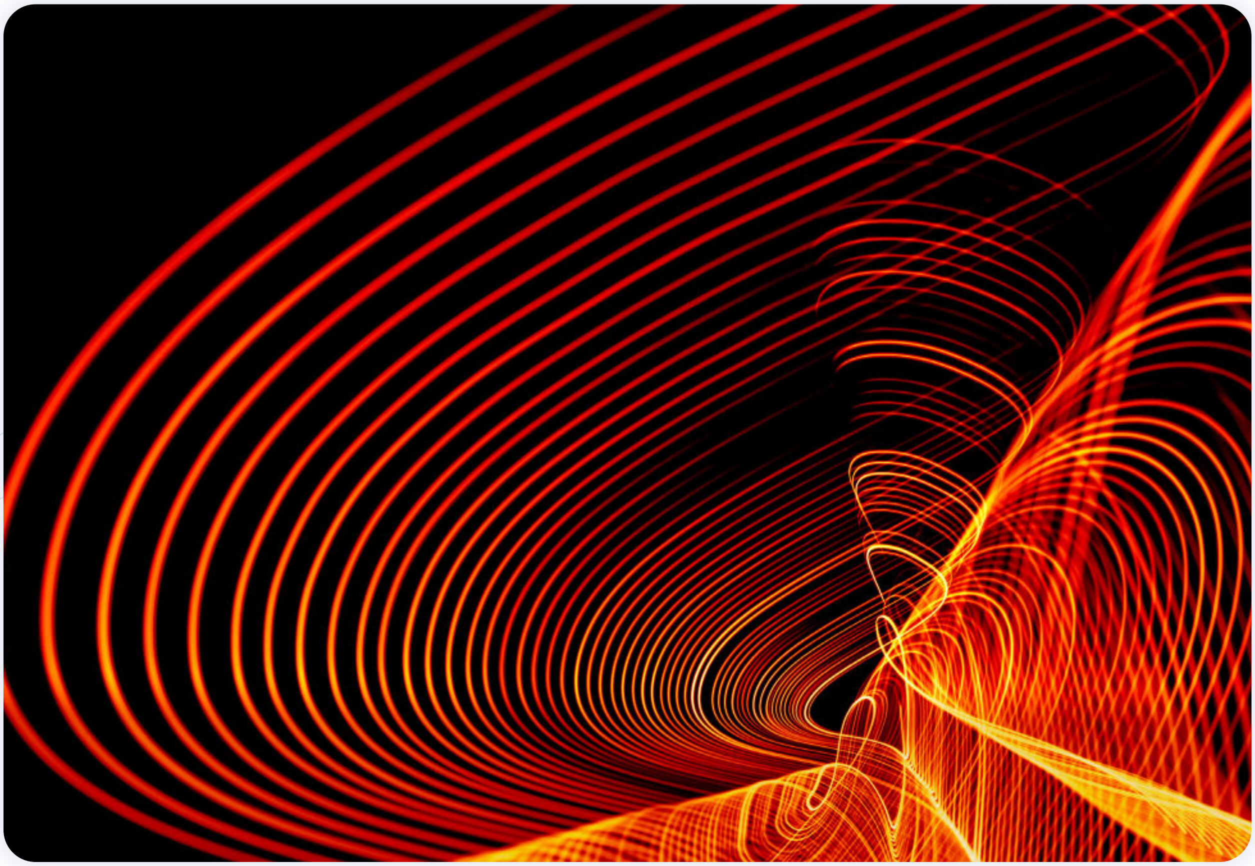
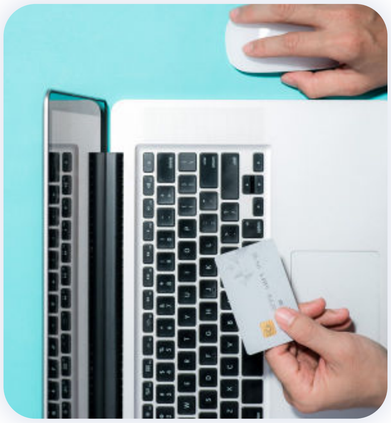


The Risk of Going All-In With Processors

How tokenizing with a processor or other payment service provider stacks the cards against you

Table of contents

In today's omnichannel payments landscape, digital transactions are growing in popularity and becoming far more efficient than their physical counterparts. Technological innovations such as digital wallets and societal developments such as the COVID-19 pandemic have only increased the value and widespread adoption of digital payments, pushing organizations to create convenient, customer-focused experiences that make it easier to pay—and in more ways—than ever before.



However, this drive toward digital has contributed to the formation of a complex and risk-filled environment for protecting and ensuring the compliance of customer payment data. Organizations that collect, store, and/or process sensitive consumer data are responsible for the safekeeping and stewardship of these valuable data sets, many of which are governed by strict regulatory compliance obligations.

When it comes to processing this information, three priorities remain top of mind: security, dependability, and affordability. Merchants need to be able to rely on the security of their payment systems without paying an arm and a leg for processing. They also need to maintain a user-friendly payment experience that enables quick and easy customer transactions.

When it comes to processing this information, three priorities remain top of mind: security, dependability, and affordability.

To address these concerns, many payment processors promise low transaction fees, offer to throw in free security services such as tokenization, or entice you with their full suite of supplementary payment technologies. However, these pitches rarely cover the fine print, which can include migration penalties and restrictions for adding processors or other third-party integrations, essentially creating an environment where you're entirely reliant upon the processor for the operation of your digital payments landscape.

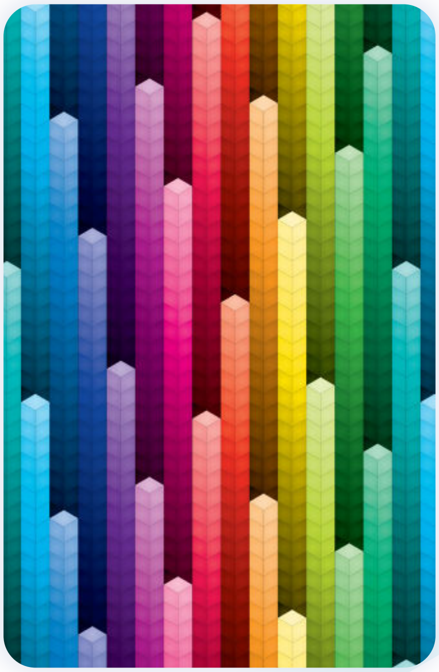
In this ebook, we'll cover the common practice of "processor lock-in," analyze the complex and often hidden pricing of transaction fees, and identify other potential red flags when working with some big-name processors. That isn't to say that all processors are out to get you or that no one within the payments industry can be trusted. However, we want to arm you with the necessary knowledge to protect your interests by asking the right questions and being aware of common deceptive practices that could ultimately hurt your organization.

PSPs: Not always what they seem

Upon learning about your internal systems, many PSPs will assure you that they can support all of the operations that are critical to your success with their own versions of whatever software or third-party applications you're currently interacting with. *Need a fraud-prevention tool and some data governance? No problem, just integrate with ours!*

On its face, this seems like a great solution, especially if you're offered discounts by bundling these services together. However, the immediate convenience of this type of one-stop shopping can quickly be negated when you want to migrate to a different processor or work with a different third-party provider on any ancillary services.

> **"When you integrate with a processor, you're not just locking into processing—you're locking into their entire stack. So because you're tied to their whole technology ecosystem, you're liable to have to replace every component of your payments stream in order to leave. That means you quite literally have to rebuild your payment processing infrastructure.**



Beware of "free" & hidden fees

Another thing to be particularly wary of is a processor's ability to assess fees dynamically. This is especially true of acquisition-driven merchant-processing providers that have purchased companies specifically for their ability to dynamically price complex and obscure interchange fees.

When enterprise organizations choose to integrate with a PSP's "free" tokenization platform, they are often lured in by suspiciously low per-item fees and other attention-grabbing offers, such as a 0% mark-up on interchange fees. However, once they convert to the provider's platform and migrate their data, everything changes. They experience increased interchange rates and network-related fees. All of a sudden, that sweet-sounding tokenization deal is not only not free, but it's actually become quite costly.

Unfortunately, these types of deceptive "bait and switch" tactics are common practice within the industry today, despite the fact that many lawsuits have been successfully litigated against prominent global payment service providers. Many organizations fall prey to these empty promises and sign multiyear contracts that lock them in until the terms expire. And even then, if an organization decides to leave once the contract is up, they'll have to deal with the headache of starting from scratch with another provider.

Who's charging me?

Interchange Fees: Non-negotiable fees levied by the issuing bank.
Assessment Fees: Non-negotiable fees levied by the credit card companies.
Processing Fees: Negotiable fees levied by the processor.

Source: Merchant Maverick

Beware of these suspicious fees

Transactional downgrades

“Qualified” low-risk transactions are considered safer, so they don’t cost as much to process as higher-risk “nonqualified” transactions. However, it’s not always clear what criteria a processor is using to evaluate the qualification of a given transaction. This lack of transparency can lead to unexplained downgrades of seemingly low-risk transactions.

Account fees

Once the ink is dry, it’s not uncommon for processors to require account application and setup fees as part of the onboarding process. Although setting up merchant accounts requires minimal lift and expense on behalf of the processor, these fees are often tacked on in an attempt to nickel-and-dime merchants with needless markups

Compliance fees

Some processors will charge merchants for PCI compliance but fail to disclose exactly what services they’re providing or which areas of the assessment they’re helping to address. Some also charge fees for noncompliance, regardless of whether they’re assisting with the compliance process. Bottom line: You shouldn’t be charged for services that don’t help or don’t exist.

Source: Merchant Maverick

Problem

A multichannel payment application required greater versatility and affordability in its operations to develop a new version of its app.

Solution

Although PNS's existing payment partners offered free tokenization if it used their processing services exclusively, they couldn't deliver the freedom and flexibility PNS needed to fully control its tokens. By instead working with TokenEx to create a cloud token environment independent of its internal systems and PSP, PNS was able to retain ownership of its tokens, leverage those tokens to build consumer profiles for future payments, and reduce the scope and cost of PCI compliance.

Results

- Reduced PCI scope by ***75 percent***
- Estimated cost savings of ***33 percent*** on PCI compliance
- Used tokens to create consumer profiles-enabling ***flexible scheduled and recurring payments***
- Facilitated seamless processing of ***hundreds of thousands*** of daily transactions

Leaving will cost you

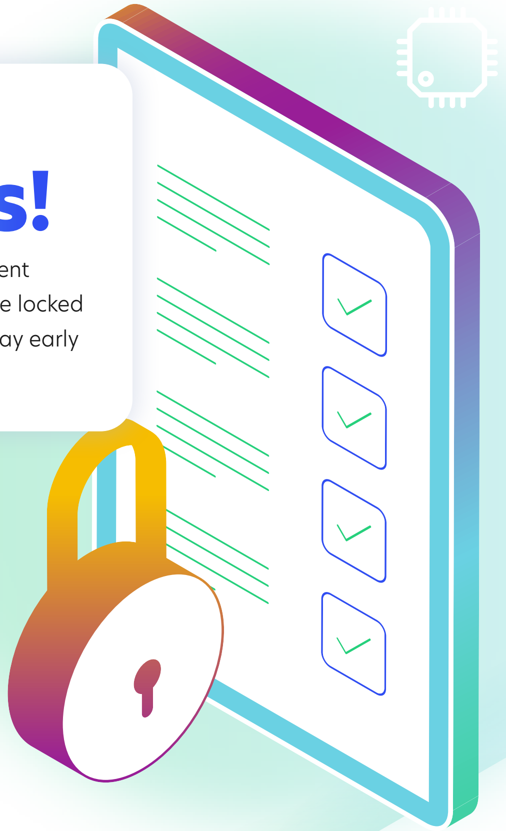
So now that you're aware of a few things to watch out for when pushing all-in with a PSP, let's dig a little deeper into what it takes to leave. The primary concern here is cost—both in terms of any penalties you might be subject to for ending a contract early, as well as the subsequent expense of rebuilding your payments stream with another provider. These are known as deconversions costs, and they require a significant investment of time, labor, and other valuable IT resources.

Ultimately, though, leaving behind a PSP or processor tokenization platform requires the provider's cooperation. You simply cannot move on without it. In many instances, once you tokenize with a processor, not only are you surrendering control of your sensitive data, but you're also relying on processor-created and -owned tokens. So if you decide to leave, you first need the processor's cooperation to retrieve your original data. Then, even if your data is returned, you'll still likely lose all of the associated tokens. That means you'll need to retokenize all of your data with your new provider, adding insult to injury as you're essentially forced to start from scratch.

Processor lock-in

36 months!

The standard contract length for payment processing is 36 months, meaning you're locked in for three years—unless you want to pay early termination fees.



Problem

A point-of-sale leasing technology needed to increase the redundancy, flexibility, and affordability of its payment processing

Solution

By leveraging the TokenEx Data Protection Platform as a proxy through which Acima could tokenize with any processor it so chose, Acima began directing all transactions to TokenEx, enabling the fintech organization to migrate without paying its previous processor for token retrieval. Now, whenever Acima adds a new processor to its payments stream, it can quickly and easily redirect its tokens from TokenEx—with no additional cost.

Results

- Saved ***tens of thousands of dollars*** per year via new ability to negotiate with multiple PSPs
- Became capable of instantly transitioning ***100 percent*** of its transaction volume to new processors
- Implementation of Account Updater enabled ***seamless recurring payments*** by eliminating processing failures due to card expiration, theft, or loss

Fact vs. fiction

For these reasons, processors have all of the leverage. They are acutely aware of this and will use it to their advantage, especially when it comes to pricing. Once you are fully committed to a single PSP, it is very difficult to monitor the hundreds of categories of line-item interchange costs, which can lead to exorbitant "net effective rates"—or total cost to accept credit cards after moving to a single processor—for many large enterprise organizations.

So, before entering into a relationship with a PSP or other processor, how can you thoroughly vet its claims to determine which are legitimate and which are too good to be true? Here are a few considerations to keep in mind:

Large, global PSPs know it's hard to leave

These providers understand how much leverage they have over merchants once the ink dries. Don't let them:

- Sweet-talk you with promises of low introductory transaction rates
- Entice you with discounts on bundled services that actually decrease your flexibility
- Lock you into long-term contracts that prevent you from leaving

Always consider deconversion costs

Moving off of a PSP's tokenization/encryption platform will:

- Require the provider's cooperation
- Result in significant investment of time and valuable IT resources
- Cause significant business disruption and come at the lost opportunity cost of value-enhancing initiatives

Don't underestimate the value of flexibility

The ability to work with multiple processors allows you to control your total card-type mix, view and compare fees, and keep processors honest. Committing to a single processor:

- Severely restricts your ability to leave or add another processing relationship
- Complicates omnichannel use cases (refunds, support, cross-channel purchasing) due to limited functionality of processor tokens
- Requires the full support of the PSP in order for you to regain control of your payments landscape

The case for third-party tokenization

Flexibility extends backward and forward

Perhaps the greatest benefit of working with a third-party provider is the flexibility this enables. Not only does it allow you to customize your payments stream by working with your preferred supplementary technologies, but it also makes existing relationships easier and enables previously unavailable ones.

In addition to the benefit of more options for third-party integrations, you can easily migrate to and work with multiple processors. As a result, you can quickly and easily increase redundancy via simple lift-and-shift implementations. It also gives you significant leverage during the procurement process, allowing you to shop around for the best deal and negotiate the best possible rates—all while retaining control over your integrations and ownership of your data.

Today's omnichannel landscape requires flexible, multifaceted capabilities, so maintaining multiple processor relationships to maximize the benefit of different specializations allows you to respond rapidly to changing payment technologies and compliance regulations without requiring you to wait for your PSPs to adjust. This ability to integrate with third parties helps you to easily onboard new processors and facilitate the evolution of these relationships to ensure your needs are continually being met.

In short, greater flexibility equals greater control, and greater control often means greater success. That's what you gain by working with a third-party provider instead of a single PSP: the freedom to operate without compromise.

Flexibility equals freedom

Implementing adaptable technology helps maximize the value of your digital operations.

Why TokenEx?

Data protection that drives business

Since 2010, the TokenEx Data Protection Platform has been safeguarding the world's most sensitive data from theft. By entrusting the protection of sensitive data to security and compliance experts, we allow you to simplify your data-driven operations. Additionally, we enable you to outsource the cost, effort, and complexity of maintaining secure systems for sensitive data and streamline the compliance process so you can focus on what matters most: enhancing efficiency, maximizing value, and generating revenue.

Ultimately, our platform derives its true value from the business initiatives and positive outcomes it helps create. Whether that's reducing friction, minimizing cost, simplifying systems, or facilitating critical business processes, the ability to align security with operations to achieve overall organizational success is the key differentiator.

How can TokenEx help?

Get the expertise you need.

Meet with TokenEx today to learn more about how we can help you with your payment solutions.

Connect with us

The Problem

Enterprise tire retailer needed to simplify its credit application and enhance its security posture.

The Solution

By working with TokenEx to create a proxy form on the payment encryption device, Discount Tire was able to securely send sensitive data to TokenEx for tokenization without it traversing Discount Tire's IT infrastructure. Additionally, it drove higher ticket value and improved customer retention by enhancing the customer experience in a way that also saved time, labor, and cost.

Results

- Marked increase in monthly credit application volume, adding ***millions a year*** in otherwise unrecognized revenue.
- Flexibility provided by Transparent Gateway enabled second-tier financing, increasing blended approval rates to roughly ***95 percent***
- Recouped the cost of the project within ***six months*** of implementation
- Process time on 10-15 percent of sales was reduced by ***more than 50 percent***
- Completed full enterprise implemention within ***90 days*** of project approval