A US PAYMENTS FORUM WHITE PAPER

Leading Practices for Securing Mobile and Contactless Payments

Version 1.0

August 2025

U.S. Payments Forum
544 Hillside Road
Redwood City, CA 94062

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body that brings stakeholders together on neutral ground to enable efficient, timely and effective implementation of emerging and existing payment technologies. This is achieved through education, guidance and alternative paths to adoption. The Forum is the only non-profit organization whose membership includes the whole payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on and have a voice in the future of the U.S. payments industry. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies.

Comments or recommendations for edits or additions to this document should be submitted to: info@uspaymentsforum.org.

Executive Summary

This “Leading Practices for Securing Mobile and Contactless Payments” white paper offers numerous considerations for helping to ensure the security of the increasingly widespread mobile and contactless payment, also known as touchless payment, methods. As digital transactions become more embedded in daily commerce, their security is critical for maintaining consumer trust and ensuring the robustness of financial transactions against threats and fraud.

This white paper discusses important security mechanisms such as tokenization, biometrics, secure card provisioning, fraud management, and the significance of consumer education. It highlights the collaborative efforts required across stakeholders in the payments ecosystem, including issuers, merchants, payment processors, and technology providers, to implement effective security practices.

This paper is structured to support readers with varying roles—from strategists to implementers. While each section can stand alone, readers not involved in technical integration may choose to focus on high-level summaries, fraud trends, consumer education, and best practices, while others may find value in the detailed guidance provided in areas such as tokenization and card provisioning.

Additionally, the white paper outlines various emerging threats in digital payments and sophisticated technologies that can help combat these threats, such as AI-driven anomaly detection and multifactor authentication strategies. Our hope in providing this educational resource is to inform industry stakeholders considering how best to ensure both the security and the seamless operation of their mobile and contactless payment systems.

Table of Contents

1. Introduction

In the fast-evolving landscape of digital commerce, mobile and contactless payments are becoming increasingly central to consumers' daily transactions worldwide. This white paper is designed to provide a comprehensive overview of effective security measures that protect these modern payment methods. The objective is to highlight essential practices that ensure the integrity and security of remote card payments and mobile-device-based payment systems.

The scope of this document includes a detailed examination of key security practices such as tokenization, biometrics, secure card provisioning, fraud management and account takeover prevention, and extensive consumer education on digital payments. Each of these areas is critical in building a robust defense against potential security threats, thereby enhancing the overall security framework of mobile and contactless payment systems.

The target audience includes a broad spectrum of stakeholders in the payment ecosystem who all rely on these payment systems: issuers, merchants, issuer processors, acquirer processors, wallet providers, networks, and consumers. For merchants, understanding operational and point-of-sale (POS) security can significantly reduce the risk of fraud and data breaches, while issuers and processors will find the discussions on provisioning and tokenization directly relevant to their operations.

The importance of securing these payment methods cannot be overstated: security is the foundation upon which trust in and adoption of mobile and contactless payments rest. As these payment technologies become more integrated into financial transactions, the need to reinforce them with strong, reliable security measures becomes increasingly critical. This white paper serves as an educational resource, aiming to cultivate a deeper understanding of the security challenges and solutions in digital payments, thereby fostering an environment where safety and efficiency coexist.

To support a diverse audience across the payments ecosystem, this paper includes both strategic guidance and technical implementation detail. Readers may choose to focus on sections most relevant to their roles—for example, those interested in policy or consumer protection may prioritize high-level practices, while those working on wallet integration or provisioning may benefit from deeper technical content.

2. Tokenization

Tokenization is a foundational component of mobile and contactless payment security. Because it underpins both wallet-based and card-on-file transactions, this section includes implementation-level detail to support technical teams. Readers already familiar with tokenization mechanics may wish to focus on challenges, innovations, and leading practices covered later in the section.

Tokenization is a process used to protect sensitive payment data, like the card's primary account number (PAN), by replacing it with an algorithmically generated number, known as a token. This token acts as a proxy for the real card number during transactions, whether the card is stored in a digital wallet on the phone, in a smartwatch, or on a merchant's site.

2.1 Card-on-File or Merchant Payment Tokenization

Card-on-file (CoF) or merchant payment tokenization replaces the PAN with a unique identifier, or token, which can only be used with a specific transaction, merchant, or payment processor. Merchant payment tokenization is typically managed by a merchant or a payment processor.

Although card-on-file transactions may not involve physical contactless interaction, they are frequently initiated through mobile devices, as seen with apps like Walmart Pay and Starbucks. These payments rely on stored credentials and tokenization infrastructure similar to that used in mobile wallets, making them relevant to mobile and touchless payment security.

Merchant payment tokenization is commonly used for securing card-on-file transactions (e.g., e-commerce transactions) to protect stored credit card information. Tokens are usually restricted and can only be used with the merchant or processor that created them. This restriction reduces the risk of a compromised token since it would not be usable outside of that specific context.

2.2 Network Tokenization

Network tokenization[1] also replaces the PAN with a token, but is managed by the payment network (e.g., American Express, Discover, Mastercard, Visa) rather than by the merchant or processor. The network token acts as a proxy for the actual PAN across different merchants. Network tokens are managed by the payment networks or token service providers (TSPs), have a direct link to the consumer’s/cardholder’s issuing bank, and can be universally recognized.

Network tokens are often used in digital wallets (like Apple Pay® or Google Pay™) and can be used across multiple merchants and payment networks for single purchases, recurring payments, or subscription models. These tokens have broader utility than merchant tokens and can be used in multiple environments while maintaining a consistent link to the original cardholder's account.

[1] Network tokenization is also referred to as EMV tokenization.

Figure 1 illustrates how network tokenization works in the transaction flow.

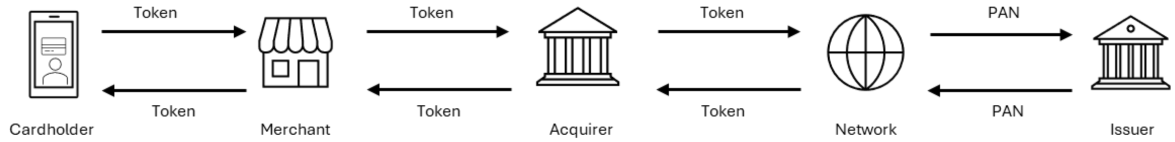


Figure 1. How Network Tokenization Works

2.3 Network Tokenization in Digital Wallets

Digital wallets (such as Apple Pay, Google Pay, and Samsung Pay®) allow users to store their payment card information securely on their mobile devices or wearables and use it to make contactless payments in stores, online, and in apps.

Figure 2 illustrates the card registration and network token provisioning process with digital wallets.

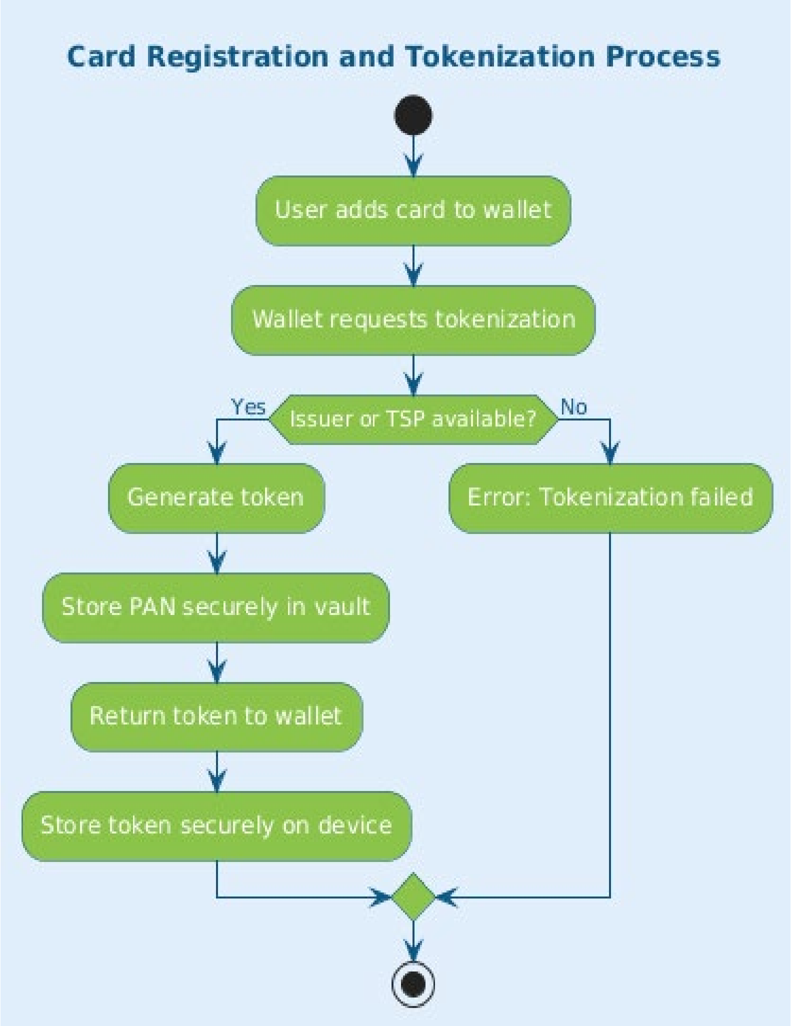

Card Registration and Tokenization Process
User adds card to wallet
Wallet requests tokenization
Issuer or TSP available?
Yes
No
Generate token
Error: Tokenization failed
Store PAN securely in vault
Return token to wallet
Store token securely on device

Figure 2. Registration and Tokenization Process in Digital Wallets

The registration and tokenization process with a digital wallet includes the following steps:

- **Card registration**: When a user adds their payment card (debit or credit) to a digital wallet, the wallet requests tokenization from the card issuer or the TSP.
- **Token creation**: The card issuer or TSP generates a unique token to replace the card's PAN. This token is linked to the user's device (e.g., a smartphone or smartwatch) and can only be used with that device.
- **Token storage**: The token is stored in the mobile device's secure element (a tamper-proof chip designed to store sensitive information securely) or in a cloud-based system, depending on the wallet provider. The actual card details, including the PAN, are stored in a secure vault by the card issuer or TSP.

When the user makes a payment using their digital wallet, the payment authorization includes the following steps:

1. **Initiation of transaction by the cardholder**
   - When the cardholder initiates a payment using the digital wallet (e.g., tapping their phone on a contactless terminal), the wallet provides the token (rather than the PAN) along with a cryptogram unique to the transaction.
   - This cryptogram acts as a form of digital signature, proving the transaction request's authenticity.
2. **Transmission of token and cryptogram**
   - The POS terminal receives the token and cryptogram and sends them to the acquirer/processor.
   - The PAN itself is never exposed at any stage of the process, reducing the risk of exposure to fraud.
3. **Transmission of authorization request to the payment network**
   - The acquirer forwards the token and cryptogram to one of the supported payment networks for authorization. The payment network verifies the validity of the token and cryptogram, and if valid, proceeds with the next steps.
   - The payment network maps the token back to the cardholder's actual PAN using its secure token vault, which links tokens to the original PANs.
4. **Transmission to the issuing bank**
   - The payment network then forwards the mapped PAN and other transaction details to the cardholder's issuing bank.
   - The issuing bank checks the account for available funds, verifies that the transaction is consistent with the cardholder's spending behavior, and performs other fraud checks.
5. **Completion of the authorization decision**
   - Based on the checks, the issuing bank makes an authorization decision (approve or decline) and sends it back to the payment network, which translates the decision and PAN to match the original token format.
   - The payment network then sends the authorization response back to the acquirer, which relays it to the merchant's POS terminal.
6. **Completion of transaction**
   - If approved, the merchant receives the authorization response, and the transaction is completed.

- The cardholder is notified of the successful transaction, and no sensitive card data (e.g., the PAN) is exposed in the process.

Figure 3 illustrates the payment authorization process with a digital wallet using network tokens.

Using tokens in digital wallets provides significant benefits, including:

- **Security**: Even if the token is intercepted, it cannot be used without the associated device or authentication (e.g., fingerprint, face ID, or PIN).
- **Device specific**: The token is tied to the device, so even if the token is stolen, it cannot be used on another device.
- **Multiple use cases**: Tokens can be used for in-store, in-app, and online payments, making them versatile.

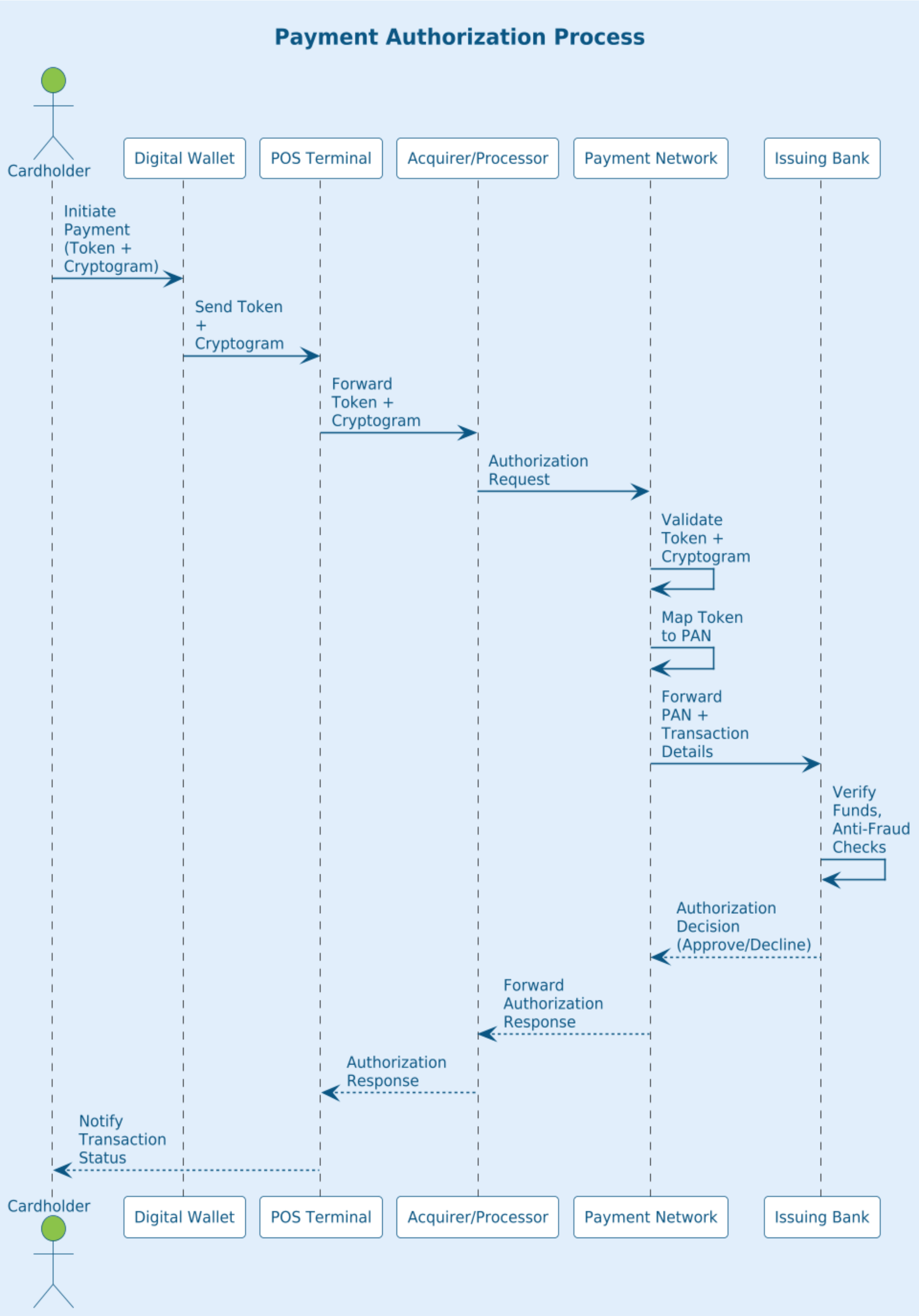

Payment Authorization Process
Cardholder
Digital Wallet
POS Terminal
Acquirer/Processor
Payment Network
Issuing Bank
Initiate Payment (Token + Cryptogram)
Send Token + Cryptogram
Forward Token + Cryptogram
Authorization Request
Validate Token + Cryptogram
Map Token to PAN
Forward PAN + Transaction Details
Verify Funds, Anti-Fraud Checks
Authorization Decision (Approve/Decline)
Forward Authorization Response
Authorization Response
Notify Transaction Status
Cardholder
Digital Wallet
POS Terminal
Acquirer/Processor
Payment Network
Issuing Bank

Figure 3. Payment Authorization Using a Network Token from a Digital Wallet

2.4 Tokenization for CoF Transactions

CoF tokenization is commonly used when a merchant stores a customer's card details for future transactions, such as for recurring payments (e.g., subscriptions) or one-click checkouts in e-commerce.

Figure 4 illustrates the tokenization process for CoF transactions where the token is created and stored by a payment gateway or TSP. Generally, tokenization is handled by a TSP.

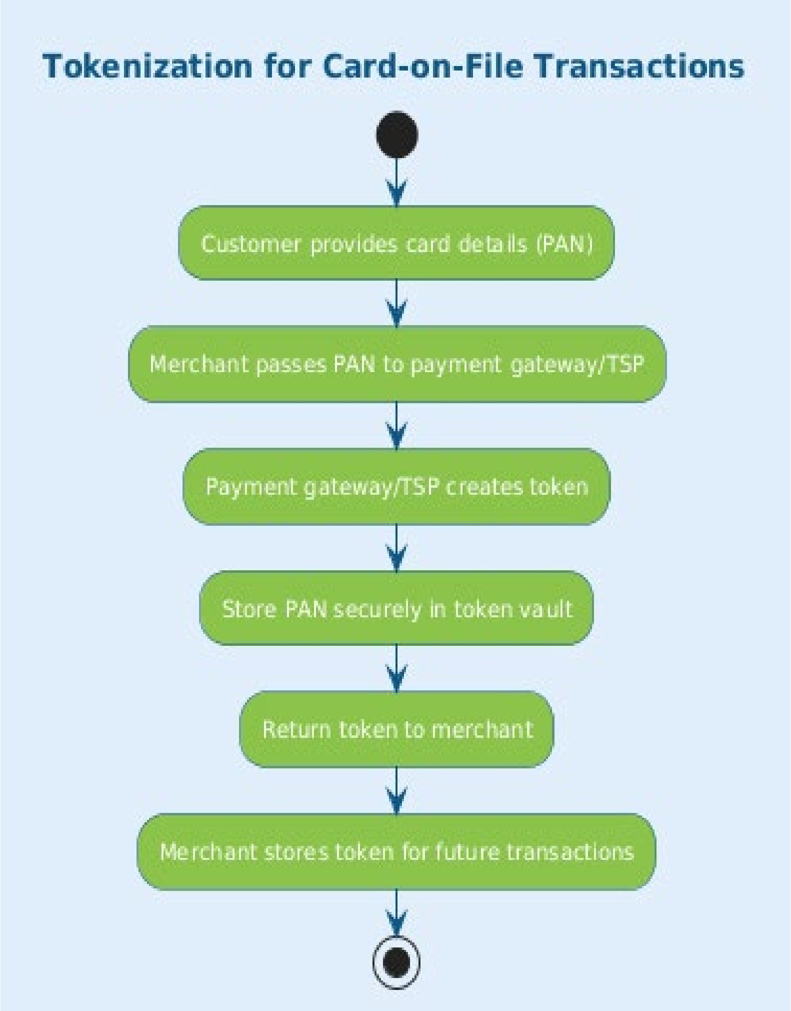
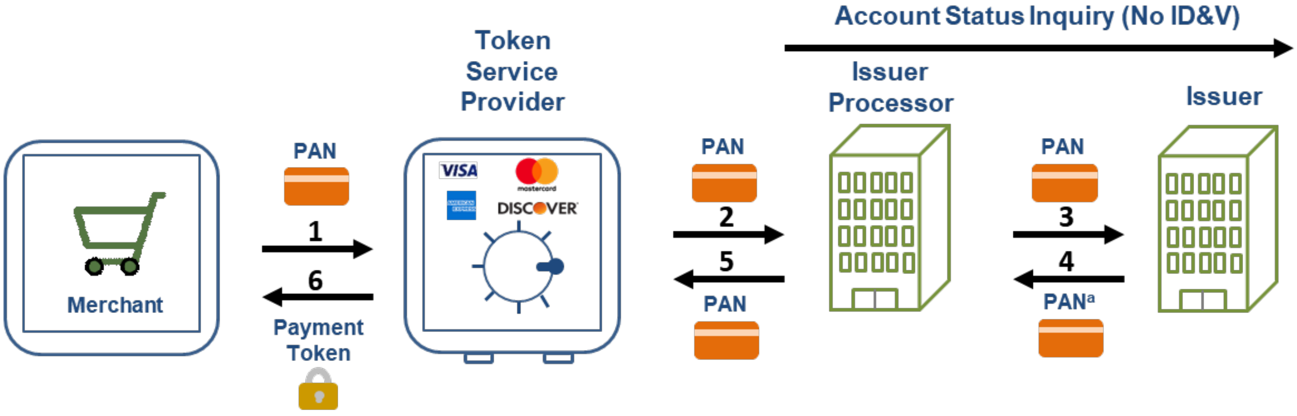

Tokenization for Card-on-File Transactions
Customer provides card details (PAN)
Merchant passes PAN to payment gateway/TSP
Payment gateway/TSP creates token
Store PAN securely in token vault
Return token to merchant
Merchant stores token for future transactions

Figure 4. Tokenization Process for CoF Transactions

Figure 5 illustrates the token provisioning process for transactions at a merchant.



[a] In some cases, this may be the last 4 digits of the PAN rather than whole PAN.

Figure 5. Token Provisioning at Merchant Sites that Store a Card (Card-on-File)[2]

The registration and tokenization process for card-on-file transactions includes the following steps:

- **Card details submission**: When a customer first provides their payment details to a merchant (e.g., during an initial purchase or account setup), the merchant passes the card details (PAN) to a payment gateway or TSP.
- **Token creation**: The payment gateway or TSP replaces the PAN with a unique token and stores it on behalf of the merchant. The PAN is stored securely in a token vault, and only the token is returned to the merchant.
- **Token storage**: The merchant keeps the token (not the actual card number) in their system to be used for future transactions. For example, when a customer subscribes to a service, the merchant can use the token instead of requesting the card information again.

When the user makes a subsequent payment to the merchant, the payment authorization includes the following steps:

- For each transaction (e.g., a recurring charge or an on-demand purchase), the merchant initiates the payment using the stored token. This token replaces the PAN and is unique to the merchant and the cardholder’s account.
- The merchant sends the tokenized data, along with the transaction amount and other details, to the acquirer for authorization.
- The acquirer forwards the token to the TSP, which is typically operated by the payment network (e.g., American Express, Discover, Mastercard, Visa) for authorization.
- The payment network sends the actual PAN, along with transaction details, to the issuing bank (the cardholder’s bank).
- The issuing bank performs necessary checks, including available balance, spending patterns, and fraud detection, before making an authorization decision.

[2] “EMV Payment Tokenization Primer and Lessons Learned,” U.S. Payments Forum, 2019, https://www.uspaymentsforum.org/emv-payment-tokenization-primer-and-lessons-learned/

- The issuing bank approves or declines the transaction based on the checks and sends the authorization response back to the payment network.
- The payment network maps the response to match the original tokenized data format and sends it back to the acquirer, who then forwards it to the merchant.
- The merchant receives the authorization response and completes the transaction. If approved, the cardholder is notified, and the transaction is settled in the usual way.

Figure 6 illustrates the payment authorization process with card-on-file tokens.

Using card-on-file tokenization provides significant benefits, including:

- **Enhanced security**: Merchants do not store sensitive card data, reducing the risk of data breaches. Even if the merchant’s system is compromised, attackers would only gain access to tokens, which are useless without access to the token vault.
- **Streamlined checkou**t: Tokenization enables faster checkouts (e.g., one-click) without needing to ask customers to enter card information again, improving the customer experience.
- **Secure recurring transactions**: The merchant can safely store tokens for recurring transactions like subscriptions or automatic billing without exposing the customer's actual card number.

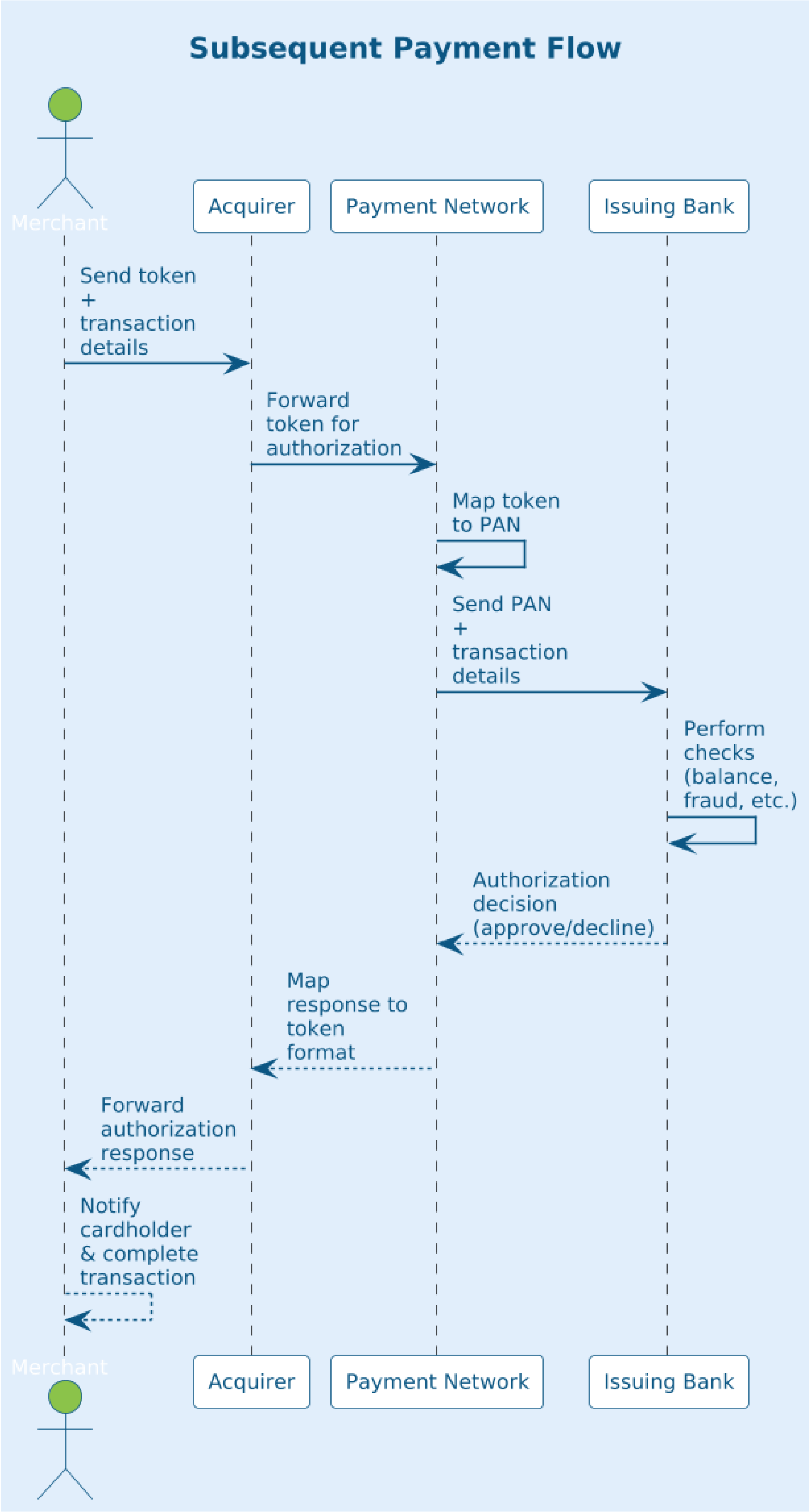

Subsequent Payment Flow
Merchant
Acquirer
Payment Network
Issuing Bank
Send token + transaction details
Forward token for authorization
Map token to PAN
Send PAN + transaction details
Perform checks (balance, fraud, etc.)
Authorization decision (approve/decline)
Map response to token format
Forward authorization response
Notify cardholder & complete transaction
Merchant
Acquirer
Payment Network
Issuing Bank

Figure 6. Payment Authorization Using a Token with a Card-on-File Transaction

2.5 Tokenization Challenges and Solutions

While payments stakeholders face challenges with tokenization implementation, industry solutions have emerged that address these challenges.

Token Management

Managing large volumes of tokens across multiple platforms and devices (e.g., mobile devices, wearables, browsers) can be challenging. In order to help ensure they are effective, tokens must be correctly mapped to users, accounts, and transactions; this can get complicated for global merchants operating across different regions.

Token vaults—secure environments for storing and mapping tokens to their original payment information—provide solutions that can centralize and simplify token management. To help ensure security, interoperability, and a seamless customer experience, companies should consider adopting strong token lifecycle management strategies to track and update tokens across all devices and platforms.

Token Lifecycle Management

Managing the lifecycle of tokens can be complicated, especially when dealing with card expiration, renewal, or customer updates (such as a new phone or card). Failure to manage these lifecycle events can lead to declined transactions or payment disruption.

Tokenization solutions can minimize these potential issues by employing automated processes to manage card reissuance, updates, and expiration. For example, payment processors can automatically map new cards to existing tokens, ensuring seamless customer experiences.

Integration Complexity

Implementing tokenization requires significant changes to existing payment systems, especially for merchants with older infrastructure, including upgrading POS systems, e-commerce platforms, and backend processes.

Payment gateways and TSPs can offer integration tools, APIs, and development kits to simplify the process. Adopting tokenization as a service (TaaS) can also help reduce the burden on merchants by outsourcing token management to a third-party provider.

Security and Data Breaches

While tokenization minimizes exposure to sensitive data, the process is not immune to attacks. If a token vault is compromised, fraudsters may gain access to tokens and their mappings to real card data.

Implementing advanced encryption, multifactor authentication (MFA), and strict access controls can help protect the token vault. Regular security audits, vulnerability testing, and Payment Card Industry Data Security Standard (PCI DSS) compliance can also reduce the risk of breaches.

2.6 Emerging Solutions and Innovations

Artificial intelligence (AI) and machine learning for token management are emerging solutions. AI can be used to track token usage patterns, flag suspicious activity, and even predict token expirations, ensuring a smooth lifecycle management process. Machine-learning models can improve fraud detection and enhance security across tokenized payment ecosystems.

3. Biometrics in Payments

This section explores biometric authentication as a key enabler of secure mobile and contactless payments. While technical readers may benefit from the detail on biometric integration and architecture, others may choose to focus on the broader use cases and privacy considerations.

Biometric authentication is positioned as a fundamental security measure for mobile and contactless payments, enabling faster and more secure user authentication. With the move to contactless transactions accelerated by the COVID-19 pandemic, the demand for seamless and secure payment solutions has surged. Biometric technologies—such as fingerprint scanning, facial recognition, and voice authentication—leverage unique physical and behavioral traits to provide reliable user authentication. Unlike traditional passwords or PINs, biometric data cannot be easily stolen, making these technologies critical in reducing the risk of fraud in digital transactions.[3]

Biometric authentication confirms access to the device, but does not independently verify cardholder identity, and should be combined with other ID&V methods when used during provisioning. For more information on this, see section 4, Secure Card Provisioning.

3.1 Types of Biometrics Used in Payments

Biometric authentication includes both physical and behavioral modalities.

- Physical biometrics include fingerprint scanning, iris recognition, and facial recognition, which authenticate users based on their inherent physical traits. These modalities are commonly integrated into smartphones and other devices, offering a convenient, yet secure way for users to authenticate payments.
- Behavioral biometrics track subtle patterns such as keystroke dynamics, swipe gestures, and voice recognition. These systems continuously monitor user behavior, providing an additional layer of protection that adapts to each user's unique habits and can help detect anomalous activities indicating fraud.

Figure 7 illustrates the distinction between physical and behavioral biometrics, and between active and passive (i.e., when the user does not need to perform an action) biometrics. These classifications help to clarify the various approaches used for mobile payment security.

[3] "Device Authentication and Consumer Verification Techniques for Mobile In-App and Remote Payments," U.S. Payments Forum, 2023, https://www.uspaymentsforum.org/wp-content/uploads/2023/03/FINAL-Device-Authentication-and-Consumer-Verification-Techniques-for-Mobile-In-App-and-Remote-Payments.pdf

	Physical	Behavioral
Active	Fingerprint Facial Recognition	Voice Signature
Passive	Vein Heartbeat	Keystroke

Figure 7. Physical vs. Behavioral Biometrics

3.2 Security Enhancements through Biometrics

Biometric systems are inherently more secure than traditional security methods like passwords or PINs since they rely on characteristics unique to each user. Notably, biometrics often function alongside device-based security measures, such as secure enclaves or hardware security modules, which ensure biometric data is stored safely and isolated from the device's main operating system. Secure enclaves further encrypt and protect biometric data from potential breaches, safeguarding it even if the device is compromised.[4]

Although privacy concerns can be addressed with the right architecture, nearly all payment providers have adopted on-device biometric storage. Server-side models may be appropriate in high-risk or high-value scenarios but are not commonly used for routine transactions.

Recent biometric security innovations include advances in multimodal biometrics, which combine several biometric indicators (e.g., both fingerprint and facial recognition) to further enhance security. This method significantly reduces the risk of false positives and negatives, helping to ensure that users are accurately verified before a transaction is completed. Moreover, the increasing implementation of liveness detection in facial recognition systems can reduce the risk of spoofing by ensuring that biometric data is captured from a live person rather than from a static image or video.[5]

Figure 8 Illustrates how a shared platform authentication mechanism securely integrates biometrics into mobile payments. The figure highlights the data flow from the device to the payment application, emphasizing the secure storage and validation of biometric data.

[4] "Device Authentication and Consumer Verification Techniques for Mobile In-App and Remote Payments," US Payments Forum, 2023, https://www.uspaymentsforum.org/wp-content/uploads/2023/03/FINAL-Device-Authentication-and-Consumer-Verification-Techniques-for-Mobile-In-App-and-Remote-Payments.pdf

[5] "Enabling fraud prevention with advances in biometrics and Liveness detection, "The Paypers, 2022, https://thepaypers.com/expert-opinion/enabling-fraud-prevention-with-advances-in-biometrics-and-liveness-detection--1257804

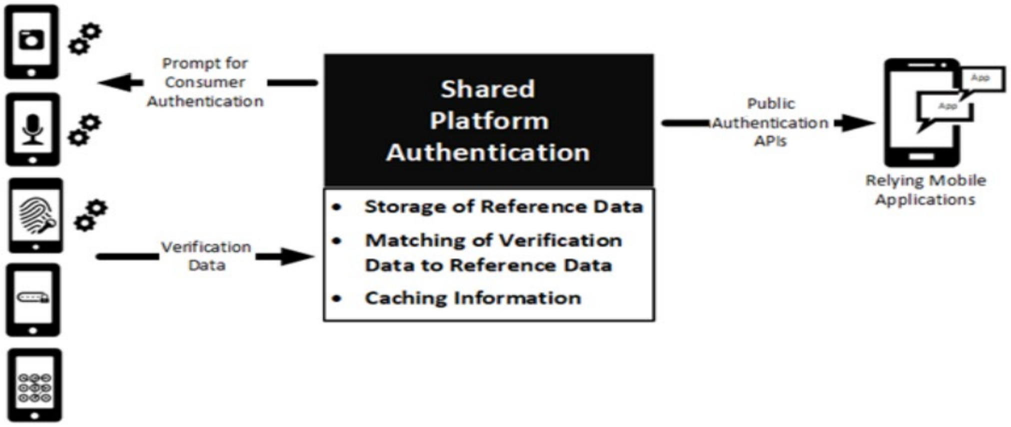

Prompt for Consumer Authentication
Shared Platform Authentication
Storage of Reference Data
Matching of Verification Data to Reference Data
Caching Information
Verification Data
Public Authentication APIs
App
App
Relying Mobile Applications

Figure 8. EMVCo Shared Platform Authentication[6]

3.3 Integration with Payment Systems

Biometric authentication seamlessly integrates into payment systems with solutions such as the Consumer Device Cardholder Verification Method (CDCVM). This method allows consumers to authenticate transactions directly on their mobile devices using biometrics like fingerprint or facial recognition. Major digital wallets, including Apple Pay, Google Pay, and Samsung Pay, have adopted CDCVM, leveraging the secure elements within the devices to protect biometric data and facilitate contactless payments. Biometrics adoption in payment systems has accelerated as more consumers shift to digital and contactless payment methods, and as businesses prioritize secure and user-friendly solutions to meet these demands.[7]

3.4 Challenges and Solutions in Biometric Authentication

Biometrics provide a convenient and secure method to unlock mobile devices and authorize payments, but their role in securing mobile and contactless payments is context-dependent. Biometrics confirm that an enrolled user is accessing the device—they do not verify the identity of the cardholder who originally provisioned the credential. For example, if a fraudster uses stolen card credentials to provision a wallet on their own phone, biometric authentication may work flawlessly and still fail to prevent fraud.

As a result, biometrics must be paired with strong identity verification (ID&V) and risk-based controls during provisioning to be effective in fraud prevention. Their primary benefit lies in preventing unauthorized access to a legitimate user's device or app—serving as a post-provisioning security layer.

Additional challenges include biometric system accuracy and user experience. False rejection rates (FRR) and false acceptance rates (FAR) can impact usability and security, though these are being mitigated through improved algorithms, liveness detection, and multimodal systems that combine multiple biometric inputs.

[6] "Consumer Device Cardholder Verification Method Security Requirements," EMVCo, 2018, EMVCo-SBMP-18-G02-V1.0_CDCVM_Security_Requirements.pdf

[7] "5 Emerging Security Imperatives for Digital Wallets," PYMNTS.com, 2024, https://www.pymnts.com/mobile-wallets/2024/5-emerging-security-imperatives-for-digital-wallets/

Privacy concerns are another key barrier. To address them, most payment providers have adopted on-device biometric storage models, using secure elements or hardware security modules to keep biometric data local. This reduces the risk of centralized breaches and aligns with regulations like GDPR and CCPA.

While centralized biometric databases may be used in some high-risk or high-value contexts, their adoption in payments remains limited. As biometric technologies evolve, their continued role will depend on balancing privacy, accuracy, and trust—particularly in environments where they support seamless, password-free user experiences without undermining fraud defenses.

4. Secure Card Provisioning

When provisioning a card to a mobile digital wallet (i.e., device-centric contactless/Near Field Communication (NFC) or device-centric online wallets), several important security considerations should be kept in mind. These considerations include built-in security features, the use of network tokenization, encryption, identification and verification (ID&V) capabilities, device validation, and fraud/risk signal analysis.

For the purposes of this white paper, a distinction is made between device-centric mobile wallets created and maintained by hardware manufacturers (e.g., Apple Wallet, Google Wallet™, Samsung Wallet®, HUAWEI Pay®) and third-party or merchant wallets (e.g., Venmo®, Walmart® Pay). A further distinction is made between these mobile-based wallets (e.g., a mobile application, either standalone as part of the mobile operating system or a third-party mobile application, merchant or otherwise) and CoF wallets (e.g., Paze™, PayPal®, Amazon Pay®).

As a generalization, device manufacturer wallets historically give card issuers and merchants less direct control over the card provisioning process, since the wallet is owned and operated by the hardware manufacturer. These wallets are designed with a standard set of security features and offer a standard set of provisioning methods. This approach is in contrast with third-party or merchant wallets where development is done by a party other than the device manufacturer. In this case, the third party has full control over the wallet's functionality (constrained by the system calls and APIs made available by the host device's mobile operating system).

This section outlines the mechanisms and risk controls involved in provisioning cards to mobile wallets. While the technical detail may be most useful to issuers and wallet providers, other readers may prefer to focus on the high-level considerations and security practices summarized throughout the section.

4.1 Security Considerations

For the purposes of this white paper, a distinction is made between "first-party wallets" - device-centric mobile wallets created and maintained by hardware manufacturers (e.g., Apple Wallet, Google Wallet™, Samsung Wallet®, HUAWEI Pay®) - and "third-party" such as merchant or other wallets (e.g. Venmo).

Both major mobile operating systems (iOS™ and Android™) provide built-in security features for provisioning cards to their respective mobile wallets. At the time that this white paper was published, the iOS platform provides a single mobile wallet offering, Apple Pay (see section 4.3, Future Outlook, for additional information). On Android devices, both first-party (Google Wallet [formerly Google Pay]) and third-party (e.g., Samsung Wallet® [formerly Samsung Pay], HUAWEI Wallet®) wallets are supported.

Built-In Wallet Security Features

As of the date of this white paper, all hardware manufacturer/first-party wallets use EMV tokenization and strong encryption and have a process for secure card provisioning. The provisioning process typically involves a risk assessment at the time of provisioning to classify the session as a "red," "yellow," or "green" path. These paths are representative of the perceived risk associated with the session, with red being the most risky, yellow being moderately risky, and green being low risk. This risk assessment typically is fed back to the card issuer to determine which authentication mechanism(s) should be invoked (if any) and what level of risk is acceptable for the issuer's risk tolerance.

Considerations of PAN Tokenization

By design, device-centric NFC mobile wallets from hardware manufacturers use tokenization and do not transmit the PAN during purchases. They also use encryption in transit and at rest to secure card data. NFC wallets work in tandem with the card issuer to authenticate the cardholder during card provisioning, using a variety of techniques depending on the device capabilities, manufacturer, and issuer. Note that a merchant's mobile application or online wallet may or may not use EMV tokenization. While EMV tokenization is generally considered a best practice, it is not mandatory.

Cardholder Verification/Identity and Verification (ID&V) Capabilities

The ID&V process is designed to verify the identity of the cardholder who is provisioning the card to a wallet. This process can leverage one or more authentication mechanisms. The mechanism used and the amount of end-user friction can vary depending on the card issuer's risk tolerance and the type of wallet into which the card is being provisioned. The following ID&V authentication mechanisms are generally available in the market at the time that this white paper was published:

- **Knowledge-based authentication (KBA)**: This form of authentication requires the end user to input privileged information that should only be known to the cardholder. The information may include the card verification code (CVC), billing information, security questions, Social Security number, or other information.
- **One-time passcodes (OTP)**: This form of authentication seeks to establish that the cardholder has possession of the device into which the card is being provisioned by transmitting a single-use, one-time passcode to a device, telephone, or email account.
- **Mobile push authentication**: If the cardholder has the issuer's mobile application installed either on the same device being provisioned or on a different mobile device, the issuer may send a mobile push authentication message to the cardholder. The message can contain information about the device being provisioned if available.
- **Relying-party/push provisioning**: In this scenario, the issuer's mobile application can initiate card provisioning to a device-centric/first party wallet (typically the hardware manufacturer's device-based wallet). This approach has an authentication advantage since the provisioning is being initiated from a higher assurance session, i.e., the end user has already passed the necessary authentication checks to access the issuer's mobile application.
- **Biometric authentication**: Typically used in tandem with push authentication, this mechanism allows the issuer to authenticate the cardholder using biometrics such as face, fingerprint, palm, retina, or voice. A key factor in biometric enablement is the security, reliability, and availability of a biometric capture sensor.
- **QR-code-based authentication**: QR-code authentication can be leveraged for cross-channel card onboarding. For example, an issuer may require a wallet provisioning process using a QR code that is generated in a higher-assurance session, such as post-authentication in online banking or with a mobile passkey. The QR code must be unique, have the necessary embedded security features to prevent reuse, and only be consumable by the authorized cardholder's device(s).

Device Validation

All major hardware/operating system manufacturers create a device ID that can be used in tandem with or in place of a mobile application developer's device ID. This ID allows devices to be tracked across user journeys to determine if a device is the same returning device or a new device. This information can be used as part of the card provisioning process to establish the relative age of the mobile device and access any historical information which may be useful (e.g., if the device has been implicated in fraud in the past or if it is a "known good" device).

Mobile application device IDs should ideally be cryptographically bound to hardware-backed secure elements or trusted execution environments to prevent device spoofing or exfiltration of key material that could lead to a compromised device or provisioning session.

Fraud/Risk Signal Analysis

An issuing bank or merchant may have first-party risk signals available, as well as those provided by the hardware manufacturers; however, additional data points may be available to help make an informed provisioning decision. Third-party data sources, including those from other issuers and/or merchants, may be available in a data-sharing agreement or consortium. Commercial fraud consortium vendors can provide additional device intelligence insights for making risk-based authentication decisions. These additional signals may also be fed into AI/machine-learning-based systems to profile a cardholder's behavior over time, thus further increasing the security of provisioning.

4.2 Leading Practices for Hardware Security Features, ID&V and Wallets

Generally speaking, taking full advantage of the security features built into the hardware manufacturer mobile wallets will help reduce risk. Due to the closed nature of the manufacturer ecosystem, only a subset of security considerations needs to be managed by the implementing party. For example, all hardware manufacturer wallets to date use EMV tokenization and strong encryption and have a process for secure card provisioning. Wallet stakeholders can tailor their provisioning experiences to the available cardholder journeys while using the data made available from the wallet itself. While the processes for third-party wallets vary considerably and may not even involve the issuing bank, issuers may wish to use available data to validate provisioning.

Identity and Verification (ID&V)

All ID&V mechanisms have strengths and weaknesses which need to be taken into consideration when designing wallet provisioning. It is generally considered to be a best practice at the time of this publication to phase out and eliminate knowledge-based authentication methods where possible. These authentication methods rely on information that should only be known to the cardholder, but still represent potential risk because they could be stolen or obtained through social engineering or coercion. Risk-based authentication (RBA) can be used to help ensure the authentication mechanism employed is determined based on a session's level of perceived risk and the available authentication options.

Additionally, leveraging industry standards or specifications for payments authentication may be prudent, especially if a stakeholder already has investments in such systems (e.g., EMV 3-D Secure [EMV 3DS] non-payment authentication, EMVCo Secure Remote Commerce [SRC]). Other standards such as the FIDO Alliance passkeys provide a standardized mechanism for strong authentication and are a generally accepted security practice.

Third-Party Mobile Wallets

While hardware manufacturer wallets provide a standard set of security features and functionality, third-party wallets can vary considerably. Some general guidelines should be taken into consideration for their use. Software-based implementations that do not leverage secure elements (or trusted execution environments [TEE], though those are less secure by nature) increase the risk of malware or bad actors intercepting or manipulating a provisioning experience. This risk is especially true for a rooted device as it exposes Host Card Emulation (HCE)-based payments to additional vulnerabilities. A rooted device has the fundamental security protections removed and an application has “root” access to the entire software file structure, including access to sensitive data such as third-party wallets.

Card-on-File Wallets

CoF wallets store payment credentials for repeated use, typically by either a merchant or payment service provider (PSP). In this scenario, since the payment credential is not provisioned by the issuer, there is no requirement for a specific level of cardholder verification or for card tokenization. It is up to the merchant/PSP to apply the appropriate level of authentication, including those listed in the “Cardholder Verification/ID&V Capabilities” in section 4.1. Thus, a key consideration with CoF wallets is the lack of specific, industry-wide security requirements for implementation. Mandatory requirements typically only involve adhering to PCI DSS requirements for handling card data.

However, since the merchant likely has an existing relationship with the cardholder, using merchant data to augment commonly accepted verification techniques can bolster the authentication assurance level. For example, a merchant may require a user to have an account, with a verified mailing address, username, password, registered passkey, and other information. The merchant can use their existing authentication processes to ensure cardholder details match, beyond simply verifying billing zip code, PAN, and CVC. Ideally, the CoF wallet will also use card tokenization to further enhance security.

Of particular note, a new type of emerging CoF wallet moves beyond the traditional merchant and PSP wallets and involves issuers. Notable examples of this include EMVCo’s Secure Remote Commerce or “Click to Pay” technology as well as issuer wallet services such as Paze. These new CoF wallets directly involve the issuer in the card provisioning process and allow the issuer to apply their own desired level of authentication for card provisioning, similar to that found in the mobile wallet ecosystem. If a cardholder registers for Click to Pay, the payment network will tokenize the CoF without the involvement of the issuer.

4.3 Future Outlook

Historically, NFC could not be used in iOS systems for third-party wallets; however, the release of iOS 18.1[8] changed this for the U.S. market. Third-party wallet developers can now create new applications that use the NFC and secure element functions in the iPhone®. At the time of this white paper publication, it is too early to determine what the third-party offerings and adoption will be, although many possibilities for wallet offerings exist, including in-store payments (e.g., tap-to-pay[9]), transit payments (open and closed loop), and loyalty/rewards programs.[10] For each of these new iOS ecosystem third-party wallet offerings, the same general security principles outlined for third-party Android-based wallets would also be applicable.

An additional feature in iOS 18.1 is a new method of Apple Pay card provisioning called "tap to provision."[11] This method allows a user to either: simply tap a contactless-enabled physical payment card instead of manually entering the card details; or do an image capture of details using optical character recognition (OCR). After the initial tap, the user may need to enter the card's security code to complete phase one (e.g., pre-authentication) of the onboarding. However, it is important to recognize that tap to provision is a convenience factor for initial card provisioning and not a replacement for cardholder verification (see the "ID&V Capabilities" portion of section 4.2 for more information). In a typical scenario, the card would be provisionally added to Apple Pay but not available for use in payments until verification is completed. The same verification process would be invoked for cards added via OCR or manual entry.

Regardless, it is critical for stakeholders to keep abreast of the latest trends in fraud and security. The proliferation of cryptocurrency, AI, state-sponsored threat actors, organized crime, and a general trend of increasing fraud activity globally requires a proactive approach to security. Furthermore, emerging technologies tangential to or outside the realm of payments can potentially be beneficial in informing security measures. In the future, there is a potential for mobile driver's licenses (mDLs) to further improve security provisioning.

Finally, while mobile app stores and manufacturers provide mechanisms to block harmful or malicious mobile applications, they cannot prevent their introduction to the mobile ecosystem entirely. Fraudulent mobile wallets, as well as legitimate wallets and merchant apps injected with malicious code, are a persistent threat to cardholder security.

[8] "NFC & SE Platform for secure contactless transactions," Apple, https://developer.apple.com/support/nfc-se-platform/

[9] "Tap to pay on iPhone security," Apple, https://support.apple.com/guide/security/tap-to-pay-on-iphone-sec72cb155f4/web

[10] "Developers can soon offer in-app NFC transactions using the Secure Element," Apple, August 14, 2024, https://www.apple.com/newsroom/2024/08/developers-can-soon-offer-in-app-nfc-transactions-using-the-secure-element/

[11] "Apple celebrates 10 years of Apple Pay," Apple, October 17, 2004, https://www.apple.com/newsroom/2024/10/apple-celebrates-10-years-of-apple-pay/

5. Fraud Management and Account Takeover Prevention

This section outlines the evolving fraud landscape, with a focus on account takeover (ATO) and API-related threats. Readers primarily interested in fraud trends and risk strategies may find the use cases and best practices especially relevant.

As fraudsters become increasingly sophisticated, identifying account takeover (ATO) events has become more challenging. However, the convergence of secure technology tools and enhanced customer experiences is evolving, leading to innovative methods for distinguishing authorized payments from unauthorized ones. Device-present transactions that use tokenization and biometrics have resulted in reduced fraud and improved customer experience.

5.1 The Impact of EMV Technology and Biometrics on Fraud Reduction

The introduction of EMV chip technology has been instrumental in significantly reducing counterfeit debit and credit card fraud. When combined with biometric authentication methods, this technology has led to a dramatic decline in counterfeit transactions. Additionally, the use of tokenization in mobile wallets and contactless payment transactions has devalued stolen data, prompting fraudsters to shift their focus towards account takeover (ATO) attacks.

Profiting from stolen account numbers has become significantly harder and less profitable for fraudsters. Consequently, they have invested more time and resources into either tricking individuals into sending money through authorized push payment (APP) fraud or taking over customer accounts, such as those on merchant websites, or financial institution accounts.

When it comes to fraud within the mobile and contactless payment space, ATO is the most prevalent threat. The shift toward mobile and contactless transactions has made ATO a primary focus for fraudsters, necessitating enhanced security measures to protect consumers and businesses alike. Additionally, fraudsters are increasingly targeting APIs that are not configured properly, exploiting these vulnerabilities to gain unauthorized access to sensitive information.

By leveraging advanced technologies and continuously evolving security practices, merchants and issuers can better safeguard against the growing threat of account takeovers.

5.2 Forms of Account Takeover Fraud

ATO fraud manifests in several forms, each exploiting different vulnerabilities. Primary types include mobile wallet provisioning and credential stuffing.

Mobile Wallet Provisioning Fraud

Fraudsters attempt to provision a device (such as a mobile phone, watch, or iPad®/tablet) using stolen PAN data along with other credentials like expiration dates, CVCs, and cardholder names. This stolen data often originates from e-commerce breaches. Typically, fraudsters use social engineering tactics to trick issuer customer service representatives into provisioning a device with stolen information. Once a device is fraudulently provisioned, it can be used for contactless payments and mobile app transactions, making it a versatile tool for fraudulent activities.

Credential Stuffing

Credential stuffing is a type of cyberattack where attackers use stolen usernames and passwords from one site to gain access to accounts on other sites. This method is effective because many people reuse the same login credentials across multiple platforms. A recent study revealed that 70% of adults still use the same password for multiple accounts. Attackers employ automated tools to test these credentials on various websites, seeking matches to gain unauthorized access. Once they succeed, they can exploit the compromised accounts for illegal financial gain, whether by accessing merchant or financial accounts.

By understanding these forms of ATO fraud, merchants and issuers can better prepare and implement robust security measures to protect their customers and their own operations.

5.3 Understanding the Fraudster's Mindset in Account Takeovers

Why Take Over a Person's Merchant Account?

With merchants increasingly tokenizing card-on-file data, fraudsters find it challenging to use the stolen card information elsewhere. However, they can still exploit a person's merchant account in several ways. Table 1 illustrates the different fraud activities and their impact on merchants and customers.

Fraud Activity		How It Works	Merchant and Customer Impact
Ordering Merchandise	📦	Fraudsters use stolen accounts to order valuable items for in-store pickup or delivery to another address.	Loss of inventory, increased fraud-related costs, and potential reputational damage for merchants
Address Manipulation	🏠	Fraudsters temporarily change the account's saved address to a drop location to receive stolen goods.	Chargebacks, shipping costs, and disrupted customer service operations that lead to financial and trust losses
Monetizing Loyalty Awards	🎁	Fraudsters redeem loyalty rewards or points from compromised accounts for financial gain or goods.	Loss of customer trust, increased costs for account recovery, and reduced effectiveness of loyalty programs

Table 1. Fraud Activities from Merchant Account Takeovers

Why Take Over a Person's Financial Institution Account?

ATO fraud targeting financial institutions has been prevalent for a longer time due to the direct access it provides to a person's funds. Table 2 highlights primary motivations for financial account takeover.

Motivation		How It Works	Financial Institution and Customer Impact
Access to Funds	💰	Fraudsters transfer funds directly from the victim's account to their own, often through online banking or wire transfers.	Financial loss for the customer, increased liability and investigation costs for the financial institution.
Address Changes	🏠	Fraudsters update the victim's account address and request a new chip card, which they intercept or redirect to a drop location.	Customer inconvenience, potential unauthorized spending, and reputational damage for the institution.

Table 2. Motivations for Financial Account Takeovers

By understanding these motivations, merchants and financial institutions can better anticipate and mitigate the risks associated with account takeovers.

5.4 Fraud and ATO Detection Technologies

Combating the threat of account takeover requires merchants and issuers to use a balanced mix of modern tools to protect their customers while minimizing friction. This section reviews key technologies used to detect and prevent fraud.

Behavioral Biometrics

Behavioral biometrics analyze how users interact with their devices, such as typing speed, mouse movements, and touch patterns. By establishing a baseline of normal behavior, these systems can detect anomalies that may indicate an account takeover attempt. For example, if a user typically types at a certain speed and suddenly types much faster or slower, the system can flag this as suspicious.

Anomaly Detection

Anomaly detection platforms use machine learning to identify unusual patterns in user behavior and transaction activities. These systems provide real-time alerts and automated responses to potential threats. For example, if a user who usually makes small purchases suddenly makes a large transaction from a new device, the system can trigger an alert and require additional verification.

Predictive Modeling

Predictive modeling involves using AI to create models that can anticipate and prevent ATO attempts by identifying patterns that precede such attacks. These models analyze vast amounts of data to predict which accounts are at risk and take preemptive actions to secure them. For example, if the model detects a pattern of login attempts from multiple locations within a short period, it can flag the account for further review.

Additional Technologies

- **Multifactor authentication**: Requiring multiple forms of verification (e.g., password and fingerprint) adds an extra layer of security.
- **Bot management solutions**: These solutions use AI to differentiate between legitimate users and malicious bots, blocking automated attacks like credential stuffing.

- **Continuous monitoring and alerts**: AI systems continuously monitor accounts for signs of takeover attempts and send alerts to both the merchant and the customer if suspicious activity is detected.

By integrating these advanced technologies, merchants can significantly enhance their security posture and protect their customers from the growing threat of account takeovers. The combination of behavioral biometrics, anomaly detection, predictive modeling, and other security measures helps create a robust defense against sophisticated fraud tactics.

5.5 Leading Practices for Merchants, Issuers, and Consumers

This section outlines a variety (not an exhaustive list) of important considerations for merchants, issuers, and consumers seeking to combat fraud.

First, both merchants and issuers must adopt solutions that protect customers and payments, regardless of where fraud liability lies. To grow business and safeguard customers and revenue, it is crucial to determine whether to build solutions in-house, use vendor solutions, or implement a combination of both. No one-size-fits-all solution exists, but many companies are increasingly relying on vendors to address specific or combined ATO threats. Notably, API attacks have surged, with incidents more than doubling in the past year[12], highlighting the critical need for robust API security measures.

Merchant and Issuer Security

The following is a non-exhaustive list of practices that merchants and/or issuers can generally employ to help strengthen their payment security posture and protect consumers and payments:

- **Develop a comprehensive fraud risk strategy**: Regularly update your strategy, whether you build, buy, or use a combination of both.
- **Use enhanced monitoring**: Increase monitoring efforts during peak times such as holidays, Prime Day, Singles' Day, and major world events like the Olympics or World Cup.
- **Enforce strong password policies**: Implement and enforce policies for strong passwords.
- **Implement MFA**: Ensure MFA is in place to add an extra layer of security.
- **Monitor accounts**: Track accounts for unknown devices, IP addresses, or any changes.
- **Monitor failed login limits**: Set velocity limits for failed login attempts to prevent brute force attacks.
- **Use passkeys**: Consider using passkeys as a secure alternative to passwords.
- **Stay informed**: Engage with industry risk forums to stay updated on the latest trends and solutions, as fraud prevention is a collaborative effort.
- **Use unique and strong passwords**: Never reuse passwords or use similar ones across different online accounts. Use passwords with more than 11 characters, including a mix of uppercase, lowercase, numbers, and symbols.
- **Implement secure API practices**: Implement strong authentication and authorization mechanisms, encrypt data in transit, and regularly conduct security audits to prevent unauthorized access and protect sensitive information.

[12] Digital Fortresses Under Siege: Threats to Modern Application Architectures, Akakai, July, 2024

- **Issuers only – implement secure wallet provisioning**: To ensure secure provisioning of digital wallets like Apple Pay, Google Pay, and Samsung Pay, issuers should implement robust authentication measures. This includes multifactor authentication, device fingerprinting, and behavioral analytics to verify the genuine cardholder. Monitoring for unusual activity, such as multiple provisioning attempts from different devices or locations, and requiring additional verification for suspicious transactions can further mitigate fraud risks.

Consumer Practices

Consumers can help to improve the security of their own payments and payment accounts in a variety of ways, including (but not limited to) the following:

- **Use unique and strong passwords**: Never reuse passwords or use similar ones across different online accounts. Use passwords with more than 11 characters, including a mix of uppercase, lowercase, numbers, and symbols.
- **Consider using passkeys**: If available, set up passkeys, which are more secure than passwords and harder for fraudsters to obtain.
- **Enable MFA**: Activate MFA on all accounts where it is available.
- **Monitor accounts**: Set up alerts to advise of any changes to accounts (e.g., password reset, address, phone). Regularly check for unauthorized purchases and report any suspicious activity to the bank immediately.
- **Protect one-time passwords**: Do not share OTPs with anyone who contacts you.
- **Be aware of who is calling**. Be on the lookout for people calling with a sense of urgency; always call the institution directly if in doubt

In conclusion, the evolving landscape of digital payments necessitates a proactive approach to security for merchants, issuers, and consumers alike. The rise in sophisticated attacks, particularly on APIs, underscores the importance of robust security measures. By investing in comprehensive customer protection solutions, whether developed in-house, through vendors, or with a combination of both, businesses can help to safeguard their revenue and customer trust.

For merchants and issuers, developing a comprehensive fraud risk strategy, enhancing monitoring during peak times, enforcing strong password policies, implementing multifactor authentication, and staying informed through industry forums are critical. Additionally, adopting secure technologies like passkeys and maintaining vigilance over account activities can significantly reduce the risk of fraud.

Consumers also play a vital role in this ecosystem. By using unique and strong passwords, enabling multifactor authentication, and monitoring accounts for unauthorized activities, consumers can protect themselves from account takeover threats.

The use of secure mobile and contactless payment technologies not only enhances security but also improves the customer experience. However, achieving frictionless yet secure transactions requires the implementation of proper risk controls. By balancing security with user convenience, stakeholders can help to create a safer and more efficient payment environment for everyone.

6. Consumer Education

Knowledge is power for consumers in mobile payments, particularly regarding the security features inherent in payment tools. As more people turn to mobile payment solutions for convenience, understanding the security measures in place becomes essential for protecting personal and financial information. When consumers feel confident in the security of their mobile payment tools, they are more likely to adopt and use them, fostering a greater acceptance of these transactions.

To empower consumers, providers can focus on several key educational topics.

- Knowing how to securely set up and use digital wallets is critical. This includes providing guidance on creating strong passwords, enabling biometric authentication, and regularly updating software.
- Understanding how tokenization protects accounts can demystify the technology behind mobile payments, illustrating how sensitive information is safeguarded during transactions and inspiring confidence in the security of these transactions.
- Recognizing phishing scams is critically important; educating consumers on how to identify suspicious emails and messages can help them to avoid falling victim to fraud.
- The advantages and potential pitfalls of virtual cards should also be discussed. While virtual cards offer enhanced security by providing a temporary card number for online transactions, users should also be aware of issues like expiration dates and limitations on usage.
- Peer-to-peer (P2P) payments are another crucial area for education. For example, consumers should be informed about the importance of sending small test payments to verify the intended recipient before making larger transactions, as well as maintaining vigilance against fraudulent QR codes that could lead to malicious destinations.

To effectively engage consumers on this educational journey, financial institutions and other industry stakeholders can use various strategies. Offering interactive tutorials can create an engaging learning experience to guide users on securely setting up their payment tools. Regularly sending security tips through e-mail and mobile apps helps to ensure that consumers can remain informed and alert to known and emerging threats. Additionally, producing and disseminating informative videos that cover these topics in an easily digestible format can enhance understanding and retention of information.

With this knowledge, consumers are empowered to navigate the mobile payment landscape confidently and securely, ultimately fostering a more secure digital economy where consumers can make informed decisions about their financial transactions.

7. Conclusion

As the digital payments landscape continues to evolve, the strategies for securing these transactions must also advance. This white paper has outlined practices that we believe stakeholders across the payment ecosystem should consider to enhance security. The integration of technologies such as tokenization and biometrics has been shown to significantly reduce the risk of fraud, while consumer education plays a critical role in mitigating the impact of potential security breaches.

Throughout this paper, we have aimed to provide both high-level guidance and detailed technical considerations to support a range of readers across the payments ecosystem. Framing language has been included to help readers navigate the content based on their needs—whether seeking strategic insights, implementation guidance, or practical fraud mitigation tactics.

Looking forward, it is imperative for all parties involved—payment networks, financial institutions, merchants, and technology providers—to continue their collaboration in developing and implementing advanced security measures. Stakeholders must remain vigilant, adaptable, and proactive in their approach to security, anticipating new threats and responding with innovative solutions. Through collaboration, vigilance, and implementation of evolving security practices and strategies, the payments industry can help to ensure that it remains resilient against attacks and continues to offer safe, efficient, and user-friendly payment options to consumers worldwide.

8. Appendix: Glossary of Terms

Account takeover (ATO). A form of identity theft in which a criminal gains unauthorized access to a registered customer's account.

Application programming interface (API). A set of rules and tools for building software applications, specifying how software components should interact.

Biometrics. The measurement and statistical analysis of people's unique physical and behavioral characteristics, used for identification and access control.

Consumer Device Cardholder Verification Method (CDCVM). Technology that allows consumers to use a device-centric verification method for a transaction with a mobile contactless device.

EMV. Specifications developed by Europay, MasterCard, and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

Fraud management. The process of detecting, analyzing, and seeking to prevent fraudulent actions or transactions.

Near Field Communication (NFC). A set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 2-4 cm of each other.

Phishing. The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Secure element (SE). A microprocessor chip that can store sensitive data and run secure apps such as payment and personal data services.

Tokenization. The process of substituting sensitive data elements with non-sensitive equivalents, known as tokens, which have no exploitable value.

9. References and Further Reading

“Card-on-File Tokenization Considerations, Including Debit Routing,” U.S. Payments Forum, https://www.uspaymentsforum.org/card-on-file-tokenization-considerations-including-debit-routing/

“EMV Payment Tokenization Primer and Lessons Learned,” U.S. Payments Forum, https://www.uspaymentsforum.org/emv-payment-tokenization-primer-and-lessons-learned/

“Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions,” U.S. Payments Forum, https://www.uspaymentsforum.org/mobile-and-digital-wallets-u-s-landscape-and-strategic-considerations-for-merchants-and-financial-institutions/

“Payments Resource Brief – Account Takeover,” U.S. Payments Forum, https://www.uspaymentsforum.org/payments-resource-brief-account-takeover/

“Strengthening the Security of Consumer Authentication through Phishing-Resistant Multi-Factor Authentication,” U.S. Payments Forum, https://www.uspaymentsforum.org/phishing-resistant-multi-factor-authentication/

10. Legal Notice

This document is provided solely as a convenience to its readers, as a high-level overview of various strategies, technologies and related considerations that we believe are germane to the question of how to improve the security of mobile and contactless payments. However, the particular strategies, technologies and related considerations identified in this paper do not represent an exhaustive list, and an organization's security practices and strategies must be tailored to its specific needs, risk profile, and other factors. Accordingly, considerations, approaches and technologies not addressed in this paper may be as or more important to a given organization. While great effort has been made to ensure that the information provided in this document is accurate and current, this document is informational only, is not legally binding, does not constitute legal or technical advice, and should not be relied upon for any legal, technical, or other purpose. Importantly, readers should understand that following the practices described in this paper do not in any way guarantee security, compliance, or immunity from breach. Accordingly, all warranties of any kind, whether express or implied, relating to this document, the information herein, or the use thereof are expressly disclaimed, including but not limited to warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. Any person that uses or otherwise relies on the information in this white paper does so at his or her sole risk. Without limiting the foregoing, it is important to note that this document provides only a high-level description of the subject matter; and the concepts described in this paper should not be considered standards, requirements, recommendations or guidelines. Readers interested in securing mobile and contactless payments should therefore consult with their respective security providers, subject matter experts and professional and legal advisors, as well as relevant payments industry stakeholders, such as payment networks, issuers, acquirers, and others, prior to any implementation decisions.