential to deliver comparable results in U.S. banking environments especially for banks that have not adopted this authentication model.

Comparative Assessment with Existing Systems

Compared to traditional single-factor authentication systems, the proposed model:

- Enhances Security: OTPs provide time-bound, single-use credentials, mitigating risks posed by intercepted or reused login data.
- Improves Resilience to Phishing: Even if a user's primary credentials are phished, the lack of a valid OTP prevents transaction approval.
- Reduces Exposure to Brute Force Attacks: OTP expiration and entry limits significantly limit the effectiveness of brute-force methods.

However, the model also surpasses basic OTP-SMS systems by optionally supporting TOTP generation via mobile apps, which are immune to SIM-swapping and SMS interception attacks — a known vulnerability of traditional SMS-based systems.

Implementation Feasibility

From a technical standpoint, the system can be integrated into most banking infrastructures using standard APIs and existing authentication frameworks. OTP libraries (e.g., based on RFC 4226 and RFC 6238) are widely available, and secure token delivery mechanisms via SMS or mobile apps are already in use in many banks(Panjwani, 2011; Penna et al., 2019).

Nonetheless, implementation may face operational and infrastructural challenges, such as:

- Integration with legacy banking systems.
- User resistance to added authentication steps.
- Need for comprehensive customer education and support.

These issues must be addressed through phased rollouts, user experience optimization, and regulatory alignment.

Regulatory and Compliance Considerations

The proposed system aligns well with emerging cybersecurity regulations and guidelines in the United States, including:

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

- NIST SP 800-63B: Recommends multi-factor authentication for sensitive online transactions.
- FFIEC Guidelines: Encourage layered security, including OTPs and device-based authentication.
- GLBA (Gramm-Leach-Bliley Act): Mandates safeguarding consumer data, which the proposed framework supports through strengthened access controls.

Proper documentation, audit trails, and compliance checks must be built into the system to satisfy legal and regulatory requirements.

CONCLUSION AND RECOMMENDATION

Conclusion

The increasing prevalence of debit and credit card fraud in U.S. banking systems has underscored the urgent need for more robust and adaptive authentication mechanisms(Al-Furiah & Al-Braheem, 2009; Yang et al., 2022). Traditional single-factor authentication methods, although widely used, have consistently failed to protect users from evolving threats such as phishing, SIM-swapping, and credential stuffing. This research has examined the technical, regulatory, and operational shortcomings of current systems and proposed a secure OTP-based Two-Factor Authentication (2FA) framework designed to significantly enhance the security of digital and card-not-present transactions(Jover, 2020).

The proposed framework leverages time-sensitive One-Time Passwords (OTPs) delivered via SMS or generated through mobile authenticator applications to establish a secondary verification layer. By binding OTPs to specific transaction data and ensuring their time-bound validity, the system is able to mitigate many of the most common attack vectors affecting online banking and payment systems today(Akinyede & Esese, 2019; Ku et al., 2012).

The literature supports the effectiveness of OTP-based 2FA in reducing fraud-related incidents, and case studies from international banking environments suggest substantial improvements in both system resilience and user trust. While implementation in the U.S. context may pose technical and operational challenges, these are outweighed by the potential benefits in fraud mitigation, regulatory compliance, and consumer protection(Khiaonarong et al., 2021; Yousafzai et al., 2004).

Looking ahead, the evolution of authentication technologies will continue to shape the cybersecurity posture of financial institutions. While OTP-based 2FA offers an immediate and effective enhancement to transactional security, future iterations of secure banking systems may benefit from the integration of biometric authentication (e.g., facial recognition, fingerprint scanning) and AI-driven fraud detection systems that leverage machine learning to identify anomalies in real time. Incorporating such technologies into a multi-layered security framework could further reduce exposure to emerging threats and ensure long-term resilience in an increasingly digital and mobile banking environment.

Recommendation

Based on the findings of this study, the following recommendations are proposed to guide effective implementation and sustained impact of OTP-based Two-Factor Authentication in U.S. banking systems:

1. **Adopt App-Based OTPs Over SMS OTPs**

   While SMS-based OTPs are easier to implement, mobile authenticator applications or hardware tokens offer significantly stronger protection against interception, SIM swapping, and SMS-related attacks.

2. **Phase Implementation Across Transaction Types**

   Begin with high-risk card-not-present (CNP) transactions and gradually expand to include other sensitive operations such as account logins, wire transfers, and password resets.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

3. **Ensure Regulatory Compliance**

Develop the authentication framework in alignment with cybersecurity regulations such as NIST SP 800-63B, FFIEC guidance, and the Gramm-Leach-Bliley Act (GLBA), incorporating audit trails and documentation to support compliance verification.

4. **Optimize User Experience and Accessibility**

To maximize adoption, the system must be intuitive, fast, and minimally disruptive. This includes ensuring OTP delivery speed, providing fallback mechanisms, and addressing accessibility issues for users without smartphones or with unreliable mobile connectivity.

5. **Conduct User Education and Awareness Campaigns**

Users should be educated about the role of OTPs in preventing fraud and trained to recognize common threats such as phishing and social engineering. Informed users are more likely to adhere to secure usage practices.

6. **Invest in Backend Security Infrastructure**

OTP validation systems and transaction binding modules must be secured against tampering, with integrated rate limiting, anomaly detection, and system-level monitoring to proactively identify and prevent authentication abuse.

REFERENCES

1. Abhishek, K., Roshan, S., Kumar, A., & Ranjan, R. (2013). A Comprehensive Study on Two-factor Authentication with One Time Passwords. In Lecture notes in electrical engineering (p. 405). Springer Science+Business Media. https://doi.org/10.1007/978-1-4614-6154-8_40
2. Aboulaiz, L., Akintade, B., Daud, H., Lansey, M., Rodden, M., Sawyer, L., & Yip, M. (2024). Offline Payments: Implications for Reliability and Resiliency in Digital Payment Systems. FEDS Notes. https://doi.org/10.17016/2380-7172.3456
3. Aibangbee, Y. (2023). Multifactor Authentication: Opportunities and Challenges. https://bpi.com/multifactor-authentication-opportunities-and-challenges/
4. Akinyede, R. O., & Esese, O. A. (2019). Development of a Secure Mobile E-Banking System. https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/download/981/442
5. Al-Furiah, S., & Al-Braheem, L. (2009). Comprehensive study on methods of fraud prevention in credit card e-payment system. 592. https://doi.org/10.1145/1806338.1806450
6. Ali, G., Dida, M. A., & Sam, A. (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures [Review of Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures]. Future Internet, 12(10), 160. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/fi12100160
7. Authentication in Internet Banking: A Lesson in Risk Management. (2023). https://www.fdic.gov/bank-examinations/authentication-internet-banking-lesson-risk-management
8. Brown, M. A., Bendiab, G., Shiaeles, S., & Ghita, B. (2021). A Novel Multimodal Biometric Authentication System Using Machine Learning and Blockchain. In Lecture notes in networks and systems (p. 31). Springer International Publishing. https://doi.org/10.1007/978-3-030-64758-2_3
9. Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The Tangled Web of Password Reuse. https://doi.org/10.14722/ndss.2014.23357
10. Federal Financial Institutions Examination Council. (2021). Authentication and access to financial institution services and systems. https://www.ffiec.gov/press/pdf/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdfNational Credit Union Administration+6
11. Federal Reserve Financial Services. (2023). 2023 Risk Officer Survey. https://www.frbservices.org/binaries/content/assets/crsocms/news/research/2023-risk-officer-survey.pdf

12. Federal Trade Commission. (2023). Consumer Sentinel Network Data Book 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf
13. Gualdoni, J., Kurtz, A., Myzyri, I., Wheeler, M., & Rizvi, S. S. (2017). Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication. Procedia Computer Science, 114, 93. https://doi.org/10.1016/j.procs.2017.09.016
14. Hassan, M. A., Shukur, Z., & Kamrul, M. (2020). An Improved Time-Based One Time Password Authentication Framework for Electronic Payments. International Journal of Advanced Computer Science and Applications, 11(11). https://doi.org/10.14569/ijacsa.2020.0111146
15. Hoffman, K. (2022). Account takeover poised to surpass malware as the No. 1 security concern. https://www.scmagazine.com/analysis/account-takeover-poised-to-surpass-malware-as-the-no-1-security-concern
16. Information Technology / Cybersecurity. (2021). Authentication and Access to Financial Institution Services and Systems. https://www.fdic.gov/news/financial-institution-letters/2021/fil21055.html
17. Jakobsson, M. (2020). Social Engineering Resistant 2FA. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2001.06075
18. Jover, R. P. (2020). Security Analysis of SMS as a Second Factor of Authentication. Queue, 18(4), 37. https://doi.org/10.1145/3424302.3425909
19. Khattri, V., & Singh, D. K. (2019). Implementation of an Additional Factor for Secure Authentication in Online Transactions. Journal of Organizational Computing and Electronic Commerce, 29(4), 258. https://doi.org/10.1080/10919392.2019.1633123
20. Khiaonarong, T., Leinonen, H., & Rizaldy, R. (2021). Operational Resilience in Digital Payments: Experiences and Issues. IMF Working Paper, 2021(288), 1. https://doi.org/10.5089/9781616355913.001
21. Ku, Y., Choi, O., Kim, K., Shon, T., Hong, M., Yeh, H., & Kim, J.-H. (2012). Two-factor authentication system based on extended OTP mechanism. International Journal of Computer Mathematics, 90(12), 2515. https://doi.org/10.1080/00207160.2012.748901
22. Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce [Review of Cyber security threats: A never-ending challenge for e-commerce]. Frontiers in Psychology, 13. Frontiers Media. https://doi.org/10.3389/fpsyg.2022.927398
23. Mekterović, I., Karan, M., Pintar, D., & Brkić, L. (2021). Credit Card Fraud Detection in Card-Not-Present Transactions: Where to Invest? Applied Sciences, 11(15), 6766. https://doi.org/10.3390/app11156766
24. Moepi, G. L., & Mathonsi, T. E. (2023). Implementation of an Enhanced Multi-Factor Authentication Scheme with a Track and Trace Capability for Online Banking Platforms. https://doi.org/10.20944/preprints202311.0950.v1
25. Mohammed, A. H. Y., Dziyauddin, R. A., & Latiff, L. A. (2023). Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges. International Journal of Advanced Computer Science and Applications, 14(1). https://doi.org/10.14569/ijacsa.2023.0140119
26. Mutemi, A., & Bação, F. (2024). E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review. Big Data Mining and Analytics, 7(2), 419. https://doi.org/10.26599/bdma.2023.9020023
27. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. Cryptography, 2(1), 1. https://doi.org/10.3390/cryptography2010001
28. Panjwani, S. (2011). Towards end-to-end security in branchless banking. 28. https://doi.org/10.1145/2184489.2184496
29. Penna, G. D., Frasca, P., & Intrigila, B. (2019). Two Factor Authentication for e-Government Services using Hardware-Like One Time Password Generators. Journal of Computer Science, 15(1), 171. https://doi.org/10.3844/jcssp.2019.171.189
30. RecordedFuture. (2022). 2024 Payment Fraud Report: Trends, Insights, and Predictions for 2025. https://www.recordedfuture.com/research/annual-payment-fraud-intelligence-report-2024
31. Sato, G. (2024). What Is Account Takeover Fraud and How Can You Prevent It? https://www.experian.com/blogs/ask-experian/what-is-account-takeover-fraud-how-to-prevent-it/

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VIII August 2025

32. Schneier, B. (2005). Two-factor authentication. Communications of the ACM, 48(4), 136. https://doi.org/10.1145/1053291.1053327
33. Simmons, C. (2024). 2025 Predictions: Eliminating Gaps in Identity Security. https://www.savvy.security/blog/2025-predictions-eliminating-gaps-in-identity-security/
34. Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management. Financial Innovation, 9(1). https://doi.org/10.1186/s40854-023-00470-w
35. Yang, M., Luo, J.-N., Vijayalakshmi, M., & Shalinie, S. M. (2022). Contactless Credit Cards Payment Fraud Protection by Ambient Authentication. Sensors, 22(5), 1989. https://doi.org/10.3390/s22051989
36. Yoo, C., Kang, B.-T., & Kim, H. K. (2014). Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. Multimedia Tools and Applications, 74(10), 3289. https://doi.org/10.1007/s11042-014-1888-3
37. Yousafzai, S., Pallister, J., & Foxall, G. R. (2004). Strategies for building and communicating trust in electronic banking: A field experiment. Psychology and Marketing, 22(2), 181. https://doi.org/10.1002/mar.20054
38. Yuza, R. (2024). Importance of Adaptive Authentication in Financial Services. https://www.secureauth.com/resources/importance-of-adaptive-authentication-in-financial-services/