

Convenience and control:

Why the future of eCommerce is tokenization

By Brian Cole, Sr. VP, Head of Product, North America, Visa, and Ansar Ansari,
Sr. VP, Global Head of Platform Products, Visa



cybersource
A Visa Solution



A message from the Senior Vice President

Payment tokenization is certainly not new. It has occupied an important place in the payment landscape for more than 15 years.

Today, it's a standard piece of nearly every payment security strategy. And most businesses with an online presence depend on tokenization to help protect their customers' sensitive card information during transactions.

But what if this familiar, broadly accepted payment security technology could do more?

What if you could use tokenization to solve new and bigger payment challenges—especially as your payment environment grows more diverse and complex?

To answer these questions, Cybersource is giving you complimentary access to this guide “Why the future of eCommerce is tokenization”. Read on to find out more this essential topic—and learn why all merchants can benefit from digital network tokens.

Best wishes,

Andre Machicao

Senior Vice President, Head of Product, Cybersource, a Visa solution

Guide

Why the future of eCommerce is tokenization



As eCommerce has accelerated, it has highlighted issues that still beset some digital payments. Compared with face-to-face transactions, the rate of declined transactions is higher, as are the fraud-to-sales ratios, while the user experience is not always smooth and can sometimes get in the way of the sale.



Why is the experience of paying online not always as seamless as it should be? The main factors are the risks related to sensitive account data.

We continue to operate in a payments ecosystem that often relies on the use of a few basic account details (the primary account number, or PAN, the expiration date, and the three-digit security code, or CVV2). If these details become compromised, or we cannot be sure that they are being used legitimately, things can go wrong. Hence, the data is under intense scrutiny from fraudsters, who are forever probing for ways to exploit it at an industrial scale. For any transaction that looks even remotely suspect, issuers and merchants alike are continually forced to make the toughest of judgement calls: do they apply the precautionary principle and decline it, or do they apply the benefit of the doubt and wave it through, knowing that the majority of declined authorizations are, in fact, genuine transactions declined as a result of this precautionary principle?

Enter tokenization, a technology that replaces a consumer's sensitive PAN information with a unique identifier (a token) that helps protect transactions when used for in-store mobile payments or online shopping.

The journey to adopting tokens is well underway. The advent of network tokens, also known as digital network tokens, was a prerequisite for the arrival of 'the pays'. For the future, it enables us to envisage a world in which any device with a digital heartbeat could be used to initiate or accept payments across any channel.

Right now, however, the challenge—and the opportunity—is for tokenization to become more deeply and widely embedded in the world of everyday eCommerce. In the wake of the COVID-19 pandemic, the shift to digital payments has unveiled the need for tokenization and the value it can bring.

We have every reason to believe that tokenization is accelerating rapidly toward ubiquity and will become the way eCommerce payments happen. Read on to find out a little more about tokenization—and learn why we believe that the future of eCommerce is tokenization.

A very quick primer— what is tokenization?

With tokenization, something of high value is replaced by something of low value (For instance, in a waterpark, cash is often replaced with a wristband, which has little intrinsic value and can only be used in the waterpark).

In our world, the PAN is replaced with a token, which looks like a PAN and can be processed much like a PAN.

But it is NOT the PAN, nor can it be mathematically reversed to reveal the PAN.

Rules can be applied around where and how each token can be used. It is protected by secure, dynamically generated cryptograms. And it can be remotely refreshed or disabled at any time. So, it's of little use to any fraudster.

What are digital network tokens, and why do they matter?

With digital network tokens, tokenization technology can be taken to a whole new level. It is about much more than just swapping PANs for a substitute number. It's about improving the user experience across the vast majority of eCommerce payments.

Through the payment network, an eCommerce merchant can ask for a unique token to be created for each of its customer credentials.

Cybersource unifies tokens from different networks, issuers, and channels, including alternative payments such as eCheck, ACH, and other debit products into a single unified super token. This helps improve customer experience, keep credentials refreshed, and reduce PCI compliance scope. It also helps resolve the tension between simple payment experiences and complex environments.



Win-win-win

tokenization can benefit all players in the payment ecosystem

With digital network tokens, it becomes possible to bring both improved security and a better user experience to the vast majority of eCommerce transactions.



Good for consumers

It makes for a better payment experience for the most popular type of online transactions, card-on-file payments. Once a token has been created, the consumer can see a visual representation of their card on the merchant's payment pages. They are less likely to experience declined transactions and, when their card expires or needs to be reissued, they don't have to go through that tedious process of updating their details.



Good for merchants

Around 95 percent of North American Visa card payment volume is already enabled to support tokenization, and a large proportion of acquirers and merchant service providers support the service. After tokenization is implemented, merchants can benefit from an increase in authorization rates. And, because they no longer need to store sensitive account data, their security liabilities are reduced.



Good for issuers

With a lower risk of fraud, fewer cards need to be replaced and there are fewer negative experiences for cardholders. Also, when a card is renewed or replaced, there's less danger of losing the coveted top-of-wallet status (because there is no need for cardholders to update their details with a merchant, or to consider reverting to an alternative card). It also minimizes the risk of data breach.

T 5B+

Cybersource tokens issued¹

2.1%

Average improvement in authorization rates²

26%

Average reduction in fraud rates³

Reason #1

Tokenization matters more than ever before

Even before the pandemic, eCommerce payment volumes had been growing fast. And despite a difficult 2020, it is estimated that worldwide retail eCommerce sales grew 27.6% for the year.⁴

While 2021 saw estimated worldwide retail eCommerce growth dip to 16.3%,⁵ the increase in new behaviors that developed out of necessity during the crisis has served as a powerful catalyst for the payments ecosystem.

These shifts have drawn attention to the shortcomings of eCommerce. Despite the advances made in recent years, it has to be acknowledged that, compared with face-to-face, online payments are not always as efficient as we would all like. This is largely because, from the issuer's perspective, eCommerce transactions are riskier, reflected in higher fraud rates, so they are more likely to be declined.

As of mid-2020, for example, the authorization gap between card present and card-not-present stood at more than 400 basis points and the volume of card-not-present fraud was forecast to continue its climb to grow 14 percent by 2023.⁶

And as the world adopted digital conveniences out of necessity in 2020, a percentage of the workforce was forced to be remote, and a 20 percent increase in security breaches was reported.⁷ Fraudsters didn't discriminate between technology giants, hospitality and entertainment chains, or health care companies.

The acceleration of eCommerce growth has amplified these challenges tremendously, but along with them, it has also amplified the value of tokenization. Today, tokens are more important than ever in the eCommerce landscape. They provide enhanced security for the credential itself, greater issuer confidence in the transaction and hence, higher authorization rates, as well as better consumer experiences through capabilities like lifecycle management and device-binding.



Reason #2

Financial institutions have recognized tokens' value in reducing friction

With the growing importance of top-of-wallet status, financial institutions have turned their attention and efforts to achieve and maintain that status. A single poor customer experience can have significant repercussions, such as loss of top-of-wallet or worse, loss of spend overall if the customer stops using the card.

For financial institutions, that seemingly higher-risk world of eCommerce can be costly. Every bit of fraud reduction can translate into tremendous savings, with

fewer card reissuances and lower impact from a negative customer experience.

With tokens, financial institutions can have more confidence in the authenticity of transactions, which leads to higher authorization rates. This is due to number of factors: richer data carried with the token (e.g., device info) enables better decision-making from the bank, and often for card-on-file, they know that a merchant has requested a token for a valued customer, so issuers are more likely to authorize.

Adding lifecycle management means even fewer declines for expired/reissued credentials. There is also the potential of greater effectiveness for loyalty and co-brand programs, for example, by using tokenization to give financial institutions access to data that could enable a 360-degree view of customer purchases.

In fact, more than 95 percent of North American payment volume is enabled by issuers to support digital network tokens. To drive continued digital token momentum, there is a heightened focus on push provisioning, which “pushes” credentials issued as tokens straight into the merchant or wallet environment, helping to preserve top-of-wallet status and of course, emphasis on overall token optimization in the ecosystem.

A large, bold, white percentage '95%' is centered on a bright yellow background. The numbers are thick and rounded, with a clean, modern sans-serif font. The percentage sign is also large and white, matching the numbers.

of North American payment volume is enabled by the issuers to support digital network tokens

Reason #3

Tokens unlock the ultimate success metric for merchants

In the eCommerce community, conversion rates tend to be the ultimate success metric—with online merchants often happy to invest in initiatives that might increase conversions by just a few basis points.

Network tokenization has been shown to increase authorization rates by an average of 2.1 percent⁸ in North America, with some pilot merchants seeing an uplift of tens of millions of dollars.

The exact magnitude of the increase will, of course, depend on many variables. All merchants can benefit from digital network

tokens, especially if they have experienced sub-optimal authorization rates, with a high rate of declines due to expired or invalid account data.

Across the payments industry, the benefits extend well-beyond higher authorization rates. For example, network tokenization has been shown to reduce average fraud rates by around 26 percent.⁹ Replacing PANs with tokens means less risk from a data compromise event—and, even if one happens, the stolen token credentials are virtually worthless for use anywhere else.

Tokens also significantly improve the customer experience, not just from better authorization rates and fewer false declines. Network token lifecycle management can significantly drive down the events of stale credentials, saving consumer frustration at the time of transaction.

And it's easier than ever for merchants to tokenize their transactions. More than 150 payment gateways and merchant service providers utilize network tokens, including many of the larger payment gateways and merchant service providers. Many more are in the process of introducing the capability. This makes it relatively simple for merchants to benefit from tokens.



150

payment gateways
and merchant service
providers utilize
network tokens

Reason #4

Quick and easy online checkouts are a reality with digital network tokens

Speaking of improved customer experience, card-on-file, whereby a cardholder authorizes a merchant to store their account details for future payments, has emerged as a prominent way of paying online. It is far quicker and easier than entering our card details afresh each time, and we can all think of examples of how it makes life quicker

and easier: when you pay for your ride by stepping out of the car, for example, or pay and tip the pizza delivery person in a mobile app before they even arrive, or your monthly subscription for the streaming TV or music service is automatically debited.

It is perhaps no surprise, therefore, that more than half of all North American eCommerce transactions are now card-on-file or recurring billers versus manual key entry.¹⁰

However, card-on-file payments do present their own particular challenges, especially when a card expires or needs to be reissued. For example, some 35 percent of survey respondents say they have forgotten to update their card information with at least one merchant¹¹ and, on average, a merchant will reach out to a customer two to three times to ask them to update their card details before cancelling services,¹² which, in addition to being irritating to consumers, adds a considerable layer of operating costs for merchants.

Meanwhile, storing sensitive data places a heavy security burden on merchants. They are required to meet stringent standards and, if they do suffer a data compromise, the average costs for 2020 have been calculated at \$3.68 million.¹³



35%

have forgotten to update their card information with at least one merchant¹¹



Tokens create the potential to truly make payments both secure and invisible

Digital network tokens remove some of these traditional card-on-file barriers.

Once a customer's credentials are authenticated via a verification process, a token can be generated on their behalf. This is then stored, in place of the PAN, and processed just like a conventional transaction, across the entire industry infrastructure—except that, unlike the card details, the token does not go stale.

Token capabilities like device-binding and lifecycle management provide a foundation for enabling truly seamless and frictionless transactions for the customer. With the ability to recognize a user more confidently through rich known-device information, or stale credentials being a thing of the past, the potential is created to truly make payments both secure and invisible, the ultimate North Star of payments' consumer experience.

Reason #5

Tokenization momentum is industry-wide, growing and global with more than 5 billion Cybersource tokens issued so far

Tokenization is nothing new. It was a prerequisite for the introduction of 'the pays'. And the use of these device-specific tokens brings additional benefits such as the potential for lower fraud-to-sales ratio among tokenized transactions.

What is more recent is the mass deployment of digital network tokens through additional third-party wallets and payment service providers. With this approach, it becomes possible to extend and accelerate the benefits of tokens to merchants across all digital commerce, in both card-on-file and guest checkout.

Importantly, tokenization has global, cross-industry backing. The specifications are managed by an independent organization, EMVCo, and the technology has been deployed in more than 193 countries worldwide. Within the Visa ecosystem alone, some 8,600+ issuers have been enabled for tokenization, more than 615,000+ merchants are transacting with Visa tokens, and more than two billion Visa tokens have so far been issued with Visa Token Service.

In the future we can see a scenario where every card-not-present Visa transaction is tokenized, which has the potential to completely eliminate the use—and the risk—of sensitive data. But, for now, the emphasis is to encourage and enable its mass deployment in the eCommerce channel.

Even before the COVID-19 pandemic, the direction of digital network tokens was clear, with many more payments shifting online. The process has now been accelerated and, in step, we need to accelerate the adoption of tools to keep the eCommerce experience secure and easy-to-use for the consumer, and for financial institutions and merchants.

Tokens play an important role in securing the eCommerce experience, creating a seamless customer experience and driving value for merchants and financial institutions. With all the necessary pieces in place, we expect them to become widely adopted in 2022.



Strong support from industry players

The introduction of network tokenization has been a collaborative, cross-industry endeavor involving a wide range of merchants, merchant service providers, and payment businesses.



Andre Machicao

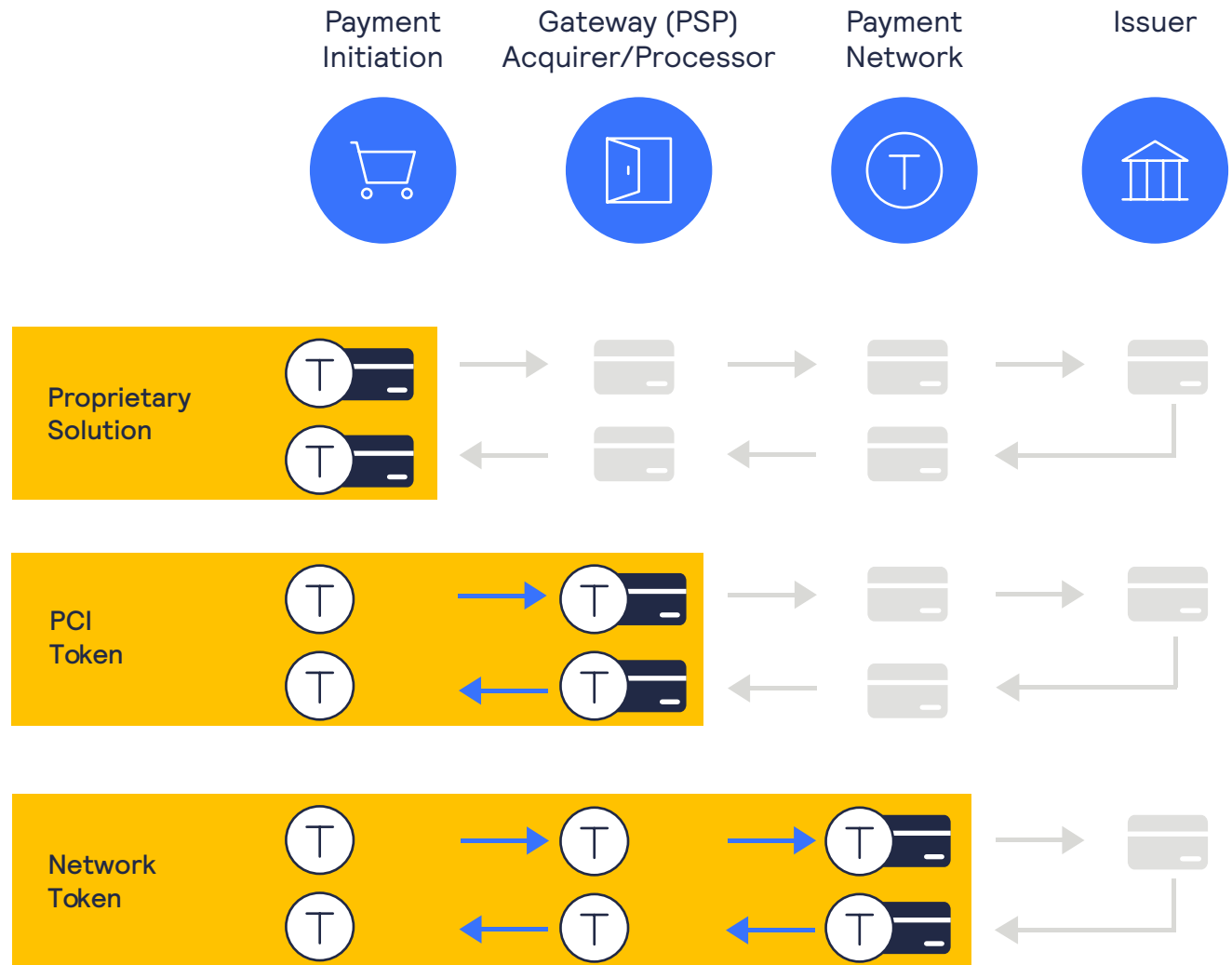
Senior Vice President, Head of Product,
Cybersource, a Visa solution



“Tokenization is the linchpin to enabling exceptional digital experiences that address rising consumer expectations for unified commerce. That is a consumer expectation to be recognized consistently in every channel in which they interact. An integrated tokenization strategy is key to unifying channels and delivering a compelling consumer experience.”

The difference between a digital network token and an acquirer or gateway token

Most eCommerce merchants already use a form of tokenization often delivered by their payment service provider. These acquirer or gateway tokens replace the PAN with tokens, protecting the PAN from compromise at the merchant. However, issuers do not have visibility of token activity on the merchant side. Issuers want to have the increased confidence that comes from digital network tokens being applied by the merchant to protect their cardholder data. Digital network tokens can either be used in partnership with these token solutions to enhance the value or as a standalone.




Digital network tokens extend the protection of the PAN through the network, giving visibility to issuers. The more visibility and control that the issuers have on the credential, the more confidence they are likely to have in approving a transaction.



Cybersource provides fast, innovative solutions for token management

Cybersource, a Visa solution, is a global, scalable, channel-agnostic platform built for the future. It can help you accelerate your token journey with fast, comprehensive solutions, providing resiliency and tremendous scale while working to innovate as early as possible with developing token technologies to help you succeed.

Using the power of Cybersource Token Management Service, you can strengthen your token strategy, identify early-mover opportunities, and make strategic decisions to improve and expand your omnichannel experiences. Cybersource's Token Management Service also provides the fastest way to ramp up and connect to Visa Token Service.



Cybersource's super token links card-on-file and other tokens to reduce complexity

Only Cybersource's Token Management Service links tokens from different networks, issuers, and channels into a unified super token to help resolve the tension between simple payment experiences and complex environments.

The Cybersource super token not only connects data from all card types and issuers, it includes alternative payments such as eCheck, ACH, and other debit products. It powers Token Management Service in managing customer data, simplifying customer models, keeping credentials refreshed and reducing PCI compliance scope. And it integrates seamlessly with

other Cybersource solutions, such as Decision Manager, Payer Authentication, Recurring Billing, and others.

Significantly, it works to help you improve customer experience by creating a unified view of your customers and their buying behaviors across channels and payment methods, seamlessly updating payment credentials to provide a smooth path to improved customer conversion.

Using Cybersource's Token Management Service, you can make payments simple and safe for your customers—no matter how complicated things get behind the scenes.

Benefits of Cybersource Token Management Service

Token Management Service can provide card-on-file lifecycle management and network tokenization to help you identify early-mover opportunities and create new payment experiences. It is ready to help you deliver:



More revenue capture

With a solution that uses one expanded source of unified data—Cybersource’s proprietary super token—to recognize more legitimate repeat customers so you can boost authorization rates, increase conversions, and lower your IT overhead.



Improved customer experience with an expanded 360-degree customer view

Using network, acquirer, and non-card tokens to connect customer payment data and purchasing information across different payment networks, card brands, channels, and loyalty programs. This makes it possible to deliver one-click checkout experiences, quickly adopt new methods of payment, and deliver more personalized shopping experiences.



Fraud reduction and better security

With a battle-tested Visa solution that keeps sensitive customer payment data encrypted at rest and in transit and stores it all inside state-of-the-art Visa data centers. This lowers your risk of data breaches and reduces your PCI DSS compliance scope.



It's the token management solution thousands of businesses already depend on to keep payments simple and secure—so payment complexity never gets in the way of better experiences and more good business. Visit [Cybersource Token Management Service](#) to learn more.

About Cybersource

At Cybersource, we believe that agility is the key to success in today's fast-changing world. We help you create and evolve payment solutions your way, so you can stay ahead.

Your customer is more than a transaction and Cybersource's Token Management Service elevates your tokenization strategy from a basic payment security tool into a complete, 360-degree view of every customer, helping you deliver the great experiences you've always wanted.

Join the thousands of businesses that already depend on Cybersource's Token Management Services to keep payments simple and secure—so payment complexity never gets in the way of better experiences and more good business.

[Contact Cybersource](#) to chat with a Cybersource representative or to request an appointment.

Note: "Why the future of eCommerce is tokenization" was originally published by Brian Cole, Sr. VP, Head of Product, North America, Visa, and Ansar Ansari, Sr. VP, Global Head of Platform Products, Visa, as "Convenience and control: Why 2021 is set to be the year of the token," in Visa Navigate, April 2021, <https://navigate.visa.com/na/money-movement/why-2021-is-set-to-be-the-year-of-the-token/>. Portions of the article were updated for this publication.



Cybersource 5B+ token quantities based on Cybersource Oct. 2020 – Sep. 2021 internal data sourced from Token Management Service and Secure Storage databases.

² VisaNet, Visa global card not present transactions for token vs non-tokenized credentials, May–July 2020

³ “VisaNet, U.S. fraud rate reduction for CNP & CP token participating merchants with digital wallet token requestors, April–June 2018

⁴ Ethan Cramer–Flood, “Global eCommerce Update 2021”, emarketer.com, Jan 13, 2021, <https://content-na1.emarketer.com/global-eCommerce-update-2021>

⁵ Ethan Cramer–Flood, “Global eCommerce Forecast 2022”, emarketer.com, Feb. 2, 2022, <https://content-na1.emarketer.com/global-eCommerce-forecast-2022>

⁶ eCommerce Fraud Trends 2019, Merchant Fraud Journal, <https://www.merchantfraudjournal.com/eCommerce-fraud-trends-2019>

⁷ U.S. Cybersecurity and data privacy council outlook and review, Gibson Dunn, January 28, 2021, <https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2021/>

⁸ VisaNet, Visa global card not present transactions for token vs non-tokenized credentials, May–July 2020

⁹ VisaNet, U.S. fraud rate reduction for CNP & CP token participating merchants with digital wallet token requestors, April–June 2018

¹⁰ VisaNet, US Visa CNP Merchants, Jan–Dec 2018

¹¹ U.S. statistics, Credential–on–file, Research conducted by Engine Group, Inc., June 2018

¹² U.S. statistics, cited in Credential–on–file le Pain Point Research conducted by Engine Group, Inc., June 2018

¹³ Cost of Data Breach Report, IBM Security, 2020, <https://www.ibm.com/security/data-breach>

¹⁴ Source: Global VisaNet and NSPK Data (Russia); Global Merchants, Jan 2020–Dec 2020

All brand names, logos and/or trademarks are the property of their respective owners, are used for identification purposes only, and do not necessarily imply product endorsement or affiliation with Visa or Cybersource.

