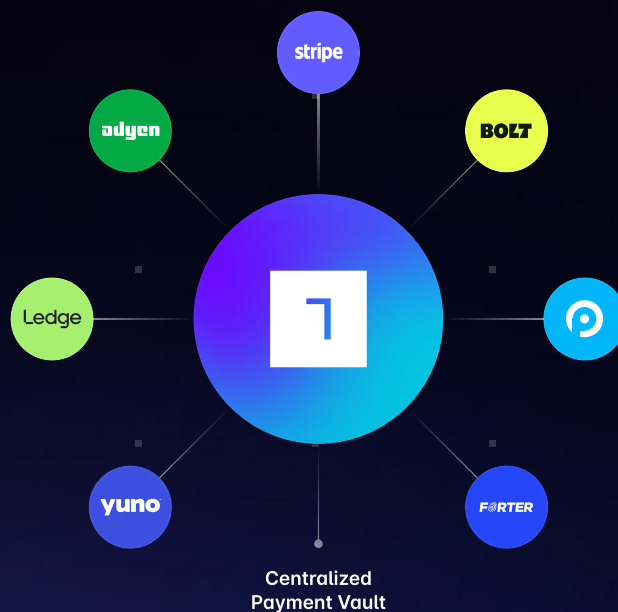




Payment Orchestration 2.0: Tokenization, Vaulting, and the Unbundling of Payments

Helping merchants decide what to buy or build.



Basis Theory

Payment Orchestration 2.0: Tokenization, Vaulting, and the Unbundling of Payments

Helping merchants decide what to buy or build.

Navigating Key Decisions for Merchants

Decision-making is hard. Choosing a definitive path forward is nerve-racking. And when it comes to checkout workflows and transaction processes, despite being largely “data-driven,” many B2B and B2C merchants lack the necessary data to optimize their payment operations.

However, merchants are going to need to make a decision soon involving payment orchestration and a multi-processor payment strategy. Whereas B2C companies are bundling features and services into “super apps,” B2B companies are debundling their payment stack and implementing a strategy around orchestration, tokenization, and vaulting.

Because the market is clearly signaling to merchants that they need payment orchestration—not because it’s just good business, it improves the customer experience.

Where the market is split is how to achieve this approach best. With no ubiquitous specification or protocol, high ambitions are being met with constrained engineering resources—leading to assumptions that a third party needs to be involved to ultimately buy this functionality.

Explore Your Options

Several options exist for achieving a multi-PSP strategy and payment orchestration:

Option 1 - Multiple PSPs without a Centralized Payment Vault

Option 2 - Have a Primary PSP with Forward API Capabilities

Option 3 - Payment Orchestration Platform

Option 4 - Token Orchestration Platform

Option 5 - Build Everything

Our Experience and Recommendation

The problem is that the magical solutions being promoted and pitched have potential downsides that can impact a merchant today, tomorrow, and in the long term. Merchants start with Stripe or Braintree because the onboarding process is so intuitive and cost-effective. As the merchant scales, the merchant begins to overpay their original PSP, but because payments are operating and working as they should, optimizing this business process is not a top priority.

Meanwhile, the world moves ever closer to a multi-processor setup. Most of you reading this will likely be working on this project in the next 12-18 months or already is.

But how to do it? Explore your options.

Option 1

Multiple PSPs without a Centralized Payment Vault

If a certain IP address is “X,” then the transaction is sent to a specific processor, compared to if the IP address is “Y,” then it goes to a different processor. The biggest complexity is that because of PCI compliance requirements, multiple front-end integrations are required.

With this approach, design teams are required to manage multiple user interfaces depending on which processor is used, which can be difficult—especially when some elements are more flexible than others. Prepare to hear about design inconsistencies!

This option can get messy—and it can happen quickly—because there’s no data centralization. We have seen this often because before options 2-4 existed, a merchant really had but option one when it came to achieving a multi-PSP approach. But not anymore.

Option 2

Have a Primary PSP with Forward API Capabilities

But with Stripe announcing its Forward API capability—and Braintree before that—Forwarding APIs are becoming more widely known. Because, as a PSP in a multi-PSP world, offering a Forward API can keep a merchant from taking its transaction volume elsewhere.

These APIs allow raw payment data to be forwarded from a PSP-hosted payment vault to a third-party that does not have to be associated with the PSP doing the forwarding. PSPs often incentivize merchants to use this functionality.

Typically, the PSP vaults the card for a one-time, flat fee and charges an additional fee per API call. Other PSPs will charge when a card is forwarded out of the vault.

With this option, the primary processor has an inherited conflict of interest. The goal of any PSP is to get as much processing volume as possible, and now the primary PSP gets to see every destination endpoint to which cards are being forwarded. The merchant has zero leverage when negotiating transaction prices or asymmetric information.

Any good partnership comes down to who has more leverage. With this option, the merchant is giving up a lot of leverage by sharing this data.

Once the primary PSP realizes meaningful volume is being forwarded to another processor, sales teams will contact them.

Option 3

Payment Orchestration Platform

A primary reason for a multi-PSP approach is to lessen the risk of a single point of failure. However, an orchestration platform should be viewed as another PSP.

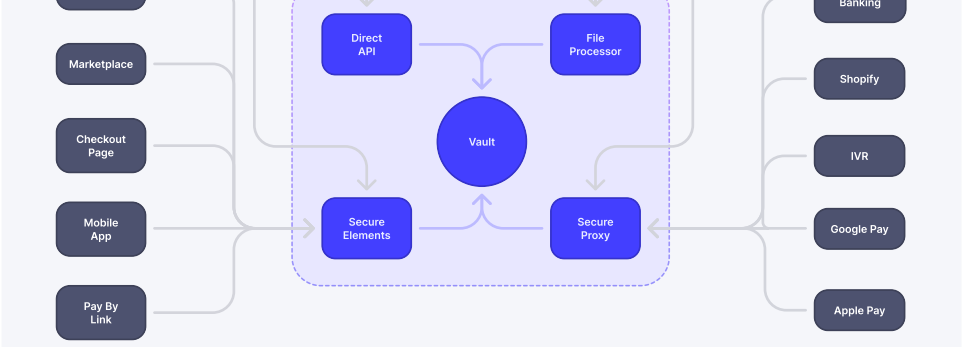
And yet, this is still a single provider (read: single-point-of-failure) who takes a cut of every transaction.

A question to ask orchestration providers: do they have referral deals with PSPs and other partners to route volume to them? As a merchant, the orchestration platform is trusted to route transactions based on what is best for business. However, if referral deals are in place with certain providers, the merchant suffers if the platform is incentivized to route transactions based on who provides the biggest kickback.

Many merchants don’t realize this is happening and may find that what seems like a no-brainer decision may actually be detrimental to them. Ask these questions before signing any contract.

Option 4

Use a Token Orchestration Platform



Tokenization is not new for a PSP or card network. Today, tokenization is being offered independently and agnostically, without any tie to a particular PSP or network. This option uses the existing proprietary tokenization solutions already being offered by networks and PSPs.

A token orchestration platform is a payment vault with a fully compliant PCI Level 1 environment. This environment captures the sensitive cardholder data right at the point of purchase, vaults it, and returns a token to the merchant, who can route it based on their logic.

A token orchestration platform allows merchants to own their data without being responsible for storing and protecting it.

When tokenization happens at the transaction level through a PSP, the PSP takes a cut of each transaction by sitting in the middle of the flow. When choosing an agnostic token orchestration solution that captures the information at the time of the transaction, merchants can choose the token type and network based on dynamic logic like IP address, location, payment type, etc.

Option 5

Build Everything

The direct costs of achieving PCI compliance alone can range from \$70,000 to \$500,000 each year.

Generally, these are the costs of PCI compliance a merchant should prepare for:

- Logging Activity:** depending on the level of logging already required for business needs, costs to implement logging sufficient to meet Requirement 10 could run an organization \$10,000/month, as well as the personnel costs of reviewing and maintaining the logs
- Vulnerability Scans:** as outlined in PCI DSS Requirement 5, these scans should be run once every quarter at a cost of \$100 to \$200 per IP address.
- Regular and Frequent Penetration Tests:** smaller organizations may see costs around \$20,000 per year, but larger enterprises will pay upwards of \$100,000 or more
- Remediation and System Needs:** building a fully redundant environment could double the cost of systems. Likewise, should a vulnerability be found, remediation of the issue could cost an organization upwards of \$100,000 or more, depending on the resources required. System and remediation costs are the most variable and may be unknowable upfront.
- Payments to Outside Auditors for Testing and Certifications:** auditors can run an organization around \$40,000 and will also file AOCs and ROCs with the PCI council, included in this fee

The cost of PCI compliance requires knowing which PCI level your business is. However, once a merchant hits a certain scale, you must follow PCI Level 1 compliance requirements.

At Level 4, for instance, a merchant needs to fill out Self Assessment Questionnaires (SAQ), run penetration tests internally, and file a self-approved Attestation of Compliance (AOC) form. Those costs are minimal.

By contrast, a PCI Level 1 merchant must bring in outside auditors, who will check and stress-test every element of the PCI compliance program. Of course, the more checking required, the higher the likelihood that problems will be uncovered and must be addressed to maintain status with the other participants in the payment process (PSPs, card networks, acquiring banks, etc.)

However, buying access to a payment vault helps a merchant avoid most of these costs and truly optimize the transaction process.

Our Recommendation

Payment optimization is not a sprint; it’s a marathon. What we see are companies trying to transform their payment stack overnight in a single project. This oftentimes results in the company doing nothing because as the project scope creeps, it becomes too big to even execute on.



The idea of being all in-house or working with an orchestration platform is much like having open heart surgery—when all that is needed is an improved diet with exercise. We recommend an iterative approach to payment optimization.

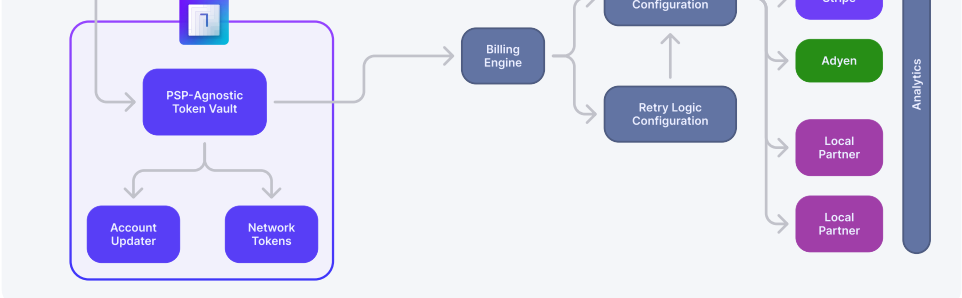
Vaulting and token orchestration is that iterative approach. This technology can shim into the existing payments stack without disrupting the current flows. That means on day one, the merchant starts getting more independence by introducing Basis Theory. Think about where there is the least amount of control in the payment workflow, start there.

Card data migration and additional PSPs can come shortly after.

We call this “tokestration,” a portmanteau of “token” and “orchestration.”

Buy the vault, and create the orchestration solution optimized for their specific transaction workflows and experiences.

Start with the vault; everything else falls into place.



Want to learn more? <http://basistheory.com/why-basis-theory>