



The Authentication Gap in Commercial Virtual Cards

How network-level authentication orchestration can help unlock broader adoption of commercial virtual cards.



Executive Summary

Commercial virtual cards are reshaping how businesses pay — but a structural friction point can limit their full potential.

As purchasing mechanisms evolve authentication can evolve from a bilateral, point-to-point challenge into a scalable, network-coordinated capability. Visa Commercial Virtual Authentication is designed to help issuers do exactly that: bring consistent, issuer-controlled authentication to distributed commercial virtual card environments, without having to build custom integrations for every single platform, partner, and use case. The result can be a simpler path to trusted commercial payment experiences that scale with the business.

The Opportunity

Commercial payments are at an inflection point. Businesses have embraced virtual cards for the control, visibility, and automation they provide, yet a quiet friction point can limit scalability: authentication. In a world where purchasing often happens inside third-party platforms, travel tools, and procurement systems, the traditional issuer-to-cardholder authentication model may not keep up.

Commercial payments are moving into the platforms where businesses already work — from travel and procurement tools to expense management, accounts payable, and fintech applications. Virtual cards are central to this shift because they can give businesses greater control, richer data, and fast ways to pay.

But as commercial virtual cards become more prevalent and distributed, authentication can become harder to execute consistently. The issuer may own the account relationship, while the purchasing experience may happen inside a third-party platform or merchant checkout. That can create a practical challenge: how can issuers support strong, consistent authentication without building bespoke connections for every platform, partner, and use case?

Visa Commercial Virtual Authentication is designed to tackle that orchestration challenge. It provides a network-based way to coordinate authentication execution across a distributed ecosystem, helping issuers bring greater consistency and scalability to commercial virtual card transactions, while preserving issuer control and accountability.



Commercial Payments Are Becoming More Integrated

Business teams increasingly want payments to happen in the flow of work. Instead of moving between disconnected systems, employees, buyers, travel managers, and finance teams often want payment credentials available directly inside the platforms they already use.

Virtual cards are well suited to this environment. They can be issued quickly, configured for specific spend needs, and integrated into enterprise workflows. Visa's commercial payments strategy is built around this same principle: helping connect banks, commercial clients, and platforms through a trusted network infrastructure that supports scale, visibility, and efficiency.

Authentication Was Built for a Different Era

Traditional authentication models were frequently designed around a clear cardholder relationship and a direct issuer-to-cardholder interaction. Commercial virtual card programs can be more complex. A single account may support multiple authorized users, different purchasing roles, dynamic spend controls, and transactions that occur across many third-party environments.

In practice, the issuer may need to authenticate a transaction even when the end-user experience is taking place somewhere else — such as a travel booking tool, procurement platform, or merchant checkout. Without a scalable coordination layer, issuers and platforms often rely on fragmented, one-off integrations that can slow adoption and create inconsistent experiences.

This is where orchestration matters. By standardizing how authentication context is resolved and routed, orchestration can reduce complexity while supporting the issuer's ability to apply its own policies and make its own authorization decisions.

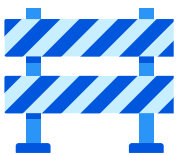


Without a scalable coordination layer, issuers and platforms often rely on fragmented, one-off integrations that can slow adoption and create inconsistent experiences.

Inconsistency Can Have a Cost — in Fraud, Friction, and Adoption

Strong authentication is most valuable when it can be applied consistently, with the right context, across the right transactions. Research has found that regulated markets with broader adoption of 3-D Secure generally experience stronger fraud prevention outcomes and lower card-not-present fraud losses than markets where adoption remains limited.¹ These findings highlight an important reality: when authentication cannot reliably reach the transactions that require it, vulnerabilities can emerge. Authentication gaps can be fraud gaps.

For commercial virtual cards, the stakes can go beyond fraud. Inconsistency can also be an adoption barrier. Issuers seek confidence that authentication can be executed in a repeatable way. Platforms seek clean integration patterns. Commercial clients seek payment experiences that feel secure without adding operational burden.



The cost of the status quo compounds over time. Each new platform integration without a standardized approach can mean additional custom builds, higher support costs, and wider gaps in authentication coverage.

As virtual card programs scale into new channels and geographies, fragmented execution can become increasingly untenable. A network-based orchestration capability brings these needs together — helping provide a more standardized, scalable way to coordinate authentication across issuers, platforms, service providers, and merchants.

1. Outseer. (n.d.). CNP Fraud and the Role of 3-D Secure (Datos Insights/Outseer report – key findings). <https://www.outseer.com/reports/datos-cnp-fraud>

Orchestration Means Issuers Can Stay in Control — at Scale

Visa Commercial Virtual Authentication is positioned as an orchestration layer — not a replacement for issuer control. It helps coordinate authentication execution and information exchange across the ecosystem, while issuers continue to define policy, apply applicable exemptions, and make final authorization decisions.

That distinction is important. The goal is not to transfer responsibility away from issuers. The goal is to make issuer-directed authentication executable at scale across modern commercial payment environments.

This approach reflects the practical reality of today's ecosystem: authentication execution may involve multiple participants, but issuer accountability and decisioning remain central. Visa's role is to make that decisioning possible at scale — not to supplant it.



How Visa Commercial Virtual Authentication Works

Commercial virtual card ecosystems can quickly become a many-to-many integration challenge: many issuers, many platforms, many spend use cases, and many merchant environments. Visa Commercial Virtual Authentication simplifies that challenge by providing a common orchestration approach across the Visa network. The capability is designed to:



For issuers and partners, this can mean fewer bespoke builds, clearer ecosystem coordination, and a more scalable path to trusted commercial virtual card experiences.

The experience, simply put: a commercial virtual card is used in a digital transaction; Visa coordinates authentication routing and execution where applicable; the issuer receives the relevant outcome; and the issuer uses that outcome as part of its authorization decisioning. The complexity sits behind the scenes and can create a more repeatable, friction-reduced experience for everyone in the chain.

What This Can Mean for Issuers, Platforms, and Commercial Clients



For issuers

Visa Commercial Virtual Authentication can reduce the need for platform-by-platform authentication builds and support more consistent execution of issuer-defined policies across commercial virtual card programs. Issuers can scale their programs into new channels without scaling their integration overhead.



For platforms and service providers

Orchestration can create a cleaner integration pattern for supporting issuer-directed authentication — without requiring platforms to manage bilateral relationships with each issuer they serve.



For commercial clients

The value is a smoother payment experience that supports security, control, and scalability as virtual card usage expands across travel, procurement, supplier payments, and employee spend. Security can become an invisible infrastructure, not operational overhead.

Key Benefits



Scale

As virtual card usage expands to new platforms and markets, network-based orchestration means issuers don't need to rebuild authentication for each new integration — the infrastructure scales with them.



Consistency

Issuer policies can be applied more reliably across distributed commercial virtual card environments, regardless of where the transaction originates or which platform hosts the payment experience.



Control

Policy ownership, exemption strategy, and authorization decisioning remain with the issuer. Orchestration can enable scale without transferring accountability.



Trust

More consistent authentication execution supports more secure integrated payment experiences — keeping friction behind the scenes where possible and surfacing it only where necessary.



Readiness

As business payments continue moving into third-party platforms and digital workflows, commercial virtual card programs often need infrastructure that grows with them. Visa Commercial Virtual Authentication is designed to support that trajectory.



Looking Ahead: The Infrastructure of Commercial Payments

The growth of commercial payments is structural. As more business spend flows through platforms, software ecosystems, and AI-powered agents, payment infrastructure must deliver speed, security, intelligence, and seamless integration at scale.

The next frontier is agentic commerce—where trusted digital agents can initiate and execute transactions on behalf of businesses within defined controls and policies. In this environment, authentication becomes the foundation of trust, verifying identity, intent, and authorization in near real-time while enabling greater automation.

Organizations that establish scalable authentication today will be best positioned to unlock new commerce experiences, expand into emerging markets, and confidently support autonomous transactions tomorrow.

As we look ahead, Visa can build the network-level infrastructure to help enable this future—equipping issuers with the capabilities to lead not only in digital commerce, but in the emerging era of agentic commerce.

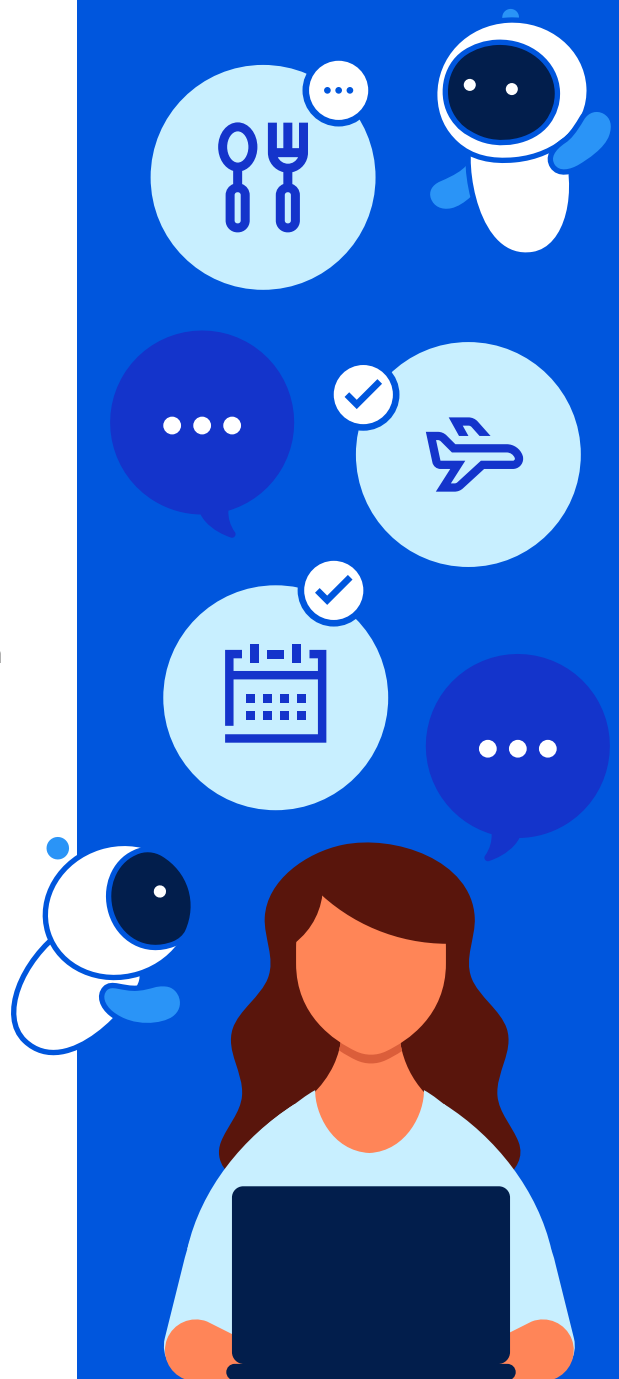
The Bottom Line

Commercial virtual cards are becoming foundational to modern business payments. As commercial virtual cards become more integrated, authentication must evolve — from fragmented, point-to-point execution toward scalable ecosystem coordination.

Visa Commercial Virtual Authentication can help issuers bring trusted authentication into distributed commercial payment experiences, supporting growth, control, and confidence as virtual card programs scale.

Ready to explore how Visa Commercial Virtual Authentication can work within your program? Contact your Visa representative to learn more.

[Learn More](#)



Disclaimers

Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The Information contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

This document is intended for illustrative purposes only. It contains depictions of a product, service or solution (the "Product") currently in the process of development or deployment and should be understood as only a representation of the potential features of a fully deployed Product. Visa is under no obligation to make this Product available, and versions of this Product, if any, may not contain the features described in this document.

These materials and best practice recommendations are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory or other advice. Materials and recommendations should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of the marketing materials, best practice recommendations, or other information, including errors of any kind, contained in this document.

