Tokenization and 3-D Secure: Complementary Components of Modern Risk Management

GLENBROOK

Introduction

A growing narrative in the payments industry suggests that network tokenization (also known as EMVCo tokenization) could one day eliminate the need for 3-D Secure (3DS). The reasoning may seem sound: if the payment credential is cryptographically protected and no longer exposed, why continue to invest in authentication?

That premise is fundamentally flawed.

Network tokenization and 3DS address different layers of the risk equation. Tokenization protects the credential by replacing the Primary Account Number (PAN) with a secure, domain-restricted token. 3DS authenticates the payer and provides the issuer with structured, standardized data needed to evaluate risk in real time. One safeguards what is being used; the other verifies who is using it in real-time on an ongoing basis.

Even in a world where every digital transaction is tokenized, the ecosystem still needs reliable authentication signals. Issuers require them to make informed authorization decisions to manage risk. Merchants rely on them to authenticate cardholders, shift liability, and comply with regulatory requirements. Networks depend on them to maintain a consistent, interoperable flow of data across participants. Tokenization strengthens the infrastructure, but it does not remove the need to validate the customer.

In practice, tokenization does not replace 3DS but rather complements it. It increases the importance of 3DS by elevating the relative value of strong, verifiable authentication signals in a token-dense environment.

Layered Controls Matter as Fraud Pressure Mounts

E-commerce fraud continues to escalate, driven less by simple card-number theft and more by sophisticated tactics like account takeover, credential stuffing, issuing tokens into attacker wallets and synthetic identities, an attack vector particularly pronounced in EMEA. These attacks create losses for both merchants and issuers, and the downstream impact is predictable: higher operating costs, more conservative authorization strategies, and declining consumer confidence in digital commerce.

In this environment, no single control mechanism can fully prevent fraud. Instead, fraud mitigation today requires multiple, complementary layers. Network tokenization strengthens the credential by reducing the usefulness of a stolen PAN, but it does not address the underlying shift in attacker behavior. As fraudsters move toward identity- and behavior-based schemes, effective mitigation depends on richer, more dynamic signals including device telemetry, behavioral analytics, historical transaction patterns, and explicit customer authentication. This is particularly important because attackers may attempt to have a token

provisioned to their wallet, sometimes even allowing the card to be updated in the fraudster's wallet when the card is replaced.

This is where 3DS plays a critical role. 3DS supplies the issuer with verified authentication outcomes and contextual data that are otherwise unavailable in a pure tokenized flow. It also enables decision-making during the authentication phase, enabling in-depth risk analysis. These signals improve real-time risk scoring and enable more accurate authorization decisions. When 3DS is absent or inconsistently applied, issuers operate with limited visibility into cardholder authentication signals, reducing authorization accuracy and creating opportunities for attackers to exploit gaps in the authentication layer.

Layered defenses are not optional. Tokenization protects the credential; 3DS helps validate the customer. Both are required to maintain trust and keep fraud pressure from overwhelming the system.

What Tokenization Does Well… and What It Doesn't

Network tokenization is one of the most important innovations in modern card-not-present commerce. By replacing the PAN with a token that is bound to a merchant, device, or identity (as in the newest Apple Pay MPAN implementations), tokenization dramatically reduces the value of compromised credentials. It lowers PCI exposure for merchants and PSPs, improves the resilience of stored credentials, and provides automatic lifecycle management when cards are reissued or updated. These attributes have made tokenization the preferred credential format for many merchants across browser, in-app, and wallet-initiated transactions.

Tokenization adoption continues to accelerate at scale. Visa reports issuing more than one billion new tokens every quarter and notes that approximately half of all transactions on its network are now tokenized.[1] Mastercard shows a similar trajectory, with more than 35 percent of its global transactions already flowing through network tokens.[2]

But while a token replaces the payment credential, it does not validate who is transacting or why. On its own, tokenization does not:

- Authenticate the payer
- Establish intent or confirm legitimate customer behavior.
- Provide device or contextual telemetry
- Guarantee liability protection across all transaction types
- Meet regulatory requirements for strong customer authentication

Tokenization makes the ecosystem safer by improving credential security, but it does not make it inherently more intelligent. For network tokens to fully deliver on their promise of reduced fraud and higher approval rates, they must be paired with strong authentication mechanisms. This is true not only for merchant card-on-file use cases but also for wallet-based transactions

such as Apple Pay and Google Pay, where device-level assurances supplement—but do not replace—the need for robust authentication signals.

Does the Token Belong to the Real Accountholder? Not All Tokens Are Created Equal

A common misconception is that all network tokens carry the same level of trust. In reality, a token's risk posture depends heavily on how it was provisioned and whether the cardholder was authenticated when the token was created. At a high level, network tokens fall into two broad categories: authenticated tokens and non-authenticated tokens.

Authenticated tokens are issued only after the cardholder has successfully completed a strong verification process with their issuing bank. This often includes strong customer authentication (SCA) methods such as biometrics or passcode-based approval inside a mobile wallet. In these flows, the issuer has high confidence in the identity of the individual requesting the token, and the resulting token is tightly bound to a verified customer and device. Data from Mastercard indicates that an authenticated token has a 3.0x impact on fraud reduction, compared to a 1.8x impact from tokenization alone.[3] Accordingly, authenticated tokens carry the strongest assurance at the point of provisioning. However, it is important to recognize that this strong authentication is typically performed only once, when the token is created, and does not provide ongoing validation of the cardholder for subsequent transactions.

However, authenticated tokens represent only a small portion of the overall token population. A growing share of network tokens are non-authenticated tokens created through merchant or PSP tokenization requests. These tokens offer meaningful operational benefits, including automatic lifecycle updates and improved authorization performance, which is why merchants are adopting them rapidly. But unlike authenticated tokens, they do not require the cardholder to authenticate during provisioning. Any merchant that receives a PAN can request a token for it, even if the PAN was obtained fraudulently.

This introduces a critical limitation: a token alone does not prove that the person transacting is the legitimate account holder. If a fraudster presents a compromised card number to a merchant, that PAN can be converted into a valid network token without any additional authentication steps. The credential becomes more secure, but the identity behind the transaction remains unverified.

For this reason, tokenization must be paired with transaction-level authentication to ensure that the consumer using the token is the rightful account owner.

Practical Challenges are Impeding the Path to a Fully Tokenized World

Visa and Mastercard have articulated an ambitious long-term vision: a future in which nearly every payment credential is tokenized, PANs fade into legacy status, manual card entry disappears, and wallets become the dominant interface for digital identity and payments. This token-by-default future is strategically coherent and technologically achievable. But the practical reality is far more complex. The broader payments ecosystem still faces significant operational, technical, and behavioral hurdles that slow the transition to end-to-end tokenization.

One of the most persistent challenges is issuer readiness and the inconsistent use of token metadata in authorization decisioning. Merchants regularly observe wide variation in how issuers treat tokenized transactions. Some large issuers do not support network tokens at all. Others support tokenization, but do not yet consume the complete set of token metadata—such as token assurance levels or domain controls—that are intended to improve issuer confidence and reduce false declines. As a result, issuer performance with tokenized transactions can differ markedly from their treatment of PAN-based transactions.

This inconsistency has produced a practical but problematic set of merchant workarounds. Many merchants that fully support tokenization still retain the PAN for fallback purposes and, in some cases, intentionally send PAN-based authorizations first to specific issuers known to exhibit lower approval rates for tokenized transactions. Others store the PAN solely as a retry credential when a tokenized authorization fails. While rational from a commercial standpoint, these practices undermine the security and lifecycle benefits of a fully tokenized ecosystem.

The implication is clear: merchants must maintain robust routing, risk management, and retry logic across both tokenized and non-tokenized transactions. Until issuer behavior becomes more consistent and token metadata is universally adopted and fully leveraged, merchants will continue to experience uneven authorization performance and will require dual strategies to manage risk, optimize approvals, and deliver a stable consumer experience.

On the issuer side, inconsistent merchant deployment of 3DS limits visibility into transaction context. As a result, issuers are forced to reconcile multiple and often inconsistent representations of e-commerce transactions, weaving together risk management approaches to account for variability in how authentication and transaction data are submitted. From a risk perspective, token assurance levels and 3DS authentication outcomes function as complementary signals across time. Authentication at token provisioning establishes an initial trust baseline for a credential at a specific point in time, while transaction-level evaluation through 3DS provides ongoing, dynamic insight into changing risk conditions as user behavior and transaction contexts evolve.

How Tokenized Transactions Work with 3DS

A tokenized transaction that runs through 3DS looks almost identical to a 3DS transaction that uses a PAN. The token replaces the PAN, and the same data elements flow through the protocol.

Tokens enhance the risk picture but don't replace critical risk signals that issuers often evaluate as part of their 3DS authentication assessment. Those signals include:

- Device information
- Merchant risk scoring
- Consumer behavioral patterns
- Exemption indicators
- Previous transaction history
- Step-up authentication results

Visa data show that "when priority data elements are included in the Merchant's authentication request, Issuers can see up to a 65% fraud detection rate lift than when the data elements are missing."[4] As noted earlier, this level of transaction scrutiny is critical, especially when a non-authenticated token is used. However, the scale and sophistication of modern synthetic identity fraud also dictate that the same level of scrutiny be applied to authenticated transactions, as this allows issuers to identify potential risk indicators that were not flagged during initial token provisioning.

Together, tokenization and 3DS give issuers a fuller picture of the transaction, often leading to higher approval rates and fewer false declines.

What Happens When 3DS Usage Declines in a Highly Tokenized Environment?

When tokenization becomes widespread, but 3DS usage falls, the ecosystem enters a paradoxical state in which the underlying credential becomes safer, yet each individual transaction becomes harder for issuers to evaluate. This imbalance produces a distinct set of risks for issuers, merchants, and consumers:

- Issuers lose critical transaction context: Receipt of fewer authenticated data fields leads to far less certainty about who is actually transacting
- Authorization models become less accurate: Models revert to broader heuristics, and risk scoring confidence drops
- Declines increase as a compensating control: Facing reduced visibility, issuers tighten their authorization thresholds to avoid increased fraud losses

- Greater fraud liability shifts to merchants: Without 3DS, merchants cannot shift liability under network rules
- Regulatory concerns arise over authentication gaps: In markets with SCA requirements (EU, UK, India, parts of APAC), regulators expect strong customer authentication on CNP transactions.
- Consumer experience becomes inconsistent: Users may experience unexplained declines, additional issuer challenges, or repeat verification requests.

In a highly tokenized ecosystem, removing or reducing 3DS does not make checkout smoother. Instead, it can introduce more friction because issuers must compensate for missing authentication data. When the balance tips too far toward tokenization without adequate authentication, issuer uncertainty increases, and the entire ecosystem absorbs the consequences.

Different Markets, Different Pressures

Regulated Markets

In regions where SCA requirements are mandated, such as under PSD2 today and the forthcoming PSD3 and PSR frameworks in Europe, tokenization cannot satisfy regulatory obligations on its own. Tokens improve credential security, but they do not verify the consumer or generate the multi-factor signals required under law. In these jurisdictions, 3DS remains the primary mechanism for delivering compliant authentication or qualifying for permitted exemptions. Even as tokenization enhances issuer confidence and lowers credential-level fraud, the regulatory mandate ensures that 3DS (or an equivalent SCA protocol) continues to serve as the backbone of authentication for most e-commerce traffic. As regulators tighten enforcement and refine exemption policies, the dependency on robust, standardized authentication only increases.

Non-Regulated Markets

In markets without statutory authentication requirements, such as the United States, merchant adoption of 3DS is driven primarily by risk, liability, and business incentives rather than regulation. Merchants often deploy 3DS selectively, using it for higher-risk segments, suspicious activity, or specific verticals.

This selective use introduces signaling asymmetry. From the issuer's perspective, 3DS appears disproportionately on riskier transactions, conditioning authorization models to treat its presence as a risk flag rather than a reassurance. A widely discussed Stripe report indicated that this is particularly true in the United States, where businesses adding 3DS saw their authorization rates remaining at a stubborn 87% when invoking the friction flow and actually decreasing to 84% on frictionless transactions.[5] As a result, these markets often struggle to achieve the performance benefits that 3DS provides in regulated environments where its usage is more uniform. Lessons from these markets demonstrate that broader and more consistent

use of 3DS across transactions strengthens issuer models over time, improving approval rates while reducing false positives.

Tokenization does not alter this dynamic and may unintentionally amplify it if merchants attempt to rely on tokens as a substitute for authentication. A token can strengthen the credential, but without the corresponding authentication signal, issuers still lack the information needed to distinguish legitimate activity from identity-based fraud. In non-regulated markets, this makes the case even stronger for thoughtful, risk-aligned use of 3DS alongside tokenization.

What Each Stakeholder Should Consider

Merchants and PSPs

For merchants and payment service providers, tokenization and 3DS function best as complementary controls. Tokenization strengthens stored credentials, reduces exposure when a PAN is compromised, and improves lifecycle management for recurring or card-on-file transactions. 3DS provides rich contextual data, authentication and liability protection that the upstream card issuers rely on to make confident authorization decisions. Merchants should not treat tokens as a standalone fraud strategy. Just as 3DS is one element within a broader layered defense, tokenization must be paired with strong transaction authentication to ensure high approval rates, minimized fraud, and a consistent customer experience.

Issuers

Issuers gain significant value from tokenization: reduced counterfeit risk, improved credential stability, and higher trust in stored credentials. However, tokens are not a proxy for cardholder identity. Issuers must continue to apply strong authentication and advanced risk models even when a token is present. Token metadata can enhance decisioning, but it does not replace behavioral, device, or contextual indicators. Treating a tokenized transaction as inherently low-risk would overlook the increasing prevalence of identity-driven fraud and account takeover schemes.

Networks

For card networks, the challenge is maintaining—and ideally strengthening—the role of 3DS in a token-centric ecosystem. As more transactions originate from wallets, apps, and browser-based token flows, robust authentication and data exchange frameworks remain essential. Networks should continue to evolve rules, enhance the protocol, and educate the ecosystem to ensure that participants understand the distinct roles of credential security and consumer authentication. Sustaining clear, high-quality data pathways between merchants, acquirers, issuers, and wallets will be critical for long-term ecosystem trust and performance.

Consumer Experience: Where 3DS and Tokenization Work Together

Consumers see the greatest benefit when tokenization and 3DS operate as complementary layers. Tokenization protects the payment credential itself, reducing the likelihood that stolen or exposed card data can be reused elsewhere. 3DS protects the consumer by confirming that the person transacting is the legitimate account holder. When these two controls work in tandem, consumers enjoy a smoother and more predictable checkout experience.

From the consumer's perspective, the payoff is twofold. First, legitimate transactions are more likely to be approved. Issuers receive both a secure credential and strong authentication signals, which helps them distinguish genuine activity from fraud attempts. This reduces false declines, the single most frustrating friction consumers encounter in online commerce. Second, the fallout from compromised cards is significantly reduced. Tokens are automatically refreshed during card reissuance and update flows, meaning consumers experience fewer service interruptions, card-on-file failures, and the need to update stored payment methods across merchants. These dynamics become even more important as agentic commerce gains traction, with software agents increasingly initiating transactions on a consumer's behalf and issuers relying more heavily on secure credentials and continuous authentication signals to distinguish authorized activity from abuse.

In contrast, a tokenized environment without strong authentication can create inconsistent user experiences. At worst, such an environment will allow tokens to be issued into illegitimate wallets, automatically refreshing as new cards are issued. Consumers may encounter unexplained declines, additional issuer challenges, or repeat verification requests because issuers lack the confidence signals needed to make accurate decisions. Tokenization alone secures the card, but it does not communicate intent or identity. Without those signals, issuer risk models become more conservative, and friction inevitably increases.

A dual-layer ecosystem—secure credentials through tokenization combined with verified identity through 3DS—gives consumers what they value most: a secure, low-friction, reliably approved checkout experience. It is this combination that aligns security, trust, and convenience in a way that neither technology can achieve on its own.

Conclusion

Tokenization is reshaping digital commerce in meaningful ways. Its rapid adoption strengthens credential security, stabilizes card-on-file experiences, and improves authorization performance. Merchants, issuers, networks, and consumers all benefit from a world where exposed PANs are no longer the default.

But tokenization does not eliminate the need for authentication. If anything, it heightens it. As credentials become more secure, attackers shift toward identity-based fraud and account takeover—threats that tokenization alone cannot address. This is where 3DS remains indispensable: it provides the structured, interoperable mechanism for validating the payer and transmitting the contextual data issuers need to make accurate decisions, removing friction from good transactions and properly securing suspicious transactions.

A resilient payments ecosystem requires both technologies working in concert, supported by clear data standards and cooperation across issuers, acquirers, networks, and merchants. The long-term growth of digital commerce depends on maintaining this balance—strengthening security without adding unnecessary friction and enabling trust without compromising the consumer experience.

References

[1] The Future Is Here: Shaping What's Next in Payments (Visa)

[2] Mastercard Incorporated (MA) Q1 2025 Earnings Call Transcript (Seeking Alpha)

[3] Mastercard Digital Payment Security Standard (Mastercard)

[4] Consistently Providing High Quality Data Helps Enhance Business Outcomes Across the Entire EMV 3DS Ecosystem (Visa)

[5] Surprising findings from our analysis of 3DS transactions in the US (Stripe)