PayPal

Enterprise Payments 101:

Everything You Need to Know About Payment Processing Solutions

Contents

Introduction

Frictionless payments make the world go around

Online or in store, via their mobile or other connected devices, customers expect that making a digital purchase will be simple. Seamless. Secure. Virtually instantaneous. That purchase process – from click, swipe or tap to "approved" – can happen in seconds. And, when it doesn't, that's when shopping carts are abandoned and sales are lost.

According to the Baymard Institute, **nearly 70% of online shopping carts are abandoned,** and 1 out of 4 shoppers abandoned due to a "too long/ complicated checkout process."[1]

Payments are now part and parcel of the overall purchase experience. More than that, they're essential for any retail or e-tail business to increase conversions and lifetime customer value, access and expand into new markets, mitigate compliance risk and reduce operational costs.

But creating a frictionless, satisfying payment experience isn't always as easy as it should appear to customers at checkout. While a delightful, split-second transaction may feel like pure magic to consumers, behind the scenes, payment processing is multi-faceted and often complex.

Let's give you a strong foundation for success

From demonstrating the step-by-step payment process and detailing all of the players involved to setting up online payments and finding the best-possible pricing and partners for your enterprise, this eBook has you covered. It even includes a quick-reference glossary at the end with definitions of common (but sometimes tricky) payment processing terminology.

Whether you're new to payments or just looking for a solid refresher, read on to find information, best practices and tips to drive your work – and your organization – forward.

[1] Source: Baymard Institute 41 Cart Abandonment Rate Statistics — Cart & Checkout, updated September 10, 2019.

The Fundamentals

How Payment Processing Works

According to Statista, global retail e-commerce sales worldwide grew to $3.53 trillion USD in 2019, and e-retail revenues are projected to reach $6.54 trillion in 2022.[2] That's a lot of money changing hands – and there are actually many hands and multiple steps involved in each individual purchase. Let's briefly review the players and payment process.

Who and what enables payments and delivery

There are three main parties involved when it comes to processing payments, whether online, via phone sales or even in person. On one end is you, the business or merchant. On the other end is your customer. And in between is a lot of technology that connects you both.

The Merchant (You)

When you get started, you may work with a merchant bank (aka merchant acquirer) that will set you up with a merchant account – which links to your payment processor, enabling you to collect funds.

Or, you'll choose to work with a company (like PayPal) that acts as your merchant account, gateway, and processor (more about this to follow).

Once you're up and selling, other players get involved. After a payment has processed, the funds are debited from your customer's account by the issuer – the bank that gave them the actual card. Then the acquirer is responsible for depositing them into your account.

The Technology

In the middle are two technologies that enable you and your customer to transact.

The first is the payment gateway, software that links your site's shopping cart to the processing network.

The second is the payment processor, which does all the heavy lifting: moving the transaction through the processing network, sending you a billing statement, working with your bank, etc. Often, your merchant bank can be your payment processor, which helps simplify things.

The Customer

In order for your customer to pay for your goods and services, she needs a credit or debit card. The bank that approves her for the card (and lends her the cash to pay you) is called the issuing bank.

When customers choose to shop with credit or debit cards, their transactions are governed by several players: the issuer, the Card Associations (Visa®, MasterCard®, etc.), and the Payment Card Industry (PCI).

Together, these companies have created a set of rules and regulations about encrypting and protecting data (more on this later as well).

[2] Source: Statista Global Retail eCommerce Market Size 2014-2023, June 2019.

How funds flow from your customer to your company

Most of a payment's journey is completely invisible to consumers and businesses. Whether you're keying-in your customer's card or your customer is hitting a "Buy Now" button, payments go through a series of stages before they reach your merchant account. By understanding the different stages, you'll have a better sense of what each of the players are doing (and charging you for) – and how to negotiate the best payment processing solution for your business. The following is a flow of a traditional transaction process.

Step 1
Your Customer Pays

Your customer has just made a purchase on your site using credit or debit. Hooray! The transaction begins its journey through your payment gateway.

Step 2
Encryption

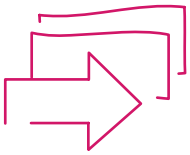
When your customer's personal information and payment transaction data goes through the payment gateway, it's encoded to ensure secure transmission across the Internet.

Step 3
Authentication

The payment processor validates (aka "authenticates") that the payment data is being sent by its claimed source, as a way to curb fraud.

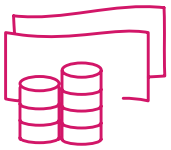
Step 4
Authorization

The payment processor requests the issuing bank to authorize a specific amount of funds from your customer's credit or debit card. The issuer checks to make sure the customer has enough credit to make the purchase and sends back an approval or decline. This entire process typically takes only a few seconds.



Step 5
Settlement

Settlement occurs when the card issuer sends the appropriate funds to your acquiring bank, which then deposits them into your merchant account. This can take a few days to complete.



Step 6
You're Paid

The funds are now accessible in your merchant account. But you may notice that some of the funds are not available, as most payment processors hold back a reserve temporarily to ensure you can take care of any liabilities, such as chargebacks or reversals.

CHECK THIS OUT!

According to the Baymard Institute, e-commerce companies can increase conversion rates by more than 35% by improving the checkout process.[3] Case in point: StubHub saw a 50% increase in mobile conversions by streamlining checkout with PayPal.

[3] Source: Baymard Institute 41 Cart Abandonment Rate Statistics — Cart & Checkout, updated September 10, 2019.

Payment Options

Parties and Methods of Payment

As you've just read, there are multiple parties involved if you want to accept credit card or other forms of digital payment. And you have choices about who you partner with to make payments possible. It's important to understand your options.

a

Merchant Acquirers (or Merchant Services Providers):

As we noted above, a merchant account is what enables your company to accept card payments online, and you need one in order to process transactions. You can obtain a merchant account from a merchant services provider, such as a bank – or from some payment processors.

b

Payment Processors:

What's the difference between using a merchant acquirer or a payment provider? They both provide a lot of the same financial business products, but payment providers like PayPal can set you up with additional built-in e-commerce options, like templates for your online store, integrated checkout, shipping, and even a payment gateway. With a merchant bank, you'd need to shop around for those services separately.

c

Payment Gateways:

A payment gateway is a technology service that sends credit card information from a website to the credit card payment networks for processing, and returns transaction details and responses from the payment networks back to the website.

Is PayPal a Merchant Account, a Processor or a Gateway?	Yes	PayPal is among the partners that can offer you one seamlessly integrated solution for your merchant account, payment processing and payment gateway. If it sounds simple and great, well, it is!

How can customers pay you?

To maximize conversions, it's important to offer the most popular payment methods in each country your company serves. In the US, credit cards are the most common method of digital payment. In Europe, real-time bank transfers often have a dominant share of online checkouts. Here's a quick review of some popular payment methods:

Credit and Debit Cards: When processing payments online, credit and debit cards are handled the same, as long as they are issued by a major card brand. Because PINs can't be accepted online, debit cards typically run as credit.

Automated Clearing House (ACH) Direct Debit: Most merchants in the US can accept ACH Direct Debit (aka electronic check) transactions from participating customers.

Real-Time Bank Transfers: Unlike ACH, real-time bank transfers are completed within seconds and are usually guaranteed and confirmed immediately. Real-time bank transfers are especially popular in Europe. Key players include Giropay in Germany, iDeal in the Netherlands, P24 in Poland, and Bancontact in Belgium.

Mobile Wallets: Mobile wallets, such as Apple Pay, Google Pay and Samsung Pay, are apps that let consumers use their smartphones to make purchases. They typically require merchants to have an available contactless payments reader for customers to "tap" their devices to in order to facilitate payment.

Special-Use Cards: Credit and debit cards issued for specific purchases – like HSAs and FSAs or P-Cards – can only be accepted if your merchant account is associated with the appropriate MCC (Merchant Category Code).

Gift Cards: Prepaid gift cards can be redeemed to purchase goods and services – and they can often be sent to recipients for use via email or text.

Dual-Branded Cards: Dual-branded cards include two different card brand logos and can be processed through either brand's network. Merchants can process these cards on whichever network is supported in their region.

PayPal: We'd be remiss not to mention PayPal's payment options, including PayPal, PayPal Credit*, Venmo (US only), and UnionPay, a major provider of credit and debit cards for customers in China.

CHECK THIS OUT!

PayPal Credit can help increase buyer loyalty. 56% of PayPal Credit users say they are more likely to shop at a retailer again if they offer PayPal Credit.[4]

* Subject to credit approval.

[4] Online study commissioned by PayPal and conducted by Logica Research in November 2018 involving 2,000 US consumers, half were PayPal Credit users and half were non-PayPal Credit users.

Security and Compliance

Protecting Customers and Your Business

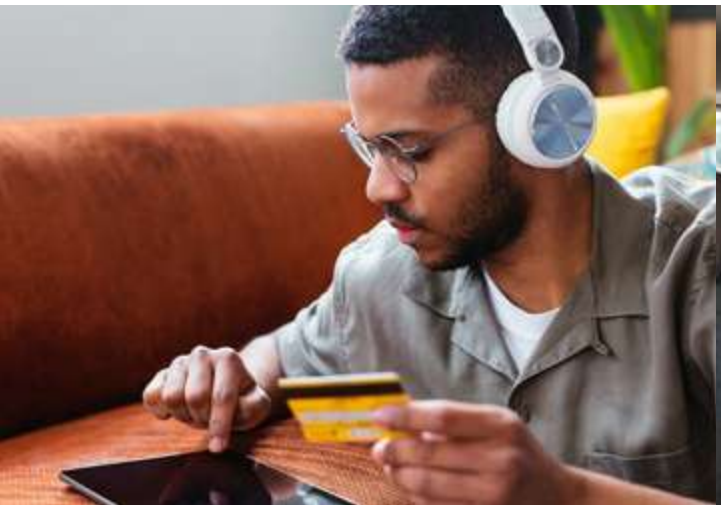
Payment fraud and data breaches can be very costly – to your company's reputation and bottom line. For example, it's estimated that retailers could lose around $130 billion in digital CNP (Card-not-Present) fraud between now and 2023.[5] Suffice to say, data security is of paramount concern for payment processing – and it's also a matter of compliance if you want to accept payments.

LexisNexis Risk Solutions research shows that, across retailer types, the cost per dollar of fraud is $3.13, up from $2.40 in 2016.[6]

About the PCI Data Security Standards (PCI DSS)

Founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc., the PCI Security Standards Council is a global organization that maintains, evolves and promotes Payment Card Industry standards for the safety of cardholder data across the globe.

PCI standards have been established to define the operational and technical requirements for any business, financial institution or other organization that stores, processes or transmits cardholder data, as well as the software developers and manufacturers of applications and devices used in those transactions.



[5] Source: Juniper Research Online Payment Fraud, published February 25, 2020.

[6] Source: 2019 LexisNexis True Cost of Fraud Study.

The 12 Requirements for PCI Compliance

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	**1)** Install and maintain a firewall configuration to protect cardholder data **2)** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3)** Protect stored cardholder data **4)** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5)** Use and regularly update anti-virus software or programs **6)** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7)** Restrict access to cardholder data by business need-to-know **8)** Assign a unique ID to each person with computer access **9)** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10)** Track and monitor all access to network resources and cardholder data **11)** Regularly test security systems and processes
Maintain an Information Security Policy	**12)** Maintain a policy that addresses information security for employees and contractors

Source: https://www.pcisecuritystandards.org

PCI is just the first of the three-letter acronyms to know

Achieving and maintaining compliance with the above PCI requirements involves several steps, players and documents, all of which are typically short-handed in three letters. Here are brief summaries to help you make sense of the alphabet soup that is compliance.

SSL

A foundation of online data security and PCI compliance, Secure Sockets Layer protocols establish an encrypted connection to securely transfer payment data from a website.

SAQ

The PCI Self-Assessment Questionnaire is a series of yes-no questions intended to help merchants and service providers assess their levels of compliance.

QSA

A Qualified Security Assessor is an independent security company qualified by the PCI Council to validate an organization's adherence to PCI standards.

ROC

A Report on Compliance assesses the standards in place to protect card information. All Level 1 Merchants (companies who process more than 6 million annual transactions with Visa and/or Mastercard) are required to pass a PCI ROC.

AOC

An Attestation of Compliance is a form used by merchants and service providers to confirm the results of a PCI DSS assessment.

A quick take on "tokens"

You may also hear payment processors talk about "tokenization." Here's what they mean.

PCI standards don't allow credit card numbers to be stored on a retailer's point-of-sale (POS) terminal or in its databases after a transaction. Compliance requires merchants to either install complex and costly encryption systems or choose a payment processing partner who can provide tokenization, which means creating virtual representations of the credit cards that do not compromise the security of the data. These virtual representations – or tokens – sit securely in the payment gateway's data vault.

Tokenization is ideal for enabling repeat customers or subscription businesses that require recurring payments. Entrusting a payment processor with tokenization can help shift PCI liability to your partner and reduce your operational costs – not to mention create a faster, more seamless and convenient customer experience for consumers by not requiring them to continually re-input their payment information.

Pricing and Contracts

Rates, Fees and What to Look Out For

You've learned about how to get your money and how to secure the transaction. Now, you may be asking: what does it all cost? It's no surprise that everyone who touches the transaction wants to get paid, including the issuing bank, the credit card associations (Visa, MasterCard, etc.), the merchant bank and the payment processor. Let's take a look at how rates and fees are typically structured – and what you should keep an eye on to ensure you're paying for what you need, nothing more or less.

Breaking down the standard fees

Simply put, every time a transaction is processed, your company pays several fees.

Interchange fee: The credit card issuer gets paid by taking a percentage of each sale, called the interchange. This fee varies depending on several things, such as industry, sale amount, and type of card used. At last check, there were about 300 different interchange fees! The fee could look like this: 2.0% of the volume + $0.10 per transaction.

Assessment fee: The credit card association (Visa, MasterCard, etc.) also charges a fee, called an assessment. For example, 0.10% + $0.02. This rate is usually bundled with (and called the same thing as) the interchange fee.

Markup fee: This is a set of fees charged by everyone else who moves the transaction through the network, including your merchant bank, the gateway, and the payments processor (who might all be the same company, like PayPal). The amount of the markup fee varies by industry, amount of sale, monthly processing volume, etc. Again, it is usually structured as a percent of the sale amount and a per-transaction fee (for example, 0.25% + $0.10).

Other fees: There can also be fees charged for setup, monthly usage, hardware, PCI compliance, cross-border transactions and international sales, and even account cancellation.

Sales representatives may sometimes try to tell you otherwise. But if a vendor tells you they can lower the interchange fee, this simply isn't true.

How processors package their fees

As you research payment processing partners, you'll likely run into a variety of pricing models for processing transactions. Understanding how these rate structures work can help you choose what's best for your business – without unnecessary costs weighing you down.

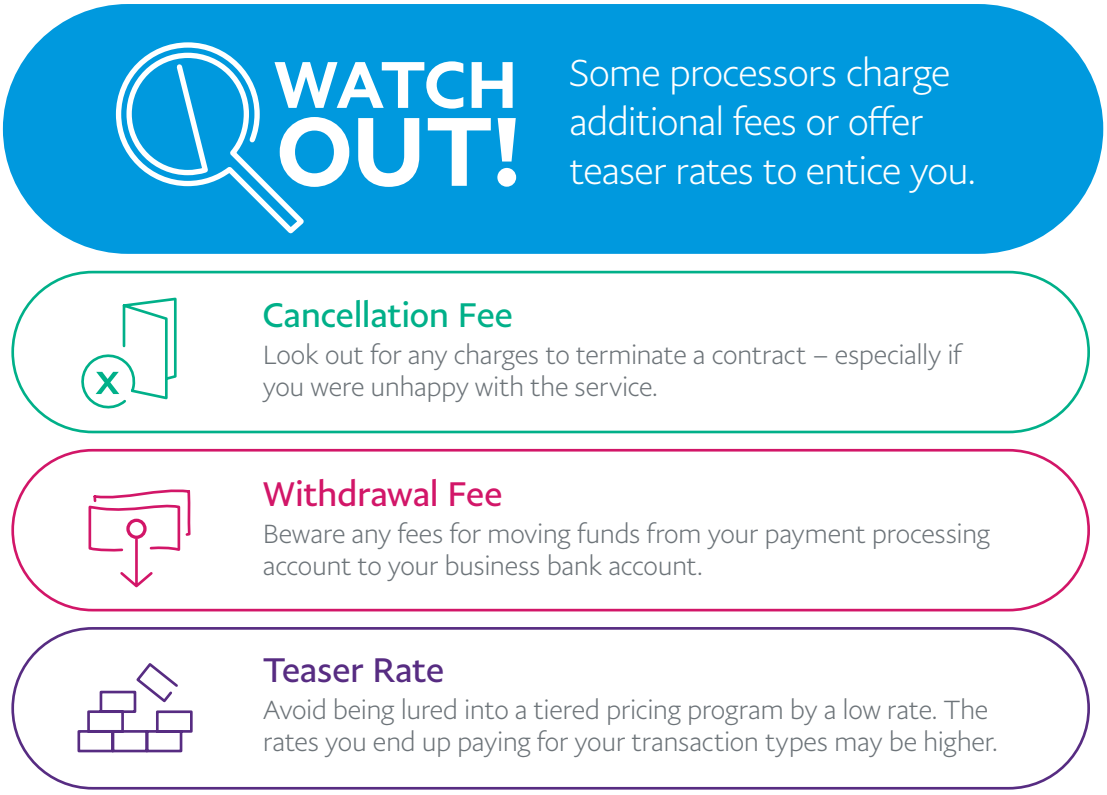
Flat-rate pricing is the easiest pricing model to understand. It involves paying the processor a flat fee for all credit and debit card transactions, which covers all the fees mentioned above. (At PayPal, we offer flat-rate pricing.)

With interchange plus pricing, your merchant service charges you a fixed fee on top of the interchange, instead of bundling a fee directly into the interchange. For instance: 1.8% for interchange fees + a markup of 2% + $0.102 = $3.90 fee on a $100 sale. While this pricing model gives you a bit more visibility into the breakdown of your rates, the tradeoff is that your statements are more complicated to figure out and reconcile. Also, remember there are about 300 interchanges, so that 1.8% fee in this example can vary!

In tiered pricing, the processor takes the 300 or so different interchange rates and lumps them into three buckets or pricing tiers based on risk of fraud: qualified (usually transactions swiped at physical terminals), mid-qualified (usually transactions that are key-entered), and nonqualified (usually e-commerce transactions). This makes it simpler for you (and them) to understand. However, because the processor defines the buckets any way it wants, it can be expensive. As an example, the fees you pay on a $100 sale could range from $2.50 to $3.50, depending how it has been classified.

A few more notes on fees

When comparing different pricing structures, be sure to keep in mind that some processors charge additional fees, and these may be buried in the fine print. For example, a processor may charge a cancellation fee if you decide to terminate a contract early, even if you've been unhappy with their services. At the same time, they may try to charge for liquidation damages, a type of early termination fee that allows the provider to collect thousands of dollars in "damages" from projected revenue loss based on your early cancellation. On the other hand, they may have auto-renewal clauses.



You may also get charged a withdrawal fee for moving funds from your payment processing account to your business bank account, even though that's a standard activity for sellers. Before signing any contract, look for such hidden fees, because they could significantly affect your profits.

CHECK THIS OUT!

After evaluating and understanding the fees, it's a good idea to assess the overall value of the contract. Fees are not the whole story. What if your company needs a gateway, shopping cart, payment processing data, virtual terminal, etc.? How much would it cost to get these additional features elsewhere? Make sure your payments/legal departments are analyzing the contracts to get the best value; but also to find the best provider that can grow with your business.

Payment Data

Maximizing Your Growth and Revenue Opportunities

Your point of purchase is just the beginning of a broader digital payment ecosystem, in which you can leverage your payment data to create additional revenue opportunities and enhance your customer's experience. As you consider your options, look beyond the checkout experience to explore data-sharing tools that help you securely connect with partners or service providers, so you can better manage and help grow your business.

A few ways you can do more with your payment data

Capture new customers by creating new opportunities to buy:

Today's consumers expect brands to find them wherever they are. Your business can reach new audiences by building native checkout flows in the places where customers are primed to buy from you.

Protect your payments:

Want or need added layers of security and fraud prevention? There are solutions available to securely share even the most sensitive customer and payment data with third-party services or secondary vault providers.

Optimize checkout flow:

If you want fewer cart abandonments, streamline the buying process. Reduce the need to constantly enter passwords, usernames, addresses, and credit card numbers with PayPal One Touch Payments.

Create purchase incentives or cash rebates to reward repeat customers:

Maximize relationships with existing buyers and help improve customer acquisition by connecting merchants to rewards and loyalty partners that can help incentivize purchases and keep customers coming back.

Check This Out

A connected payment experience that's really smart

Curious what it actually looks like to use payment data to the fullest? Follow college student Emma, as seamless and secure data connections between partners make her purchase experiences seamless.

1 

Paying for tuition

Emma is a sophomore at a large state university, where she pays for her tuition at the start of every semester. To make life easier, she provided the university with her payment information for automatic deductions.

2 

Adding a dining plan

Emma decides to also purchase a food plan. Even though the university dining halls are managed by a third-party vendor, she's able to pay for her dining plan without entering all her payment information again.

3 

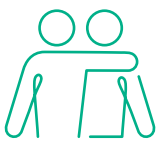
Behind the scenes

Without impeding Emma's seamless checkout experience, the university leveraged a custom fraud prevention solution during the transaction for added fraud detection at checkout.

4 

Buying textbooks

When Emma buys her textbooks online, she's notified about a rewards offer linked to her credit card. Because she purchases 15 books, she gets 15% off her next purchase!

5 

Enjoying campus life

Emma can go to many merchants around campus without bringing her wallet. She can buy supplies, fan gear, tickets to the game, even do laundry with a single click.

Key Takeaways

Whew, you did it!

Congrats on completing Payments 101! As you've seen, modern payment processing is a complex and business-critical component of growing and protecting an enterprise. And, by covering the basic process, players, and considerations around cost and compliance, this eBook has only scratched the surface.

As you continue your payments journey, we know that it may still be a bit daunting when exploring and comparing solutions and partners. To help you make the right choice for your business, we'll leave you with a few common pitfalls to avoid.

1. Failing to read the fine print regarding rates and fees

When comparison shopping for a payment processor, keep in mind that a low rate doesn't always mean a low overall cost. Processors can have high processing fees and even variable rates that can make it hard to tell what you'll really be paying. For example, many credit card processors charge higher rates for "nonqualified" cards – such as corporate and rewards cards. These cards earn customers airline miles, loyalty points, or cash-back bonuses. They're popular, and many customers use them, so finding out that these include a higher rate can be an unpleasant surprise. Look for a payment processor with transparent fees to avoid the shock.

2. Choosing based on rates alone

While low processing rates might seem great, you shouldn't choose a payment processor based on rates alone. There are many factors that can dramatically affect your business, including security, technical support, international reach, and brand trust among consumers.

3. Underestimating security and fraud protection

Data breaches have hit retailers large and small, and customers now demand the best protection possible to help lower their risk of card fraud. As you evaluate vendors, look for a payment gateway that's backed by a secure, reliable payment processing company. Also, look for partners that offer services to help you proactively prevent fraud. It can not only help protect both your customers and your business, but also help ensure that you'll be compliant with the Payment Card Industry Data Security Standard (PCI DSS).

4. Limiting customers' payment options

Today's customers expect more options than ever, and not just in products and services. They expect to be able to pay online with a range of options, including Apple Pay, Google Pay, or PayPal services. If your payment processing company imposes limits on what you can accept, you might see an increase in abandoned shopping carts on your site. Choose a provider that can offer your customers a range of payment options.

5. Going DIY with setup and support

Finding a payment processing company that can deliver easy setup along with your account is imperative, and backing that up with technical support is crucial. You need a processor that understands these challenges, and has a dedicated team to help support you on payment-related problems. At the same time, payment processors should do the heavy lifting of building networks in the countries that merchants are eyeing for expansion. If the payment solution allows overseas buyers to pay in their local currencies, shoppers are happier.

Appendix:

Payment Processing Terminology

The world of payments is filled with specialized terms and complex acronyms that may be a bit confusing to keep straight. But, once you've got the language down, you'll gain a better understanding of the flow of payments and how you can choose the right payment processing partner for your business' needs. Here's a short glossary you can refer back to, whenever you need it.

Acquirer or Merchant Acquirer

In this sense, to "acquire" means to "accept" payments. So, an Acquirer is a banking partner for businesses. They take the risk that you're going to be a trustworthy business (aka underwriting).

Authentication

When a customer submits a payment, the payment processor needs to validate (aka "authenticate") that the payment data is being sent by its claimed source. Payment processor companies use this process as a best practice to curb fraud.

Authorization

The first half of transaction processing, authorization is a request from the payment processor to the issuing bank to authorize a specific amount of funds from your customer's credit or debit card.

Batch Processing

A method used by the payment processor to process all the day's transactions at once. The acquiring bank uses this to help drive operational efficiency for your business. In the online world, transactions are usually processed at the same time they're authorized.

Card Association or Credit Card Network

Companies, such as MasterCard and Visa, that set the rules and standards for processing transactions. See PCI Compliance.

Discount Rate

This is a percentage of every sale that you pay to your acquiring bank for accepting consumer credit cards (like Visa, MasterCard, etc.). All applicable fees are bundled into a single percentage rate (aka "the discount rate"), which typically includes interchange, assessments, and processor fees. For example, if the discount rate is 2.5% on a sale of $100, the cost will be $2.50.

Dongle (aka Card Reader)

A small accessory that you plug in to your mobile device to securely process in-person payments – either with a physical card or electronically. Once you've got your system all set up, it comes with other perks for your business, such as enabling your shoppers to find and check in with you on their phones and receive personalized offers.

Encryption

The process in which your customer's personal information and payment processing transactional data is encoded to ensure secure transmission across the Internet.

Flat-Rate Pricing

A highly transparent pricing model where you pay the payment service provider a flat percentage on the transaction volume for all credit and debit cards. (This is generally preferred by businesses over other more complicated ways to pay for credit processing.)

Interchange Plus Pricing

When your customers make a credit or debit card purchase, their bank card association charges a percentage of the transaction – this is called an interchange rate, and it varies based on the card category. With Interchange Plus Pricing, a fixed markup is added by your payment processor on top of that interchange fee. (This is also sometimes called "cost plus pricing.")

Issuer or Issuing Bank

This is where credit and debit cards come from. An Issuer is any financial institution or company that issues physical cards to cardholders.

Merchant Account

If you want to accept credit and debit cards, you need a Merchant Account, a special bank account set up between you and your acquiring (or merchant) bank. The bank is responsible for debiting the funds from your customer and depositing them into your account.

Payment Gateway

A Payment Gateway is the software that connects your website (or cash register) to the processing networks. When you process a credit card (or other form of electronic payment) the Payment Gateway securely authorizes cards and electronic payments by encrypting and protecting the customer's sensitive information – like credit card numbers and other account information.

Payment Processor

A Payment Processor is the company that actually gets the work done. It is responsible for moving the transaction from point A to point B and back again. They handle the authorization and settlement, figure out how much to charge you for each transaction, and transfer the money from your customer's bank to your merchant bank. You may not know who your payment processor is, unless you work with a provider like PayPal, as the processor's relationship is often with your acquiring bank, not you directly.

(PCI) Payment Card Industry compliance

If you want to take credit or any other electronic payment, you'll need to follow the rules set by the Payment Card Industry (PCI). PCI compliance is mandated by all card brands to protect and encrypt card information during and after a financial transaction. All organizations or businesses, regardless of size or number of transactions, are required to follow the rules to be PCI compliant if they accept, transmit, or store any cardholder data.

Reserve

Most payment processors hold back a percentage of the transaction or a flat amount – and this amount is called a Reserve. It's important to note that this is NOT a fee – it's still your money. However, you cannot access it for a certain amount of time. Why do they do this? They need to ensure that you can meet liabilities you may incur from a chargeback, claim, or bank reversal. Reserves are a common industry practice and are used to create a safer shopping experience.

Settlement

The last step in card processing, settlement occurs when the card issuer sends the appropriate funds to your acquiring bank, which then deposits them into your merchant account.

Tiered Pricing

This is a rate structure for fees you pay the payment processor for every card or electronic payment transaction. Rate structure criteria are based on a system of qualification. While it's more complicated than this, there are generally three tiers (also called buckets):

1. Qualified rate: This is sometimes called a card-swiped rate, since it is (usually) applied to a transaction where businesses swipe the credit card through a terminal. Since businesses can easily verify that the shopper is the owner of the credit card, the incidence of fraud is quite low – so, the rate is the lowest.

2. Mid-qualified rate: This rate is usually applied when businesses key-enter a customer's credit card (in phone or mail order sales, for example). Since there is no physical credit card present, the risk is higher—and so the rate is also higher.

3. Non-qualified rate: Transactions that are processed without supplying the customer's billing address are often downgraded to the non-qualified rate, which is not surprisingly the most expensive fee. E-commerce transactions fall into this category. Rewards cards and commercial card transactions do, too.

Transaction Fee or Authorization Fee

This is a flat service fee (e.g., $0.30 per transaction) you pay the payment processor every time you send a customer's card details to your payment gateway, regardless of the outcome. For example, a customer tries to buy something from you, but their card is declined. You, the business owner, still pay a transaction fee to cover the cost of the processor handling that transaction.

Virtual Terminal

An online way to accept in-person payments. It's the electronic equivalent of a physical point-of-sale terminal that retailers use to swipe cards. Instead, you manually enter the card information. Virtual terminals let you take your business on the road – all you need is an Internet connection.

About PayPal

Fueled by a fundamental belief that having access to financial services creates opportunity, PayPal (NASDAQ: PYPL) is committed to democratizing financial services and empowering people and businesses to join and thrive in the global economy.

Our open digital payments platform gives PayPal's over 280 million active account holders the confidence to connect and transact in new and powerful ways, whether they are online, on a mobile device, in an app, or in person. Through a combination of technological innovation and strategic partnerships, PayPal creates better ways to manage and move money, and offers choice and flexibility when sending payments, paying or getting paid.

The PayPal platform is available in more than 200 countries/regions and supports 25 currencies. You can send and receive payments easily over borders and language barriers. We're here for you, wherever you are.