12 Key Questions to Ask When Selecting a Digital Commerce Payment Vendor

Published 10 November 2021 - ID G00760963 - 28 min read

By Analyst(s): Dayna Ford

Initiatives: Digital Commerce and CRM Sales Technologies

As customers demand low-effort check-out experiences, businesses must choose the right payment providers for their digital commerce platform. Application leaders responsible for payments can optimize customer experience and save time and money by asking vendors 12 key questions.

Overview

Key Findings

- Application leaders responsible for digital commerce payments are struggling to keep up with rapidly changing payment technologies. They are frequently over- or underinvesting in this area, resulting in suboptimal conversion rates, unnecessary expense and/or poor user experience.

- Companies’ digital commerce expansion into new geographies requires localized payment methods and currencies as well as operational support. The need to innovate and move quickly into new channels and markets can be hindered by slow-moving and constraining payment vendors.

- Over the years, many companies have accumulated multiple payment vendors, either to support channel and geographic expansion or due to mergers and acquisitions. Now they have many vendors to manage, bear excess cost and risk, and seek to consolidate to reduce overhead and fees.

Recommendations

Application leaders responsible for digital commerce payment technologies should:

- Foster a holistic and cross-organizational approach to payment decisions. To do so, identify all constituents and work with them to identify the right balance between reduced cost, optimized experience and risk mitigation.
Introduction

With digital’s share of overall commerce continuing to expand, the related payment experience is critical to digital business success. Digital commerce application leaders must determine the best way to accept payments and with which vendors. Long gone are the days when companies operated in single channels and accepted one or two payment methods at the point of sale (POS).

The payment landscape is rapidly changing, with an ever-increasing choice of vendors and approaches to the payment experience. Simultaneously, the established incumbents are expanding their payment ecosystem footprint largely through acquisition. The distinct legacy roles of the merchant, gateway provider, processor and acquiring bank are becoming increasingly blurred as this market consolidation evolves. For more information, see Navigating the Digital Commerce Payment Market.

As your business expands geographically, the challenge escalates. You must consider unique:

- Networks
- Payment methods
- Cultural attitudes toward payments
- Customer preferences
- Regulatory and legislative concerns

While no single vendor can serve the entire globe and all the localized payment types required to support digital commerce, there are strong regional and multiregional contenders.
How do you choose the ideal vendor or vendors to serve your unique digital commerce business needs? Foster a holistic approach to payments, define a well-aligned payments strategy and use the 12 questions in this research to cover the salient business needs in the four categories shown in Figure 1.

Figure 1: An Approach to Identify Payment Vendors That Meet Digital Commerce Needs

**Analysis**

**Foster a Holistic Approach to Payment Decisions**

Many organizations compartmentalize payments as a distinct function. As a result, it may be one of the last areas addressed in commerce projects. Proactively creating a cross-functional team approach to payment strategy definition and execution will help avoid costly mistakes and delays down the line.

Payments impact many areas of the business, from customer experience and support to finance and operations to marketing. Lack of input from internal stakeholders can lead to last-minute scrambles to hire people and find budget for unanticipated impacts. When starting a payment-related project, identify all your constituents — that is, the interested parties — and be sure to include the following:
All channels where payments are accepted and those responsible for the channel — for example, store, web, mobile, kiosk, chat and call center.

All technologies that support and/or integrate to payments and those responsible for the technology — for example, billing, invoicing and ERP.

All functions involved in the processing and reconciliation of payments — for example, the finance team, dispute handling team, risk and security, fraud prevention and accounting.

Most importantly, do not lose sight of the customers. Identify the most popular payment methods used in the areas where you are doing business and offer them to your customers. Make the payment process as easy as possible. The easier it is for customers to pay, the lower the probability of cart abandonment at check-out.

Align the Payment Strategy With the Corporate Strategy

The corporate strategy must drive your payment strategy, and the two need to be kept in lockstep as each evolves. Payments cannot be an afterthought, especially when it comes to geographic and channel expansion. Imagine moving into a new country only to find the business launch delayed by months because the company cannot process payments there.

If your business has operated predominantly in a brick-and-mortar environment and is now moving meaningfully into digital commerce, or vice versa, the payment experience needs to expand accordingly and elegantly. Even a customer experience improvement initiative could impact the payment roadmap; some examples include:

- Reducing disputed transactions
- Making a payment from a chat window
- Creating more consumer transparency into currency conversion
- Enabling an online refund experience
- Unified commerce and supporting the same payment experience in every channel
- Providing buy online, pickup in store (BOPIS) or curbside pickup services
Application leaders must be prepared to move quickly to adapt the payment strategy when the corporate strategy changes. Build agility into the payment roadmap to manage strategic shifts, such as changing geographical plans, new disruptive technologies and regulatory impacts. Ensure that your team has the processes and technologies in place to move at the “speed of digital” and avoid being the bottleneck for corporate initiatives.

**Use These 12 Questions**

The search for the right payment vendor can be both overwhelming and confusing. Asking the right questions of the right vendors provides the information that companies need to identify those vendors that are offering innovation, compare those offerings and determine the best solution.

The questions posed in this research are suitable for use with payment vendors, such as payment gateways, payment processors, merchant acquirers and payment facilitators (note that definitions of these terms can be found in the Acronym Key and Glossary Terms section).

1. **Customer Experience: In What Countries/Regions Do You Operate?**

It’s often to the enterprise’s advantage to choose a vendor with a local presence in many countries — especially if the enterprise plans to operate in similar countries. Finding a vendor that can cover transactions throughout your region and that has a local presence in your countries of interest can create opportunities to increase the bottom line.

   Here’s why:

   - Vendors typically charge fees based on the volume of transactions. A vendor covering multiple geographical areas that match yours enables processing consolidation that could lower your fees. If you know that in two years your enterprise will expand to another geography, selecting a vendor today that supports those countries can prevent problems and maintain a lower processing cost.

   - Authorization requests made by local entities (versus foreign ones) typically result in higher authorization rates, thus increasing sales and revenue for sellers. The more countries in which a vendor operates, the more likely that it can support local authorization requests in your countries of interest. Vendors with local operations are more likely to be knowledgeable and equipped to handle local variations in payment methods. Without that capability, sales will be lost.
2. Customer Experience: What Payment Methods Do You Offer?

It’s important to consider vendors that support all or most of the payment methods already used or planned to be used by your enterprise. It’s also important to partner with a vendor with a solid understanding of the payment nuances of the geographies where you plan to do business.

Here’s why:

- Popular payment methods vary by country. The more methods accepted by a seller, the greater the chance of customer conversion, resulting in increased sales and revenue. Payment methods such as Boleto Bancário bank transfers in Brazil, or Alipay and WeChat Pay in China, are required for digital commerce in those countries.

- The greater the number and variety of payment types supported by a vendor, the more likely the vendor can support current and future requirements. This can reduce the time to market and make adopting additional payment methods quicker.

- New payment methods can occasionally become quite popular very quickly, as happened with buy now, pay later (BNPL) payment methods during 2020 and 2021. Be sure to discuss roadmap and product strategy with your prospective vendor to ensure that its approach aligns with yours.

3. Customer Experience: What Channels and Payment Processes Do You Support?

Many clients use different payment vendors for different channels and types of payments — primarily because the needs of the differing channels arise at different times. Payment types differ because their usage may vary by both channel and use case. Recurring and subscription payments in most regions, for example, are commonly made using direct debits, although direct debits are rarely used for one-off online purchases or at the in-store point of sale (POS).
Subscription or recurring payments are increasingly being adopted by digital commerce businesses of all sizes. While recurring payment services are offered by most payment vendors, not all support complex use cases such as usage-based pricing, which results in variable amount recurring billing. For these, many vendors will need a billing engine (see Market Guide for Subscription and Recurring Billing Management).

Be sure to evaluate how the vendor supports your various channels as well. Are all channels fully integrated into a single experience? Will customer-centric data such as tokens be shared and used across all channels? Or is the functionality disparate and disconnected, and on different platforms that will simply be managed under one contract? If your digital payment experience includes vendor-hosted pages, do those pages include responsive design to dynamically adapt the experience for different devices? Will the pages dynamically adapt for language and currency localization? For more on improving the payment customer experience, see How to Improve Customer Experiences in Digital Commerce Payments.

Payments must be routed to the appropriate parties, regardless of how the data is received. Increasingly, vendors are integrating both card-present and card-not-present processing. When considering a change of payment vendor for one channel, it is highly recommended that you consider consolidating vendors across channels. Even if you are not planning to execute that consolidation today, choose a vendor that will make it possible when your organization is ready to do so.

One special use case increasingly pertinent for many businesses is payments as a packaged service (PaaPS), also sometimes referred to as the “marketplace payment model.” Many different kinds of businesses are expanding to become marketplaces (see Create Enterprise Marketplaces to Accelerate Digital Business), and many nonmarketplace businesses can also benefit from this payment model. The key features of a marketplace payment offering are seller onboarding APIs and automatic distributed funding to sellers (see the PaaPS section of Hype Cycle for Digital Commerce, 2021). If this use case applies to your business, be sure to look for a payment vendor that supports the model efficiently and effectively.

Here's why:

- Consolidating processing vendors across channels means greater transaction volumes under a single contract, and therefore lower per-transaction costs for enterprises. Because vendors typically charge fees based on transaction volume (via tiered pricing), using one vendor to process transactions from multiple channels will lead to reduced costs.
4. Finance: In Which Currencies Do You Settle?

For large, global enterprises, it is advantageous to select a vendor that operates in the currencies in which the enterprise has the largest number of transactions.

Here's why:

- Settling in the local currency at the aggregate level is less expensive than settling at the transaction level from a foreign currency exchange perspective. This allows companies to save money by paying lower foreign exchange fees.

- In some countries, there may be limits or restrictions on the repatriation of funds. Funding in the local currency into a local bank account may be required before the funds can be moved into an enterprise’s preferred bank account or currency.

5. Finance: What Is the Frequency of Settlement?

It's important to understand both settlement and its timing. Settlement occurs between issuing banks or other account guardians and merchant acquiring banks, processors or payment facilitators that are responsible for sending the funds to the merchant (see Market Guide for Digital Commerce Payment Vendors). The timing for settlement can vary, and ranges from weekly to the same day or intraday. Same-day settlement may not be available from all vendors, or may be subject to volume requirements or additional fees. Settlement timing is often based on four criteria: the vendor, the type of transaction, the number of transactions and the currency. Both settlement and timing are important to keep in mind when choosing a vendor.

Here's why:

- The more frequently the settlement occurs, the more quickly cash is made available to the enterprise and the better the cash flow becomes. From a cash-flow perspective, receiving funds sooner is always better than later.
Some vendors will charge additional fees for faster settlement. The value of the cash flow and associated float must be evaluated against the cost of the fees to determine if this option represents a net positive return for your business.


Most payment vendors will have pricing models that fall into one of two broad categories: bundled pricing or pass-through pricing. In order to compare vendor costs and predict the payment processing budget, you need to understand both models and the elements they include.

Here's why:

- Bundled pricing generally reduces reconciliation and budgeting complexity, but may obscure opportunities to reduce costs.
- Pass-through pricing can be complex and requires some in-house payment expertise to manage.
- Every vendor has unique models for what is and isn't included in its base pricing, so careful scrutiny of additional fees is critical to avoid unanticipated costs.

Bundled Pricing

Generally presented as a percentage of the transaction value plus a flat fee per transaction, this type of pricing is fairly ubiquitous for small-to-midsize merchants and for all merchants for most digital wallets. This model benefits the organization in its predictability, and may require less payment expertise in the back office to manage the accounting and budget reconciliation for fees.

However, there may also be additional fees, usually a percentage of the transaction value, due to any transaction not including all the necessary data. These fees are often referred to as “downgrades” by payment vendors and typically only apply to debit and credit card transactions.

Pass-Through Pricing
This pricing model provides the highest level of transparency, but managing it effectively also requires the most back-office payment expertise. In this model, the actual interchange fees charged by the issuing bank (or other account guardian) and the card association (or other network) are passed through without markup. The payment facilitator, processor, gateway or acquirer that owns the relationship with the merchant applies its own fees discretely — often as a flat fee per transaction — but these fees are also increasingly presented as a percentage of the face value.

In the U.S., the major card brands may have dozens of different interchange rates. Understanding the minutiae of why a transaction qualifies at a lower rate can be overwhelming, but it can also save the enterprise money.

**Additional Fees**

Most vendors charge additional fees, so be sure to know what these are and include them in your budget calculations. Examples of common line items that result in additional fees are:

- Moving funds into your company’s bank account
- Fraud detection
- Payment authentication, such as 3D Secure
- Tokenization
- Chargeback handling, often at each step in the process
- Processing a refund (be sure to ask whether your vendor refunds fees or charges additional fees for refunds)
- Reporting fees (different types of report delivery or content may result in varying fees)
- Noncompliance fees of any kind

**7. Operations: What SLAs Do You Support?**

Any contract with a payment vendor should include at least two types of SLAs: service availability and the process for dealing with application or service issues. Some vendors are also starting to incorporate SLAs for integration with other applications and providers. Additionally, the contract should define the remedies for any missed SLA targets (see *SaaS SLAs: Reduce Risk and Improve Service by Negotiating These Key Terms*).
Here’s why:

- Payment is a basic function of commerce, and since commerce — fueled by digital technologies — has become 24/7, payment functionality must also be 24/7. Make sure the guaranteed availability for payment processing is clear and meets business requirements. It is imperative to understand a vendor’s backup and redundancy capabilities, as well as its disaster recovery plan. Customers unable to complete the payment process will go elsewhere to make their purchases.

- Establishing definitions for Level 1, 2 and 3 system problems, and the guaranteed response times for dealing with them, is crucial. Yet, what constitutes Level 1 — typically defined as major functionality for payment processing — is not always clear. Agree to definitions before a crisis occurs. What may not be a required functionality for processing the payment may be a requirement for the customer to pay and for making the sale. For example, imagine if the payment application has a glitch and one-click payment is not working, but payments can be processed manually. Vendors may not consider this a major loss of functionality, since a payment can still theoretically be processed. However, this glitch could result in lost sales for existing customers unwilling to reenter all of their payment data.

8. Operations: What Types of Processing Connections and Levels of Data Do You Support?

When it comes to branded credit card processing, it is important to understand the types of processing connections and level of data a vendor can support. There is a potential impact, both on the fees paid by the enterprise and the types of customers supported.

Here’s why:

- Providers with direct connections to branded card networks might offer lower costs for processing payment transactions as there are fewer touchpoints in the process. This also means there are fewer points of failure, so efficiency may be greater and troubleshooting more straightforward. Additionally, new functionality offered by the card brands can be implemented more quickly by a provider that is directly connected. Any provider using a third-party processor is dependent on that processor to upgrade to any new functionality before they can offer it to their customers.
Enterprises must also evaluate the technical stack upon which the vendor has built its payment technology to ensure compatibility with in-house operations. Determine what type of API technology your development team prefers (e.g., SOAP API, REST) and ensure that your chosen vendor is a good fit. Many of the larger legacy payment processors and acquirers have grown through acquisition over the years and may have many disparate platforms from which to choose. Make sure you know which platforms you’ll be connecting to and any supporting platforms behind the scenes, if applicable.

Talk to current and prospective payment vendors about their planned roadmap and their approach to innovation and roadmap planning. Then, assess whether they are likely to be able to meet your current and longer-term payment needs. You may need to consider using multiple vendors to find the options that meet the payment needs of your business.


Two key types of integrations are commonly required for payments:

- **External integrations** — Enterprises (especially larger ones) may need to connect to multiple vendors to support payment within the overall commerce experience. Different geographies, payment methods and channels may require different solutions. Specialized value-added services, such as complex fraud detection, tax or address services, and electronic bill pay and presentment (EBPP), may also require integration to additional services or vendors.

- **Internal integrations** — Within the enterprise, multiple applications may require connection to a payment vendor. Examples are the digital commerce platform, ERP applications or a centralized unified commerce platform based on a service-oriented architecture (SOA) with centralized web services. This may also be true for channel integrations at omnichannel retailers — for example, the same payment transaction service can be called from a physical location or an online channel, as is important for truly unified commerce. It’s important to understand how vendors’ products deal with integration and any available existing integration modules or plug-ins.
Here's why:

- Vendors often take different approaches to the payment ecosystem and have different key partners for enterprise application integration. You must understand a vendor’s approach to the ecosystem and know which enterprise applications have preintegrated APIs. Digitally competitive enterprises emphasize innovation and agility. The easier and fewer the integrations you need to support independently, the greater your agility and the lower your total cost of ownership. Businesses may gain competitive advantage in commerce if they can move faster and launch services quicker, fueled by an agile payment vendor.

- Some vendors provide integration to many types of players in the payment ecosystem, such as POS software, gift card providers, loyalty platforms, alternative payment methods, fraud prevention and foreign currency exchange. These integrations enable clients to reach a large majority of the payment ecosystem with a single integration. This better positions you for future payment functionality as it emerges and is supported by the same vendor.

- Some vendors create preintegrations for commonly used applications that may initiate or receive payment data, such as ERP, digital commerce platforms or supply chains. Selecting vendors that have preintegrations to many of the required vendors or applications can save time and money, enabling a quicker time to market.

10. Merchant Experience: Do You Offer Managed Payment Services and What Specific Services Are Included?

It's worth considering outsourcing some of the operational aspects of payments to an experienced third party. That's because the complex nature of handling settlement reconciliations, refunds, chargebacks and fraud management is time-consuming and often requires expertise that the organization lacks. Contingent on a client's volume and expertise, managed payment services could be a more viable option — and can actually reduce operational costs.
When outsourcing fraud management, keep in mind that the provider is dealing with the approval decisions and the outcomes, not just detecting fraud. This means a sophisticated vendor's expertise and advanced tools will reduce not only fraud, but also the cost of handling chargebacks. Frequently, this happens while simultaneously increasing authorizations or completed sales. Some vendors offer guaranteed fraud rates, which can make managed services even more enticing for inexperienced staff or organizations that no longer want to employ staff for fraud mitigation. However, any vendor fraud guarantee needs to be balanced against the risk of lost revenue due to false positives.

Here's why:

- Clients report that their operational support costs for payment processing are increasingly fueled by an uptick in the number of payment methods accepted and channels used. A further complication occurs when purchases and returns are made in different channels and stores. As the number of payment methods increases, settlement and reconciliation become more complex and tedious.

- While industry statistics suggest that fraud rates are increasing, vendors are reporting more sophisticated fraud tools that enable lower fraud rates and increased approvals. Many are starting to offer managed fraud services with guarantees, while others are partnering with data protection providers to improve security.

- Many sellers manually review transactions that fall into the gray area between acceptable and unacceptable fraud scores to assess risk and decide whether to accept the authorization. The size of the team responsible varies according to the size of the vendor and the number of transactions processed. Some clients report staff numbers of 45 or more. Maintaining a specialized in-house transaction review team can be cost-effective for some sellers, but for many others the overhead, training and staff costs outweigh the benefits. Outsourcing to a company that specializes in this area may produce both a better result and lower cost.


Fraud prevention and payment data security — although different — go hand in hand. Fraud is about the theft of the goods and services you are selling by bad actors using stolen payment information and/or credentials. Payment security refers to protecting your good customers’ payment data from being stolen in the first place.
Frequent stories about hackers stealing data from banks, retailers and other companies attest to the increasing number of security problems. Meanwhile, the increase in fraud problems leads to chargebacks and inventory or financial losses. No business is immune, and every enterprise must take steps both to reduce fraud and thwart hackers.

Vendors offer different approaches to these two problems. Clients benefit from understanding the vendor's approach because the impact can be significant to an organization.

Here's why:

- While vendors typically offer a secure, PCI-compliant environment for customers to enter payment data, they may take different approaches to compliance — especially when it comes to encryption and tokenization. Gartner recommends the combination of tokenization and hosted payment pages/fields to secure data in transit and at rest, thus minimizing the PCI DSS footprint.

- The robustness of fraud tools offered by vendors also varies. Some vendors offer rudimentary fraud tools, while others offer very sophisticated tools that enable increased approval rates and decrease fraud at the same time. Sophisticated tools provide a high degree of customization to your unique business; however, it requires an experienced and skilled professional to manage that customization. In some cases, extensive fraud services (including both technology and staff) are offered as managed services. Note that it is common for merchants to select a payment vendor that does not offer fraud tools deemed sufficiently sophisticated to meet the merchant's specific requirements. There is a mature ecosystem of fraud detection vendors that can work with merchants regardless of which payment vendor they choose (see Market Guide for Online Fraud Detection). Finally, many vendors will offer 3D Secure as standard, which enables authentication of the cardholder by the issuing bank during the check-out process. Use of 3D Secure varies greatly in different regions, but in markets such as Europe and India, local regulation requiring strong authentication effectively mandates its use in all but name.

- If you will be using tokenization services from a vendor to reduce your PCI burden, ask the vendor about data portability. Make sure there is a way to migrate your customer data and have it retokenized if you change providers down the line. If there isn’t, you would have to abandon cards on file, hurting the customer experience, or maintain redundant tokenization connections (a complicated and lengthy process). This becomes more important if your business relies strongly on recurring billing, subscription payments or stored payment credentials for return customers.
12. Merchant Experience: What Operational Tools Do You Offer?

Clients need to be able to understand their fees as part of the reconciliation process. Sometimes these charges are presented as “statements” due to fees being deducted at the time of settlement. Because payment transactions can have an extended life span, it can be important to easily identify and adjust them long after the sale has been completed. Make sure your vendor includes an operational dashboard that enables easy identification of original transactions for supporting customer service operations, such as refunds or chargebacks.

If you want to integrate the payment processor look-up into your customer support tools, look for a vendor that has a transaction request API. Some CRM software may offer preintegrations to certain payment vendors for this purpose. Otherwise, support reps will need to log in to a separate application to research payment transaction information.

Here’s why:

- If a customer returns an item or requires a price adjustment after the purchase, it is important to be able to easily identify the original transaction. This is especially true for credit card sales, due to card regulations. Poor tools result in tedious work that is typically time-consuming and costly. To facilitate dispute management, refunds linked to the original authorization and settlement are typically required, rather than unmatched credits to a consumer’s credit or debit card.

- Similarly, should a credit card chargeback occur, the burden is on the merchant to address the dispute. Merchants need appropriate tools to assist them in order to be successful. See Note 2 for more details on what constitutes a credit card chargeback.

- Another area of concern for Gartner clients is the difficulty of reconciling their settlement dollars with the corresponding statement. Settlement is typically calculated as the net of gross sales minus branded-card interchange fees and transaction processing fees. Customers must understand pricing plans to determine accurate charges and appropriate receipt of funds. Some vendors offer an interchange analysis feature, to monitor and assess interchange fees, and to help clients obtain lower processing costs.

Evidence

This research is based on inquiries with Gartner clients and briefings from digital commerce payment vendors.
## Acronym Key and Glossary Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account guardian</td>
<td>An account guardian is the party that has visibility into the buyer’s funds or holds the buyer’s funds and is responsible for authorizing payment. Account guardians may be banks that issue credit cards (i.e., issuing banks) or hold deposit monies (i.e., depository banks), or third parties that hold prepaid funds or extend private credit (such as merchants of record, digital wallets or providers of alternative payment methods).</td>
</tr>
<tr>
<td>Acquirer</td>
<td>An acquirer (aka merchant acquirer) is a financial entity with underwriting, risk management, fee and settlement responsibilities as they pertain to credit and some debit cards. The merchant account is with them, and they receive and transmit funds.</td>
</tr>
<tr>
<td>Downgrade</td>
<td>A downgrade occurs whenever a credit or debit card transaction does not qualify for the optimal interchange rate. This may happen due to missing information or other conditions that increase risk or result in more complex transaction handling.</td>
</tr>
<tr>
<td>Independent sales organization (ISO)</td>
<td>An ISO, sometimes called a payment service provider (PSP) or member service provider (MSP), is an entity authorized to resell acquiring solutions and issue merchant accounts on behalf of issuing banks. Historically, they have tended to partner with gateways in a referral relationship. Increasingly, technology providers such as gateways are also playing the role of ISO to deliver one-stop payment solutions.</td>
</tr>
<tr>
<td>Merchant</td>
<td>A merchant is any seller (e.g., company) authorized to accept credit cards, regardless of the channel or industry. For the purposes of this research on digital commerce, for which payments often expand beyond traditional credit cards, the term “merchant” is used collectively for any online seller (regardless of payment type being accepted).</td>
</tr>
<tr>
<td>Merchant of record</td>
<td>A merchant of record is the party that has a relationship with a payment processor for processing credit card (and some debit card) transactions. The merchant of record is the entity that the payment processor will pay for all transactions running through the company’s merchant account, and will hold liable for processing fees, chargebacks and legal compliance with card association rules. In the case of payment facilitators, they are responsible for disbursing settlement funds to their many submerchants.</td>
</tr>
<tr>
<td>Payment aggregator</td>
<td>A payment aggregator/facilitator (formerly known as a PSP) acts as the merchant of record with sponsored submerchants (thus aggregating multiple merchants to share a single merchant</td>
</tr>
</tbody>
</table>
or payment facilitator

A payment gateway (aka PSP) is a software solution or service that connects a seller’s digital store, mobile web store or mobile app to the party responsible for obtaining or providing payment authorization (e.g., processors, payment facilitators, payment aggregators or other account guardians). Gateways offer preexisting connections and certified integrations to key payment providers; foundational services include payment data collection and routing. Gateways initiate the payment authorization request and return the authorization response to the merchant. Gateways may provide value-added services such as tokenization, recurring billing capabilities, fraud prevention tools, hosted payment pages, virtual terminals and reconciliation reports, among others.

Payment processor

A processor is a technology platform responsible for transmitting credit and debit card transaction authorization, settlement, void, and refund and credit requests to payment networks (e.g., Visa, Mastercard, PIN debit networks). Merchants rarely integrate directly to a processor without a gateway as an intermediary. In most cases, however, the processor may offer its own proprietary gateway solution.

Note 1: Card Data Levels

Card data falls into three categories:

- **Level 1 data** typically provides the cardholder with limited purchase data and is typically associated with consumer transactions, whereas Level 2 and Level 3 data typically includes more information of interest to corporate and government cardholders.

- **Level 2 data** is additional information to benefit the corporate or government buyer, which can be captured from most POS terminals, albeit in a somewhat limited way due to the data capture restrictions on most POS terminals. Interchange fees are lower when using Level 2 data than when using Level 1 data.

- **Level 3 data** is equivalent to line-item detail on an invoice. Capturing Level 3 data results in a lower interchange rate than with Level 2 data. The restricted data capture capabilities of most POS terminals forces merchants to use specialized payment software for data entry, which most merchants simplify by integrating to their ERP systems for data retrieval.
Note 2: Credit Card Chargebacks

According to Visa guidelines, customer disputes (chargebacks) in the credit card world fall into four categories:

- Fraud
- Authorization issues
- Processing errors
- Consumer disputes

The merchant is responsible for addressing customer grievances under the card association operating rules. Visa, for example, has published Dispute Management Guidelines for Visa Merchants.

Document Revision History

12 Key Questions to Ask When Selecting a Digital Commerce Payment Vendor - 12 March 2020

12 Key Questions to Ask When Selecting a Digital Commerce Payment Vendor - 22 August 2018

The Top 10 Questions to Ask When Selecting a Digital Commerce Payment Vendor - 12 October 2016

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Market Guide for Digital Commerce Payment Vendors

Quick Answer: What Payment Acceptance Strategies Can Improve Digital Commerce Profitability?

Security and Risk Management Leaders’ Guide to Online Fraud Detection

Market Guide for Organization Security Certification Services

Toolkit: RFP for Digital Commerce Payment Solutions